Cybersecurity Threats in IoT
Towards Secure, Ethical, and Resilient Frameworks

Ketan Mone
MSc Cyber Security
University of Essex Online
6th October 2025

Introduction

- 25B+ IoT devices by 2030 (Hussain, Abbas and Zeadally, 2022).
- Attack surfaces: healthcare, transport, energy (ENISA, 2023).
- Consequences: privacy, safety, national security (Cisco, 2021).

Research Question

How can integrated frameworks combining technical, regulatory, and human-centric approaches improve IoT cybersecurity resilience in healthcare and critical infrastructure sectors?

Research Problem

- Lack of standards (ENISA, 2023).
- Reactive security (Kolias et al., 2021).
- Low literacy (Finn and Shilton, 2023).
- Innovation vs security (Fjeld et al., 2020).

Aim & Objectives (1/2)

Assess vulnerabilities.

Analyse mitigation (AI, Zero Trust, blockchain).

Aim & Objectives (2/2)

Evaluate ethical/regulatory frameworks.

Propose integrated model.

Validate via case studies.

IoT Threat Landscape

●○○○○○

Device

Weak credentials, default passwords (Alaba et al., 2021).

●●○○○○

Network

Botnets (Kolias et al., 2021).

●●●○○○

Application

Insecure APIs, poor encryption (NIST, 2022).

How to secure your data?

Healthcare ransomware (Hussain et al., 2022).

Industrial IoT sabotage.

Transport hacks (Colonial Pipeline, Jeep).

Smart homes privacy breaches.

Mitigation & Frameworks

Threat	Mitigation	Framework
Device	Secure boot, patching	NIST IoT (2022)
Network	Zero Trust, anomaly detection	ENISA (2023)
Org	Incident response	BCS (2021)
Ethics	Transparency principles	IBM (2022)

Critical Debates

Pros

AI & blockchain breakthroughs (Correa et al., 2023).

Proactive detection.

Cons

Bias, cost, energy inefficiency (Deckard, 2023).

Governance vs industry reluctance (Finn & Shilton, 2023).

Methodology & Design

Systematic literature review (Boza, 2022).

Case studies: Colonial Pipeline, HSE ransomware.

Sources: IEEE, ACM, ENISA, NIST, McKinsey (2022).

Thematic coding & comparative mapping (Dawson, 2015).

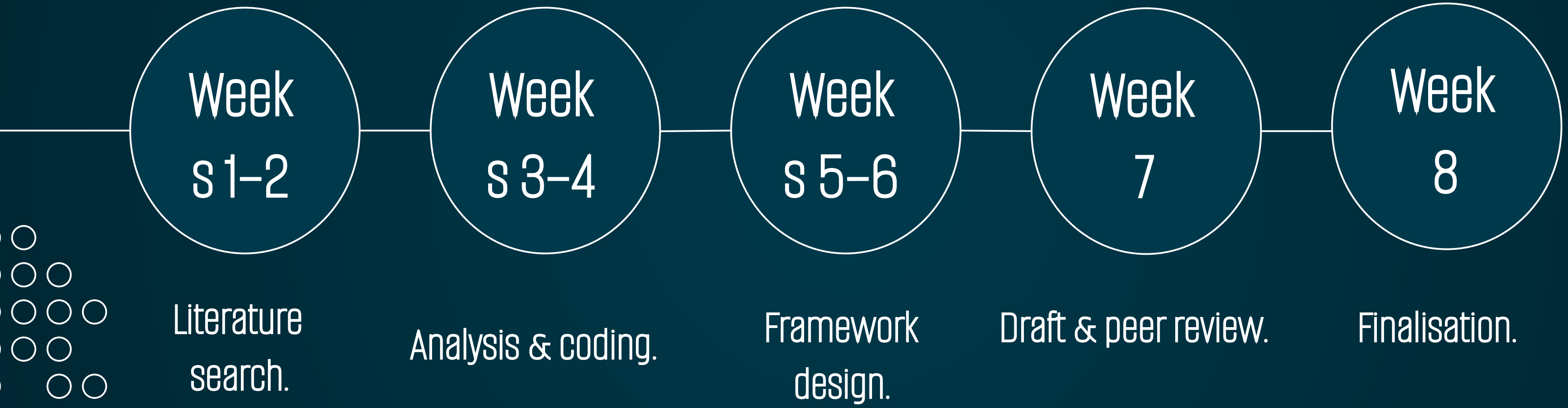
Ethical Considerations

- Secondary data only (low risk).
- Belmont Report (OHRP, 2018).
- Menlo Report (Finn & Shilton, 2023).
- Bias mitigated with inclusion/exclusion criteria (Mavroeidis & Vishi, 2021).

Proposed Artefact

- Layer 1: Device Security.
- Layer 2: Network Controls.
- Layer 3: Governance.
- Layer 4: User Awareness.

Timeline



Weeks 1–2

Literature search.

Weeks 3–4

Analysis & coding.

Weeks 5–6

Framework design.

Week 7

Draft & peer review.

Week 8

Finalisation.

Expected Contribution

Tech
Ethical
Human

Technical + Ethical + Human overlap = Multi-stakeholder Framework.

Addresses standards, awareness, proactive models (McKinsey, 2022; Microsoft, 2021).

Conclusion

- IoT = opportunity + vulnerability (ENISA, 2023).
- Security must be built-in, not bolted-on (Dawson, 2015).
- Needs cross-disciplinary collaboration (Radanliev et al., 2021).

References - Part 1

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).

Cisco (2021) Cisco Cybersecurity Threat Trends: 2021 Report. Available at: https://www.cisco.com (Accessed: 21 September 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.

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.

European Commission (2022) Proposal for a Cyber Resilience Act. Brussels: EU Publications.

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 (2022) IBM Security X-Force Threat Intelligence Index 2022. Available at: https://www.ibm.com/security/data-breach (Accessed: 25 August 2025).

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

References - Part 2

Lee, J., Park, Y. and Shin, H. (2022) 'Blockchain-based authentication and trust management in IoT', Sensors, 22(11), pp. 4012–4028.

Mavroeidis, V. and Vishi, K. (2021) 'Cyber threat intelligence and cyber situational awareness: A systematic review', Computers & Security, 102, 102–118.

McKinsey (2022) Securing the Internet of Things: A Business Imperative. Available at: https://www.mckinsey.com
(Accessed: 3 September 2025).

Microsoft (2021) The Future of Cybersecurity in IoT Ecosystems. Available at: https://www.microsoft.com
(Accessed: 28 September 2025).

Nisioti, A., Mylonas, A. and Katos, V. (2021) 'From intrusion detection to intrusion response: Taxonomy, survey, and future directions', Journal of Network and Computer Applications, 174, 102–123.

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

OECD (2021) Recommendation on the Governance of Digital Security Risk. OECD Digital Economy Papers.

Radanliev, P., De Roure, D. and Walton, R. (2021) 'AI and cybersecurity: The European dimension', AI & Society, 36(3), pp. 783–794.

Sharma, V. and You, I. (2022) 'Security of 5G-enabled IoT devices: A review and future directions', IEEE Access, 10, pp. 11045–11068.

UK Government (2021) National Cyber Strategy 2022. Available at: https://www.gov.uk
(Accessed: 4 October 2025).

Thank you!