# Security and Privacy Challenges in Standardized IoT Systems: Insights from the EU Cyber Resilience Act

Anna Maria Mandalari
University College London
a.mandalari@ucl.ac.uk

Volker Stocker
Weizenbaum Institute
volker.stocker@weizenbaum-institut.de

***Abstract*—The EU's Cyber Resilience Act (CRA) establishes mandatory cybersecurity requirements for products with digital elements, effectively acting as a security standard for the consumer Internet of Things (IoT). While standardization aims to reduce systemic vulnerabilities, security and privacy flaws in standardized requirements can be inherited at scale by widely deployed IoT products. In this paper, we analyze the CRA through the lens of standardized IoT security. We discuss implications for IoT standards and governance, stressing measurable security properties, automated evaluation, and supply-chain considerations. We argue that standardized IoT security cannot be treated as a purely procedural or compliance-driven exercise: regulatory ambiguity, limitations in conformity assessment scalability and harmonization, and gaps between formal compliance and real-world security outcomes risk turning standardization into a mechanism for scaling insecurity rather than mitigating it. Addressing these challenges requires sustained multidisciplinary research at the intersection of IoT standardization, security engineering, and governance, including systematic risk modeling approaches and the development of edge-centric threat models for local IoT environments.**

## I. Introduction

The Internet of Things (IoT) has transitioned from a niche technological domain into a foundational layer of modern digital infrastructure. Consumer IoT products, ranging from smart speakers and home security cameras to wearables and energy management systems, are now deeply embedded in domestic, commercial, and industrial environments [1], [2]. These devices increasingly mediate safety-critical functions, personal data flows, and autonomous decision-making, making their security and privacy properties matters of societal concern rather than purely technical design choices.

Despite this growing importance, IoT security remains fragmented and inconsistent. Devices often rely on proprietary protocols, vendor-specific update mechanisms, and opaque software supply chains. Security practices vary widely, even among products offering similar functionality. Empirical studies repeatedly demonstrate systemic weaknesses, including insecure local network protocols, insufficient authentication, excessive data collection, and unreliable update mechanisms [3]–[5]. These vulnerabilities do not merely affect individual devices; they propagate across networks and ecosystems, enabling large-scale exploitation and cascading failures [6], [7].

To address these challenges, the IoT industry and regulators have increasingly turned to standardization. Initiatives such as the Matter protocol [8] aim to unify device communication and management across vendors. Regulatory efforts, including the EU Cyber Resilience Act (CRA) [9] and the U.S. FCC IoT Cybersecurity Labeling Program [10], seek to establish baseline security requirements and transparency obligations for connected products [11], [12]. Supply-chain mechanisms such as Software Bills of Materials (SBOMs) [13] are promoted to improve visibility into software dependencies and vulnerabilities.

However, standardization is a double-edged sword. While it can reduce fragmentation and improve interoperability, any security or privacy weaknesses embedded in standards, or in their reference implementation, can be replicated at massive scale [14], [15]. The security of standardized IoT ecosystems therefore depends not only on the intent of regulations or standards, but on their design, interpretation, implementation, and enforcement.

In this paper, rather than treating the CRA purely as a legal instrument, we examine it as a socio-technical mechanism that translates security principles into technical requirements, conformity assessment procedures, and lifecycle obligations.

This paper makes three contributions:

- We provide a security and privacy-focused analysis of the EU CRA as a standardized IoT governance framework, grounded in empirical IoT security research.
- We identify key tensions between risk-based regulation, heterogeneous IoT implementations, and the practical limits of standard-driven conformity assessment.
- We derive implications for the design of future IoT standards and governance frameworks, highlighting the need for measurable security properties, automation-friendly assessment, and supply-chain-aware governance.

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-01-5
https://dx.doi.org/10.14722/sdiotsec.2026.23058
www.ndss-symposium.org

## II. Security & Privacy Challenges in Contemporary IoT Ecosystems

### A. Embeddedness & the Breakdown of Traditional Security Models

IoT devices differ fundamentally from traditional computing systems such as personal computers or smartphones. They are often embedded within trusted environments, homes, offices, hospitals, and industrial facilities, where they operate continuously and autonomously. Many IoT devices lack meaningful user interfaces, limiting the ability of users, even if these are sophisticated, to inspect device behavior, configure security settings, or detect anomalous activity [16], [17].

Traditional security models assume a relatively clear boundary between trusted internal systems and untrusted external attackers. This perimeter-based assumption is increasingly invalid in IoT deployments. A compromised IoT device can act as an internal adversary, enabling lateral movement within a local network, replay attacks against other devices, and long-term surveillance of user behavior. These risks are particularly pronounced in consumer environments where devices are often deployed in poorly managed networks without professional security management and oversight.

Standardization efforts that prioritize interoperability and ease of deployment, while essential for usability, risk reinforcing this embeddedness without adequately addressing its security implications. As devices become simpler to integrate and manage, they also become easier to deploy at scale. This expanding deployment magnifies the impact of shared vulnerabilities, potentially even increasing (systemic) risks associated with technology monocultures.

### B. Empirical Evidence of Systemic IoT Vulnerabilities

A substantial body of empirical research highlights recurring security and privacy failures across consumer IoT devices [18]. Large-scale black-box assessments have demonstrated that many devices accept insecure Transport Layer Security (TLS) configurations, rely on default or hardcoded credentials, and fail to properly authenticate cloud services or companion applications [4]. These weaknesses expose devices to man-in-the-middle attacks, unauthorized access, and firmware extraction.

Local network security remains a particularly underaddressed area. Studies of IoT devices supporting local connectivity have shown that a large fraction are vulnerable to replay attacks, allowing adversaries on the same network to trigger device actions without authentication [19]. Such attacks are increasingly plausible as the number of interconnected devices grows and as compromised devices are leveraged as internal attackers.

Privacy risks are equally pervasive. Traffic analysis studies reveal that many IoT devices communicate with multiple third-party servers unrelated to their core functionality, often transmitting data in plain text or using weak encryption [20]. Smart speakers and smart televisions have been shown to collect and transmit sensitive audio or viewing data, sometimes even when users attempt to opt out of explicit data collection. These behaviors are rarely transparent to users and are difficult to control without advanced technical expertise [21], [22].

Crucially, these vulnerabilities are not isolated anomalies. They reflect systemic design patterns that are frequently shared across vendors and product families. As such, they represent precisely the types of issues that standardization initiatives aim to address, but also risk perpetuating if not properly designed.

### C. AI-Enhanced IoT & the Expansion of the Threat Surface

The integration of artificial intelligence (AI), particularly machine learning and large language models, into IoT devices further expands the security and privacy threat landscape [23], [24]. Voice assistants, smart cameras, and wearables increasingly rely on cloud-based inference engines that process continuous streams of contextual data. These systems can infer sensitive attributes such as age, interests, routines, and socioeconomic status from seemingly benign interactions.

Recent research on AI-powered assistants demonstrates extensive tracking, profiling, and personalization behaviors, often without meaningful user awareness or consent. When such capabilities are embedded in physical IoT devices, the risks escalate [25], [26]. Misactivations that once resulted in accidental audio recordings can now trigger sophisticated inference pipelines capable of interpreting and storing contextual information over long periods [27].

Standardized IoT platforms exacerbate these risks by enabling consistent data flows and shared interfaces across devices and vendors. While this consistency improves interoperability, it also facilitates large-scale aggregation and inference. Existing regulatory models, which often focus on data protection and consent at a transactional level, struggle to capture these emergent, increasingly systemic risks.

## III. Standardization as a Mechanism for IoT Security Governance

### A. The Role of Standards in Shaping IoT Ecosystems

Standards play a central role in shaping IoT ecosystems [28], [29]. Network protocol standards define how devices communicate and authenticate, while governance and security standards specify baseline protections and determine how compliance is assessed and signaled to the market. Collectively, these standards influence not only technical product and process design choices but also market and industry value chain structures, innovation trajectories, and user trust.

Well-designed standards can reduce fragmentation, improve interoperability, and raise baseline security levels. Conversely, poorly specified standards can lock in insecure practices and propagate vulnerabilities across ecosystems. The security implications of standardization are therefore inseparable from broader questions of governance, enforcement, and accountability.

### B. Industry-Led Standardization: Opportunities & Risks

Industry-led initiatives such as Matter [8] exemplify the promise and peril of standardization. Matter aims to unify

smart home ecosystems by providing a common application layer for device discovery, commissioning, and communication. By reducing reliance on proprietary protocols, Matter seeks to simplify development and improve user experience

However, the security of such platforms depends on complex mechanisms, including certificate management, key distribution, and reference implementations. Any weaknesses in these components, whether due to design flaws, implementation bugs, or misconfigurations, risk being inherited by all compliant devices. Moreover, the complexity of standardized security mechanisms can obscure risks for smaller manufacturers, increasing the likelihood of incorrect or incomplete implementations.

### C. Regulatory Standardization & the Emergence of Baseline Security Requirements

Regulatory approaches to standardization seek to address market failures (e.g., due to asymmetric information and externality problems) and their consequences by mandating baseline security requirements. Rather than prescribing specific technical solutions, such frameworks typically define essential requirements that must be met by products placed on the market. Compliance is demonstrated through conformity assessment procedures that often rely on harmonized standards or certification schemes.

The EU CRA represents one of the most comprehensive regulatory attempts to govern IoT security through standardization. By introducing horizontal cybersecurity requirements for products with digital elements, the CRA seeks to systematically address both technical vulnerabilities and information asymmetries that affect users and regulators.

## IV. The EU Cyber Resilience Act: Scope & Core Mechanisms

The CRA applies to a broad range of hardware and software products with digital elements placed on the EU market [30]. Its primary objective is to raise baseline cybersecurity levels by addressing widespread vulnerabilities, insufficient update practices, and limited awareness and understanding by users. The Act recognizes that insecure products can act as vectors for systemic risks affecting consumers, businesses, and overall security levels within the digital single market [31].

At the core of the CRA are essential cybersecurity requirements that apply throughout the product lifecycle. These include obligations related to security-by-design and secure-by-default configuration principles, vulnerability handling, incident reporting, and the provision of security updates during a defined support period [32].

Manufacturers are required to conduct and document cybersecurity risk assessments for their products and document their compliance with the CRA's essential cybersecurity requirements. These assessments and documentations must be updated as necessary to reflect evolving threats and vulnerabilities. The Act further requires manufacturers to maintain detailed documentation of software components and dependencies, promoting transparency and supporting effective vulnerability management across complex supply chains.

A key element of the CRA is a multi-tiered conformity assessment framework. Based on a product risk classification, products deemed to pose lower cybersecurity risks may be subject to self-assessment, while higher-risk products require more stringent third-party evaluation or certification. Compliance is signaled through CE marking, providing a standardized indicator of conformity.

In principle, the proportionality of the conformity assessment framework is risk-based, seeking to align the regulatory burden with potential harm. In practice, however, conducting appropriate product-related risk assessments and determining risk classifications might be challenging, particularly in heterogeneous and dynamic IoT environments.

## V. Security & Privacy Implications of CRA-Driven Standardization

### A. Specification Gaps & the Challenge of Measurable Security

A central tension in the CRA lies in its reliance on high-level requirements rather than prescriptive technical controls. The CRA recognizes that diverse and dynamic technological contexts require flexibility. However, the CRA relies on broadly defined requirements at several levels (e.g., regarding specific essential cybersecurity requirements and technical controls, and risk assessment approaches), which can introduce uncertainty in interpretation and implementation.

Without standardized metrics and testable criteria [33], [34], consistent and harmonized conformity assessments and effective enforcement can hardly be expected; assessments may risk devolving into formalistic compliance exercises. The presence of an SBOM, for example, does not guarantee that vulnerabilities are actively managed or that dependencies are kept up to date. Effective security governance requires not only transparency but also actionable processes and measurable outcomes.

### B. Scalability of Conformity Assessment Infrastructure & the Risk of Regulatory Arbitrage

The CRA's effectiveness hinges on the capacity of conformity assessment bodies (CABs) to evaluate diverse IoT products, though most will rely on manufacturers' self-assessment rather than external audits. Scaling, selecting, and monitoring CABs pose significant challenges. Differences in expertise and rigor across CABs may result in non-harmonized evaluation and certification processes, creating risks of regulatory fragmentation, strategic venue shopping and regulatory arbitrage, and potentially in an erosion of trust in certification outcomes [30]. These challenges are amplified by the rapid pace of IoT innovation and the diversity of products covered by the Act. Ensuring consistent and meaningful assessments across relevant entities, member states, and product categories remains an open problem.

### C. Disproportionate Impacts on Small Manufacturers

While large manufacturers may navigate regulatory uncertainty and absorb compliance costs through dedicated security and legal teams, smaller manufacturers/vendors may be

disproportionately challenged. Although the CRA recognizes this, conducting risk assessments, maintaining documentation, translating requirements into product and process design, and navigating certification processes can impose significant burdens, potentially discouraging innovation or market entry [30]. If not carefully calibrated, standardized security requirements can have unintended consequences, such as elevated risks of reinforcing market concentration, reducing diversity, and inadvertently weakening ecosystem resilience.

## VI. Lessons for Secure Standardized IoT Design

*The Need for Automation-Friendly Security Standards:* Given the scale and complexity of IoT ecosystems, manual assessment and enforcement are insufficient. Security standards and regulatory frameworks must support automation, including continuous monitoring, automated testing, and machine-readable compliance artifacts [35].

*Supply-Chain Transparency Beyond Formal Compliance:* SBOMs represent an important step toward supply-chain transparency, but they are not a panacea. Their effectiveness depends on integration into active vulnerability management workflows and on reliable information sharing across stakeholders [36].

*Addressing Local Network & Internal Threat Models:* Many standardized IoT security frameworks focus primarily on cloud communication, neglecting local network threats such as replay attacks and lateral movement. Future standards must explicitly address these internal threat models.

*Governing AI-Driven Inference in IoT Systems:* AI-enabled inference fundamentally alters IoT risk profiles. Standardized governance mechanisms must move beyond traditional data protection models to address behavioral inference, autonomy, and long-term profiling risks.

## VII. Measurement, Verification, & the Limits of Standardized Assurance

One of the most critical and underexplored challenges in standardized IoT security governance is the lack of robust, scalable, and repeatable mechanisms for measuring security and privacy properties in real-world deployments. While the CRA emphasizes risk assessment, conformity assessment, and lifecycle obligations, it remains largely silent on how security should be empirically verified beyond high-level documentation and procedural compliance.

Security standards frequently rely on abstract requirements such as "appropriate" protection or security levels, "take measures", "effective" vulnerability handling, or "state of the art" mechanisms or security practices. While these formulations provide flexibility, they are hard to operationalise and do not translate naturally into measurable properties.

IoT security research repeatedly shows that devices can comply with high-level requirements while remaining vulnerable to practical attacks [37]. For example, a device may implement encrypted communication, yet accept self-signed certificates or fail to authenticate peers correctly [4]. Similarly, a manufacturer may provide a vulnerability disclosure policy and SBOM, while failing to issue timely updates or meaningfully reduce exposure in deployed systems.

This gap is particularly problematic in ecosystems where conformity signals such as CE marking or cybersecurity labels may be interpreted by users and integrators as indicators of substantive security guarantees. Without measurement-based assurance, such signals risk creating a false sense of security.

## VIII. International Fragmentation & the Risk of Divergent IoT Security Regimes

IoT ecosystems are inherently global. Devices designed in one jurisdiction are manufactured in another and deployed worldwide. As a result, beyond intra-EU harmonization challenges posed by the CRA, fragmented security governance risks imposing inconsistent requirements, increasing compliance complexity, and potentially weakening security outcomes.

### A. The CRA in a Global Context

The CRA is among the most ambitious regulatory efforts to date in governing product-level IoT security. However, it operates within an evolving global landscape that includes, inter alia: (i) The U.S. FCC IoT Cybersecurity Labeling Program; (ii) NIST IoT security baselines, (iii) Japan Cyber STAR (JC-STAR); (iv) sector-specific regulations in sectors like healthcare or automotive, (v) regulation focused on critical infrastructure, and (vi) other relevant legislation in the EU and beyond.

While these initiatives share overlapping goals, they differ in scope, terminology, assurance mechanisms, and enforcement models. For manufacturers operating globally, this regulatory fabric might create incentives to focus on minimum compliance rather than best-in-class security.

### B. Toward International Alignment & Mutual Recognition

From a security perspective, greater alignment between IoT security standards and labeling schemes is desirable. This does not necessarily imply uniform regulation, but needs to be predicated on: (i) Common terminology for security properties and risk categories; (ii) interoperable SBOM formats and vulnerability identifiers; (iii) mutual recognition of certification outcomes where appropriate; (iv) shared threat intelligence and coordinated disclosure mechanisms; (v) research and policy efforts that explore how standardized IoT security governance can scale across borders.

## IX. Conclusion & Future Research Directions

Standardized IoT security cannot be treated as a purely procedural or compliance-driven exercise. Regulatory ambiguity, limitations in conformity assessment scalability and harmonization, and gaps between formal compliance and real-world security outcomes risk turning standardization into a vehicle for scaling insecurity rather than mitigating it. Recognizing and addressing these challenges requires sustained (multidisciplinary) research efforts at the intersection of IoT standardization, security engineering, and governance.

A first critical research direction concerns the transition from qualitative risk assessment toward more systematic,

*model-driven risk modeling approaches*. Current regulatory frameworks largely rely on manufacturer-led assessments that struggle to account for deployment scale, network embeddedness, and dynamic ecosystem interactions. Future work should develop risk models that explicitly incorporate deployment context, lateral attack potential within local networks, dependency graphs derived from SBOMs, and interactions between device-level vulnerabilities and ecosystem-level impacts and risks.

Second, there is a pressing need to reorient IoT security standards toward local and edge-centric threat models. Many existing guidelines implicitly prioritize cloud communication and backend security, underestimating risks arising from device-to-device interactions and lateral movement within trusted environments. As edge computing and local AI inference become more prevalent, research should focus on developing standardized threat models for local IoT environments, defining security baselines for device-to-device communication. Taken together, these challenges define a critical research agenda for the IoT security community.

## Acknowledgments

The research in this paper was partially supported by the European Union's Digital Europe Programme (DEP) under Grant Agreement n.101158521 (CYBERSTAND.eu).

Volker Stocker would like to acknowledge funding by the Federal Ministry of Research, Technology and Space of Germany (BMFTR) under grant No. 16DII141 (Weizenbaum-Institut fur die vernetzte Gesellschaft – Das Deutsche Internet-Institut).

## References

[1] I. Pedersen and A. Iliadis, Eds., *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles*. The MIT Press, 2020.

[2] L. DeNardis and M. Raymond, "The internet of things as a global policy frontier," *UCDL Rev.*, vol. 51, p. 475, 2017.

[3] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer iot devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, 2017, pp. 1–6.

[4] S. Lazzaro, V. De Angelis, A. M. Mandalari, and F. Buccafurri, "A black-box assessment of authentication and reliability in consumer iot devices," *Pervasive and Mobile Computing*, vol. 110, p. 102045, 2025.

[5] N. Nino, R. Lu, W. Zhou, K. H. Lee, Z. Zhao, and L. Guan, "Unveiling IoT security in reality: A Firmware-Centric journey," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, 2024, pp. 5609–5626.

[6] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, "Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, 2019, pp. 1133–1150.

[7] S. J. Saidi, S. Matic, O. Gasser, G. Smaragdakis, and A. Feldmann, "Deep dive into the iot backend ecosystem," in *Proceedings of the 22nd ACM internet measurement conference*, 2022, pp. 488–503.

[8] W. Zegeye, A. Jemal, and K. Kornegay, "Connected smart home over matter protocol," in *2023 IEEE International Conference on Consumer Electronics (ICCE)*, 2023, pp. 1–7.

[9] European Commission, "Cyber Resilience Act," 2025, accessed: 2025-12-21. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[10] FCC, "FCC Adopts Rules for IoT Cybersecurity Labeling Program," https://www.fcc.gov/document/fcc-adopts-rules-iot-cybersecurity-labeling-program, online; Accessed 2025-12-21.

[11] ETSI, "ETSI EN 303 645," https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf, online; Accessed 2025-07-21.

[12] P. G. Chiara, "The iot and the new eu cybersecurity regulatory landscape," *International Review of Law, Computers & Technology*, vol. 36, no. 2, pp. 118–137, 2022.

[13] A. Chaora, N. Ensmenger, and L. J. Camp, "Discourse, challenges, and prospects around the adoption and dissemination of software bills of materials (sboms)," in *2023 IEEE International Symposium on Technology and Society (ISTAS)*, 2023, pp. 1–4.

[14] D. Barrera, I. Molloy, and H. Huang, "Standardizing iot network security policy enforcement," in *Workshop on decentralized IoT security and standards (DISS)*, vol. 2018, 2018, p. 6.

[15] R. Anderson and T. Moore, "The economics of information security," *science*, vol. 314, no. 5799, pp. 610–613, 2006.

[16] S. Lazzaro, V. De Angelis, A. M. Mandalari, and F. Buccafurri, "Repliot: A scalable tool for assessing replay attack vulnerabilities on consumer iot devices," in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 2024, pp. 7–8.

[17] A. Girish, T. Hu, V. Prakash, D. J. Dubois, S. Matic, D. Y. Huang, S. Egelman, J. Reardon, J. Tapiador, D. Choffnes *et al.*, "In the room where it happens: Characterizing local communication and threats in smart homes," in *Proceedings of the 2023 ACM on Internet Measurement Conference*, 2023, pp. 437–456.

[18] D. Zhao, Q. Li, Q. Zou, J. Xiao, K. Wu, R. Li, J. Lv, Y. Jiang, and K. Li, "Security and privacy in smart homes: Challenges and latest developments," in *Advances in the Internet of Things*. CRC Press, 2025, pp. 36–55.

[19] S. Lazzaro, V. De Angelis, A. M. Mandalari, and F. Buccafurri, "Is your kettle smarter than a hacker? a scalable tool for assessing replay attack vulnerabilities on consumer iot devices," in *2024 IEEE international conference on pervasive computing and communications (PerCom)*. IEEE, 2024, pp. 114–124.

[20] A. M. Mandalari, D. J. Dubois, R. Kolcun, M. T. Paracha, H. Haddadi, and D. Choffnes, "Blocking without breaking: Identification and mitigation of non-essential iot traffic," *Proceedings on Privacy Enhancing Technologies*, vol. 4, pp. 369–388, 2021.

[21] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 267–279.

[22] G. Anselmi, Y. Vekaria, A. D'Souza, P. Callejo, A. M. Mandalari, and Z. Shafiq, "Watching tv with the second-party: a first look at automatic content recognition tracking in smart tvs," in *Proceedings of the 2024 ACM on Internet Measurement Conference*, 2024, pp. 622–634.

[23] A. I. Hudig, A. M. Mandalari, C. Norval, H. Haddadi, R. Binns, and J. Singh, "Rights out of sight: Data practices and transparency gaps in smart consumer iot ecosystems," in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, 2025, pp. 2260–2273.

[24] Y. Vekaria, A. L. Canino, J. Levitsky, A. Ciechonski, P. Callejo, A. M. Mandalari, Z. Shafiq, and R. Model, "Big help or big brother? auditing tracking, profiling, and personalization in generative ai assistants," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025.

[25] OpenAI, "A Letter from Sam & Jony," May 2025. [Online]. Available: https://openai.com/sam-and-jony/

[26] P. Panay, "Introducing Alexa+, the Next Generation of Alexa," Feb 2025. [Online]. Available: https://www.aboutamazon.com/news/devices/new-alexa-generative-artificial-intelligence

[27] D. J. Dubois, R. Kolcun, A. M. Mandalari, M. T. Paracha, D. Choffnes, and H. Haddadi, "When speakers are all ears: Characterizing misactivations of iot smart speakers," *Proceedings on Privacy Enhancing Technologies*, 2020.

[28] V. A. Almeida, B. Goh, and D. Doneda, "A principles-based approach to govern the iot ecosystem," *IEEE Internet Computing*, vol. 21, no. 4, pp. 78–81, 2017.

[29] R. H. Weber, "Accountability in the internet of things," *Computer Law & Security Review*, vol. 27, no. 2, pp. 133–138, 2011.

[30] V. Stocker and A. M. Mandalari, "Governing IoT Cybersecurity in the Digital Single Market: A Techno-Economic and Policy Analysis of the EU Cyber Resilience Act," 2025. [Online]. Available: https://dx.doi.org/10.2139/ssrn.5386101

[31] M. Dalla Preda, S. Egelman, A. M. Mandalari, V. Stocker, J. Tapiador, and N. Vallina-Rodriguez, "Eu cyber resilience act: Socio-technical and research challenges (dagstuhl seminar 24112)," *Dagstuhl Reports*, vol. 14, no. 3, pp. 52–74, 2024.

[32] Federal Office for Information Security, "Cyber Resilience Act," 2025, accessed: 2025-12-21. [Online]. Available: https://www.bsi.bund.de/dok/cra-en

[33] K. Scarfone and P. Mell, "An analysis of cvss version 2 vulnerability scoring," in *2009 3rd International Symposium on Empirical Software Engineering and Measurement*. IEEE, 2009, pp. 516–525.

[34] R. Böhme, "Security Metrics and Security Investment Models," in *Advances in Information and Computer Security*, ser. Lecture Notes in Computer Science, I. Echizen, N. Kunihiro, and R. Sasaki, Eds. Berlin, Heidelberg: Springer, 2010, vol. 6434, pp. 10–24.

[35] B. Moran, H. Tschofenig, D. Brown, and M. Meriac, "A firmware update architecture for internet of things," *RFC 9019*, 2021.

[36] S. Wachter, "Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr," *Computer law & security review*, vol. 34, no. 3, pp. 436–449, 2018.

[37] M. Alhussan, F. Boem, S. S. Ghoreishizadeh, and A. M. Mandalari, "Hacking health: Unveiling vulnerabilities in ble-enabled wearable sensor nodes," in *2025 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2025, pp. 1–5.