Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 10| 2025

Research Article **Received:** 01-09-2025| **Accepted:** 21-09-2025 | **Published:** 17-10-2025

Enhancing IoT Security by Identifying Vulnerabilities, Addressing Compliance Gaps, and Strengthening Manufacturer Responsibilities

***Mildred Adwubi Bonsu* [1], *and Alice Ama Donkor* [2]**

[1]*University at Albany, State Univ. Of New York*

[2]*Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana*

Abstract: Internet of Things (IoT) has seen itself proliferating across industries and households rapidly. Its broad expansion has introduced severe present complex security risks to current safeguard. The IoT ecosystem has so much promise, but it also remains riddled with vulnerabilities, compliance inconsistencies and there is limited accountability from device manufacturers. This research investigates these three critical dimensions, that is technical weaknesses, regulatory gaps, and manufacturer responsibility, using a combined methodology of vulnerability analysis, policy review, and manufacturer case studies. This study details persistent device-level vulnerabilities, like hardcoded credentials and insecure communication protocols as well as delayed or absent firmware updates. While standards like GDPR and ETSI EN 303 645 exist, their implementation is found to be inconsistent, with many manufacturers only partially adhering to security recommendations. It exposes how compliance efforts are typically narrowed in their end-user data protection practices, overlooking the larger architectural risks with integrated IoT systems. This research further reveals how manufacturer obligations are often described as post-market obligations such as patching after incidents rather than proactive design mandates. This reactive orientation results in the delay of timely interventions and promotes a security posture which is outsourced to consumers and regulators rather than embedded right at the point of production. Through a synthesis of these technical, regulatory, and organizational shortcomings, the research offers a holistic understanding of why IoT security remains elusive despite ongoing efforts and recommends a Secure IoT Governance Model (SIGM) as a path forward.

Keywords: IoT Security, Vulnerability Assessment, Compliance, Manufacturer Accountability, Cybersecurity Frameworks.

INTRODUCTION

IoT is an essential part of the modern infrastructure and digital operations across healthcare, utilities, manufacturing, government, and consumer technology over the last decade (NIST NCCoE, 2025). But with that expansion comes economic opportunities as well as rapidly growing attack surface. This expansion brings not only economic potential but also a rapidly widening threat surface. While various market forecasts estimate that the number of IoT devices could exceed 30 billion globally by 2025, the real concern lies in securing these interconnected environments against exploitation, misconfiguration, and systemic vulnerabilities. Within Industrial Internet of Things (IIoT), it is forecast to deliver as much as USD14trillion in global economic output by 2030, as organizations increasingly adopt connected technologies to enable predictive maintenance, improve asset efficiency, and automate production processes (Miramar Global, 2025). These developments reflect the growing importance of IIoT in reshaping the industrial performance and competitiveness within digital world.

An example of how IoT proliferation outpaces security measures is demonstrated in the emergence of the BadBox 2.0 botnet, a major cybercrime operation affecting more than ten million Internet-connected Android devices (The Hacker News, 2025). This botnet was buried in firmware at the time of manufacturing, enabling a recurring malware loading even after factory resets. Compromised devices including smart TVs, digital signage and media players were incorporated into a large proxy network that was subsequently marketed to buyers for illegal uses like credential stuffing attacks and ad fraud. Default credentials are still used in many volume-based attacks. For example, the Mirai botnet is a malware that scans the internet for insecure IoT devices with open Telnet ports, tries to access them by using a hardcoded list of common factory default usernames and passwords (CISA 2016). Once compromised, the devices are locked up in a botnet used to launch massive, distributed denial-of-service (DDoS) attacks. After this, Mirai's architecture and source code have been copied and replicated in so many different ways, making it a persistent threat vector due to its simplicity and effectiveness in exploiting poor credential hygiene. The above examples highlight just how persistent configuration flaws and weak defaults render IoT devices a ready target. However, beneath the surface of these large-scale botnet campaigns emerges a deeper systemic challenge. It has been observed that most compromises begin with surprisingly basic

***Corresponding Author:** Alice Ama Donkor

DOI- https://doi.org/10.5281/zenodo.17378001

technical oversights. Insecure defaults and fragile firmware run silently through IoT networks from smart thermostats in homes to programmable logic controllers in factories, inadvertently undermining the backbone of modern communication. It is in these seemingly trivial design flaws which are often invisible to users, that the true scale of the IoT security crisis unfolds. Recognizing these technological weaknesses is the initial move toward addressing the structural limitations they showcase.

Technical Vulnerabilities in IoT Systems

Within IoT systems, some of the most persistent and foundational technical vulnerabilities are hardcoded credentials, weak or entirely absent encryption protocols, outdated firmware, and the lack of secure boot mechanisms (OWASP, 2025; JumpCloud, 2025). While these were not isolated incidents, nor a product of legacy systems. These issues are not isolated incidents or remnants of legacy systems. Rather, they reflect structural deficiencies embedded in the lifecycle of IoT product development. For instance, hardcoded credentials are still quite common throughout consumer and industrial IoT devices. While these are often configured by the manufacturer to allow for rapid deployment and ease of configuration, they are frequently either not disclosed to the end user or left unchanged as a result of weak user enforcement protocols. In some instances, particularly in older or lower-cost devices, these credentials are hardcoded into the firmware and cannot be modified by an end user even if they are aware of the risks associated with it (OWASP 2025; Check Point 2021). As a result, attackers can exploit publicly available databases of default usernames and passwords, sometimes provided by the manufacturers themselves, to automate access to vulnerable devices at scale (Ontinue, 2025).

A principal technical shortcoming is the persistent use of unauthorized or unpatched firmware. Most IoT vendors release firmware updates irregularly, neglecting critical vulnerabilities unaddressed even after they have been disclosed publicly. This is further compounded by the absence of automated update process mechanisms. While smartphones or standard operating systems update via Over-The-Air (OTA) updates and enforce regular patch cycles, many IoT devices still need manual intervention in case of firmware upgrades which is difficult at scale especially for hard-to-reach or industrial environments deployed devices (Forescout, 2025). This leads to a long-tail of susceptible endpoints that could be active for years and making them attractive targets for persistent access from adversaries.

In addition, the lack of secure boot mechanisms further weakens the trustworthiness of these devices. Secure boot is a mechanism that ensures that the firmware executed by a device is cryptographically verified by the manufacturer. Without it, attackers can overwrite firmware with malicious code that survives reboots, embeds rootkits, or intercepts communications without detection. Because many IoT devices tend to work autonomously and without direct user interaction, the attackers could have a chance to keep using compromised devices to their advantage for extended periods before detection, if it is detected at all (OWASP, 2025).

These vulnerabilities, although distinct, interact in ways that amplify systemic risk. Hardcoded Credentials in a device can be dangerous by itself, however when that device also lacks encryption and cannot be updated remotely, and is missing secure boot, it becomes a persistent, silent liability within its network environment. The aggregated effect becomes a collection of oversights and an architectural failure that compromises the integrity, confidentiality, and resilience of entire IoT ecosystems.

Consumer IoT: TP-Link Tapo L530E Smart Bulb Vulnerabilities (2023)

Cybersecurity researchers in 2023 found critical security vulnerabilities in popular consumer IoT device TP-Link Tapo L530E smart bulb which is a popular consumer IoT device used globally in smart home automation. The security audit, conducted by Bonaventura et al. (2023), revealed that the smart bulb was susceptible to authentication bypass and Wi-Fi credential leakage, both of which posed significant risks to user privacy and network security. The vulnerabilities were particularly severe because they allowed attackers within Bluetooth or Wi-Fi range of the device to exploit insecure communications between the mobile app and the bulb. By the assistance of reverse engineering and traffic interception, the researchers were able to retrieve plaintext Wi-Fi credentials stored in the device's memory and gain unauthorized access to the smart home network. Having gained access, attackers could control the lighting system, take over connected devices, or move laterally within a home network. Even though smart home security has garnered increased exposure, TP-Link was very slow in issuing patches and there are still

Publisher: SARC Publisher

many users who did not know their devices were vulnerable or lack the technical knowledge to apply the necessary updates. The implications of insufficient vendor disclosure, in addition to the problem space around vulnerability management from a user-side perspective in consumer IoT ecosystems, were also underscored with this case.

Industrial IoT (IIoT): Security Weaknesses in U.S. Critical Infrastructure (2025)

During a U.S. congressional briefing in July 2025, light was shed on rising threats across Operational Technology (OT) ecosystems that are retrofitted with IoT functionalities, known as Industrial IoT (IIoT) networks. These networks govern critical infrastructure such as energy grids, water treatment plants and industrial manufacturing systems, hence making them a high-value targets for cyber adversaries. The briefing identified that many OT systems continue to run outdated firmware, often embedded with default credentials or lacking proper access controls. These insecure configurations originate from older legacy systems that were not originally designed with cybersecurity in mind but later adapted to incorporate IoT sensors, controllers, and remote monitoring tools. Consequently, they represent an extended attack surface especially as threat actors increasingly target physical infrastructure for geopolitical or financial gain (Industrial Cyber Attacks, 2025).

In addition to the rising threat of attacks on energy plants and other critical facilities, Nozomi Networks Mid-Year ICS Threat Report (2025) also highlights a sharp increase in security vulnerabilities discovered in Industrial Control Systems (ICS), which are critical to the operation of infrastructure such as energy plants, water treatment facilities, and manufacturing lines. At the same time, as part of the broader Industrial Internet of Things (IIoT) ecosystem, ICS environments today have an ever-growing set of network-connected components like Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems, which provide real-time monitoring and automation capabilities or remote access. However, this improved connectivity also introduces additional security risks. A good number of the vulnerabilities mentioned in this report ended up on the Known Exploited Vulnerabilities (KEV) list from the US Cybersecurity and Infrastructure Security Agency (CISA), proving that they were actively targeted by attackers. Remote code execution vulnerabilities in PLCs (Programmable Logic Controllers) scoped as one of the most critical security threats, given that these are devices that directly control physical processes as well as the continued use of insecure, legacy communication protocols within SCADA networks. Many of these protocols did not have in-built security controls like encryption or mutual authentication, making it easier for malicious actors to intercept, manipulate, or disrupt critical industrial operations over the network.

Implications for Data Integrity, Privacy, and Critical Infrastructure

Aside the direct threat of unauthorized access, vulnerabilities in IoT devices create a pervasive risk to data integrity – creating a situation where an attacker might not steal information but subtly change it to undermine confidence in automated decisions. Particularly in environments such as smart manufacturing, healthcare, and energy distribution, tampered sensor outputs can lead to flawed analytics, incorrect diagnoses, or dangerous system behaviors (Garagad *et al.*, 2020). This silent corruption of data poses a greater long-term threat than overt breaches, particularly in AI-powered systems that rely on consistent and trustworthy inputs.

IoT devices constantly collect large amounts of data about people's behavior, physical movements, and even body measurements like heart rate, location or sleeping patterns. Even when these systems aren't fully hacked, exposed data metadata such as time stamps, GPS coordinates, or device IDs can still be enough to track individuals. An attacker having access to such information can study and learn patterns like where someone goes everyday or when a building is usually vacant. That kind of *"invisible surveillance"* easily enables companies or hackers to provide very detailed user profiles without actually having visibility into the full data. This problem gets worse when you consider smart cities or modern hospitals where many devices talk to each other and share data across systems. In these environments, it is more difficult to differentiate between personal data and operational data and, as a result, privacy risks multiply quickly (Ziegeldorf *et al.*, 2014).

Compliance and Regulatory Gaps

The rise of Internet of Things (IoT) has prompted the development of a number of regulatory and standards-based frameworks aimed at increasing security, protecting user privacy, and guiding good behavioral practice. Significant among them are

Publisher: SARC Publisher

the European Union's General Data Protection Regulation (GDPR), the European Telecommunications Standards Institute's (ETSI) EN 303 645 standard for consumer IoT security and the U.S. National Institute of Standards and Technology's (NIST) IoT Cybersecurity Framework. These frameworks are major milestones towards formalizing expectations around data protection, device hardening, and system resilience.

But the limits of scale and enforcement mechanisms are beginning to show as IoT systems grows more varied and globally distributed. The GDPR, for example, excels in establishing comprehensive data privacy rights for individuals but offers minimal guidance on the technical specifications necessary to secure complex, embedded systems throughout their operational lifespan (Voigt and Von dem Bussche, 2017). Similarly, as ETSI EN 303 645 sets out minimum cybersecurity requirements for consumer IoT such as eliminating default passwords and making sure consumers can get software updates promptly, its voluntary nature and uneven adoption across manufacturers reduce its practical enforceability (ETSI, 2020).

Furthermore, lifecycle-related issues like patch management, third party integrations, and device decommissioning are often underregulated. Many present-day standards and laws seem to concentrate a great deal on frontend privacy compliance, often without sufficiently addressing backend system integrity or device end-of-life issues. For example, regulatory mechanisms rarely impose binding obligations on manufacturers to support long-term firmware updates, leaving countless IoT devices unpatched and vulnerable long after deployment (Wang *et al.*, 2021).

A critical blind spot emerges in the regulation of supply chain and third-party service providers. Real-world incidents such as the 2021 Verkada breach highlight this challenge, where hackers accessed over 150,000 live camera feeds, including in hospitals, prisons, and schools, by exploiting hardcoded credentials within a third-party vendor's development tools (Wired, 2021). Though the company was compliant with a number of privacy regulations, the breach showed how architectural oversights and weak integration controls can make formal compliance inadequate.

In addition, enforcement differs tremendously across jurisdictions. For example, although companies like D-Link and TRENDnet have been penalized for weak IoT security practices by the U.S. Federal Trade Commission (FTC) (FTC 2019), the absence of federal IoT-specific legislation creates patchwork compliance obligations that often conflict across states. A more centralized approach embodied by programs like Singapore's Cybersecurity Labelling Scheme (CLS), which labels IoT products according to their security readiness, has been lauded for incentivizing proactive compliance (Cyber Security Agency of Singapore, 2022).

MANUFACTURER RESPONSIBILITY AND MARKET INCENTIVES

Lack of Built-in Accountability Mechanisms

Despite rising regulatory pressure, many manufacturers still fail to incorporate essential accountability structures, such as mandated firmware support periods or automated update mechanisms. Research points to a large number of IoT devices outdated or unsupported firmware, with some remaining unpatched for extended periods, exposing users to preventable security risks (Prakash *et al.*, 2022; Ebbers, 2020). Automated over-the-air (OTA)update infrastructure remains underutilized, with many vendors lacking consistent patch management pipelines. The UK's Product Security and Telecommunications Infrastructure (PSTI) Act, which came into effect in 2024, aims to address such gaps by requiring manufacturers to disclose the minimum length of time firmware will be supported and banning default passwords on consumer smart devices. Violations of the law may face fines of up to £10 million or 4% of global turnover (Help Net Security, 2024). While this is a definitive step in the direction of regulatory enforcement and built-in accountability, similar legislative uptake remains limited or entirely absent in many jurisdictions globally.

Vendor Behavior and Product Lifecycle Patterns

In the United States, a lack of standardized requirements continues to allow major vendors especially in the consumer IoT space to operate with minimal transparency. While larger companies often have more brand reputation to protect, smaller or budget device manufacturers rarely disclose software lifespans. A Consumer Reports investigation revealed that only 3 out of 21 smart appliance brands publicly stated how long their devices would receive updates, and nearly 90% provided no information about

Publisher: SARC Publisher

software support periods—leaving consumers unaware of potential security risks (Consumer Reports, 2024; Consumer Reports, 2025). In the absence of binding federal mandates or contractual enforcement by retailers and distributors, this opacity persists across the market.

Since there are no regulations requiring mandatory disclosure, or merchants or distributors who enforce contractually binding standards on transparency, this non-transparency permeates the market.

In addition, recent federal initiatives and Executive Orders are starting to influence procurement requirements. For example, the White House Executive Order 14028 mandates that federal agencies ask for software bills of materials (SBOMs) from vendors, promoting increased software supply chain transparency. To meet these procurement standards, major U.S.-based industrial vendors such as Rockwell Automation have begun SBOMs integrations within their product suites like FactoryTalk, aligning with procurement expectations from both public and private sector clients (NIST, 2021; CISA, 2024). These measures reflect a growing preference for vendors that offer visibility, auditability, and long-term support assurances.

Impact on Consumers, Governments, and Enterprises

The collective impact of inadequate manufacturer accountability in the IoT ecosystem extends far beyond isolated device vulnerabilities. For consumers, the absence of predictable support lifecycles and built-in security defaults have eroded trust in smart technologies, resulting in reluctance in adoption and growing concerns over digital autonomy (Deloitte, 2024).

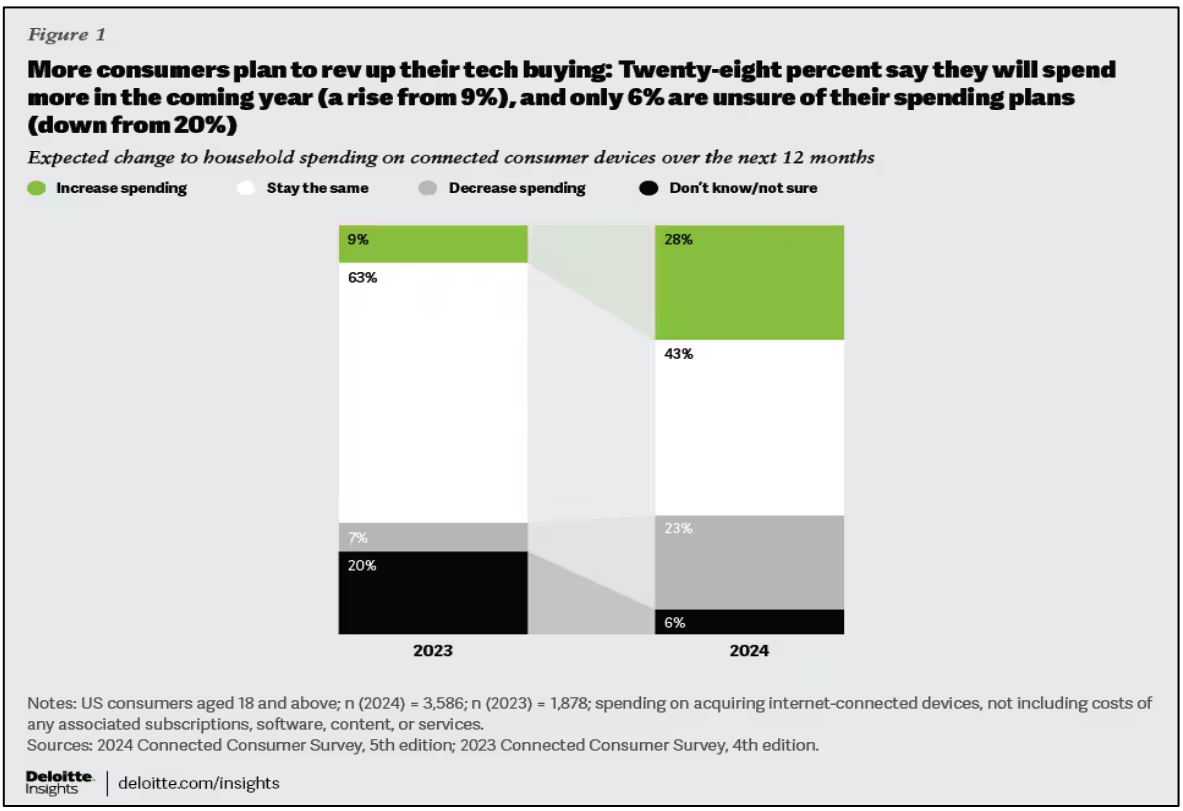

Figure 1: Deloitte, Mobile Consumer Survey, 2024 The Growing Trust Gap in Smart Devices.

As Figure 1 above from the Deloitte 2024 Mobile Consumer Survey shows, device support and longevity have now become top three purchase criteria for many people, often surpassing price or brand. The above reluctance undermines the societal benefits of IoT integration, from energy saving through to assisted living, especially for those in society that may lack the technical means to be able to independently manage device security.

These systemic weaknesses translate into operational and financial overheads for enterprises. The result is an ecosystem where organizations are forced to absorb the cost of compensating for insecure defaults, that is investing in network segmentation, third-party patching workflows, and

Publisher: SARC Publisher

continuous threat monitoring simply to maintain acceptable risk thresholds (Help Net Security, 2018). It diverts resources from innovation and often leads to misaligned vendor relationships, where businesses must demand security assurances post-procurement rather than receiving them by design. There are similar problems within procurement among public sector organizations for infrastructure deployment as well. Federal agencies, according to a 2025 U.S. Government Accountability Office (GAO) report, are issuing updated guidance to help ensure secure IoT acquisitions under Executive Order 14028, however implementation gaps persist (GAO, 2025). ithout enforceable manufacturer obligations such as long-term support or transparency via Software Bills of Materials (SBOMs), government systems remain vulnerable to device-level security decay and fragmentation.

Recommendations: The Secure IoT Governance Model (SIGM)

To address the persistent and evolving risks posed by insecure and unsupported IoT devices, this paper introduces the Secure IoT Governance Model (SIGM), a forward-looking, policy-oriented model for ensuring the safety, accountability, and resilience of IoT ecosystems. It is built upon five foundational pillars that work closely to provide a holistic governance and security coverage across the IoT lifecycle.

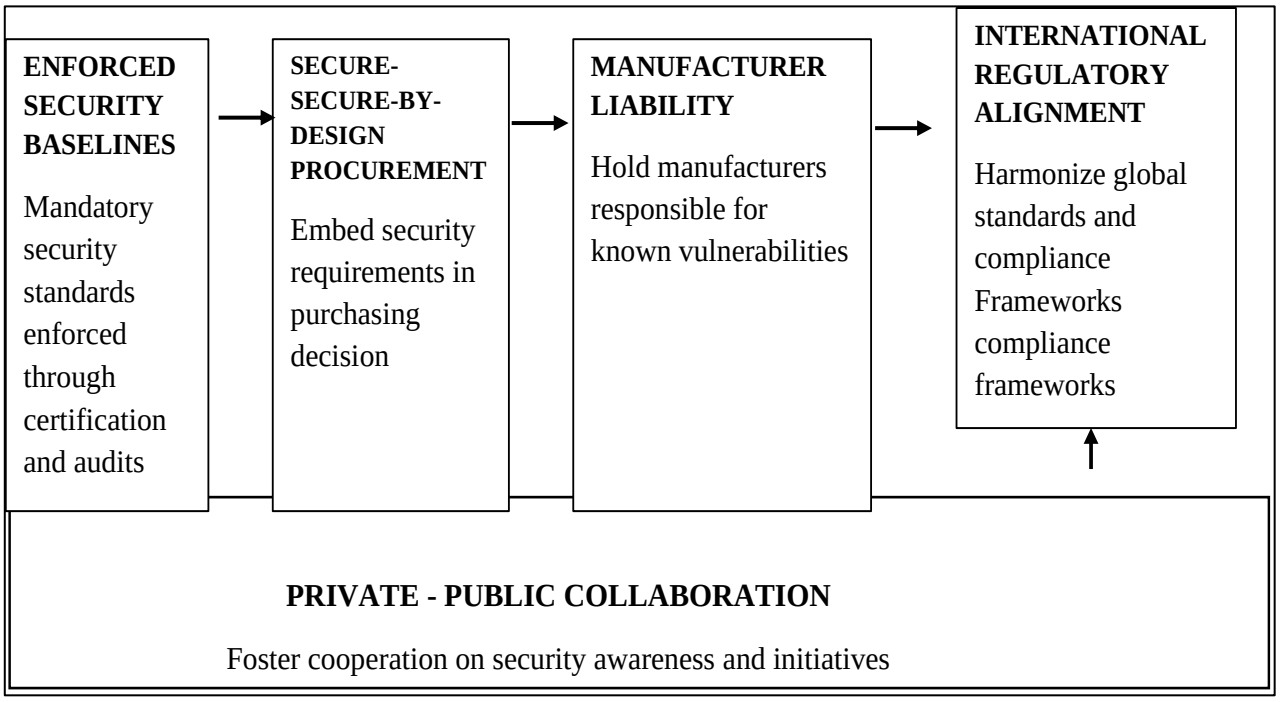

Figure 2: The Secure IoT Governance Model (SIGM)

The first pillar calls for the establishment of compulsory security baselines and technical standards (not leaving those to voluntary compliance). These baselines would require all devices to enforce fundamental security controls, such as secure boot processes, strong password defaults and encryption of data at rest and in transit and validated using rigorous certification programs and third-party audits. By aligning with widely recognized frameworks like NIST IR 8259 and ETSI EN 303 645, these enforced standards would foster consistency in device-level protections, irrespective of market or geography, and close the gap created by fragmented or manufacturer-specific security practices.

The second key element of the SIGM focuses on embedding security into procurement protocols throughout life cycle of an IoT device. This approach requires vendors to unambiguously define the minimum duration of their support, software update policies, end-of-life practices, and maintain a complete Software Bill of Materials (SBOM). Embedding these requirements in procurement contracts makes security non-negotiable factor in acquisition decisions, and ensures that any device purchased by governments or enterprises remain maintainable and secure throughout their operational lifespan.

Also, a critical aspect is the pillar addressing manufacturer accountability. To eliminate the

Publisher: SARC Publisher

systemic neglect of unresolved vulnerabilities, SIGM proposes clear legal obligations for vendors who fail to provide timely patches or who misrepresent their product support policies. Legal liabilities reinforced by civil penalties or sanctions such as market-access restrictions would serve as a strong deterrent against poor security practices. Additionally, by standardizing vulnerability disclosure norms such as an established 90-day remediation period would enable transparency and predictability in post-market support.

Because IoT supply chains are global in nature, SIGM also demands well-guided international regulatory intervention. Harmonizing security regulations across jurisdictions via multilateral agreements or continental initiatives like Africa's Smart Africa Alliance would prevent regulatory arbitrage and facilitate uniform standards for compliance. Such coordination would also support the exchange of international threat intelligence and facilitate cross-border portability of certifications, relieving some manufacturers from the obligation to maintain multiple different standards while lifting the collective bar of security.

The model also highlights the need for public-private partnership and consumer empowerment. This includes co-developed programs such as recognizable security labeling systems (e.g. the U.S. Cyber Trust Mark), national awareness campaigns on digital hygiene and device decommissioning, as well as accessible secure-by-design training for developers and small businesses. These measures work to embed a culture of security throughout the entire IoT value chain, ensuring that users are better informed, developers are better trained, and industry actors are more accountable.

Through the integrated application of these five pillars, the Secure IoT Governance Model (SIGM) provides a practical, scalable roadmap for transforming IoT security from reactive fixes into a coordinated system of proactive, enforceable measures.

CONCLUSION

IoT is growing exponentially, intertwining with key sectors such as health care, energy, finance, transportation and our daily lives. While promising, this new connected world also creates sprawling attack surfaces that existing security solutions are underequipped to defend against. What began as a convenience-driven innovation has become a high-stakes ecosystem where device insecurity can multiplies into real-world disruption, surveillance, or harm. This paper demonstrates a path forward. By architecting the IoT fabric through policy, standards, roles and enforcement, it is possible to build trust into the IoT fabric without slowing down innovation. Securing the Internet of Things does not require an endless stream of tools, frameworks, or firewalls. It demands transparency, responsibility and accountability across board, from manufacturers and partners to governments, right down to end users. The future of IoT security is not in isolated fixes but in a holistic, extending action. In the end, it is not a problem of technological capabilities anymore, since we possess the necessary tools at our disposal to secure IoT systems. Instead, it lays in our collective capacity to align political will, institutional governance and cross-sector accountability to ensure its secure and responsible integration into society.

REFERENCES

1. NIST National Cybersecurity Center of Excellence (NCCoE). "Securing the Internet of Things (IoT)." (2025)
2. Miramar Global. *Industrial IoT could boost global economy by $14 trillion*. (2025)
3. Hacker News, "Google Sues 25 Chinese Entities Over BADBOX 2.0 Botnet Affecting 10M Android Devices." 18 July. (2025)
4. CISA "Heightened DDoS Threat Posed by Mirai and Other Botnets. Cybersecurity and Infrastructure Security Agency." (2016)
5. Bonaventura, D., Esposito, S., & Bella, G. "Smart bulbs can be hacked to hack into your household." *arXiv preprint arXiv:2308.09019* (2023).
6. Cymulate, "How to Stay Ahead of IoT Security Issues." *Cymulate blog,* May (2025)
7. Forescout "Riskiest Connected Devices of 2025 Report." *Forescout,* April. (2025)
8. Industrial Cyber Attacks "US critical infrastructure remains exposed." 22 July. (2025)
9. JumpCloud "IoT Security Risks: Stats and Trends to Know in 2025." 10 January. (2025)
10. Nozomi Networks "OT/IoT Cybersecurity Trends & Insights 2025." (2025) February.
11. Ontinue "Hidden Dangers of IoT Device." *Ontinue,* (2025).
12. OWASP "OWASP IoT Top 10 Vulnerabilities (2025 Updated)." *Wattlecorp,* (2025).
13. SentinelOne "Top 10 IoT Security Risks and How to Mitigate Them." *SentinelOne,* (2025).

Publisher: SARC Publisher

14. Check Point "IoT Security Issues – What Is IoT Security? (2021)
15. OWASP "OWASP IoT Top 10: Weak, Guessable or Hard-coded Passwords; Lack of Secure Update Mechanism. OWASP Foundation." (2025)
16. Akinpelu, Z.O. "The Looming Threat of Unsecured IoT Devices: A Deep Dive." *ISACA Now Blog*, 10 July. (2024).
17. Information Systems Frontiers, "Analysis of the Cryptographic Algorithms in IoT Communications', Information Systems Frontiers, 26(6)." pp. 1243–1260. (2023)
18. Bonaventura, D., Esposito, S., & Bella, G. "Smart Bulbs Can Be Hacked to Hack into Your Household." *arXiv.* (2023)
19. Industrial Cyber Attacks "US critical infrastructure remains exposed as Congress confronts OT cybersecurity gaps, fifteen years after Stuxnet." *Industrial Cyber Attacks*, 22 July. (2025).
20. Garagad, V. G., Iyer, N. C., & Wali, H. G. "Data integrity: a security threat for internet of things and cyber-physical systems." *2020 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, (2020).
21. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. "Privacy in the Internet of Things: threats and challenges." *Security and Communication Networks* 7.12 (2014): 2728-2742.
22. Wang, D., Jiang, M., Chang, R., Zhou, Y., Hou, B., Luo, X., ... & Ren, K. "A measurement study on the (in) security of end-of-life (eol) embedded devices." *arXiv preprint arXiv:2105.14298* (2021).
23. Wired, "Hackers Access Security Cams Inside Tesla and Beyond, Wired." 9 March. (2021)
24. Cyber Security Agency of Singapore, "Cybersecurity Labelling Scheme." (2022)
25. ETSI, "Cyber Security for Consumer Internet of Things: Baseline Requirements." *ETSI EN* 303 645 V2.1.1. (2020)
26. Voigt, P., & Von dem Bussche, A. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10.3152676 (2017): 10-5555.
27. Federal Trade Commission (FTC), "D-Link Agrees to Make Security Enhancements to Settle FTC Litigation." (2019) 2 July.
28. Prakash, V., Xie, S., & Huang, D. Y. "Software update practices on smart home IoT devices." *arXiv preprint arXiv:2208.14367* (2022).
29. Ebbers, F. "A large-scale analysis of iot firmware version distribution in the wild." *IEEE Transactions on Software Engineering* 49.2 (2022): 816-830.
30. Help Net Security "UK enacts IoT cybersecurity law." *Infosecurity Magazine*, 29 April. (2024)
31. Consumer Reports, "The Hidden Lifespan of Smart Devices: What the FTC's Report Means for Consumers, Innovation Blog." (2024)
32. Consumer Reports, "More Smart Home Companies Want to Hear from Security Researchers." *Innovation Blog*, 14 July. (2025).
33. U.S. Government Cybersecurity Software Requirements (SBOMs): CISA, "Software Bill of Materials (SBOM)." (2024).
34. NIST, "Executive Order 14028: Improving the Nation's Cybersecurity." (2021).
35. Deloitte, "Connected Consumer: Trust and Gen AI Survey." June. (2024).
36. GAO, "Internet of Things: Federal Actions Needed to Ensure Secure Procurement and Acquisition Practices (GAO-25-107179)." (2025).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Bonsu, M. A. and Donkor, A. A. "Enhancing IoT Security by Identifying Vulnerabilities, Addressing Compliance Gaps, and Strengthening Manufacturer Responsibilities." *Sarcouncil Journal of Engineering and Computer Sciences* 4.10 (2025): pp 120-127.

Publisher: SARC Publisher