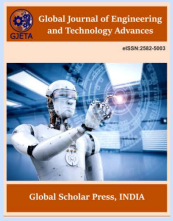
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(REVIEW ARTICLE)

Check for updates

CYBERSECURITY RISKS IN CONNECTED DEVICES: A REVIEW OF VULNERABILITIES, THREATS, AND PROTECTIVE STRATEGIES

Ayorinde Oduroye, Benjamin Thompson Ayodele *, Kenechukwu Adolphus Ezeagu, Talabi Ibrahim, Elizabeth Irebhose Ojenor, Olaore Olaniyi Ademola and Solomon Enobong Umanah

Department of Computer Science, Faculty of COPOS, Caleb University, Imota,Lagos, Nigeria.
* Corresponding Author

ORCID Details
Ayorinde Oduroye: https://orcid.org/0000-0001-8755-9816

Global Journal of Engineering and Technology Advances, 2026, 28(02), 218–223

Publication history: Received on 18 July 2026; revised on 26 August 2026; accepted on 28 August 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.28.2.0227

ABSTRACT

Connected devices, ranging from smartphones and wearables to industrial sensors, medical equipment, and connected vehicles, have become integral to modern personal, commercial, and industrial life. This growing reliance on Internet of Things (IoT) technology has expanded the digital attack surface available to malicious actors, introducing cybersecurity risks that extend well beyond traditional computers and networks. This paper reviews the major categories of cybersecurity risk facing connected devices, including weak or default credentials, outdated firmware, insecure communication, poor configuration, and inadequate device management, and examines the principal forms of cyberattack these weaknesses enable, including credential-based attacks, malware, botnets, distributed denial-of-service attacks, man-in-the-middle attacks, spoofing, and physical tampering. The review further considers the privacy, financial, and physical-safety consequences of connected-device compromise, the practical challenges organizations and individual users face in securing heterogeneous device environments, and the layered technical and organizational measures, including strong authentication, encryption, network segmentation, device inventory management, and continuous monitoring, that can reduce these risks. Drawing on foundational IoT literature and established cybersecurity guidance from standards bodies, the review concludes that securing connected devices is a shared responsibility among manufacturers, organizations, and users, and that no single control is sufficient on its own. As connected technology continues to expand, layered, continuously updated security practices will remain essential to protecting individuals, organizations, and critical services.

Keywords: Internet Of Things; Cybersecurity; Connected Devices; Data Privacy; Network Security

1 INTRODUCTION

A device capable of connecting to the Internet is also, by that same capability, a potential target for a cyberattack. Contemporary life depends heavily on connected devices for communication, entertainment, transportation, healthcare, education, business, and security: smartphones, smart televisions, fitness trackers, security cameras, smart speakers, routers, vehicles, medical equipment, and industrial machinery all exchange information across digital networks as a matter of course. This class of technology is generally understood as part of the Internet of Things (IoT), a paradigm in

which physical objects collect information through sensors, communicate with other systems, and, in many cases, act on that information automatically; an early and still widely cited definition frames IoT as the convergence of ubiquitous computing, embedded devices, and internet connectivity into smart objects capable of continuous interaction with their environment [1]. Subsequent work has extended this vision to describe the architectural elements, from sensing and networking layers through to cloud-based processing, that allow the scale of interconnection now seen across consumer, industrial, and civic contexts [2].

While these capabilities provide genuine convenience and efficiency, they also introduce cybersecurity risks that users and organizations must understand. Many connected devices are not designed or maintained with strong security as a priority: weak or default passwords, outdated software, insecure communication methods, and poorly configured settings are common [3]. Where such weaknesses exist, an attacker may gain unauthorized access to a device and use it to steal information or monitor activity [4]. The scale of the problem compounds the difficulty: a traditional computer network may involve a limited number of major systems requiring protection, whereas an organization with hundreds or thousands of connected sensors, cameras, and machines must protect many independent endpoints, each with its own software, hardware, and configuration profile.

Connected devices also raise privacy concerns distinct from conventional network security. Many such devices continuously collect information about their users and surroundings, smart cameras capture images, wearables record physical activity, and location-enabled devices track movement, and mishandling of this information can expose individuals to serious privacy harm [5]. Beyond individual devices, a compromised connected device can also serve as a building block in larger attacks: an attacker who gains control of a vulnerable device may use it as a network entry point or combine many compromised devices into a botnet capable of attacking third-party systems, meaning that the security posture of a single device can have consequences well beyond that device itself [6]. These risks are especially serious in critical environments, healthcare facilities, factories, transportation systems, energy infrastructure, financial institutions, and government bodies, where a successful attack could cause financial loss, interrupt essential services, damage equipment, expose sensitive information, or create genuine safety concerns [7].

Connected devices are not, however, inherently insecure. Appropriate security practices, strong and unique passwords, multi-factor authentication, encryption, timely software updates, network segmentation, secure configuration, continuous monitoring, and responsible data management, can substantially reduce these risks, and manufacturers bear an important share of responsibility for building security into products from the design stage onward [7][10]. This paper reviews the cybersecurity risks facing connected devices and explains why these risks are of growing importance: it examines common vulnerabilities, the major categories of cyberattack that exploit them, the privacy and real-world consequences of compromise, the practical challenges facing organizations and individual users, and the layered methods available for protecting connected devices. As dependence on connected technology deepens, cybersecurity can no longer be treated as a concern limited to computers and traditional networks; every connected device is properly understood as part of the wider security environment that individuals, organizations, and critical services now depend on.

2 METHODOLOGY

This paper is a narrative literature review rather than an empirical study. It synthesizes foundational peer-reviewed literature on the Internet of Things together with established technical guidance from recognized standards and regulatory bodies, selected to jointly represent both the architectural and conceptual basis of connected-device technology and the practical security guidance developed for it. Sources were drawn from four categories: foundational IoT architecture and vision literature [1,2,8–10], peer-reviewed security, privacy, and trust research specific to IoT environments [11,12], baseline security guidance issued by cybersecurity standards and regulatory bodies [13,14], and manufacturer-facing cybersecurity capability guidance issued by a national standards agency [15,16]. Sources were selected for relevance to connected-device security risk, threat typology, privacy consequence, and mitigation practice, and were synthesized thematically into the structure presented in Section 3, moving from device and ecosystem context, through risk and threat categories, to real-world consequence and mitigation practice.

3 RESULTS AND DISCUSSION

3.1 Understanding Connected Devices and Their Role in Modern Life

Connected devices have become a normal part of modern life. A connected device is a physical object capable of communicating with another device, network, or online service through technologies such as Wi-Fi, Bluetooth, cellular networks, or other communication systems, collecting information via sensors, processing it internally, and exchanging data with other systems largely without constant human control [8,9]. The smartphone remains the most familiar example, connecting continuously to applications, cloud services, and other devices, and collecting location,

communication, and usage information in the process. Smart home devices, televisions, speakers, thermostats, lighting, locks, and cameras, extend this same pattern into the domestic environment, typically with remote control through a mobile application. Healthcare has adopted connected technology for patient monitoring and wearable health tracking, industry uses connected sensors to monitor machinery and production processes, connected vehicles communicate with navigation services and infrastructure, and agriculture increasingly relies on sensor networks to monitor soil and environmental conditions.

Taken together, these devices form an expansive digital ecosystem in which devices communicate directly with one another, through routers and gateways, or via cloud platforms, an interconnected structure that enables rapid information flow but also means a weakness in one device can create risk for others connected to it [17]. A further defining characteristic of this ecosystem is continuous operation: many connected devices remain active on networks for extended periods, sometimes constantly, which gives a compromised device a persistent window of opportunity for malicious use, particularly where the device is rarely monitored or updated.

3.2 Major Cybersecurity Risks in Connected Devices

The rapid growth in connected devices has created a correspondingly larger digital environment requiring protection, and security research on IoT environments commonly identifies device-level weaknesses, poor configuration, and inadequate maintenance as significant sources of risk [11]. Weak or default passwords remain a foundational risk: many devices ship with simple, well-known default credentials, giving attackers an easy path to unauthorized access [18]. Outdated software and firmware compound this problem, as vulnerabilities discovered after a device's release require manufacturer patches that may never be installed, particularly on older devices no longer receiving security support. Insecure network communication, exchanging information without adequate protection, exposes data to interception, while poor security configuration provides attackers with additional avenues into a device [19].

Malware infection is another major risk: attackers can target vulnerable devices with malicious software designed to seize control of device operations [20]. Data exposure is a related concern, since connected devices often collect personal, confidential, or commercially valuable information that becomes vulnerable once a device is compromised. Weak device management compounds all of the above: organizations that deploy large numbers of connected devices without maintaining an accurate inventory may be unaware which devices require updates or monitoring, leaving gaps that recognized baseline-security guidance specifically identifies as a priority risk area for IoT deployments [7]. Physical access represents a final major risk category, since many connected devices, unlike servers housed in protected data centers, are more exposed to unauthorized physical contact, and interconnection itself creates a chain of risk in which a single vulnerable device can serve as an entry point into a larger, otherwise well-protected network [19]. Emerging evidence also points to hidden software supply-chain dependencies as an increasingly systemic source of risk, sometimes bypassing traditional perimeter defenses entirely [22].

3.3 Common Cyberattacks Against Connected Devices

Connected devices are exposed to many of the same categories of attack that affect conventional computers and networks, but their specific characteristics, limited processing power, weak built-in security controls, and long operational lifetimes, create additional opportunities for attackers [8]. Credential-based attacks remain among the most common: attackers attempt access using stolen, guessed, or default credentials, a risk magnified by password reuse across services and by the ease of automating credential-guessing attempts against internet-accessible devices. Malware represents a related and equally prevalent threat, capable of altering device behavior, granting remote control, or spreading rapidly where multiple devices share the same vulnerable software configuration. Increasingly, generative artificial intelligence is also being used by attackers to develop adaptive malware and to automate vulnerability discovery, extending the sophistication of these threats beyond earlier, more static attack patterns [23].

Botnets constitute one of the more consequential outcomes of unsecured IoT deployments: a botnet is a collection of compromised devices controlled by an attacker, and IoT devices are attractive botnet material precisely because they are numerous and frequently remain connected around the clock [12,13]. Botnets are commonly used to conduct Distributed Denial-of-Service (DDoS) attacks [4], in which large numbers of compromised devices generate traffic against a target, degrading or eliminating service availability; strong device-level security remains an important defense against a device becoming part of such a network in the first place. Man-in-the-Middle (MitM) attacks, in which an attacker intercepts or manipulates communication between two systems, exploit inadequately encrypted or authenticated device communication, while spoofing attacks involve an attacker impersonating a legitimate device or service to systems that do not properly verify identity. Phishing and social engineering extend these technical threats into the human layer, deceiving users into revealing credentials or installing malicious applications, while direct exploitation of unpatched software vulnerabilities, physical tampering with accessible devices, and ransomware or data-extortion techniques against connected environments round out the major attack categories connected-device operators must anticipate.

3.4 Privacy, Data Protection, and Real-World Consequences

The cybersecurity risks associated with connected devices extend well beyond financial or technical loss into personal privacy, business confidentiality, and physical safety. Because many connected devices continuously collect and transmit information, a security failure can expose data revealing substantial detail about individuals and organizations [14]. Personal privacy is a primary concern: smartphones record location, smart speakers process voice commands, fitness trackers log activity, and security cameras capture images of people and their surroundings, and the risk compounds when data from multiple devices is combined to construct a detailed picture of an individual's behavior and routine. Business data faces parallel exposure, since organizations increasingly use connected sensors and equipment to monitor production, inventory, and operations, information that carries real competitive and reputational value if accessed by an attacker. Healthcare privacy is particularly sensitive given the nature of information collected by connected medical devices and wearables, and identity theft risk grows as connected devices accumulate personal detail useful to attackers conducting further attacks.

Beyond privacy, the consequences of connected-device compromise are frequently financial, organizations may bear costs for incident investigation, system recovery, legal support, and customer notification, and can extend to physical safety where compromised devices control or monitor physical environments such as industrial machinery, connected vehicles, medical equipment, or building management systems. A further consequence is erosion of trust: a major security incident involving connected devices can damage an organization's reputation well beyond the immediate technical incident [21]. These risks underscore the importance of proactive data protection practice, collecting information only when necessary, protecting it throughout its lifecycle via encryption and access control, and maintaining clear policies for storage, sharing, and deletion, alongside individual user responsibility for understanding what data a device collects and adjusting privacy settings accordingly.

3.5 Security Challenges for Organizations and Users

Protecting connected devices is not the responsibility of any single actor; manufacturers, organizations, employees, and individual users all contribute to the security of connected systems, and the difficulty of this shared task is compounded by the sheer diversity of devices in design, purpose, software, age, and security capability. Device visibility is a foundational organizational challenge: an organization cannot protect devices it does not know exist, and smaller connected devices, sensors, cameras, printers, and smart appliances, are frequently overlooked relative to formally inventoried computers and servers, a gap that manufacturer-facing cybersecurity guidance identifies as a priority for organizations to close through systematic device identification and lifecycle management [15]. Device diversity compounds this problem, since products from many manufacturers bring different operating systems, interfaces, and update procedures, complicating efforts to apply consistent security policy across an environment.

Software update management presents further difficulty, since applying updates can interrupt operations or require specialized procedures , and some older devices may not support updates at all, requiring organizations to plan for eventual replacement. Weak authentication practices, reused or unchanged default credentials, remain common at both individual and organizational scale , while network complexity, connected devices routinely communicating with cloud services, mobile applications, and internal systems, creates room for attackers to move laterally where networks are not properly segmented. Resource constraints are a practical barrier for many organizations: effective connected-device security requires hardware, software, monitoring tools, and trained personnel that smaller organizations may not have in sufficient supply, requiring risk-based prioritization of protective effort [3]. For individual users, limited cybersecurity awareness remains a persistent problem, users may prioritize convenience over security responsibility, and vendor dependence adds a further layer of risk, since a manufacturer that discontinues support leaves users with devices that will accumulate unpatched vulnerabilities over time . Effective privacy management and continuous monitoring, adapting security practice as devices, users, and threats change over time, round out the challenges organizations and users alike must sustain rather than solve once.

3.6 Methods for Protecting Connected Devices

Protecting connected devices requires a combination of technical controls, responsible user behavior, and effective organizational policy; no single measure eliminates every threat, and a strong strategy therefore layers multiple protections so that the failure of one control does not compromise the whole system [16]. Strong, unique passwords, changed immediately from manufacturer defaults, together with multi-factor authentication where available, remain among the simplest and most effective measures [4]. Regular software and firmware updates address vulnerabilities as they are discovered, and devices that no longer receive security updates should be assessed for replacement [21]. Encryption protects information in transit between devices, applications, and servers, while network segmentation limits an attacker's ability to move from a compromised device toward more sensitive systems [21]. More recent guidance frames network segmentation as one component of a broader Zero Trust Architecture, which assumes no device or user is inherently trustworthy and requires continuous verification rather than relying on perimeter defense alone [24].

Accurate device inventory management allows administrators to know what devices exist, where they are located, and how they communicate, directly addressing the device-visibility challenge described in Section 3.5 and reflecting the asset-management practices that manufacturer-facing IoT security guidance recommends as a baseline capability [15,16]. Access control following the principle of least privilege, ensuring devices and users receive only the permissions their function requires, further limits the potential impact of any single compromise [21]. Continuous monitoring of network traffic, device activity, and authentication events can surface anomalous behavior before it escalates, and physical protection, locked cabinets, restricted areas, and tamper detection, remains relevant precisely because physical access can bypass digital controls entirely. Regular security assessment, vulnerability scanning, penetration testing, and configuration review, helps identify weaknesses proactively, and cybersecurity awareness training ensures that the human element of a security strategy is as prepared as its technical controls. A Software Bill of Materials (SBOM), an inventory of the software components and dependencies within a device, is an emerging complement to device-level inventory management, helping organizations identify hidden or outdated components within their connected-device software supply chain [25].

4 CONCLUSION

Connected devices have become an important part of modern society, extending from smartphones and smart home appliances to medical equipment, industrial machinery, vehicles, and agricultural sensors, and providing genuine value by allowing physical objects to collect, process, and exchange information. This growth has, however, introduced cybersecurity challenges that extend well beyond any single device: weak or default credentials, outdated software, insecure communication, poor configuration, malware, inadequate device management, and unauthorized physical access all expose connected devices to compromise, and a single vulnerable device can provide an entry point into far larger, otherwise well-protected systems. The major attack categories reviewed here, credential attacks, malware, botnets, distributed denial-of-service attacks, man-in-the-middle attacks, spoofing, social engineering, software exploitation, and physical tampering, demonstrate that connected devices require protection at multiple levels simultaneously , and the consequences of compromise extend from technical disruption into privacy violation, financial loss, reputational damage, and, in some contexts, physical safety.

Securing connected devices is ultimately a shared responsibility: manufacturers must build security into products and sustain update support, organizations must maintain accurate inventories and monitor their environments, and individual users must adopt basic protective practices. The layered methods reviewed here, strong authentication, encryption, network segmentation, access control, continuous monitoring, physical protection, and cybersecurity awareness, are most effective when implemented together rather than in isolation. As connected technology continues to expand alongside developments such as artificial intelligence, edge computing, and advanced wireless networks, cybersecurity must remain a fundamental part of the design, deployment, and ongoing use of every connected device, not a consideration addressed only after an incident occurs.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The authors used JenniAI, an AI-assisted tool during the initial literature synthesis and drafting of this manuscript. The authors independently reviewed, verified, revised, and substantially rewrote the resulting material and assumed full responsibility for the accuracy, originality, interpretation, and conclusions presented in the final manuscript.

Disclosure of conflict of interest

The authors declare no financial or non-financial conflict of interest related to this research.

REFERENCES

[1] Atzori L, Iera A, Morabito G. The Internet of Things: a survey. Computer Networks. 2010;54(15):2787-2805.

[2] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Generation Computer Systems. 2013;29(7):1645-1660.

[3] International Telecommunication Union. Overview of the Internet of Things. Recommendation ITU-T Y.2060. Geneva: International Telecommunication Union; 2012.

[4] Rose K, Eldridge S, Chapin L. The Internet of Things: an overview. Reston (VA): Internet Society; 2015.

[5] Borgia E. The Internet of Things vision: key features, applications and open issues. Computer Communications. 2014;54:1-31.

[6] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Computer Networks. 2015;76:146-164.

[7] European Union Agency for Cybersecurity (ENISA). Baseline security recommendations for IoT in the context of critical information infrastructures. Athens: ENISA; 2020.

[8] Whitmore A, Agarwal A, Da Silva LM. The Internet of Things—a survey of topics and trends. Information Systems Frontiers. 2015;17:261-274.

[9] Federal Trade Commission. Internet of Things: privacy & security in a connected world. Washington (DC): Federal Trade Commission; 2015.

[10] National Institute of Standards and Technology. Foundational cybersecurity activities for IoT device manufacturers (NISTIR 8259). Washington (DC): U.S. Department of Commerce; 2020.

[11] National Institute of Standards and Technology. IoT device cybersecurity capability core baseline (NISTIR 8259A). Washington (DC): U.S. Department of Commerce; 2020.

[12] Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. arXiv preprint. 2019. arXiv:1910.13312(cited in §1 on weak/default credentials; also §3.5 on resource-constrained devices)

[13] Makhdoom I, Abolhasan M, Lipman J, et al. Anatomy of Threats to the Internet of Things. IEEE Communications Surveys & Tutorials. 2018. https://doi.org/10.1109/comst.2018.2874978(cited in §1 and §3.3 on unauthorized access, data theft, botnets/DDoS)

[14] Lu Y, Papagiannidis S, Alamanos E. Internet of Things: A systematic review of the business literature from the user and organisational perspectives. Technological Forecasting and Social Change. 2018. https://doi.org/10.1016/j.techfore.2018.01.022 (cited in §1 on privacy harm from continuous data collection)

[15] Hussain F, Abbas SG, Fayyaz UU, et al. Towards a Universal Features Set for IoT Botnet Attacks Detection. IEEE INMIC. 2020. https://doi.org/10.1109/inmic50486.2020.9318106 (cited in §1 on compromised devices as botnet building blocks)

[16] Francis EG, Sheeja S, Antony John EF, et al. IoT and Smart Device Security. In: IoT and Smart Device Security. 2025. https://doi.org/10.1002/9781394268917.ch10 (cited in §1 on manufacturer responsibility for secure design)

[17] Al-Garadi MA, Mohamed A, Al-Ali A, et al. A Survey of Machine and Deep Learning Methods for Internet of Things Security. 2022. http://hdl.handle.net/10576/30089 (cited in §3.1 on interconnected devices creating cascading risk)

[18] Jaafar AG, Ismail SA, Habir A, et al. A Raise of Security Concern in IoT Devices: Measuring IoT Security Through Penetration Testing Framework. IJACSA. 2024. https://doi.org/10.14569/ijacsa.2024.0150568(cited in §3.2 on weak/default credentials)

[19] Sunanda N, Shailaja K, Kandukuri P, et al. Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection. IJACSA. 2024. https://doi.org/10.14569/ijacsa.2024.0150497 (cited in §3.2 on insecure communication and poor configuration)

[20] El-Sofany HF, Abou El-Seoud S, Karam OH, et al. Using machine learning algorithms to enhance IoT system security. Scientific Reports. 2024. https://doi.org/10.1038/s41598-024-62861-y (cited in §3.2 on malware and continuously running devices)

[21] Amoo OO, Osasona F, Atadoga A, et al. Cybersecurity threats in the age of IoT: A review of protective measures. IJSRA. 2024.

[22] Liu C, Tan R, Wu Y, Feng Y, Jin Z, Zhang F, Liu Y, Liu Q. Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity. 2024;7:20. https://doi.org/10.1186/s42400-024-00212-0

[23] Mirakhorli M, Garcia D, Dillon S, Laporte K, Morrison M, Lu H, Koscinski V, Enoch C. A Landscape Study of Open Source and Proprietary Tools for Software Bill of Materials (SBOM). arXiv preprint arXiv:2402.11151. 2024.

[24] Radanliev P, De Roure D, Maple C, Nurse JRC, Nicolescu R, Ani U. AI security and cyber risk in IoT systems. Frontiers in Big Data. 2024;7:1402745. https://doi.org/10.3389/fdata.2024.1402745

[25] Alwahedi F, Aldhaheri A, Ferrag MA, Battah A, Tihanyi N. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems. 2024;4:167-185. https://doi.org/10.1016/j.iotcps.2023.12.003