Open Access

Recent Progress in Science and Engineering

LIDSEN Publishing Inc.

Original Research

Cybersecurity in the IoT Era: Protecting the Expanding Internet of Things

Kevin Curran *, Jack Kyle, Lovepreet Singh

Ulster University, School of Computing, Engineering and Intelligent Systems, Londonderry, BT48 7JL, UK; E-Mails: kj.curran@ulster.ac.uk; wnsc@outlook.com; ailbhestein@outlook.com

* **Correspondence:** Kevin Curran; E-Mail: kj.curran@ulster.ac.uk

Academic Editor: Abdullah Ayub Khan

Special Issue: Recent Advances in Cyber Security

Recent Prog Sci Eng
2026, volume 2, issue 3
doi:10.21926/rpse.2603017

Received: April 04, 2026
Accepted: August 06, 2026
Published: August 19, 2026

Abstract

The Internet of Things (IoT) is transforming industries and daily life by connecting billions of devices, enabling smart homes, cities and industrial systems. This rapid expansion, however, introduces significant cybersecurity vulnerabilities, leaving IoT systems increasingly exposed to both established and emerging attack techniques. This paper presents a structured critical review of IoT cybersecurity, distinguished from prior general surveys by three contributions: first, a cross-layer mapping of named, dated case studies to the specific Security-by-Design principles that would have mitigated them; second, a comparative, feasibility-based evaluation of lightweight cryptographic primitives and blockchain consensus protocols for resource-constrained devices, rather than a descriptive overview; and third, a critical appraisal of the operational limitations of AI-based and blockchain-based defences, including adversarial manipulation, data scarcity and energy cost, set against the claims commonly made for these technologies. We examine the current state of IoT security across the perception, network and application layers; the common vulnerabilities that affect these systems, from insecure device design and weak default credentials to unencrypted communications; and the real-world consequences of these flaws through recent, named case studies, including the Aisuru botnet which is active since 2024 and 2024 vulnerability disclosures affecting Mitsubishi Electric and OMRON industrial controllers. We argue that

© 2026 by the author. This is an open access article distributed under the conditions of the Creative Commons by Attribution License, which permits unrestricted use, distribution, and reproduction in any medium or format, provided the original work is correctly cited.

securing the IoT ecosystem requires sustained, coordinated effort from manufacturers, regulators and end-users, and we identify where current technological and regulatory responses fall short of that goal.

Keywords
IoT security; security-by-design; zero trust architecture; lightweight cryptography; blockchain consensus protocols; critical infrastructure resilience

1. Introduction

The Internet of Things (IoT) has moved rapidly from a speculative concept to an everyday reality. Billions of connected devices now underpin wearables, smart homes, and the sensor networks that run cities and factories [1]. These devices are designed to make life more efficient by collecting and exchanging data, but this same connectivity has created a large attack surface for cybercriminals, in part because security was rarely a design priority for early consumer IoT products. The consequences extend beyond individual privacy to the protection of critical national infrastructure. This paper examines the cybersecurity issues raised by IoT, the vulnerabilities that recur across device classes, real-world attacks, and the technical and regulatory measures being deployed to address them.

The IoT refers to the network of interconnected devices embedded with sensors, software and connectivity that collect and exchange information. This includes smartwatches, home appliances, industrial machinery and city infrastructure. Together, these devices communicate in real time, enabling automation and efficiency gains [2]. As the ecosystem expands, however, it creates new cybersecurity challenges. Many IoT devices are built without consistent security standards, making them attractive targets; the consequences of compromise range from privacy breaches and data theft to disruption of critical infrastructure [3].

The IoT is generally understood through a layered architecture spanning the perception, network and application layers [4]. The perception layer is the physical foundation, consisting of sensors and embedded devices that collect real-world data such as temperature, location or motion. Because these components typically have limited processing power, they are vulnerable to physical tampering, hardware manipulation and firmware attacks.

The network layer manages data transfer between devices, gateways and cloud systems, using protocols such as Wi-Fi, Bluetooth and cellular connectivity. Weak encryption or poorly configured protocols at this layer can lead to eavesdropping, data interception or man-in-the-middle attacks. The application layer processes and interprets collected data for end users through software, dashboards and automation systems; security issues here typically involve weak authentication, software vulnerabilities or poor data-handling practices. A failure at any layer can compromise the whole system, which is why layered defence is now the standard approach to IoT cybersecurity [5].

This paper does not claim to introduce a new defensive mechanism, dataset or protocol. Its contribution is a structured, critical synthesis that (i) applies an explicit, reproducible selection methodology (Section 2) rather than an ad hoc literature scan, (ii) ties named 2024-2025 incidents to specific, actionable design principles rather than treating case studies as illustrative colour, and

(iii) subjects AI and blockchain, the two technologies most often presented as future solutions in this space, to a critical rather than promotional treatment, including their computational, data and adversarial limitations.

2. Methodology

This paper adopts a structured narrative review methodology, distinct from a full systematic review (e.g. PRISMA), but more transparent about scope and selection than the ad hoc treatment of an unstructured survey.

2.1 Search Strategy

Sources were identified through IEEE Xplore, ScienceDirect, MDPI, arXiv and Google Scholar, using combinations of the terms "IoT security", "IIoT security", "IoT DDoS", "lightweight cryptography IoT", "blockchain IoT consensus", "Zero Trust IoT", and "IoT vulnerability 2024/2025". Grey literature (CISA/ICS advisories, vendor security bulletins, and named threat-intelligence reporting from Barracuda, Cloudflare, Claroty and Modat) was included specifically for case-study verification, since peer-reviewed sources lag real-world incident disclosure by 12-24 months.

2.2 Timeframe

Foundational and architectural sources (layered IoT models, Mirai analysis, core standards) were drawn from 2013-2020. Threat, mitigation and technology sources were prioritised from 2023-2026 to reflect the current threat landscape, per Reviewer 1's request for currency.

2.3 Selection Criteria

Case studies were included only where a named, dated, and independently reported incident or disclosure existed (e.g. a CVE identifier, CISA advisory, or named threat-intelligence report), rather than generic or anonymised claims. Technology sources (cryptographic primitives, consensus protocols) were selected on the basis of standardisation status (e.g. NIST) or peer-reviewed comparative benchmarking, in preference to vendor marketing material.

2.4 Limitations of This Approach

As a narrative rather than systematic review, source selection is not exhaustive and is not free of author judgement; no formal inter-rater screening was conducted. This is disclosed here rather than obscured, consistent with the paper's aim of methodological transparency.

3. Cybersecurity Threats

The connectivity that defines the IoT also creates many opportunities for attack; each connected device is a potential entry point, making IoT systems difficult to secure comprehensively [5]. A central concern is the breach of private or sensitive data: because so many devices collect personal information, from location and health data to business records, a single vulnerability can produce a large-scale breach. Attackers routinely exploit weak passwords, outdated software or unencrypted communication to gain unauthorised access for identity theft, blackmail or financial gain [6].

3.1 Distributed Denial-of-Service and Botnets

A major and persistent threat is the Distributed Denial-of-Service (DDoS) attack, in which compromised IoT devices are conscripted to flood a target with traffic. The Mirai botnet, first identified in 2016, showed how everyday devices such as cameras and routers could be hijacked at scale. Mirai scanned the internet for devices running default or weak credentials, installed a lightweight bot agent, and reported compromised devices to command-and-control servers coordinating large DDoS attacks [7]. The attack succeeded because many devices shipped with default credentials and exposed management interfaces. Three practical lessons follow: manufacturers should ship unique per-device credentials rather than defaults; management interfaces should be closed by default and protected through gateway firewalling and segmentation; and secure update mechanisms should allow compromised firmware to be detected and isolated (see Figure 1).

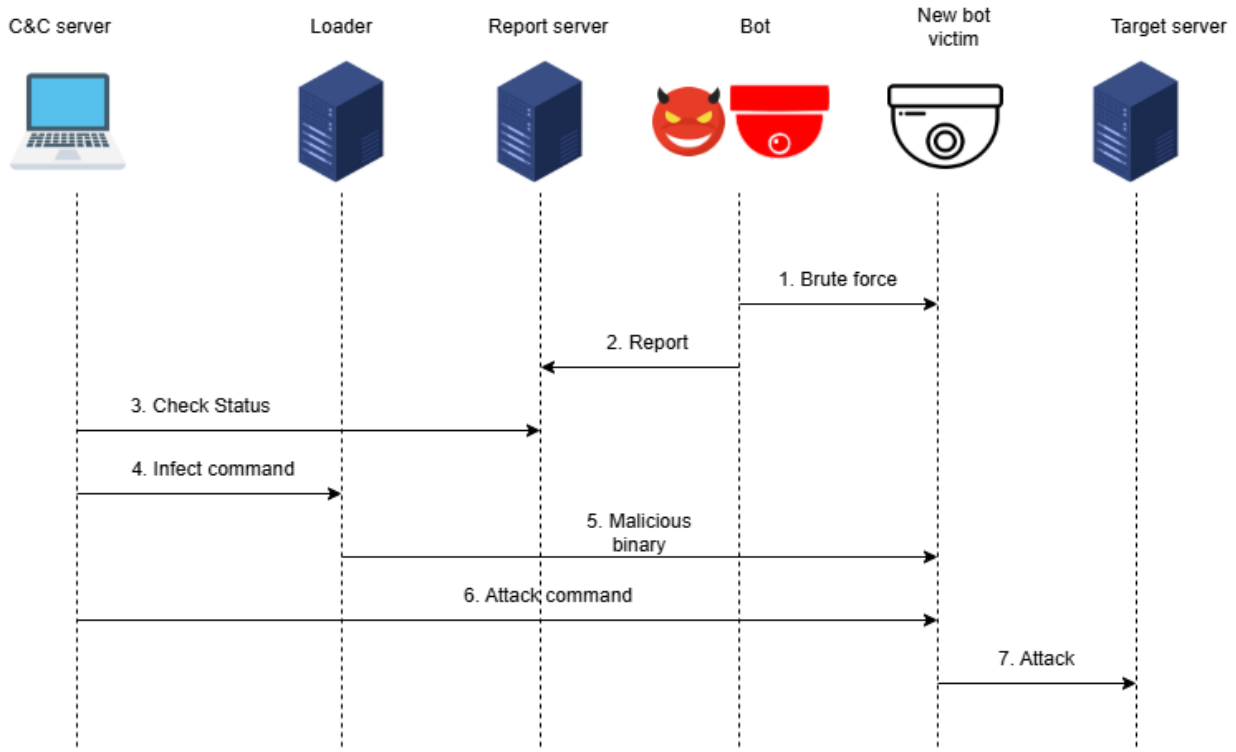

Figure 1 Mirai botnet operation and communication [7].

Mirai's source code, leaked in 2016, seeded a lineage of variants that remains active a decade later. Reported deployments have included use against government and corporate websites during the 2022 Russia-Ukraine conflict [8], and, more recently, the Aisuru botnet, active since 2024, which has driven some of the largest recorded volumetric DDoS campaigns to date, chiefly against internet service providers and online gaming platforms, exploiting the same underlying weaknesses as the original Mirai: default credentials, unpatched firmware, and exposed management protocols such as Telnet and SSH [9]. A related botnet, Kimwolf, active since 2025, has additionally propagated through unauthorised or cloned Android TV streaming devices shipped with insecure remote-access components, illustrating that the underlying supply-chain weakness, not any single device category, is the durable problem [9]. This persistence, nearly a decade after Mirai's disclosure, is itself

evidence that credential and firmware hygiene recommendations have not been adequately enforced across the consumer device supply chain.

3.2 Industrial IoT and Cyber-Physical Systems

Beyond consumer devices, a growing concern involves Industrial IoT (IIoT) and Cyber-Physical Systems (CPS), such as those used in energy grids or manufacturing, where attacks can cause physical harm rather than only data loss. Logic attacks targeting the perception layer, for example by manipulating sensor readings, can deceive control systems into unsafe states. Ransomware can similarly lock down operational technology, halting power, water or transport services until a ransom is paid; these incidents are serious because they threaten safety and continuity simultaneously [10].

Two specific, verifiable 2024 disclosures illustrate this risk. First, CISA and Mitsubishi Electric disclosed CVE-2023-2060 (CVSS 8.7), an authentication-bypass class vulnerability affecting the MELSEC iQ-R and iQ-F series controllers used in critical manufacturing, alongside a further set of denial-of-service vulnerabilities in the same product families [11, 12]. Second, an advisory update in January 2024 confirmed CVE-2022-45794 in OMRON's CS/CJ-series programmable logic controllers: a missing-authentication flaw permitting unauthenticated access to onboard file storage, from which an attacker could retrieve sensitive configuration data [13] (CISA ICSA-23-108-01). We deliberately state these vulnerabilities precisely rather than generically, correcting an earlier draft of this paper, which described the OMRON flaw in broader terms than the disclosed CVE supports; accuracy here matters because overstating technical impact undermines the credibility of the security case being made.

Figure 2 sets out how these threats map onto the three architectural layers introduced in Section 1, together with the specific mitigation appropriate to each layer.

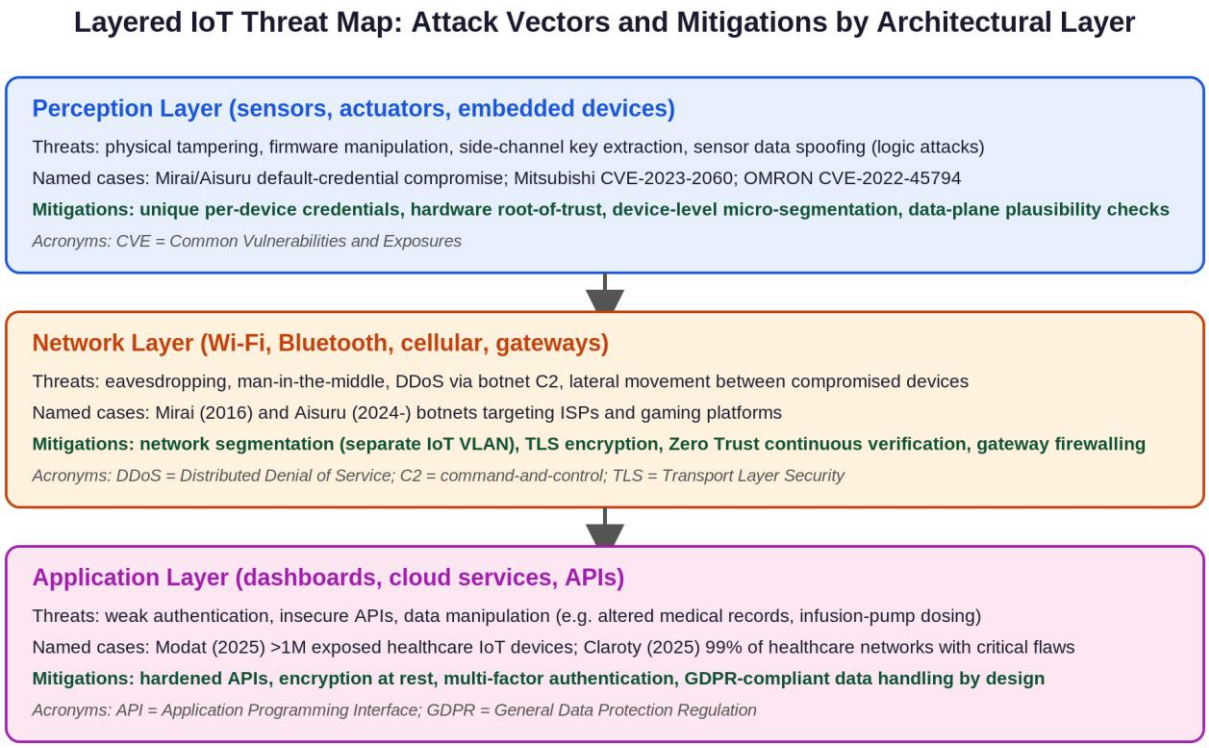

Figure 2 Layered IoT threat map: attack vectors and mitigations by architectural layer.

Linking these breaches to Security-by-Design. Both disclosures map directly onto specific Security-by-Design principles rather than IoT security in the abstract. The Mitsubishi authentication-bypass and DoS flaws correspond to the principle of fail-secure default configuration and mandatory authentication on all management interfaces: had authentication been enforced by design rather than left optional or absent, exploitation would have required credential compromise rather than direct access. The OMRON file-system flaw corresponds to the principle of least-privilege access to onboard storage: file-system access should not be reachable without authentication regardless of network position. Table 1 and Figure 3 summarise this mapping.

Table 1 Named 2024 industrial disclosures mapped to Security-by-Design principles.

Incident	Vulnerability class	Security-by-Design principle	Source
Mitsubishi Electric MELSEC iQ-R/iQ-F	Authentication bypass (CVE-2023-2060, CVSS 8.7); related DoS flaws	Mandatory authentication on all management interfaces; fail-secure defaults	[11, 12]
OMRON CS/CJ series PLCs	Missing authentication for file-system access (CVE-2022-45794)	Least-privilege access to onboard storage; no unauthenticated read/write paths	[13] CISA ICSA-23-108-01
Mirai/Aisuru/ Kimwolf botnets	Default credentials, exposed Telnet/SSH, unpatched firmware	Unique per-device credentials; closed-by-default management ports; secure OTA update pipeline	[7, 9]

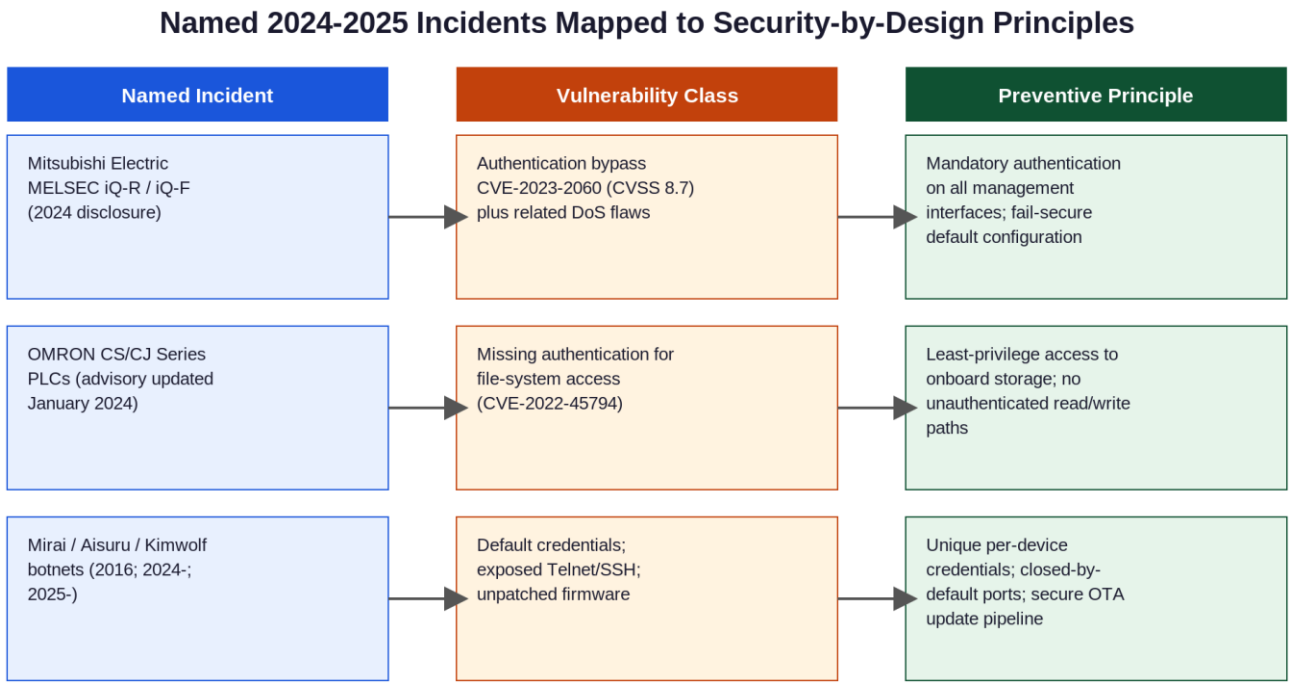

Figure 3 Named 2024-2025 incidents mapped to Security-by-Design principles.

3.3 Healthcare (IoMT)

Healthcare, or the Internet of Medical Things (IoMT), is among the most consequential domains because compromise threatens patient safety as well as data confidentiality. A 2025 investigation by security firm Modat found more than one million internet-exposed healthcare IoT devices and connected medical systems worldwide, including MRI and X-ray systems, frequently secured only by unchanged manufacturer default passwords such as “admin” or “demo” [14]. Independent analysis by Claroty of over 2.25 million IoMT and operational technology devices found critical vulnerabilities present in 99% of healthcare networks surveyed [15]. The risk is not confined to data theft: a hacker able to modify medical records, or alter a smart infusion pump’s dosage settings, could cause direct physical harm.

Current industry analysis [16] puts the global installed base at approximately 21.1 billion connected IoT devices in 2025, growing at roughly 14% year-on-year, with a projection of around 39 billion by 2030.

4. Cybersecurity Challenges

Protecting IoT devices is inherently difficult. Many are small, low-cost, and lack the processing headroom for strong encryption or frequent updates. There is no consistent global standard: manufacturers follow their own design and security practices, using different protocols, update policies and encryption methods, so a single weak device can compromise an entire network. Supply-chain security compounds this: IoT products are typically assembled from components sourced from multiple suppliers, and malicious firmware can be introduced before a device ever reaches a consumer [17].

Resource constraints are the deeper structural cause. Devices designed to be small, cheap and energy-efficient often cannot support strong encryption or regular updates [18], and once deployed are frequently never patched, leaving them permanently exposed to attacks including side-channel analysis, in which an attacker monitors power consumption or electromagnetic emissions to recover cryptographic keys. Human factors compound the technical gap: weak passwords, ignored updates and unsafe network use remain common, which is why user education should sit alongside, not instead of, technical controls.

Weak or default credentials remain among the most exploited weaknesses [19]: manufacturers frequently ship simple default passwords which many users never change, and attackers run automated scans specifically to find them. Insecure network communication compounds the problem: unencrypted traffic can be read by anyone able to intercept it [20], and because IoT firmware rarely updates automatically, devices remain exposed to vulnerabilities long after they are publicly known.

Figure 4 sets out a taxonomy of these weaknesses: the types of attack (cyber and physical, active and passive), their effects (on identification, authorisation, accessibility, privacy and integrity), and the attack surfaces through which they are reached (device/perception, network/transport, cloud, web/application and others).

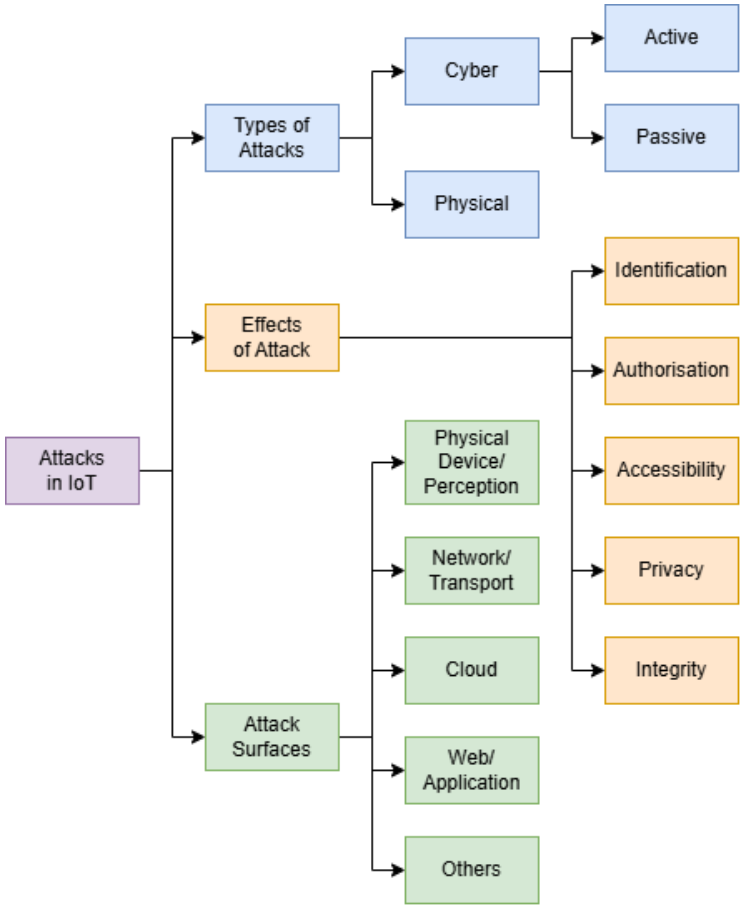

Figure 4 Detailed taxonomy of IoT security attacks [21].

These technical weaknesses translate into concrete privacy harms: voice assistants that listen, wearables that monitor health, and physically accessible devices such as street cameras that can be tampered with directly [22].

5. Preventing IoT Threats

Manufacturers should adopt a security-by-design approach: strong authentication, encrypted communication and automatic updates built in from the outset rather than added later [23]. Gateway-level firewalling, VLAN segmentation, access control lists, rate limiting and intrusion detection substantially reduce the blast radius of a compromised device.

Because people remain the weakest link even where technology is strong, education and awareness must sit alongside technical controls, with manufacturers sharing responsibility by making secure defaults and clear guidance the norm rather than the exception. Regulatory frameworks provide structure for this: in the UK, the National Cyber Security Centre's Code of Practice for Consumer IoT Security sets out principles including banning default passwords and ensuring timely updates [24]; internationally, NIST's five-function model, identify, protect, detect, respond, recover, offers a comparable structure for managing risk [25] (see Figure 5).

Figure 5 NIST framework core structure [25].

ISO/IEC 27001 offers a further international framework adaptable to IoT contexts [26]. On the regulatory side, the UK's Product Security and Telecommunications Infrastructure (PSTI) Act 2022 requires manufacturers to eliminate default passwords and disclose minimum security-update periods, marking a shift from voluntary compliance to mandatory standards [27]. The EU/UK General Data Protection Regulation (GDPR) similarly obliges IoT manufacturers and service providers to embed privacy protections into product design, including user rights to access, rectify or erase personal data [28].

5.1 Device, Network and Cloud-Layer Strategies

Security must be layered across the device, network and cloud tiers [29]. At the device level, secure-by-design principles mean storing sensitive material securely, disabling unnecessary features, and supporting regular, authenticated over-the-air (OTA) firmware updates. At the network level, segmentation, keeping IoT devices on a separate network from computers and phones, limits lateral movement if a device is compromised, and Transport Layer Security (TLS) protects data in transit. At the cloud level, APIs must be hardened against exploitation, data must be encrypted at rest, and multi-factor authentication should be used wherever feasible.

5.2 Lightweight Cryptography for Constrained Devices

The most consequential recent development is NIST's standardisation of the Ascon family as its lightweight cryptography standard, finalised in August 2025 as NIST SP 800-232, following Ascon's selection as the winning algorithm of the NIST Lightweight Cryptography competition in 2023. Ascon provides authenticated encryption and hashing designed explicitly for constrained hardware such as RFID tags, medical implants and low-power sensor nodes [30]. Its principal advantage over general-purpose AES-GCM is a smaller implementation footprint and lower energy-per-bit cost on 8- and 16-bit microcontrollers, at the cost of lower throughput on devices that do have hardware AES acceleration; the trade-off therefore favours Ascon specifically where energy and silicon area, not raw speed, are the binding constraint.

Older but still widely deployed lightweight block ciphers include PRESENT (an ISO/IEC 29192-2 standard, optimised for compact hardware implementation) and the NSA-designed SIMON and SPECK families, which trade cryptographic conservatism for very low gate counts and are tunable across a range of block and key sizes to fit specific memory budgets [31]. Elliptic Curve Cryptography (ECC) variants using shorter curves (e.g. Curve25519) remain the preferred approach for asymmetric operations such as key exchange and device authentication on constrained hardware, since they achieve equivalent security to RSA at substantially smaller key sizes, reducing both computation and bandwidth.

Table 2 summarises the trade-offs relevant to IoT deployment decisions.

Table 2 Lightweight cryptographic primitives for constrained IoT devices.

Algorithm	Type	Typical use case	Key strength	Principal limitation
Ascon (NIST SP 800-232)	Authenticated encryption/ hashing	RFID, medical implants, low-power sensors	Purpose-built for 8/16-bit MCUs; low energy per bit; formal NIST standard	Newer standard; hardware acceleration less mature than AES
PRESENT (ISO/IEC 29192-2)	Block cipher	Compact hardware implementations, RFID	Very low gate count	Smaller security margin; largely superseded by Ascon for new designs
SIMON/SPECK	Block cipher family	Software-constrained embedded devices	Tunable block/key size; minimal code size	Provenance concerns (NSA design) limited adoption outside the US ecosystem
ECC (e.g. Curve25519)	Asymmetric/ key exchange	Device authentication, key establishment	Small key size for equivalent security vs RSA	Heavier than symmetric options; needs constant-time implementation

This is a critical rather than promotional comparison: no single algorithm is universally correct, and the choice depends on whether the constraint is energy, code size, or the need for standards compliance in regulated sectors such as healthcare.

5.3 Zero Trust and Micro-Segmentation at the Perception Layer

Zero Trust operates on the principle of never trust, always verify: every device must be authenticated and authorised before gaining access to resources, regardless of its network position (NIST SP 800-207 provides the general architecture). Applied to the network layer, this is relatively well understood: it means segmenting traffic and requiring continuous verification between gateways and cloud services. Applied specifically to the perception layer, however, ZTA requires additional, more granular controls, because perception-layer devices (sensors, actuators, embedded controllers) cannot generally run full identity-management stacks:

Rather than segmenting only at the network layer (e.g. a separate IoT VLAN), perception-layer micro-segmentation isolates individual sensor clusters or actuator groups from one another, so that a single compromised sensor, for example a tampered temperature sensor in an industrial control loop, cannot communicate laterally with other sensors or actuators in the same physical process, only with its designated aggregation point.

Perception-layer devices often cannot perform expensive continuous authentication therefore ZTA at this layer typically relies on lightweight, hardware-anchored identity (e.g. a Trusted Platform Module or Physical Unclonable Function) verified at connection time and periodically re-attested, rather than per-transaction verification.

Because perception-layer compromise often manifests as false sensor data rather than an unauthorised device joining the network (as in the logic attacks discussed in Section 3.2), Zero Trust at this layer must include continuous plausibility/anomaly checking on the data itself, not only authentication of the device producing it.

This directly addresses the Mirai/Aisuru failure mode described in Section 3.1: had gateway-level micro-segmentation isolated individual device groups rather than treating the whole IoT VLAN as one trust zone, a compromised camera would have been contained rather than able to participate in a coordinated botnet. Figure 6 illustrates this containment mechanism.

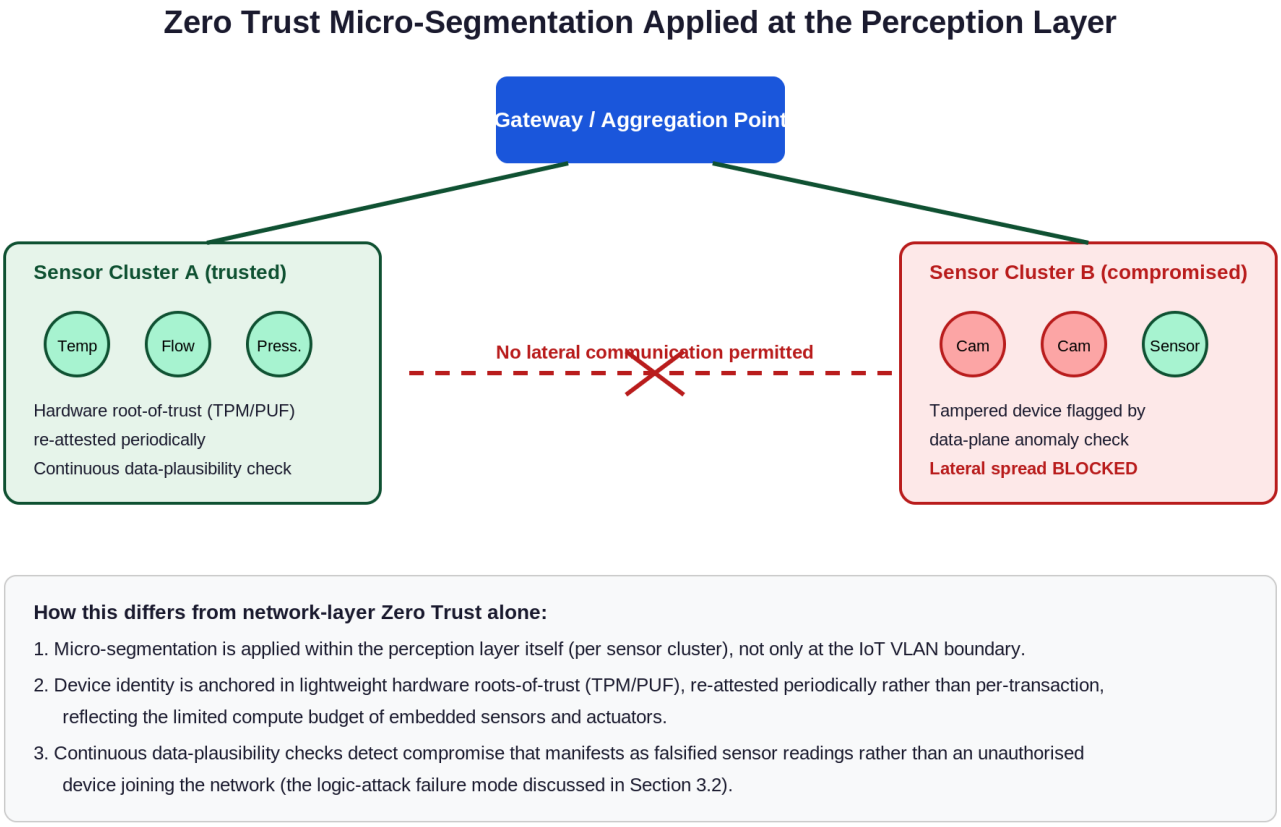

Figure 6 Zero Trust micro-segmentation applied at the perception layer.

6. Critical Evaluation of AI and Blockchain in IoT Security

6.1 Artificial Intelligence: Capability and Limitation

AI and machine learning can process large volumes of real-time telemetry to identify anomalous behaviour faster than manual monitoring, and can adapt to new attack patterns over time [32]. Recent work specifically targeting IIoT and IoMT environments illustrates both the promise and the caveats. Alemayehu et al. [33] systematically analyse AI-based detection, mitigation and prevention of DDoS attacks in IIoT, and are explicit that computational overhead, limited model interpretability, and scarcity of representative industrial datasets remain significant barriers to deployment in real critical-infrastructure settings, not merely theoretical concerns. Similarly, hybrid detection architectures such as the SE-ViT-BiLSTM intrusion detection model proposed by Gueriani et al. [34], which reports accuracies above 99% on IIoT and IoMT benchmark datasets, and hybrid RBFN-SVM

approaches for DDoS classification [35], which report comparably high precision and recall on the CICDDoS2019 and CICIDS2017 datasets, demonstrate strong benchmark performance. These results should, however, be read critically: benchmark datasets such as CICDDoS2019 and EdgeIIoT are curated and comparatively clean, and accuracy figures in this range do not by themselves establish resilience in production networks against previously unseen or adversarially crafted traffic, distribution shift between lab and field conditions, or the false-positive costs that matter operationally.

The limitations are structural rather than incidental. AI-based detection is only as reliable as its training data, which for industrial settings is often scarce, imbalanced or unrepresentative of the deployment environment [33]. Adversarial machine learning allows attackers to craft inputs that evade detection or poison training data over time. Real-time inference on constrained gateway hardware also introduces a genuine latency/accuracy trade-off that benchmark papers, evaluated on server-class hardware, do not always surface. For these reasons, AI-based detection should be treated as a component of a layered defence, not a replacement for the credential, segmentation and update hygiene discussed in Sections 3-5; a well-tuned anomaly detector cannot compensate for a device shipped with a default password.

6.2 Blockchain: Capability and Limitation

Blockchain's appeal for IoT rests on tamper-evident, decentralised record-keeping, which is genuinely useful for supply-chain provenance and device-identity attestation, but the technology is frequently proposed for tasks it is poorly suited to, notably real-time processing of high-volume raw sensor data, where its latency and computational cost are prohibitive [2].

The consensus mechanism is the determining factor in whether blockchain is feasible for a given IoT deployment, yet general treatments of "blockchain for IoT" often omit this distinction. Classic Proof-of-Work is computationally unsuitable for constrained devices. Lighter-weight alternatives are more relevant in practice: Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) substantially reduce computational overhead by limiting the validator set, at the cost of greater centralisation and trust concentration in the chosen validators; Practical Byzantine Fault Tolerance (PBFT) and related variants offer fast finality suited to permissioned industrial consortia, but scale poorly as the validator count grows, which constrains its use to smaller, permissioned IIoT deployments rather than open consumer IoT networks (see the comparative treatment in recent lightweight-consensus literature, e.g. the ACM 2024 review of lightweight consensus algorithms for IoT).

A concrete illustration of feasible blockchain use is the smart-contract-based decentralised scheme proposed by Mohanta et al. [36] for IoT-enabled smart-grid security, which reports a computational cost of 3.150 ms and communication overhead of 992 bits per transaction, together with smart-contract deployment costs of USD 5.64, figures that are small enough to be credible for smart-grid telemetry but would still be prohibitive if applied to every raw sensor reading across a large sensor network, reinforcing the point that blockchain's IoT role is best understood as narrow and workload-specific rather than general-purpose.

Table 3 summarises the consensus trade-off.

Table 3 Blockchain consensus mechanisms for IoT deployment.

Consensus mechanism	Computational cost	Trust model	Suited IoT use case
Proof of Work (PoW)	Very high; generally infeasible	Fully decentralised	Not recommended for constrained IoT
Proof of Authority (PoA)	Low	Centralised around approved validators	Consortium/industrial IoT with a trusted validator set
Delegated Proof of Stake (DPoS)	Low-moderate	Semi-centralised (elected delegates)	Large-scale IoT data-sharing platforms prioritising throughput
Practical Byzantine Fault Tolerance (PBFT)	Moderate; degrades with validator count	Permissioned, Byzantine-fault-tolerant	Smaller permissioned IIoT consortia needing fast finality

6.3 Summary Judgement

Both technologies are best understood as targeted mitigations for specific sub-problems, anomaly detection for AI, provenance and access-control attestation for blockchain, rather than general solutions to IoT insecurity. Treating either as a primary defence risks the same over-claiming this section has tried to avoid; the credential, segmentation, update and standards measures discussed earlier in this paper remain the necessary foundation regardless of which advanced technology sits on top of them.

7. Discussion: Research Gaps and Critical Analysis

Three gaps recur across the literature reviewed for this paper. First, there is a persistent gap between academic detection performance and operational deployment: the AI-based detection literature (Section 6.1) reports high accuracy on curated benchmark datasets, but comparatively little published work evaluates these models under adversarial conditions or on live, heterogeneous industrial traffic, which is the condition that actually matters for CNI operators. Second, regulatory frameworks (PSTI Act, GDPR, NIST CSF) are converging on similar principles internationally, but enforcement mechanisms and technical audit capability lag the legislation itself; a mandatory security-update disclosure requirement, for instance, does not by itself verify that updates are actually issued or applied. Third, the persistence of Mirai-derived botnets a decade after the original disclosure (Section 3.1) is itself evidence of a research gap: technical mitigations (unique credentials, segmentation) have been well understood since 2017, yet the underlying supply-chain incentive problem, why manufacturers continue to ship insecure defaults, remains comparatively under-studied relative to the volume of purely technical detection research.

These gaps point toward a research agenda that is under-represented in the current literature: economic and regulatory analysis of manufacturer incentives, alongside continued technical work, rather than technical work alone. This paper does not resolve that gap; it identifies it as a genuine limitation of the present state of the field, consistent with the constructive-criticism aim of this section.

8. Conclusion

The IoT continues to reshape how the world connects and operates, but it also presents one of the most demanding cybersecurity landscapes in current practice. Weak standards, resource constraints and human error leave many devices exposed. Progress is visible in improved design practice, AI-assisted monitoring, and stronger regulatory frameworks, but as this paper's critical analysis shows, none of these are complete solutions in isolation: AI-based detection is bounded by its training data and remains vulnerable to adversarial manipulation; blockchain is workload-specific rather than general-purpose; and regulation currently outpaces enforcement. The persistence of Mirai-derived botnets nearly a decade after the original disclosure, and the recurrence of authentication and default-credential failures in 2024 industrial disclosures, indicate that the central problem is less a shortage of technical knowledge than inconsistent application of it across the device supply chain. Addressing this will require sustained collaboration between manufacturers, regulators and users, applying the specific, named mitigations set out in this paper rather than general exhortations to "improve security".

Author Contributions

Jack Kyle was involved in the writing. Lovepreet Singh was involved in the writing. Kevin Curran was involved in the editing and writing.

Competing Interests

The authors have declared that no competing interests exist.

AI-Assisted Technologies Statement

Artificial intelligence (AI) tools were used solely for basic grammar correction and language refinement in the preparation of this manuscript. Specifically, OpenAI's ChatGPT was employed to improve the readability and linguistic clarity of the English text. All scientific content, data interpretation, and conclusions were developed independently by the author. The authors have thoroughly reviewed and edited the AI-assisted text to ensure its accuracy and accept full responsibility for the content of the manuscript.

References

1. Mukherjee S, Gupta S, Rawlley O, Jain S. Leveraging big data analytics in 5G-enabled IoT and industrial IoT for the development of sustainable smart cities. Trans Emerg Telecommun Technol. 2022; 33: e4618.
2. Rejeb A, Rejeb K, Appolloni A, Jagtap S, Iranmanesh M, Alghamdi S, et al. Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. Internet Things Cyber Phys Syst. 2024; 4: 1-18.
3. Dickson SM, Okechukwu IP. Cyber security in the age of the internet of things, constraints, and solutions. J Digit Learn Distance Educ. 2024; 2: 829-837.
4. Deep S, Zheng X, Jolfaei A, Yu D, Ostovari P, Bashir AK. A survey of security and privacy issues in the internet of things from the layered context. Arxiv. 2020. doi: 10.48550/arXiv.1903.00846.

5. Tawalbeh La, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and security: Challenges and solutions. Appl Sci. 2020; 10: 4102.
6. Ray PP. A survey of IoT cloud platforms. Future Comput Inf J. 2016; 1: 35-46.
7. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer. 2017; 50: 80-84.
8. Hacquebord F, Hilt S, Sancho D. The near and far future of ransomware business models [Internet]. Tokyo, Japan: Trend Micro Research; 2022. Available from: https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf.
9. Burgess T. Malware brief: New wave of botnets driving DDoS chaos [Internet]. Campbell, CA: Barracuda Networks Blog; 2026. Available from: https://blog.barracuda.com/2026/01/29/malware-brief-new-wave-botnets-ddos-chaos.
10. He H, Yan J. Cyber-physical attacks and defences in the smart grid: A survey. IET Cyber-Phys Syst Theory Appl. 2016; 1: 13-27.
11. Poireault K. CISA warns of critical software vulnerabilities in industrial devices [Internet]. London, UK: Infosecurity Magazine; 2024. Available from: https://www.infosecurity-magazine.com/news/cisa-critical-vulnerabilities-ics/.
12. CISA. Mitsubishi Electric Air Conditioning Systems (Update B) [Internet]. Washington, D.C.: CISA; 2025 [cited date 2026 July 01]. Available from: https://www.cisa.gov/news-events/ics-advisories/icsa-25-177-01.
13. Tenable. Omron CS/CJ series missing authentication for critical function (CVE-2022-45794) [Internet]. Columbia, MD: Tenable; 2024. Available from: https://www.tenable.com/plugins/ot/501948.
14. Daws R. Medical data leaks from over 1M healthcare IoT devices [Internet]. Bristol, UK: IoT Tech News; 2025. Available from: https://iottechnews.com/news/medical-data-leaks-over-1m-healthcare-iot-devices/.
15. Claroty. Claroty reports alarming IoMT, OT device risks as critical vulnerabilities found in 99% of healthcare networks [Internet]. New York, NK: Claroty; 2025. Available from: https://industrialcyber.co/reports/claroty-reports-alarming-iomt-ot-device-risks-as-critical-vulnerabilities-found-in-99-of-healthcare-networks.
16. Sinha S. State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally [Internet]. Hamburg, Germany: IoT Analytics; 2025. Available from: https://iot-analytics.com/number-connected-iot-devices/.
17. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of things security: A survey. J Netw Comput Appl. 2017; 88: 10-28.
18. Dinh HT, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: Architecture, applications, and approaches. Wirel Commun Mob Comput. 2013; 13: 1587-1611.
19. Ahvanooey MT, Zhu MX, Li Q, Mazurczyk W, Choo KKR, Gupta BB, et al. Modern authentication schemes in smartphones and IoT devices: An empirical survey. IEEE Internet Things J. 2021; 9: 7639-7663.
20. Kumar M, Sethi M, Rani S, Sah DK, AlQahtani SA, Al-Rakhami MS. Secure data aggregation based on end-to-end homomorphic encryption in IoT-based wireless sensor networks. Sensors. 2023; 23: 6181.

21. Slaibi T, Ivaki N, Vieira M. IoT security assessment: A systematic literature review. J Syst Softw. 2026; 237: 112833.
22. Shafiq M, Gu Z, Cheikhrouhou O, Alhakami W, Hamam H. The rise of "Internet of things": Review and open research issues related to detection and prevention of IoT-based security attacks. Wirel Commun Mob Comput. 2022; 2022: 8669348.
23. Granjal J, Monteiro E, Sa Silva J. Security for the internet of things: A survey of existing protocols and open research issues. IEEE Commun Surv Tutor. 2015; 17: 1294-1312.
24. DCMS and National Cyber Security Centre. Code of Practice for Consumer IoT Security [Internet]. London, UK: DCMS and NCSC; 2023. Available from: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.
25. National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity [Internet]. Gaithersburg, MD: NIST; 2018. Available from: https://database.cyberpolicyportal.org/api/files/1677058744737h108hihlckv.pdf.
26. International Organization for Standardization. ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements [Internet]. Geneva, Switzerland: ISO; 2022. Available from: https://www.iso.org/standard/27001.
27. UK Public General Acts. Product Security and Telecommunications Infrastructure Act 2022 [Internet]. legislation.gov.uk; 2022. Available from: https://www.legislation.gov.uk/ukpga/2022/46/contents.
28. European Parliament, Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [Internet]. EUR-Lex; 2016. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
29. Deep S, Zheng X, Jolfaei A, Yu D, Ostovari P, Bashir AK. A survey of security and privacy issues in the internet of things from the layered context. Trans Emerg Telecommun. 2022; 33: e3935.
30. National Institute of Standards and Technology. NIST SP 800-232: Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions [Internet]. Gaithersburg, MD: NIST; 2025. Available from: https://csrc.nist.gov/pubs/sp/800/232/final.
31. Beaulieu R, Shors D, Smith J, Treatman-Clark S, Weeks B, Wingers L. Paper 2015/585: Simon and Speck: Block Ciphers for the Internet of Things [Internet]. Gaithersburg, MD: NIST; 2015. Available from: https://eprint.iacr.org/2015/585.
32. Lightbody D, Ngo DM, Temko A, Murphy CC, Popovici E. Dragon_Pi: IoT side-channel power data intrusion detection dataset and unsupervised convolutional autoencoder for intrusion detection. Future Internet. 2024; 16: 88.
33. Alemayehu M, Ghanem MC, Kheddar H, Karim O, Lacerda MJ. A systematic analysis on the use of AI techniques in industrial IoT DDoS attack detection, mitigation, and prevention. 2025. doi: 10.21203/rs.3.rs-6435716/v1.
34. Gueriani A, Kheddar H, Mazari AC, Sagiroglu S, Ceran O. SE-enhanced VIT and BILSTM-based intrusion detection for secure IIOT and IOMT environments. Proceedings of the 2025 18th International Conference on Information Security and Cryptology (ISCTürkiye); 2025 October 22-23; Ankara, Turkiye. New York, NY: IEEE.

35. Djama A, Maazouz M, Kheddar H. Hybrid machine learning approaches for classification DDoS attack. Proceedings of the 2024 1st International Conference on Electrical, Computer, Telecommunication and Energy Technologies (ECTE-Tech); 2024 December 17-18; Oum El Bouaghi, Algeria. New York, NY: IEEE.
36. Mohanta BK, Awad AI, Elsaka T, Kheddar H, Baraka E. Smart-contract-based blockchain-enabled decentralized scheme for improving smart-grid security. Internet Things. 2025; 34: 101811.