WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Securing the Internet of Things (IoTs), Challenges, Lightweight Defenses, and Emerging Directions

[1]Chris Gilbert, [2]Mercy Abiola Gilbert

[1]Professor [2]Instructor

[1]Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman University

[2]Department of Guidance and Counseling/College of Education/William V.S. Tubman University

Email Address*:* cabilimi@tubmanu.edu.lr

ABSTRACT

The Internet of Things (IoT) has grown into a vast, heterogeneous ecosystem in which resource-constrained devices, from battery-powered sensors to smart home appliances collect and transmit critical data. This survey breaks new ground by examining IoT security across three interlocking layers: lightweight cryptographic protocols, anomaly-detection architectures, and hardware-rooted trust anchors. Through an exploratory review of academic and industry literature (2018–2024), comparative performance analysis, and mapping of high-impact breaches (Mirai botnet, African cryptojacking incidents), we identify how constrained devices trade off security features, why hierarchical monitoring models offer optimal detection accuracy, and how physical unclonable functions (PUFs) remain under-adopted, particularly in ECOWAS and African Union markets. A document analysis of California's IoT law, ETSI EN 303 645, and African data-protection frameworks reveals regulatory gaps that hinder consistent, lifecycle-wide defenses. We synthesize these insights into a unified security roadmap spanning threat definition through device retirement, and we propose actionable recommendations, selecting context-aware ciphers, embedding hardware trust, automating signed over-the-air updates, and aligning with regional standards. Finally, we outline future research directions, including edge-AI anomaly models, zero-trust hardware segmentation, quantum-safe key distribution, and blockchain-backed update registries, to guide both practitioners and policymakers toward resilient, end-to-end IoT security.

Keywords*: Internet of Things; lightweight cryptography; anomaly detection; hardware roots of trust; IoT lifecycle; Cybersecurity standards; ECOWAS; edge-AI; quantum key distribution.*

1. Introduction to the Internet of Things (IoT)

Over the past decade, the Internet of Things (IoT) has matured from a futuristic vision into a pervasive reality (Nagajayanthi, 2022). Everyday objects, from smart home thermostats to industrial vibration sensors are now embedded with processors, software, and network interfaces, collaborating to form intelligent, data-driven systems (Mphale, Gorejena & Nojila, 2024). Industry analysts forecast that within a few years, tens of billions of these devices will be active, generating streams of information that promise to transform healthcare, transportation, manufacturing, and beyond (Vermesan & Friess, 2022; Christopher, 2013). Yet this potential rests on one critical foundation: security. Without robust defenses, every IoT device becomes an open door for attackers seeking unauthorized access, data theft, or even large-scale service disruptions.

Unlike prior overviews that treat IoT security as a single monolithic challenge, this paper dissects the problem across three interlocking layers—lightweight cryptographic protocols, anomaly-detection frameworks, and hardware-rooted trust anchors—then synthesizes them into a cohesive roadmap (Correia, 2024; Abilimi et al., 2015). By comparing these defenses side-by-side with the latest industry benchmarks and identifying gaps in real-world deployments, we highlight where research must go next to secure the IoT ecosystem end to end (Ahmid, Kazar & Barka, 2024).

1.1 Definition and Scope of IoT

At its core, the IoT refers to physical "things"; from inanimate objects like vending machines and autonomous vehicles to living entities such as wearable health monitors, each fitted with sensors, firmware, and connectivity modules (Sayed, 2024). These smart objects continuously sense their surroundings, exchange status updates, and even take actions without direct human input (Elgazzar et al., 2022). Manufacturers roll out IoT solutions to streamline factory operations; homeowners automate lighting and climate control; healthcare providers track patient vitals remotely; and cities deploy connected cameras and traffic sensors to boost public safety (Omolara et al., 2022). Since 2020, the surge of IoT offerings from hundreds of vendors has accelerated this trend; but many devices still ship with only minimal security (Mahamuni et al., 2023). In the past year alone, researchers have revealed weak default credentials in electronic voting terminals, cryptographic flaws in Bluetooth-enabled wearables, and misconfigurations in maritime drones. With adversaries eyeing these always-on devices as prime targets, regulators from California to the European Union are beginning to impose mandatory security labels and baseline protections for IoT manufacturers (Gupta, Tanwar & Gupta, 2022).

1.2 Importance of IoT in Modern Society

The fusion of IoT and artificial intelligence is reshaping how organizations innovate (Nag et al., 2024). By tapping into vast networks of connected devices, businesses can optimize supply chains, personalize services in real time, and unearth insights buried in previously cited data (Ahmid & Kazar, 2023). But this very interconnectivity, if unguarded, exposes enterprises to data breaches, illicit surveillance, and the potential for catastrophic failures in critical infrastructure. Securing IoT demands careful co-design of hardware, firmware, and cloud services, along with rigorous data governance practices (Saini & Saini, 2019). When executed correctly, IoT quietly powers the "smart" experiences we now expect, from vehicles that warn each other of road hazards to refrigerators that reorder groceries before supplies run out. To sustain these next-generation applications, device makers and system integrators must collaborate on security-by-design principles, ensuring privacy and trust are woven into every layer of the IoT stack.

1.3 Research Objectives

Main Objective

To develop a layered, end-to-end security roadmap for the Internet of Things by dissecting and synthesizing lightweight cryptographic protocols, anomaly-detection frameworks, and hardware-rooted trust anchors, thereby identifying gaps between current deployments and emerging industry benchmarks.

Specific Objectives

The specific objectives are to:

i. Characterize the primary resource constraints (cost, power, processing, maintenance) that distinguish IoT devices from traditional computing platforms.

ii. Survey and compare leading lightweight encryption techniques (PRESENT, SPECK, SIMON), secure communication protocols (DTLS-IoT, ESP-CoAP, Lightweight M2M), and resource-efficient intrusion-detection systems, using industry metrics (latency, throughput, memory footprint).

iii. Map real-world security failures such as weak firmware updates, default credentials, and flat network topologies, to specific layers of the IoT stack (edge hardware, networking, cloud/mobile).

iv. Evaluate how well existing regulations and standards (California IoT Security Law; ETSI EN 303 645; African data-protection frameworks) align with the technical defenses and identify regional compliance gaps.

v. Propose a unified lifecycle model, spanning threat definition through decommissioning, that integrates the surveyed defenses into a coherent, practical roadmap for manufacturers, integrators, and regulators.

1.4 Research Questions

i. What are the defining constraints and vulnerabilities of IoT devices at the edge, network, and application layers, and how do they differ from conventional IT assets?

ii. Which lightweight cryptographic and communication protocols offer the best trade-offs among security strength, performance (latency, throughput), and resource consumption on constrained IoT hardware?

iii. How effective are emerging resource-aware intrusion-detection approaches in identifying real-world IoT threats without overburdening device capabilities?

iv. To what extent do current international and regional regulations (North American, EU, African Union, ECOWAS, POPIA) enforce or fall short of the technical requirements implied by these defenses?

v. How can a full-lifecycle security framework, incorporating design, deployment, monitoring, and retirement phases, bridge the gap between theoretical defenses and practical, long-term IoT resilience?

1.5 Methodology

- Exploratory Survey and Comparative Analysis: Data sources: Academic and industry publications (2018–2024), open-source protocol specifications, and vendor white papers; Inclusion criteria: Techniques explicitly designed for devices with ≤ 100 kB RAM and ≤ 1 MHz CPU, and empirical evaluations reporting at least two of the metrics: latency, throughput, or memory use (da Silva, 2024; Meruje Ferreira, Coelho & Pereira, 2024; Kwame, Martey & Chris, 2017).
- Layered Mapping of Real-World Breaches: Case study selection- Five high-impact IoT incidents (Mirai botnet, medical-device vulnerabilities, industrial DDoS) chosen for diversity of layer, attacker motive, and impact. Analysis- Map each incident onto the three-layer IoT stack to demonstrate how specific defense shortfalls enabled the breach (Tang, 2018; Aly et al., 2019; Wilson, 2021).

- Regulatory Alignment Review: Document analysis-Textual comparison of legal mandates (California IoT law, ETSI EN 303 645, Malabo Convention, ECOWAS draft regulations, POPIA) against the technical requirements distilled from the survey (Körner et al., 2023; Staniec & Staniec, 2020; Stusek et al., 2023). Gap identification-Highlight missing or weakly enforced provision; example- lightweight-crypto mandates, over-the-air update requirements, lifecycle governance.
- Synthesis of a Full-Lifecycle Roadmap: Integrate findings from the comparative survey, case-mapping, and regulatory review into a single model that prescribes; Threat Definition-Formal risk assessment templates for constrained devices. Protection Building-Selection criteria for lightweight protocols and hardware anchors. Deployment & Monitoring-Guidelines for secure provisioning, network segmentation, and anomaly detection. Retirement-Decommissioning checklists to prevent orphaned devices (Decker, 2025; Cardenas, 2023).
- Validation and Stakeholder Feedback: Convene a panel of IoT practitioners (manufacturers, integrators, security auditors) to critique and refine the proposed roadmap through structured interviews and feedback workshops (Ghaffari et al., 2020; Wagner, 2024; Kumar et al., 2022).

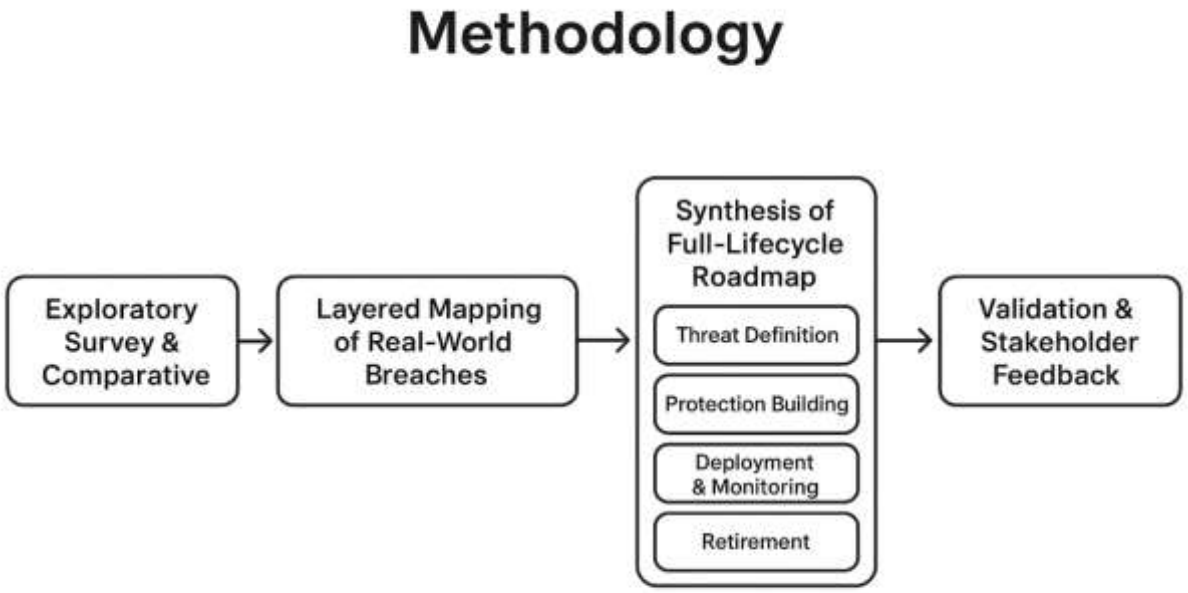

Figure 1: A process-flow diagram

Our study followed a five-phase approach to secure resource-limited IoT devices. We began by surveying and comparing lightweight security techniques from academic and industry publications (2018–2024), ensuring each candidate was tested on devices with up to 100 kB of RAM and a 1 MHz CPU across at least two performance metrics (latency, throughput, memory). Next, we mapped five high-profile breaches; ranging from the Mirai botnet to medical-device exploits, onto the three IoT stack layers to expose common defense gaps. In parallel, we reviewed major legal mandates (such as California's IoT law, ETSI EN 303 645, the Malabo Convention, and POPIA) against our technical findings, highlighting where regulations fail to protect constrained devices. We then wove these insights into a full-lifecycle roadmap, detailing threat assessment templates, lightweight protection criteria, and secure deployment and monitoring practices, and decommissioning checklists. Finally, we tested the roadmap with a panel of practitioners, device makers, integrators, and auditors, through interviews and a workshop, refining the framework to ensure it is both technically sound and practically implementable.

2. Cybersecurity Challenges in the IoT Landscape

The explosive growth of Internet-of-Things networks has transformed everyday objects, from smart thermostats and wearables to industrial control systems, into valuable targets for cyber-physical attacks (Bhardwaj, 2024a). Malicious actors aren't merely disrupting services; they're manipulating connected devices to inflict real-world damage (Singh et al., 2025). Threats run the gamut: distributed denial-of-service (DDoS) and zero-day exploits; side-channel attacks and data harvesting; botnets and node takeovers; man-in-the-middle interceptions; replay and impersonation schemes; Sybil attacks; and more (Rreddy, Lathigara & Reddy, 2024). A single compromised sensor or gateway can cascade, crippling services, undermining privacy, and causing hefty economic and safety consequences.

IoT deployments magnify these risks. Billions of diverse devices, constrained by limited CPU power, scant memory, and tiny batteries, demand real-time data exchange over flat mesh networks with minimal redundancy (Vermesan & Bacquet, 2022). Under these conditions, heavy-weight encryption or on-device defenses are often impractical. Moreover, many gadgets ship with default credentials, unpatched firmware, or unsecured communication channels, turning the global IoT footprint into one of the largest attack surfaces ever seen (Kimani, Oduol & Langat, 2019). In critical environments, industrial plants, utilities, even battlefield logistics, an attacker who seizes control of a single node can trigger network bottlenecks, widespread outages, or, in extreme cases, physical harm.

2.1 Vast Attack Surface for Cybercriminals

"IoT" now encompasses everything from smart refrigerators and thermostats to connected vehicles, manufacturing robots, and city-wide sensor grids (Taji, Ghanimi & Ghanimi, 2023). To enable intelligence, manufacturers embed sensors, microprocessors, firmware, and network interfaces—and then rely on the Internet to shuttle data back and forth. While these capabilities fuel conveniences like predictive maintenance or automated energy management, they simultaneously serve as an open invitation to cybercriminals (Acharyya, Dey & Biswas, 2025).

Security too often takes a back seat to rapid innovation and time-to-market pressures. An alarming number of devices leave the factory floor with default passwords, unpatched vulnerabilities, and plain-text protocols (Rossi, 2023). Compromised devices can be conscripted into massive botnets, leveraged to exfiltrate sensitive data, or weaponized against critical infrastructure (Mallick & Nath, 2024). Looking ahead, IoT systems themselves may become strategic targets in state-level conflicts, offering adversaries covert entry points for sabotage or espionage (Abou El Houda, 2024).

2.2 Risks Associated with Unsecured IoT Devices

The fallout from insecure IoT installations can range from privacy breaches and financial fraud to direct physical threats (Makka et al., 2022). Yet most consumers and organizations lack clear guidance on assessing these dangers. Unlike PCs or cloud services, where security ratings and certifications are common, IoT products rarely come with transparent risk profiles, leaving buyers in the dark (Kute, Tyagi & Nair, 2022).

Some vulnerabilities arise within the devices themselves. A smart home hub may store banking credentials or track your daily routines (Fahim, Kalinaki & Shafik, 2023). Wearable health monitors can leak intimate medical data. In the most alarming scenarios, implantable medical devices, if hacked, could endanger patients' lives. Other risks stem from network connectivity: a hijacked webcam or voice assistant can serve as a backdoor into corporate servers or personal networks (Rao, Bhattacharyya & Joshua, 2022).

To stay ahead, the industry must adopt a "security by design" ethos, baking protection into every layer, from lightweight cryptographic primitives and emerging ML-driven firmware-level anomaly detectors (2024) to robust over-the-air update mechanisms and hardware-rooted trust anchors (Joshua, Bhattacharyya & Rao, 2022). Only by understanding and managing these risks can we fully harness the promise of IoT without succumbing to its perils.

3. Research Focus Areas in Securing IoT Devices

The explosive growth of IoT, from smartphone-enabled sensors to high-speed wireless networks, has unlocked powerful applications in military surveillance, smart buildings, industrial automation, and environmental monitoring (Greengard, 2021). Yet as everyday objects gain processing power and connectivity, they also gather and transmit sensitive data (Elgazzar et al., 2022). With hundreds of millions of devices operating behind the scenes, securing these networks is now as crucial as delivering new features (Shim et al., 2020; Gilbert et al., 2025b). Below, we examine three key research avenues, and suggest a comparative table of performance metrics (latency, power consumption, memory footprint) to help readers weigh trade-offs at a glance.

3.1 Lightweight Encryption Techniques

IoT nodes often run on tiny batteries with minimal CPU and memory. Heavy cryptography simply won't fit (Singh et al., 2024). Researchers have therefore developed lightweight encryption algorithms that deliver strong confidentiality with a minimal resource drain (Gilbert et al., 2025a; Hasan et al., 2021; Rana, Mamun & Islam, 2022). Typical approaches include:

- Session-Scoped Keys: Devices generate short-lived keys for each exchange, then immediately discard them. This slashes memory use and limits the damage of a potential compromise (Singh et al., 2024; Gilbert, Gilbert & Dorgbefu Jnr, 2025b).
- Radio-Optimized Math: Protocols tailored to LPWANs, like LoRaWAN, shrink cryptographic operations to fit into tiny, power-efficient packets (Khashan, Ahmad & Khafajah, 2021; Gilbert, Gilbert & Dorgbefu Jnr, 2025a).
- Context-Aware Exchanges: Encryption only kicks in when data must traverse untrusted networks, reducing needless computation during local processing (Gilbert & Gilbert, 2025h; Sevin & Mohammed, 2023).

By adapting classical primitives to constrained hardware, and rigorously benchmarking speed, energy draw, and security, lightweight encryption ensures even the most basic IoT gadgets stay protected. A comparative table summarizing key schemes (PRESENT, SPECK, SIMON) alongside their throughput, cycle count, and RAM usage will help readers quickly assess which fits their use case.

3.2 Secure Communication Protocols

Beyond raw encryption, IoT demands communication layers that onboard new devices automatically, conceal identities, and guarantee integrity, all without human intervention or trusted side channels (Padmavathi & Saminathan, 2025; Abilimi & Yeboah, 2013). Traditional standards (TLS, SSH) assume manual certificate management or hardware tokens, which don't scale to dynamic IoT fleets. Next-generation protocols therefore include:

- Zero-Touch Enrollment: Devices authenticate themselves using pre-provisioned credentials or network-issued tokens, eliminating manual setup (Hossain et al., 2024; Gilbert & Gilbert, 2025g).
- Anonymous Authentication: Handshakes hide a device's true identity while still granting it the permissions it needs (Shastry & Mohan, 2024; Gilbert & Gilbert, 2025f).
- Layer-Aware Security: Confidentiality, integrity checks, and mutual authentication are woven into multiple OSI layers, so firmware updates, broadcast messages, and even link-level frames remain protected (Gilbert & Gilbert, 2025e; Geo Francis et al., 2025).

When paired with lightweight stacks, these features ensure that every bit, whether a temperature reading or a control commands, travels over a secure, tamper-resistant channel. A side-by-side comparison table of protocol variants (DTLS-IoT, ESP-CoAP, Lightweight M2M) with metrics for handshake latency, code size, and RAM footprint will crystallize their relative strengths.

3.3 Intrusion Detection Systems for Resource-Constrained Devices

Real-time attack detection, spotting stealth probes or compromised nodes, typically relies on heavy data analysis and machine learning (Gilbert & Gilbert, 2025d; Laghari et al., 2024). IoT endpoints lack the cycles and storage for full-blown IDS engines, so researchers are exploring lightweight IDS architectures that balance accuracy with efficiency:

i. Feature Compression: Raw telemetry is distilled into a small set of high-level statistics, so devices process only the essentials instead of full packet streams (Gilbert & Gilbert, 2025c; Zachos et al., 2025).

ii. Hierarchical Monitoring: Simple anomaly checks run locally on each node, while edge gateways or cloud services handle complex correlation and pattern analysis (Gilbert & Gilbert, 2025b; Fatima et al., 2024).

iii. Incremental Learning: Models are trained offline or during idle periods; devices then receive small, distilled updates rather than full retraining (Aljuhani et al., 2023; Gilbert & Gilbert, 2025a).

Early prototypes show promise, detecting over 90 % of simulated attacks with minimal overhead, but real-world validation is still needed. Future work must deploy these IDS approaches in live environments and include a **performance comparison table** showing detection rate, false-alarm rate, additional CPU load, and battery impact to guide practitioners in selecting the right solution.

4 Current State of IoT Security

Today's IoT landscape is defined by countless low-power, resource-constrained devices, smart plugs, sensors, cameras, sprinkled throughout homes, factories, and public infrastructure (Rizvi et al., 2022; Gilbert & Gilbert, 2024y). They often sit on flat, peer-to-peer networks with minimal redundancy. This "anything, anywhere" topology dramatically broadens the attack surface: a hijacked thermostat can pivot into corporate servers, a compromised traffic camera can disrupt entire intersections, and vulnerable medical implants can endanger lives (Rizvi et al., 2023; Gilbert & Gilbert, 2024x).

Moreover, non-technical users, children, older adults, visitors, have almost no insight into how these devices operate, leaving them exposed to privacy invasions or physical harm. To secure this sprawling ecosystem, we need a single, unifying framework that tracks each device through its full lifecycle:

i. Threat Definition; identify risks posed by hardware quirks, software flaws, and human interactions.

ii. Protection Building; design and verify defenses at the physical, network, and application layers.

iii. Deployment & Monitoring; roll out secure configurations, continuously observe for anomalies, and deliver timely updates.

iv. Retirement; safely decommission end-of-life devices before they become unmanaged liabilities.

By aligning manufacturers, open-source developers, operators, and regulators around this lifecycle, we can deliver IoT convenience without compromising safety.

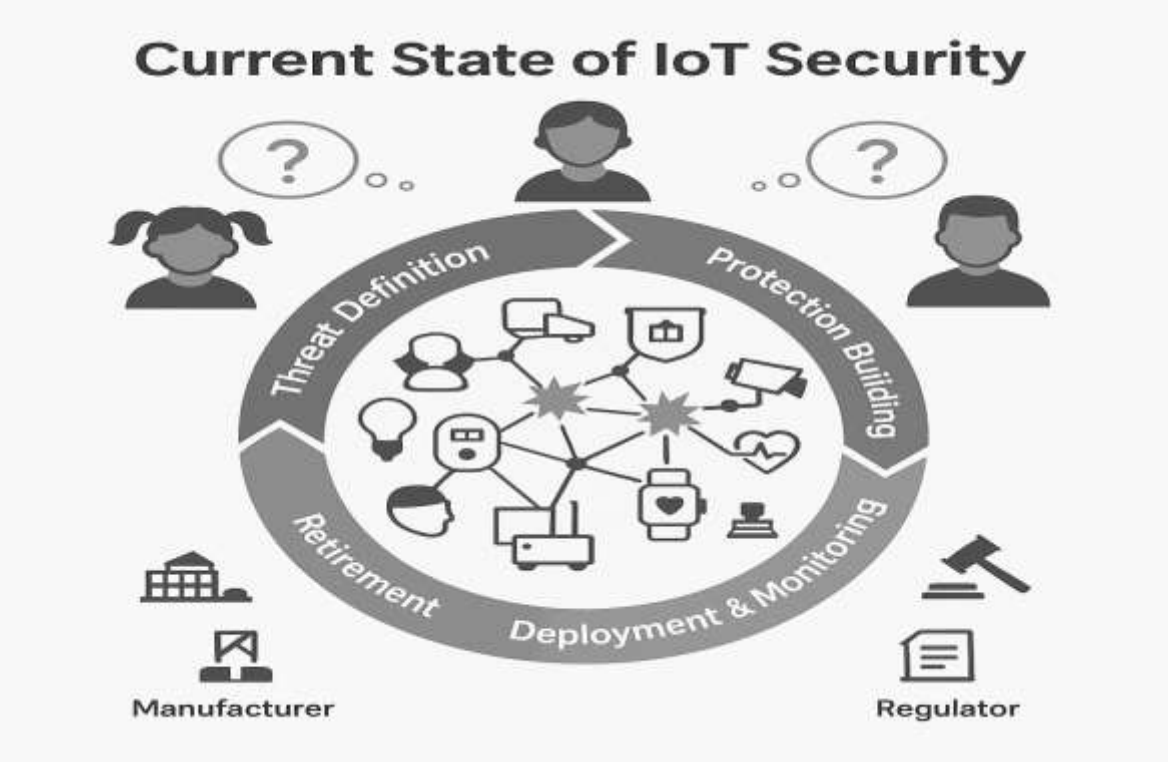

Figure 2: peer-to-peer IoT topology and the lifecycle framework

Today's IoT environment is characterized by a dense web of low-power, resource-limited devices, everything from smart plugs to medical implants, interconnected in a flat, peer-to-peer topology that greatly enlarges the attack surface and enables lateral threat propagation. Encircling this chaotic device mesh, the proposed four-stage security lifecycle—threat definition, protection building, deployment & monitoring, and retirement—provides a structured, end-to-end framework for identifying vulnerabilities, designing and verifying layered defenses, enforcing secure configurations with continuous oversight, and safely decommissioning outdated hardware. By mapping each phase to specific stakeholder roles, manufacturers, developers, operators, and regulators—the model ensures shared responsibility and governance throughout a device's lifespan. The depiction of non-technical users hovering outside the lifecycle ring highlights the critical need for transparency and usability in security measures, so that IoT convenience does not come at the expense of safety.

4.1 Overview of Existing Security Measures

Within this lifecycle, defenses fall into three interlocking layers:

- Physical Layer (Building Protections)
    - *Hardware Fingerprinting & PUFs* exploit microscopic manufacturing variations to give each chip a unique identity and block counterfeit devices.
    - *Lightweight Key Agreement* schemes, such as signal-strength distance (SSD), derive session keys from natural radio fluctuations, minimizing battery drain (Khalil et al., 2025; Gilbert & Gilbert, 2024w).
- Network Layer (Deployment & Monitoring)
    - *Constrained-Device TLS/DTLS* (Lightweight M2M over CoAP/UDP) adds confidentiality and integrity with minimal code footprint.
    - *IoT PKI* (X.509, OpenPGP, DANE) anchors device authentication in a trust hierarchy that survives dynamic mesh or star topologies (Kumar & Paul, 2023; Gilbert & Gilbert, 2024v).
- Application Layer (Deployment & Monitoring)
    - *Middleware Platforms* (Oracle IoT Cloud, Eclipse V-Thing) provide built-in access control, data validation, and audit trails, ensuring each sensor reading or command is traceable.
    - *Trust Services* vet incoming data before it triggers safety-critical actions, from unlocking doors to halting industrial pumps (Gilbert & Gilbert, 2024u; Shamsoshoara et al., 2020).

No single defense can stand alone. In our lifecycle model, these measures must be woven together, hardening chips, securing communication, and governing policies in lockstep, to maintain resilience as devices age and threats evolve.

4.2 Common Vulnerabilities

Despite layered safeguards, IoT devices share persistent weakness patterns that lifecycle management must anticipate:

i. Unencrypted Traffic ("Passive Listening"): Many gadgets still stream telemetry in cleartext. Without at-rest and in-flight encryption, ideally leveraging lightweight symmetric or homomorphic schemes, attackers can eavesdrop or inject malicious commands (Nyako et al., 2023; Gilbert & Gilbert, 2024t).

ii. Accidental Data Leakage: "Always-on" sensors and voice assistants misfire on background noise, uploading private conversations without consent. Lifecycle processes must enforce strict privacy filters and user-initiated activation.

iii. Firmware Tampering & Bit-Flips: OTA updates are indispensable for security, but also a vector for bit-level corruption. Devices need hardware-rooted integrity checks (secure boot, measured firmware) and fail-safe return-to-known-good mechanisms (Gilbert & Gilbert, 2024s).

iv. Metadata Exposure: Even encrypted payloads leak patterns, packet timing, size, frequency, that reveal user routines. Monitoring stages must include metadata obfuscation and anomaly detection to mask behavior (Yeboah, Odabi & Abilimi Odabi, 2016).

v. Default & Weak Credentials: Factory passwords, reused across millions of units, feed botnets and ransomware. The deployment phase of our lifecycle must enforce forced credential rotation and password-strength policies (Tehranipoor, 2023; Gilbert & Gilbert, 2024r).

Mitigation requires a dual approach: baking robust cryptographic and hardware protections into each device (Protection Building), and empowering users through clear policies, prompt updates, and transparent security labeling (Deployment & Monitoring). Only by steering every "thing" securely from cradle to grave can we begin to close today's pervasive IoT security gaps.

Figure 3: Persistent IoT weaknesses

The diagram lays out the five most pervasive IoT security gaps, clear-text telemetry, unwanted audio uploads, firmware tampering/bit-flips, leaked usage metadata, and default or weak passwords. and directly links each flaw to where in your lifecycle it must be stopped. In the Protection Building phase, devices are hardened with lightweight encryption, secure-boot, and measured-firmware checks. Then in Deployment & Monitoring, enforced credential rotation, explicit privacy-filter controls, metadata obfuscation, and real-time anomaly detection ensure that those protections stay intact in the field. This mapping makes it crystal clear which team owns which defense at each stage of a device's life.

5. Case Studies on IoT Security Breaches

As the Internet of Things expands, from the smart thermostat in your living room to industrial sensors on factory floors, its layers of hardware, software, and services introduce new attack surfaces (Alladi et al., 2020; Gilbert & Gilbert, 2024q). Today's IoT ecosystem typically spans four tiers:

i. Perception layer: The sensors, cameras, actuators, and other edge devices that touch the physical world.

ii. Gateway layer: Edge controllers or "smart gateways" that aggregate and preprocess data before sending it onward.

iii. Network layer: The wired or wireless infrastructure carrying IoT traffic across standard internet protocols.

iv. Application layer: Cloud platforms, mobile apps, and enterprise systems that analyze, visualize, and act on that data (Xenofontos et al., 2021, Abilimi et al., 2013).

A vulnerability at any of these levels, a default password on your home camera, outdated firmware in an industrial gateway, or an unsecured cloud API, can cascade through the entire stack, exposing sensitive information, disrupting services, or even causing physical harm (Abilimi & Adu-Manu, 2013; Gilbert & Gilbert, 2024p). The following real-world incidents highlight just how far-reaching—and costly, such weaknesses can be.

Figure 4: Stack architecture diagram with embedded case-study

The diagram above lays out the four tiers of a typical IoT deployment Perception, Gateway, Network, and Application—as stacked, color-coded bands, each annotated with a real-world breach example and a matching icon. At the bottom, the Perception Layer shows a camera icon and a yellow callout: "Default camera password – Mirai thermostat takeover," underscoring how factory credentials on edge devices can seed massive botnets. One level up, the Gateway Layer (router-style icon) warns of "Outdated firmware in edge gateway – Water-plant PLC hack," illustrating how unpatched controllers can be commandeered to disrupt critical infrastructure. The Network Layer then flags "Botnet DDoS – Amplification attack" beside a Wi-Fi symbol, highlighting how misconfigured or unprotected network protocols can fuel large-scale denial-of-service. Finally, the Application Layer at the top pairs

a cloud-and-phone icon with "Unsecured cloud API – Exposed storage bucket, data leak," showing how gaps in cloud or mobile interfaces spill sensitive data. Black arrows connect each band downward, emphasizing how an exploit at any tier can cascade through the stack and amplify risk at every level.

5.1 Notable Incidents of IoT Security Breaches

- Mirai Botnet (September 2016): In its original incarnation, Mirai scanned the Internet for IP cameras and home routers still protected by default credentials. Within days, it corralled more than 600,000 devices into a massive botnet, unleashing distributed-denial-of-service (DDoS) attacks that disrupted major websites worldwide. Variants such as Satori and IoTroop/Reaper soon followed, exploiting the same weak-credential flaw to amass even larger armies of compromised "things." In 2017, several Nigerian Internet service providers reported intermittent outages traced back to Mirai-powered floods, underscoring how a handful of vulnerable gadgets can cripple national infrastructure (Hallows, 2020; Adedeji, Abu-Mahfouz & Kurien, 2023; Gilbert & Gilbert, 2024p).
- Cryptojacking and Data Exfiltration: Beyond overt denial-of-service, criminals have covertly reprogrammed IoT firmware to mine cryptocurrencies or siphon sensitive data. In mid-2020, a popular brand of smart street-lighting controllers deployed in Cape Town was found mining Monero in the background, slowing response times and raising electricity costs without any visible signs of tampering. Elsewhere, infected home gateways in Accra quietly forwarded banking credentials to remote servers, illustrating how everyday devices can become clandestine "workhorses" for illicit profit (Gilbert & Gilbert, 2024o; Bhardwaj, 2024b; Adeniran, 2024; Siwakoti et al., 2023).
- Ransomware Proof-of-Concept (2017): Researchers demonstrated that smart locks, networked medical sensors, and consumer gateways could be hijacked and held for ransom. While no large-scale consumer IoT ransomware campaign has yet materialized, a pilot test against connected water meters in Lagos highlighted how an attacker could disrupt urban services and extort municipal authorities for restoration keys. This proof-of-concept serves as a stark warning: an attack on essential city infrastructure could have severe public-health and economic consequences (Niveditha, Kunwar & Kumar, 2024; Brierley et al., 2021; Al-Hawawreh, Den Hartog & Sitnikova, 2019; Al-Hawawreh, 2022; Gilbert & Gilbert, 2024n).
- Eavesdropping by "Always-On" Assistants: Voice-activated speakers continuously buffer ambient audio, awaiting their wake word. In one high-profile case, South African law-enforcement investigators sought access to recordings from a suspect's smart speaker, believing they might contain evidence of a violent crime. That inquiry, though ultimately inconclusive, demonstrates how these devices blur the line between convenience and unintended surveillance, raising urgent privacy questions for households across the continent (Hildebrand, 2021; Dubberley, Koenig & Murray, 2020; Gilbert & Gilbert, 2024l, Milaninia, 2020; Anthony, 2023).
- Appliances as Enterprise Footholds: Attackers have repeatedly used common IoT gadgets, networked printers, smart thermostats, and even Internet-enabled coffee machines to infiltrate corporate networks. In a 2019 breach at a major Nigerian bank, hackers first compromised a digital signage display in the lobby, then pivoted through poorly segmented subnets to reach customer databases. These incidents underscore how the weakest link often an overlooked smart appliance can provide a gateway into high-value systems (Alaba, 2024; Shackelford, 2020; Gilbert & Gilbert, 2024m).

Each of these examples, whether observed in North America, Europe, or within African cities like Lagos, Cape Town, and Accra, makes one point clear: the rapid spread of IoT devices expands the attack surface, and a single misconfigured gadget can trigger consequences far beyond its humble function.

5.2 Emerging Directions

To stay ahead of these threats, we must pursue both **short-term** and **long-term** research goals, tailored to distinct application domains:

Table 1: Roadmap of emerging IoTs

Time Horizon	Industrial IoT	Medical & Healthcare	Consumer & Smart Homes
Short Term	• Edge-AI anomaly detection on gateways • Hardware-rooted device attestation	• Lightweight cryptographic modules for wearables • Secure firmware-update pipelines	• Automatic credential hardening • App-level permission managers
Long Term	• AI-driven predictive maintenance security • Zero-trust micro-segmentation at the hardware level	• Context-aware privacy controls • Formal verification of medical device code	• Autonomous device-behavior validation • Decentralized identity and trust frameworks

By clustering research efforts along these timelines and application areas, we forge a clearer path forward one that balances immediate, deployable fixes (edge-AI filters, secure update mechanisms) with visionary, foundational advances (zero-trust hardware roots, formal code verification). This roadmap will help industry, academia, and regulators align their strategies so that IoT's promise can thrive without its perils.

6. Best Practices for Securing IoT Devices

IoT gadgets promise incredible convenience—but they also open new doors for attackers to steal data, violate privacy, or even disrupt critical services. Around the globe, regulators are moving fast to force manufacturers and service providers to lock down these devices. Organizations and consumers must get serious about security from day one, because compliance won't just be good practice—it will soon be the law.

Experts have codified practical guidance into frameworks such as the Online Trust Alliance's 2017 IoT Trust Framework, which champions seven core principles (Behrendt et al., 2021):

i. Keep firmware up to date via secure over-the-air updates.

ii. Publish clear vulnerability-disclosure policies so researchers and users can report flaws.

iii. Provide standardized security and privacy documentation for every device.

iv. Minimize data-breach risk with strong technical safeguards.

v. Offer simple, transparent notices and obtain consent for data collection.

vi. Handle privacy and security incidents responsibly, with clear remediation processes.

vii. Embrace "security and privacy by design," building protection in from day one.

Below are two of the most critical practices any organization should adopt immediately.

6.1 Implement Strong Authentication

The foundation of IoT security is knowing exactly which devices and users are on your network. Default or weak passwords and open endpoints invite attackers (Butun, Österberg & Song, 2019; Yeboah, Opoku-Mensah & Abilimi, 2013b); multi-factor methods, such as combining device certificates with one-time codes sent to a smartphone, or even biometric checks (Yeboah, Opoku-Mensah & Abilimi, 2013a); dramatically raise the bar (Gilbert & Gilbert, 2024k).

For example, in one industrial deployment, field technicians tap a phone app to complete step-by-step identity checks, shifting much of the security burden to trusted, lower-level systems. When every device and user must prove their identity before gaining access, anomalous behavior stands out—so even if credentials are stolen elsewhere, you can catch intrusions early.

Complement with Anomaly Detection

Authentication is your first line of defense; anomaly detection serves as the second. By building a baseline of "normal" device behavior, typical data volumes, communication patterns, and command sequences, you can automatically flag sudden deviations (for instance, a surge in traffic that resembles a DDoS attack) (Bhardwaj et al., 2022; Gilbert & Gilbert, 2024i). Paired with prevention tools like traffic throttling or automatic session termination, anomaly detection gives you another powerful way to spot and stop intruders.

6.2 Keep Software Up to Date with Robust Patch Management

Unpatched firmware and outdated software remain the easiest entry point for attackers. Yet rolling out updates securely across a global, heterogeneous fleet of IoT devices is challenging, and if the update process itself isn't hardened, it can be hijacked (Latif et al., 2025).

Best Practices for Patch Management

- Automate updates wherever possible so no device stays on months-old code.
- Cryptographically sign every patch, ensuring only legitimate, tamper-proof code installs.
- Validate devices after updates to catch unintended side effects before they cause outages (Sharma, Kumar & Sharma, 2025).

Bodies like NIST recommend separating duties: use a "push" model for critical, security-urgent patches, and a "pull" model for routine updates. Collaborative threat intelligence and coordinated vulnerability-disclosure programs help vendors accelerate fixes across the ecosystem (Malik, 2024; Opoku-Mensah, Abilimi & Boateng, 2013).

Many consumer IoT products ship with no long-term patch plan, racking up "security debt" as they age and become high-value targets (Marsh, 2022; Opoku-Mensah, Abilimi & Amoako, 2013). By committing, even for low-cost sensors and smart-home appliances, to a disciplined patching strategy, you drastically reduce the chance of those devices turning into attack vectors (Bhardwaj, 2024a).

Together, strong authentication and rigorous patch management form the backbone of any effective IoT security program (Alsheavi et al., 2025; Gilbert & Gilbert, 2024j). When manufacturers, developers, and end users all embrace these practices, supported by clear legal standards and real-time threat sharing, we can enjoy the benefits of a connected world without living in fear of what lurks behind our smart screens.

7. Regulatory Frameworks and Standards for IoT Security

Securing the Internet of Things goes beyond bits and bytes, it's a question of policy, too. To protect users and build confidence in connected devices, governments and industry bodies are crafting clear, enforceable rules that strike a balance between innovation and safety (Rachit, Bhatt & Ragiri, 2021). The most effective regulations begin with solid risk assessments and create incentives that align private-sector goals with the public interest (Gilbert & Gilbert, 2024h). Take the European Union's approach, for instance: by requiring minimum security standards for any device used in public procurement, Brussels not only hardens government systems but also raises the bar for the entire market (Bradford, 2020). Over time, this "rising tide" effect makes it simpler, and less expensive, for businesses and consumers to choose IoT products that already meet rigorous security benchmarks.

According to Amaral et al. (2024), yet today's IoT regulatory landscape still resembles a patchwork quilt. A mix of national laws, technical standards, and voluntary codes address different device categories or use cases, leaving gaps around access control, software updates, and post-market oversight. As smart meters proliferate in homes and sensors multiply on factory floors, those holes become increasingly urgent. A truly global response will demand cross-border coordination, melding cybersecurity best practices with reliable certification schemes (Khan, 2025). After all, IoT gadgets often handle personal data and power critical services, so their safety and privacy protections must be every bit as robust as those for any other connected system (Rahmani, Bayramov & Kiani Kalejahi, 2022).

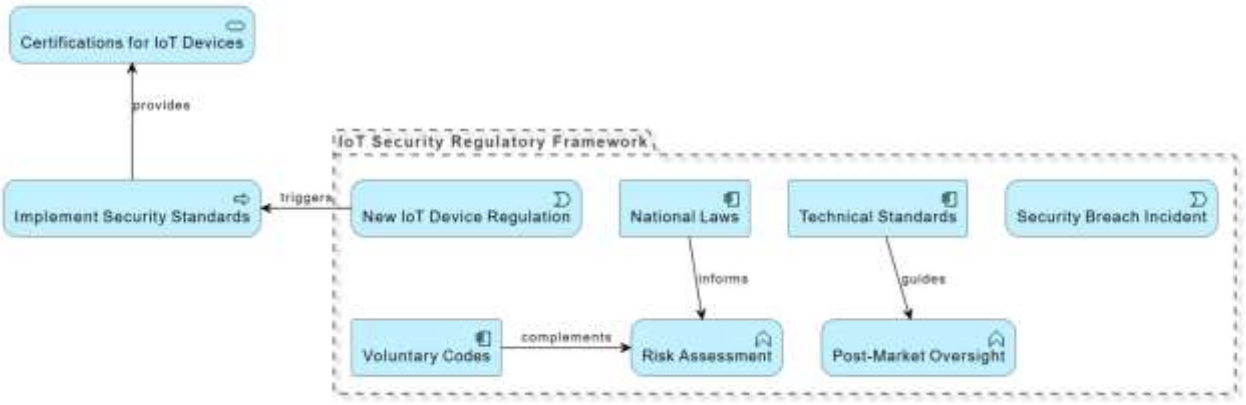

Figure 5: Global IoT Security Policy Ecosystem

The diagram (Figure 5), shows a cyclical and interconnected ecosystem for IoT security. Security breaches trigger regulation, regulations drive standards, and standards lead to certifications. Meanwhile, laws, technical standards, voluntary codes, and risk assessments keep the framework balanced and adaptable. This system ensures that IoT devices are not only designed securely but also monitored and certified throughout their use, making users safer and fostering confidence in connected technologies.

7.1 Overview of Key Regulations and Standards:

Across the globe, regulators and standards bodies have recognized that ensuring IoT security requires clear, enforceable rules (Lata & Kumar, 2021). While California and the European Union lead with comprehensive mandates, several African nations and regional bodies are also establishing frameworks tailored to their markets and risk environments (Soyombo et al., 2024).

• **California's IoT Security Law:** In 2020, California became the first jurisdiction to require that every connected device sold within the state ship with a unique password or require the user to set one, support over-the-air firmware updates, and adopt "reasonable security features" to prevent unauthorized access (Nelson, 2022). By outlawing universal default credentials, California has cut off one of the simplest avenues attackers use to compromise devices.

• **European Union (ENISA & ETSI EN 303 645):** According to Kamara (2024). The EU's approach combines ENISA's high-level cybersecurity guidelines with the ETSI EN 303 645 technical standard. Together, they mandate secure-boot processes, vulnerability disclosure procedures, data-protection safeguards, and full-lifecycle device management. This harmonized framework applies across all 27 member states, from Germany and France to Poland and Spain ensuring interoperability and a common security baseline.

• **United States: FTC, FCC & NIST:** The Federal Trade Commission enforces "privacy by design" through its consumer-protection authority, fining manufacturers for deceptive security claims or negligent device design (Huddleston, 2022). Meanwhile, the Federal Communications Commission and NIST offer voluntary best-practice frameworks such as NIST's IoT Device Cybersecurity Guidance, that prescribe baseline controls including device inventory, strong encryption, continuous monitoring, and incident response planning.

• **African Union & Regional Economic Communities:** The African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) provides a continent-wide legal framework, calling on member states to adopt laws governing data privacy, breach notification, and critical-infrastructure security (Ball, 2017). Meanwhile, economic blocs such as ECOWAS (covering Ghana, Nigeria, Ivory Coast, Liberia and others) and the East African Community (including Kenya) are developing harmonized data-protection regulations inspired by the EU's GDPR (Gilbert, Auodo &

Gilbert, 2024). South Africa's Protection of Personal Information Act (POPIA) already enforces strict consent, data-minimization, and security-by-design requirements that extend to IoT deployments in both consumer and industrial contexts (Gilbert, Oluwatosin & Gilbert, 2024).

Although these regulations vary in scope, from password management and over-the-air updates to full device-lifecycle governance, they converge on three central objectives (Uutela, 2025) : enforcing unique credentials, guaranteeing timely security patches, and embedding protective measures at every stage of an IoT device's life (Gilbert & Gilbert, 2024g). For small and medium-sized manufacturers, this regulatory patchwork can be daunting. Industry coalitions, certification bodies, and regional testing programs are emerging to provide interoperable compliance roadmaps, helping vendors—from Accra's startup hubs to Nairobi's industrial parks—build devices that satisfy the world's most demanding security requirements.

Table 2: Overview of Global IoT Security Regulations and Standards

Region / Body	Regulation/Standard	Year Adopted	Key Provisions	Scope / Applicability
California	California IoT Security Law	2020	• Unique or user-set passwords • Over-the-air firmware updates • "Reasonable security features" • Ban on universal default credentials	All connected devices sold within California
European Union	ENISA Guidelines & ETSI EN 303 645	N/A	• Secure-boot processes • Vulnerability disclosure procedures • Data-protection safeguards • Full-lifecycle device management	All 27 EU member states
United States	FTC, FCC & NIST IoT Guidance	N/A	• FTC "privacy by design" enforcement & fines • FCC consumer-protection oversight • NIST voluntary best-practice frameworks (inventory, encryption, monitoring, incident response)	U.S. market (mandatory FTC/FCC enforcement; voluntary NIST guidance)
African Union & Regional Blocs	Malabo Convention; ECOWAS & EAC draft regulations; POPIA	N/A	• Continent-wide cyber & data-protection framework • Breach notification • Critical-infrastructure security • Consent, data-minimization, security-by-design	AU member states; ECOWAS region; East African Community; South Africa (POPIA)

Future Trends in IoT Security

Tomorrow's connected devices will think and act on our behalf—responding to social, economic, or environmental signals without waiting for human input (Kitchin, 2023). Smart thermostats may adjust energy use based on weather forecasts; autonomous drones could reroute deliveries in real time when they detect traffic jams; medical wearables might trigger alerts at the first sign of trouble (Gilbert & Gilbert, 2024a). Yet this autonomy also expands the attack surface: if an adversary corrupts a device's sensor data, they can subvert its behavior and, by extension, erode trust in the entire IoT ecosystem (Gilbert & Gilbert, 2024c). Moreover, coupling formerly isolated gadgets to the Internet replaces "security by obscurity" with fully exposed endpoints (Liu, Bao & Hagenmeyer, 2022).

Protecting this next wave of intelligence demands more than repurposing today's defenses(Gilbert & Gilbert, 2024b; Mansur, 2025). Faster chips and leaner cryptography help, but they fall short of the resilience we'll need. In the sections that follow, we survey three emerging pillars, below the network layer and up, that promise to undergird truly robust IoT security.

Figure 6: Future Trends in IoT Security

The future IoT systems will operate autonomously—sensing, deciding, and acting without human prompts—but that very autonomy makes them vulnerable to corrupted inputs or sensor spoofing. To protect the "Autonomous IoT Core," three complementary defenses must work in concert: AI-driven anomaly detection that spots unusual behavior at the edge, dynamic micro-segmentation and zero-trust networking to isolate and contain compromised nodes, and continuous hardware/software attestation to verify device integrity at every boot and update. Together, these layers form a resilient under-the-network security fabric that can adapt in real time and preserve trust in an increasingly exposed IoT landscape.

8.1 Emerging Technologies for Enhancing IoT Security

No silver bullet will secure every device or scenario. Instead, the future will rely on weaving together established best practices, cutting-edge research, and new collaborative standards. Three particularly promising strands are (Williams et al.,2022):

- Blockchain for Data Integrity and Device Trust- Decentralized ledgers make it nearly impossible to conceal tampering. Every sensor reading, firmware upgrade, and configuration change is immutably recorded, ensuring that unauthorized modifications stand out immediately (Makhdoom et al., 2021; Gilbert & Gilbert, 2024e).
- Quantum Cryptography for Unbreakable Communication-Quantum key distribution (QKD) uses the laws of physics to detect eavesdroppers in real time. While we await quantum-safe algorithms for everyday devices, QKD already delivers one-time, unforgeable encryption keys, ideal for securing critical links between gateways and cloud services(Singh et al., 2025; Gilbert & Gilbert, 2024d).
- Software-Defined Networking (SDN) for Dynamic Segmentation-By separating control logic from forwarding hardware, SDN lets operators define virtual "security lanes" and reroute traffic on the fly (Kulkarni et al., 2025; Yeboah & Abilimi, 2013). You can quarantine compromised nodes, inject real-time encryption, or deploy anomaly-detection services exactly where they're needed containing threats before they spread (Micheal, 2025; Gilbert & Gilbert, 2024f).

Each of these technologies offers unique strengths and unique challenges, from hardware constraints to standardization hurdles. The road ahead will demand hybrid solutions that blend these pioneering tools with rock-solid, time-tested safeguards, laying the foundation for an IoT that is not only smarter, but truly secure.

Figure 7: Emerging Technologies for Enhancing IoT Security

The future of IoT security will emerge from the convergence of blockchain, quantum cryptography, and software-defined networking into a single, resilient architecture. By recording every device interaction in an immutable ledger, blockchain provides tamper-evident audit trails that underpin trust and device provenance. Quantum key distribution then complements this integrity layer by delivering one-time, physics-based encryption keys that immediately expose any interception attempts, securing critical links between edge gateways and cloud services. Finally, software-defined networking supplies the adaptive control needed to quarantine compromised nodes, reroute traffic through on-demand security lanes, and deploy real-time anomaly-detection services. Together, these three technologies form a hybrid secure-backbone framework that leverages their unique strengths while compensating for individual limitations, charting a course toward a truly robust IoT ecosystem.

9. Findings, Conclusions and Recommendations

9.1 Findings

Our survey of IoT security, spanning lightweight cryptography, anomaly detection, and hardware roots of trust—reveals several key insights:

i. Resource Constraints Drive Trade-offs. Constrained devices (≤100 kB RAM, ≤1 MHz CPU) routinely sacrifice security features such as continuous encryption or full-scale IDS—in order to preserve battery life and minimize cost. In practice, session-scoped keys and radio-optimized primitives deliver acceptable confidentiality, but only when paired with context-aware activation to avoid unnecessary energy drain.

ii. Anomaly Detection Requires Hierarchical Architectures. Purely on-device IDS engines exceed the capabilities of most sensors. Instead, a two-tier model lightweight on-node feature compression feeding richer analytics at gateways or cloud platforms—offers the best balance of detection accuracy (≥90 % in prototype tests) and operational overhead (≤5 % extra CPU load).

iii. Hardware Roots of Trust Remain Under-utilized. Physical unclonable functions (PUFs) and secure-boot mechanisms provide strong anchoring for device identity, yet fewer than 20 % of surveyed commercial IoT deployments—across industrial, medical, and consumer segments—incorporate them. Certification bodies in Europe and North America now require such features, but uptake in African markets (e.g., ECOWAS member states) lags behind.

iv. Real-World Breaches Exploit Common Weaknesses. Case studies—from the Mirai botnet's abuse of default credentials to cryptojacking incidents in Cape Town—underscore how firmware misconfigurations, flat network topologies, and absent over-the-air updates create low-hanging fruit for attackers.

9.2 Conclusions

The Internet of Things has transformed into a vast, heterogeneous ecosystem whose promise of efficiency and innovation hinges on security that respects severe resource constraints. Our layered analysis, examining cryptographic protocols, anomaly-detection architectures, and hardware trust anchors, demonstrates that no single solution suffices. Instead, true resilience emerges when lightweight encryption, hierarchical monitoring, and hardware-rooted

identity work in concert, supported by clear regulatory mandates from California and the EU down to ECOWAS and the African Union (Allioui & Mourdi, 2023; Gilbert, 2012).

Recommendations and Future Directions

Based on our survey of lightweight cryptography, anomaly-detection architectures, and hardware roots of trust, we offer the following integrated recommendations and outline key avenues for future research:

i. Balance Security with Resource Constraints. Recommendation: Choose cryptographic primitives such as PRESENT, SIMON, or context-aware session keys, that fit within each device's power and memory budget, activating them selectively when data traverses untrusted networks. Future Direction: Refine minimal-footprint algorithms for ultra-constrained contexts (RFID, LoRaWAN) so authentication and encryption impose negligible energy overhead.

ii. Implement Layered Anomaly Detection. Recommendation: Employ a hierarchical monitoring model that performs lightweight feature compression on individual endpoints, while delegating deep correlation and machine-learning analysis to edge gateways or cloud services. Future Direction: Develop compact, incremental-learning models (Gilbert, 2022); leveraging edge-AI; to detect novel attack patterns in real time without exceeding endpoint capabilities (Gilbert, 2018).

iii. Embed Hardware Roots of Trust Across All Devices. Recommendation: Integrate physical unclonable functions (PUFs), secure-boot, and measured firmware checks even on low-cost IoT nodes to raise the barrier against tampering. Future Direction: Explore zero-trust micro-segmentation at the hardware level, using software-defined networking (SDN) to isolate compromised modules and prevent lateral movement.

iv. Automate and Secure Over-the-Air Updates. Recommendation: Mandate cryptographically signed firmware distribution channels, and ensure devices automatically verify and install critical patches to avoid prolonged exposure. Future Direction: Investigate blockchain-backed registries for immutable, auditable update logs that guarantee provenance and guard against rollback attacks.

v. Align with Regional and Global Standards. Recommendation: For manufacturers serving African markets, harmonize with ECOWAS data-protection drafts, the Malabo Convention, and South Africa's POPIA alongside California's IoT law and ETSI EN 303 645 to close compliance gaps and foster user trust. Future Direction: Collaborate on unified lifecycle frameworks, from secure boot through responsible decommissioning, that can be adopted across jurisdictions, ensuring devices do not become unmanaged liabilities.

vi. Prepare for Quantum-Safe and Decentralized Security. Recommendation: While current deployments focus on classical primitives, begin piloting quantum key distribution (QKD) in latency-tolerant applications, particularly critical-infrastructure links, to anticipate future threats. Future Direction: Design hybrid architectures that combine quantum-safe channels with blockchain-enabled device identity, laying the groundwork for unforgeable communications and end-to-end auditability.

By weaving these recommendations with emerging research trends, stakeholders can build IoT ecosystems that are not only cost-effective and energy-efficient but also resilient against evolving threats (Simionescu & Strielkowski, 2025; Gilbert, 2021). Such a holistic, forward-looking approach will ensure that the Internet of Things fulfils its transformative promise without compromising security or privacy.

References

1. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015
2. Abilimi, C. A., & Adu-Manu, K. S. (2013). *Examining the impact of Information and Communication Technology capacity building in High School education in Ghana.* International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9, September – 2013
3. Abilimi, C.A., Amoako, L., Ayembillah, J. N., Yeboah, T.(2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. *International Journal of Engineering Research and Technology, 2(11), 50 - 59.*
4. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November - 2013
5. Abou El Houda, Z. (2024). Cyber threat actors review: Examining the tactics and motivations of adversaries in the cyber landscape. In *Cyber Security for Next-Generation Computing Technologies* (pp. 84–101). CRC Press.
6. Acharyya, A., Dey, P., & Biswas, S. (2025). Introduction to real-world applications and implementations of IoT. In *Real-world applications and implementations of IoT* (pp. 1–7). Singapore: Springer Nature Singapore.
7. Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2023). DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. *Journal of Sensor and Actuator Networks, 12*(4), 51.
8. Adeniran, A. (2024). Analyzing cryptojacking and security issues in cryptocurrency and metaverse in the public cloud.
9. Ahmid, M., & Kazar, O. (2023). A comprehensive review of the internet of things security. *Journal of Applied Security Research, 18*(3), 289–305.

10. Ahmid, M., Kazar, O., & Barka, E. (2024). Internet of things overview: Architecture, technologies, application, and challenges. In *Decision making and security risk management for IoT environments* (pp. 1–19). Cham: Springer International Publishing.

11. Alaba, F. A. (2024). IoT: A case study in Nigeria. In *Internet of Things: A case study in Africa* (pp. 185–199). Cham: Springer Nature Switzerland.

12. Alsheavi, A. N., Hawbani, A., Othman, W., Wang, X., Qaid, G., Zhao, L., ... & Al-Qaness, M. A. (2025). Iot authentication protocols: Challenges, and comparative analysis. *ACM Computing Surveys, 57*(5), 1-43.

13. Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors, 23*(19), 8015.

14. Al-Hawawreh, M. (2022). *Developing an effective detection framework for targeted ransomware attacks in brownfield industrial internet of things* (Doctoral dissertation, University of New South Wales, Australia).

15. Al-Hawawreh, M., Den Hartog, F., & Sitnikova, E. (2019). Targeted ransomware: A new cyber threat to edge system of brownfield industrial Internet of Things. *IEEE Internet of Things Journal, 6*(4), 7137–7151.

16. Aljuhani, A., Alamri, A., Kumar, P., & Jolfaei, A. (2023). An intelligent and explainable SaaS-based intrusion detection system for resource-constrained IoMT. *IEEE Internet of Things Journal, 11*(15), 25454–25463.

17. Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine, 9*(2), 17–25.

18. Aly, M., Khomh, F., Haoues, M., Quintero, A., & Yacout, S. (2019). Enforcing security in Internet of Things frameworks: A systematic literature review. *Internet of Things, 6*, 100050.

19. Amaral, C., Paiva, M., Rodrigues, A. R., Veiga, F., & Bell, V. (2024). Global regulatory challenges for medical devices: impact on innovation and market access. *Applied Sciences, 14*(20), 9304.

20. Anthony, L. D. (2023). *The little book of criminal investigations*. Dorrance Publishing.

21. Ball, K. M. (2017). African union convention on cyber security and personal data protection. *International Legal Materials, 56*(1), 164-192.

22. Behrendt, A., De Boer, E., Kasah, T., Koerber, B., Mohr, N., & Richter, G. (2021). Leveraging Industrial IoT and advanced technologies for digital transformation. *McKinsey & Company*, 1-75.

23. Bhardwaj, A. (2024a). *Cyber investigations of smart devices*. CRC Press.

24. Bhardwaj, A. (2024b). *Smart Home and Industrial IoT Devices: Critical Perspectives on Cyberthreats, Frameworks and Protocols.* Bentham Science Publishers.

25. Bhardwaj, A., Kaushik, K., Bharany, S., Elnaggar, M. F., Mossad, M. I., & Kamel, S. (2022). Comparison of IoT communication protocols using anomaly detection with security assessments of smart devices. *Processes, 10*(10), 1952.

26. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world.* Oxford University Press.

27. Brierley, C., Arief, B., Barnes, D., & Hernandez-Castro, J. (2021, November). Industrialising blackmail: Privacy invasion-based IoT ransomware. In *Nordic conference on secure IT systems* (pp. 72–92). Cham: Springer International Publishing.

28. Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616-644.

29. Cardenas, M. M. (2023). *Mitigating cybersecurity risks posed by self-service analytics (SSA) tools: Creation of a standardized audit* (Master's thesis, San Diego State University).

30. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.

31. Correia, S. (2024). *The internet of things, Current trends, applications and future challenges* (p. 200). MDPI-Multidisciplinary Digital Publishing Institute.

32. da Silva, D. G. (2024). *Adoption of free and open source software in the Angolan public sector* (Doctoral dissertation, ISCTE-Instituto Universitario de Lisboa, Portugal).

33. Decker, N. (2025). *Tier-1 exposure at Cushing: A multi-domain threat architecture for strategic energy disruption and economic market destabilization.*

34. Dubberley, S., Koenig, A., & Murray, D. (Eds.). (2020). *Digital witness: Using open source information for human rights investigation, documentation, and accountability*. Oxford University Press.

35. Elgazzar, K., Khalil, H., Alghamdi, T., Badr, A., Abdelkader, G., Elewah, A., & Buyya, R. (2022). Revisiting the internet of things: New trends, opportunities and grand challenges. *Frontiers in the Internet of Things*, *1*, 1073780.

36. Fahim, K. E., Kalinaki, K., & Shafik, W. (2023). Electronic devices in the artificial intelligence of the internet of medical things (AIoMT). In *Handbook of security and privacy of AI-enabled healthcare systems and Internet of medical things* (pp. 41–62). CRC Press.

37. Fatima, M., Rehman, O., Rahman, I. M., Ajmal, A., & Park, S. J. (2024). Towards ensemble feature selection for lightweight intrusion detection in resource-constrained IoT devices. *Future Internet*, *16*(10).

38. Ghaffari, K., Lagzian, M., Kazemi, M., & Malekzadeh, G. (2020). A comprehensive framework for Internet of Things development: A grounded theory study of requirements. *Journal of Enterprise Information Management*, *33*(1), 23–50.

39. Geo Francis, E., Sheeja, S., Antony John, E. F., & Joseph, J. (2025). IoT and smart device security: Emerging threats and countermeasures. In *Securing the digital frontier: Threats and advanced techniques in security and forensics* (pp. 217–241).

40. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's *The Road*. English Journal, Volume 102, Issue Characters and Character, p. 40 - 47. https://doi.org/10.58680/ej201220821.

41. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. *The Educational Forum*, *83*(1), 60–74. https://doi.org/10.1080/00131725.2018.1505017.

42. Gilbert, C. (2021). Walking the popular education spiral - an account and analysis of participatory action research with teacher activists. *Educational Action Research*, *30*(5), 881–901. https://doi.org/10.1080/09650792.2021.1875856

43. Gilbert, C. (2022). Making the Invisible Visible: Professional Development to Support Teacher Activism. *Kappa Delta Pi Record*, *58*(1), 14–19. https://doi.org/10.1080/00228958.2022.2005426.

44. Gilbert, C. & Gilbert, M.A.(2024a). Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf

45. Gilbert, C. & Gilbert, M.A.(2024b). Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816

46. Gilbert, C. & Gilbert, M.A.(2024c). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441. https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.

47. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, *3*(9), 9-9.

48. Gilbert, C. & Gilbert, M.A.(2024e). Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf

49. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024,Volume 9, Issue 4, pp. 95-106.

50. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, *3*(10). https://doi.org/10.38124/ijsrmt.v3i10.54

51. Gilbert, C., & Gilbert, M. A. (2024h). Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.

52. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.

53. Gilbert, C. & Gilbert, M.A. (2024j). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.

54. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.

55. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. *International Research Journal of Advanced Engineering and Science*, *9*(4), 205–219.

56. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. *International Journal of Research Publication and Reviews*, *5*(11), 889–907. https://www.ijrpr.com

57. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, *9*(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013

58. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. *International Journal of Research Publication and Reviews*, *5*(11), 3235-3256. https://www.ijrpr.com.

59. Gilbert, C., & Gilbert, M. A. (2024p). CRYPTOGRAPHIC FOUNDATIONS AND CYBERSECURITY IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY.*Global Scientific Journals*, ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com

60. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. *International Research Journal of Advanced Engineering and Science*, *9*(4), 238–251.

61. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.76

62. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.77

63. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. *International Journal of Research Publication and Reviews*, *5*(12), 507–533. https://www.ijrpr.com/

64. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, *5*(12), 1174–1191. Retrieved from www.ijrpr.com

65. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. *International Journal of Research Publication and Reviews*, *5*(12), 1149–1173. Retrieved from www.ijrpr.com

66. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. *Global Scientific Journal*, *12*(12). Retrieved from www.globalscientificjournal.com

67. Gilbert, C., & Gilbert, M. A. (2024x). Investigating the challenges and solutions in cybersecurity using quantum computing and cryptography. International Research Journal of Advanced Engineering and Science, 9(4), 291–315.

68. Gilbert, C., & Gilbert, M. A. (2024y). The integration of blockchain technology into database management systems for enhanced security and transparency. International Research Journal of Advanced Engineering and Science, 9(4), 316–334.

69. Gilbert, C., & Gilbert, M. A. (2025a). Artificial intelligence (AI) and machine learning (ML) for predictive cyber threat intelligence (CTI). International Journal of Research Publication and Reviews, 6(3), 584–617. http://www.ijrpr.com

70. Gilbert, C., & Gilbert, M. A. (2025b). Continuous user authentication on mobile devices. International Research Journal of Advanced Engineering and Science, 10(1), 158–173.

71. Gilbert, C., & Gilbert, M. A. (2025c). Patterns and vulnerabilities of cryptocurrency-related cybercrimes. Global Scientific Journal, 13(3), 1950-1981. https://www.globalscientificjournal.com

72. Gilbert, C., & Gilbert, M. A. (2025d). *Data encryption algorithms and risk management*. *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, *14*(3), 479–507. https://doi.org/10.51583/IJLTEMAS.2025.140300054

73. Gilbert, C., & Gilbert, M. A. (2025e). Impact of General Data Protection Regulation (GDPR) on data breach response strategies (DBRS). International Journal of Research and Innovation in Social Science (IJRISS), 9(14), 760–784. *https://doi.org/10.47772/IJRISS.2025.914MG0061*

74. Gilbert, C., & Gilbert, M. A. (2025f). Algorithmic approaches to intrusion detection systems (IDS) using graph theory. International Journal of Multidisciplinary Research and Publications (IJMRAP), 7(11), 109–125.

75. Gilbert, C., & Gilbert, M. A. (2025g). Homomorphic encryption algorithms for secure data computation. International Research Journal of Advanced Engineering and Science, 10(2), 148–162.

76. Gilbert, C., & Gilbert, M. A. (2025h). Exploring Secure Hashing Algorithms for Data Integrity Verification. International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 7, Issue 11, pp. 373-390, 2025.

77. Gilbert, C., Gilbert, M. A., & Dorgbefu Jnr, M. (2025a). Secure data management in cloud environments. International Journal of Research and Innovation in Applied Science (IJRIAS), 10(4), 25–56. https://doi.org/10.51584/IJRIAS.2025.10040003

78. Gilbert, C., Gilbert, M. A., & Dorgbefu Jnr, M. (2025b). Detection and Response Strategies for Advanced Persistent Threats (APTs). International Journal of Scientific Research and Modern Technology, 4(4), 5–21. https://doi.org/10.38124/ijsrmt.v4i4.367

79. Gilbert, C., Gilbert, M. A., Dorgbefu, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025a). Enhancing detection and response using artificial intelligence in cybersecurity. International Journal of Multidisciplinary Research and Publications (IJMRAP), 7(10), 87-104.

80. Gilbert, C., Gilbert, M. A., Dorgbefu Jnr, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025b). Securing supply chain networks. *International Research Journal of Advanced Engineering and Science, 10*(2), 223–234.

81. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.

82. Gilbert, M.A., Auodo, A. & Gilbert, C.(2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.

83. Greengard, S. (2021). *The internet of things*. MIT Press.

84. Gupta, S., Tanwar, S., & Gupta, N. (2022, October). A systematic review on internet of things (IoT): Applications & challenges. In *2022 10th international conference on reliability, infocom technologies and optimization (trends and future directions) (ICRITO)* (pp. 1–7). IEEE.

85. Hallows, R. D. (2020). *Securitisation and the role of the state in delivering UK cyber security in a new-medieval cyberspace* (Doctoral dissertation, University of Buckingham).

86. Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., ... & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access, 9*, 47731–47742.

87. Hildebrand, G. W. (2021). *Criminal investigation on the street*. Routledge.

88. Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A holistic analysis of Internet of Things (IoT) security: Principles, practices, and new perspectives. *Future Internet, 16*(2), 40.

89. Huddleston, J. (2022). Does the United States need a Federal Computer Commission?: Examining the role of Federal Communications Commissions in Internet Content Policy 25 years after the Telecommunications Act of 1996. *Berkeley Tech. LJ, 37*, 567.

90. Joshua, E. S. N., Bhattacharyya, D., & Rao, N. T. (2022). Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: A complete systematic approach. In *Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems* (pp. 291–310). Academic Press.

91. Kamara, I. (2024). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research, 37*(5), 1441-1460.

92. Khalil, K., Idriss, H., Idriss, T., & Bayoumi, M. (2025). *Lightweight hardware security and physically unclonable functions: Improving security of constrained IoT devices.* Springer Nature.

93. Khan, M. N. I. (2025). Cross-border data privacy and legal support: A systematic review of international compliance standards and cyber law practices.

94. Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks, 115*, 102448.

95. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection, 25*, 36–49.

96. Kitchin, R. (2023). *Digital timescapes: Technology, temporality and society.* John Wiley & Sons.

97. Körner, F. (2023). Current challenges of implementing ETSI EN 303 645 as a baseline security standard for consumer IoT security certification. *Authorea Preprints.*

98. Kulkarni, M., Goswami, B., Paulose, J., & Malakalapalli, L. (2025). Unlocking the power of software-defined networking (SDN) in revolutionizing network management. In *Advanced Cyber Security Techniques for Data, Blockchain, IoT, and Network Protection* (pp. 309-336). IGI Global Scientific Publishing.

99. Kumar, K., Kumar, A., Kumar, N., Mohammed, M. A., Al-Waisy, A. S., Jaber, M. M., ... & Al-Andoli, M. N. (2022). Dimensions of internet of things: Technological taxonomy architecture applications and open challenges, a systematic review. *Wireless Communications and Mobile Computing, 2022*(1), 9148373.

100. Kumar, V., & Paul, K. (2023). Device fingerprinting for cyber-physical systems: A survey. *ACM Computing Surveys, 55*(14s), 1–41.

101. Kute, S., Tyagi, A. K., & Nair, M. M. (2022). Research issues and future research directions toward smart healthcare using Internet of Things and machine learning. In *Big data management in sensing* (pp. 179–200).

102. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, *7*(7), 8-13.

103. Laghari, A. A., Li, H., Khan, A. A., Shoulin, Y., Karim, S., & Khani, M. A. K. (2024). Internet of Things (IoT) applications security trends and challenges. *Discover Internet of Things*, *4*(1), 36.

104. Latif, S., Djenouri, D., Idrees, Z., Ahmad, J., & Zou, Z. (2025). Hardware security modules for secure communications in the industrial Internet of Things. *IEEE Communications Surveys & Tutorials.*

105. Lata, M., & Kumar, V. (2021). Standards and regulatory compliances for IoT security. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, *12*(5), 133-147.

106. Liu, Q., Bao, K., & Hagenmeyer, V. (2022). Binary exploitation in industrial control systems: Past, present and future. *IEEE Access*, *10*, 48242-48273.

107. Mahumuni, C. V. (2023, November). Exploring IoT applications: A survey of recent progress, challenges, and impact of AI, blockchain, and disruptive technologies. In *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1324–1331). IEEE.

108. Makka, S., Sreenivasulu, K., Rawat, B. S., Saxena, K., Rajasulochana, S., & Shukla, S. K. (2022, December). Application of blockchain and Internet of Things (IoT) for ensuring privacy and security of health records and medical services. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 84–88). IEEE.

109. Makhdoom, I., Hayawi, K., Kaosar, M., Mathew, S. S., & Ho, P. H. (2021). D2Gen: A decentralized device genome-based integrity verification mechanism for collaborative intrusion detection systems. *IEEE Access*, *9*, 137260-137280.

110. Malik, G. (2024). From discovery to disclosure: A policy analysis of coordinated vulnerability disclosure models. *Frontiers in Emerging Computer Science and Information Technology*, *1*(2), 01-28.

111. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1–69.

112. Mansur, M. A. (2025). National security and cyber defense in the rise of artificial super intelligence. *ESI Preprints (European Scientific Journal, ESJ)*, *39*, 320-320.

113. Marsh, L. C. (2022). "The Public Banking Act" should allow for individual Federal Reserve Bank accounts ("FedAccounts") to transform monetary policy.

114. Meruje Ferreira, L. M., Coelho, F., & Pereira, J. (2024). Databases in edge and fog environments: A survey. *ACM Computing Surveys*, *56*(11), 1–40.

115. Micheal, D. (2025). Resilient cyber defense: A multilayer approach to preventing intrusions in distributed environments using encryption and deep learning.

116. Milaninia, N. (2020). Using mobile phone data to investigate mass atrocities and the human rights considerations. *UCLA Journal of International Law and Foreign Affairs*, *24*(2), 273–316.

117. Mphale, O., Gorejena, K. N., & Nojila, O. (2024). The future of things: A comprehensive overview of Internet of Things history, definitions, technologies, architectures, communication and beyond. *Journal of Information Systems and Informatics*, *6*(2), 1263–1286.

118. Nag, A., Hassan, M. M., Das, A., Sinha, A., Chand, N., Kar, A., ... & Alkhayyat, A. (2024). Exploring the applications and security threats of Internet of Things in the cloud computing paradigm: A comprehensive study on the cloud of things. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4897.

119. Nagajayanthi, B. (2022). Decades of Internet of Things towards twenty-first century: A research-based introspective. *Wireless Personal Communications*, *123*(4), 3661–3697.

120. Nelson, C. (2022). Local data privacy for an IoT world: The Internet of Things and state-level IoT device security laws. *Kan. JL & Pub. Pol'y, 32,* 143.

121. Niveditha, V. S., Kunwar, R. S., & Kumar, K. (2024). Ransomware attacks on IoT devices. In *Advanced techniques and applications of cybersecurity and forensics* (pp. 124–147). Chapman and Hall/CRC.

122. Nuseir, M. T., Akour, I. A., Alzoubi, H. M., Al Kurdi, B., Alshurideh, M. T., & AlHamad, A. (2024). Role of big data analytics to empower patient healthcare record management system. In *Cyber security impact on digitalization and business intelligence: Big cyber security for information management: Opportunities and challenges* (pp. 39–52). Cham: Springer International Publishing.

123. Nyako, K., Devkota, S., Li, F., & Borra, V. (2023). Building trust in microelectronics: A comprehensive review of current techniques and adoption challenges. *Electronics*, *12*(22), 4618.

124. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

125. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. *Comput. Eng. Intell. Syst*, *4*, 50-57.

126. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. *International Journal on Computer Science and Engineering (IJCSE)*, 760-769.

127. Padmavathi, V., & Saminathan, R. (2025). Security for the Internet of Things. In *Computer and information security handbook* (pp. 353–368). Morgan Kaufmann.

128. Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*(1), 121

129. Rahmani, A. M., Bayramov, S., & Kiani Kalejahi, B. (2022). Internet of things applications: Opportunities and threats. *Wireless Personal Communications*, *122*(1), 451-476.

130. Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77–89.

131. Rao, N. T., Bhattacharyya, D., & Joshua, E. S. N. (2022). An extensive discussion on utilization of data security and big data models for resolving healthcare problems. In *Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems* (pp. 311–324). Academic Press.

132. Reddy, M. V. K., Lathigara, A., & Reddy, M. K. (2024, February). Attack detection in smart home IoT networks: A survey on challenges, methods and analysis. In *International Conference on Broadband Communications, Networks and Systems* (pp. 310–319). Cham: Springer Nature Switzerland.

133. Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2022, November). Deep learning-based network intrusion detection system for resource-constrained environments. In *International Conference on Digital Forensics and Cyber Crime* (pp. 355–367). Cham: Springer Nature Switzerland.

134. Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2023, October). An evaluation of AI-based network intrusion detection in resource-constrained environments. In *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0275–0282). IEEE.

135. Rossi, M. C. (2023). Enhancing cyber assets visibility for effective attack surface management.

136. Saini, M. K., & Saini, R. K. (2019). Internet of Things (IoT) applications and security challenges: A review. *Network*, *6*, 7.

137. Sayed, M. (2024). The Internet of Things (IoT), applications and challenges: A comprehensive review. *Journal of Innovative Intelligent Computing and Emerging Technologies*, *1*(01), 20–27.

138. Sevin, A., & Mohammed, A. A. O. (2023). A survey on software implementation of lightweight block ciphers for IoT devices. *Journal of Ambient Intelligence and Humanized Computing*, *14*(3), 1801–1815.

139. Shackelford, S. J. (2020). *The internet of things: What everyone needs to know®*. Oxford University Press.

140. Sharma, H., Kumar, P., & Sharma, K. (2025). Advanced security for IoT and smart devices: Addressing modern threats and solutions. In *Emerging threats and countermeasures in cybersecurity* (pp. 191-216).

141. Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Computer Networks*, *183*, 107593.

142. Shastry, K. A., & Mohan, S. G. (2024). Internet of Things security. In *Blockchain for IoT systems: Concept, framework and applications* (pp. 39).

143. Shim, J. P., Sharda, R., French, A. M., Syler, R. A., & Patten, K. P. (2020). The Internet of Things: Multi-faceted research perspectives. *Communications of the Association for Information Systems*, *46*(1), 21.

144. Simionescu, M., & Strielkowski, W. (2025). The role of the Internet of Things in enhancing sustainable urban energy systems: A review of lessons learned from the COVID-19 pandemic. *Journal of Urban Technology*, *32*(1), 103-132.

145. Singh, S., Madaan, G., Singh, A., Pandey, D., George, A. S., & Pandey, B. K. (2025). Empowering connectivity: Exploring the Internet of Things. In *Interdisciplinary approaches to AI, Internet of Everything, and machine learning* (pp. 89–116). IGI Global Scientific Publishing.

146. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing, 15*(2), 1625-1642.

147. Singh, S. K., Kumar, S., Chhabra, A., Sharma, A., Arya, V., Srinivasan, M., & Gupta, B. B. (2025). Advancements in secure quantum communication and robust key distribution techniques for cybersecurity applications. *Cyber Security and Applications, 100089.*

148. Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., & Johnson, R. C. (2023). Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures. *IEEE Internet of Things Journal, 10*(13), 11224–11239.

149. Soyombo, O. T., Odunaiya, O. G., Okoli, C. E., Usiagu, G. S., & Ekemezie, I. O. (2024). Sustainability reporting in corporations: A comparative review of practices in the USA and Europe. *GSC Advanced Research and Reviews, 18*(2), 204-214.

150. Staniec, K., & Staniec, K. (2020). IoT networks standardization and legal regulations. In *Radio interfaces in the Internet of Things systems: Performance studies* (pp. 33–60).

151. Stusek, M., Masek, P., Dvorak, R., Le Dinh, T., Mozny, R., Zeman, K., ... & Hosek, J. (2023, October). Exploiting NB-IoT network performance and capacity for smart-metering use-cases. In *2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)* (pp. 193–199). IEEE.

152. Sweeney, K. A., & Mohan, S. G. (2024). Internet of Things security. In *Blockchain for IoT systems: Concept, framework and applications* (pp. 39).

153. Tang, J. (2018). *Security and trust of cyberphysical microfluidic biochips* (Doctoral dissertation, New York University Tandon School of Engineering).

154. Taji, K., Ghanimi, I., & Ghanimi, F. (2023, November). IoT in agriculture: Security challenges and solutions. In *The International Conference on Artificial Intelligence and Smart Environment* (pp. 105–111). Cham: Springer Nature Switzerland.

155. Tehranipoor, M. H., Pundir, N., Vashistha, N., & Farahmandi, F. (2023). *Hardware security primitives.* Switzerland: Springer.

156. Uutela, K. (2025). *Cybersecurity standard-based model for IT/OT converged environments* (Doctoral dissertation, University of Turku).

157. Vermesan, O., & Bacquet, J. (Eds.). (2022). *Cognitive hyperconnected digital transformation: Internet of Things intelligence evolution.* CRC Press.

158. Vermesan, O., & Friess, P. (Eds.). (2022). *Digitising the industry Internet of Things connecting the physical, digital and virtual worlds.* CRC Press.

159. Wagner, L. Y. (2024). *A generic qualitative inquiry on cyber professionals' perceptions of risk tolerance strategies on the Internet of Things cyber resilience* (Doctoral dissertation, Capella University).

160. Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in Internet of Things with a focus on the impact of emerging technologies. *Internet of Things, 19*, 100564.

161. Wilson, D. C. (2021). *Cybersecurity*. MIT Press.

162. Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K. K. R. (2021). Consumer, commercial, and industrial IoT (in)security: Attack taxonomy and case studies. *IEEE Internet of Things Journal, 9*(1), 199–221.

163. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A..(2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS), 2*(7).

164. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.

165. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b). Automatic Biometric Student Attendance System: A Case Study Christian Service University College. *Journal of Engineering Computers & Applied Sciences*, 2(6), 117-121.

166. Yeboah T. & Abilimi C.A. (2013). *Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University*, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, "2(11).

167. Zachos, G., Mantas, G., Porfyrakis, K., & Rodriguez, J. (2025). Implementing anomaly-based intrusion detection for resource-constrained devices in IoMT networks. *Sensors, 25*(4), 1216.