International Journal of Multidisciplinary Research and Growth Evaluation.

The Unified Smart Device Integrity Framework (US-DIF): A Secure Architecture for Scalable Consumer Electronics Platforms in the U.S.

Lamin Saidy [1*], Abraham Ayodeji Abayomi [2], Abel Chukwuemeke Uzoka [3], Bolaji Iyanu Adekunle [4]
[1] Globallogic Inc, Santa Clara, CA, USA
[2] Adepsol Consult, Lagos State, Nigeria
[3] Kennesaw State University, Kennesaw, Georgia, USA
[4] Data Scientist, GSFEN Limited, Nigeria

* Corresponding Author: **Lamin Saidy**

Article Info

ISSN (online): 2582-7138
Volume: 03
Issue: 03
May-June 2022
Received: 20-04-2022
Accepted: 13-05-2022
Page No: 686-691

Abstract
The rapid proliferation of smart consumer electronics—particularly cloud-connected televisions, soundbars, and home automation devices—has introduced significant challenges related to device security, system integrity, and maintenance scalability. This paper presents the Unified Smart Device Integrity Framework (US-DIF), a conceptual model designed to address these issues through an integrated architecture for software security, fault detection, and automated patch management. Grounded in a layered design that combines device-level security agents, cloud-based diagnostics, and a national governance interface, US-DIF provides a scalable and enforceable structure for enhancing device reliability across the U.S. consumer market. The framework is situated within the broader literature on IoT security, fault response systems, and firmware lifecycle management, highlighting limitations in current fragmented practices. Detailed architectural specifications are proposed alongside implementation considerations for retrofitting existing devices and deploying at scale through cloud infrastructures. Additionally, the paper evaluates the regulatory, privacy, and coordination challenges involved in national adoption and identifies future research opportunities in AI-driven fault analytics and blockchain-enabled patch verification. US-DIF aims to set a precedent for secure, standards-based operation of smart devices in an increasingly connected domestic environment.

DOI: https://doi.org/10.54660/.IJMRGE.2022.3.3.686-691

Keywords: Smart Device Security, IoT Fault Detection, Automated Firmware Patching, Consumer Electronics Integrity, Cloud Monitoring Architecture, National IoT Governance Framework

1. Introduction

1.1 Background

The rapid proliferation of cloud-connected consumer electronics in the American household—ranging from smart televisions and soundbars to integrated home assistants—has reshaped how individuals interact with digital environments [1]. These devices, once standalone and limited in functionality, now participate in a complex ecosystem of data exchange, remote control, and multimedia delivery [2]. This transformation has been driven by advancements in affordable computing hardware, accessible cloud services, and user demand for seamless interoperability. However, the increased functionality and interconnectivity of these devices also introduce new layers of technical complexity and risk [3]. As consumer electronics become persistent nodes within broader digital infrastructures, their vulnerabilities can be exploited at scale. Notable incidents of malicious firmware injection, unauthorized data harvesting, and botnet inclusion have highlighted the fragility of current security implementations [4]. While traditional IT environments often benefit from enterprise-grade monitoring and defensive protocols, consumer-grade electronics frequently lack even baseline protection mechanisms.

Furthermore, vendors often prioritize market speed and aesthetic appeal over long-term security assurance, creating a fertile ground for breaches [5]. Given this backdrop, the need for a national, coordinated framework that embeds security, real-time fault detection, and self-healing capabilities within the architecture of these devices becomes imperative. The motivation behind the proposed model stems not only from protecting individual consumers but also from securing digital sovereignty, given the increasing role of these devices in sensitive environments such as remote workstations, telehealth hubs, and educational platforms. A structured, scalable framework will provide a foundation for ensuring trust, reliability, and resilience in the digital homes of the future.

1.2 Problem Statement

Current approaches to smart device security in consumer electronics remain fragmented and inconsistent, leading to substantial system-wide vulnerabilities. Each manufacturer typically employs proprietary security methods, often with minimal oversight or third-party verification. In the absence of industry-wide interoperability standards, patching schedules and diagnostic protocols are left to vendor discretion [6]. This results in non-uniform protection across households and environments, especially when older models are neglected or unsupported. The reliance on manual updates and reactive security further worsens the exposure, particularly for non-technical users [7].

Another critical issue lies in the absence of real-time, integrated fault detection systems across these platforms. Unlike enterprise infrastructure, where faults are often identified proactively using system logs, telemetry, and AI-driven alerts, consumer devices largely operate in isolation until a failure occurs [8]. When faults do arise—whether from hardware degradation, software corruption, or network interference—users often lack the means or knowledge to resolve them, leading to prolonged vulnerabilities and device downtime [9].

Additionally, many consumer electronics suffer from delayed or inaccessible patching. Firmware updates are infrequent, and when provided, may not be automatically installed due to user configuration barriers or system limitations. In some cases, updates are abandoned altogether due to obsolescence or vendor discontinuation. These gaps create opportunities for long-term exploitation, even after vulnerabilities have been publicly disclosed. The systemic failure to embed patching mechanisms within a secure and unified framework leaves devices—and by extension, users—exposed to evolving threats in an increasingly connected world [10].

1.3 Research Objectives and Scope

This paper introduces a conceptual framework, the Unified Smart Device Integrity Framework, designed to standardize security, fault detection, and automated patching for smart TVs, soundbars, and similar home electronics within the United States. The primary objective is to propose a national model that transcends individual vendor practices, aiming to establish a baseline for device resilience that is enforceable, extensible, and scalable. The framework draws inspiration from secure software engineering principles, cloud-native observability models, and national cybersecurity imperatives.

The scope of this research is restricted to mainstream consumer electronics commonly found in American households that rely on cloud connectivity for updates, streaming services, or remote control. These devices often possess embedded operating systems and offer limited user access to internal settings, making them particularly susceptible to undetected faults and security misconfigurations. By focusing on these categories, the framework targets devices with high penetration rates and critical functionality, especially those integrated into work-from-home setups or multimedia networks.

Additionally, the framework aligns with ongoing federal discussions about national digital infrastructure resilience, reflecting priorities set forth by agencies such as NIST and CISA. The objective is not only to protect consumers but to promote a policy-backed ecosystem of trust between manufacturers, regulators, and end-users. Through this model, the framework seeks to unify disparate device ecosystems under a shared architecture that embeds protection, self-diagnosis, and recovery, thereby ensuring long-term scalability and national cyber readiness.

2. Literature Review and Existing Models

2.1 Smart Device Security Paradigms

Security models for consumer electronics typically rely on embedded software protections, basic encryption protocols, and device-level authentication mechanisms [11]. Early models prioritized confidentiality and access control, employing simple password-based systems or local-only access. However, with the rise of cloud integration and always-on connectivity, these models became insufficient [12].

Contemporary approaches have introduced stronger cryptographic protections (e.g., AES encryption, secure bootloaders, and trusted execution environments), but implementation remains uneven. Many smart home devices either lack encrypted communication protocols or transmit sensitive data without user consent. Additionally, security is often considered a "bolt-on" rather than a foundational design element, leading to inconsistent resilience across products [13].

A significant limitation in current paradigms is the absence of third-party security validation. While smartphones and computers undergo certification (e.g., Common Criteria, FIPS), smart TVs and soundbars generally do not [14]. Furthermore, the software supply chain for these devices often includes unvetted third-party code and proprietary modules, which introduces hidden vulnerabilities. This lack of standardization is a primary challenge that the US-DIF framework seeks to address by embedding a unified security baseline at the architectural level [6].

2.2 Fault Detection and Response in IoT

Fault detection in IoT devices has typically been treated as a post-deployment problem. In consumer electronics, diagnostics are often passive—users discover issues when functionality fails. Unlike enterprise IoT systems, which utilize telemetry, real-time monitoring, and AI-assisted anomaly detection, consumer-grade devices offer minimal introspection [15].

Techniques for detecting faults in embedded systems include watchdog timers, heartbeat mechanisms, and log-based analysis [16]. However, many smart devices operate with constrained computational resources, limiting the feasibility of comprehensive on-device diagnostics. Efforts like TinyML have begun to address this by deploying lightweight machine learning models on edge devices for predictive fault

detection , but commercial adoption remains rare in consumer electronics [17]. Moreover, response protocols to detected faults are underdeveloped in this space. Most systems lack auto-recovery mechanisms or user-friendly error handling, leading to device replacement rather than repair [18].

2.3 Patching and Firmware Management Strategies

Firmware updates are essential for maintaining security and functionality, but current strategies vary widely. Many consumer devices rely on manual updates, requiring users to initiate downloads or approve installations. Even when automatic updates are available, they may be delayed by region, device model, or vendor-specific restrictions. This results in heterogeneous patch coverage and persistent exposure to known vulnerabilities [19].

The industry has explored several models for patch delivery, including over-the-air (OTA) updates, delta updates (which minimize download size), and version rollback systems. Notable platforms such as Android and iOS have implemented robust OTA infrastructure, but such mechanisms are rarely extended to smart TVs, soundbars, and similar devices. According to studies, a large percentage of firmware for smart home products is either not maintained or abandoned after initial release, creating a growing base of vulnerable systems [20].

Furthermore, the absence of a unified compliance mechanism makes it difficult to enforce patch distribution timelines. Unlike regulated industries (e.g., healthcare or automotive), consumer electronics are not subject to mandatory patching standards. As a result, even critical security vulnerabilities may go unaddressed for months or indefinitely [21]. US-DIF addresses this by proposing a vendor-neutral patching protocol that integrates cloud-based firmware registries, auto-deployment triggers, and national-level compliance dashboards. This structure allows for transparent patch lifecycle management, real-time monitoring of device update status, and coordinated vulnerability response [7].

3. The US-DIF Conceptual Framework

The Unified Smart Device Integrity Framework (US-DIF) proposes a standardized, multi-layered architecture that addresses persistent security, fault detection, and patching issues in consumer electronics across the U.S. device ecosystem. The framework aims to unify currently disparate vendor practices under a national model that is secure by design, cloud-augmented, and capable of self-regulation. US-DIF does not seek to replace existing device platforms, but instead overlays a structured reference model to which vendors can align new and legacy products [22].

The architecture builds on principles from secure software engineering, resilient systems design, and zero-trust models, adapting them to the constraints and affordances of consumer-grade hardware [23]. It incorporates a vertically integrated approach, where each component—whether local firmware, diagnostic telemetry, or remote command execution—is managed in coordination with a central cloud-based system. The key advantage of US-DIF is its emphasis on interoperability, enabling a range of manufacturers to adopt a shared infrastructure without relinquishing proprietary control over device features [24].

By establishing a national baseline for device integrity, the framework ensures that common protections—such as encrypted communications, verified firmware chains, continuous monitoring, and automatic patching—are implemented uniformly. This is particularly critical in the context of expanding device usage in sensitive environments like telehealth, home-based education, and hybrid workspaces, where household electronics now serve functions traditionally reserved for enterprise-grade systems [25].

3.1 Core Architecture Design

At the heart of US-DIF is a layered architecture that integrates three primary components: embedded security controls, local and remote fault detection modules, and a secure firmware management system. These components are configured in a modular fashion, allowing vendors to adopt the framework incrementally without full system redesign. The lowest layer includes hardware-level security features such as trusted execution environments (TEEs), secure boot processes, and hardware root-of-trust mechanisms. These ensure that only authenticated and untampered firmware can execute on the device.

The second layer introduces software-based integrity management, incorporating tamper detection, logging mechanisms, and failure isolation routines. Fault detection is enabled through the deployment of lightweight diagnostics engines that monitor device temperature, memory consumption, connectivity health, and application behavior. These engines operate continuously in the background, and in the event of an anomaly, initiate local containment or trigger alerts to the remote monitoring system.

The topmost layer handles secure firmware management and patch automation. This layer leverages encrypted update channels, digital signature validation, and rollback safeguards to prevent unauthorized or faulty firmware from being installed. Updates are delivered using a tiered deployment strategy that allows for staggered releases across different regions and device batches, reducing systemic risks. The core architecture is designed to minimize the burden on end-users, relying instead on automation, cloud intelligence, and regulatory triggers to maintain device health and security.

3.2 Cloud-Centric Monitoring and Response

A critical innovation within the US-DIF framework is its reliance on cloud infrastructure for real-time monitoring, diagnostic analytics, and coordinated response. Each device enrolled in the framework transmits anonymized telemetry data to a secure national cloud node. This data includes information about firmware version, patch status, system performance metrics, and operational logs. Advanced analytics engines process this data in near real time to detect anomalies, predict failure conditions, and flag non-compliant configurations.

The cloud system is capable of initiating remote diagnostics, whereby a diagnostic agent is temporarily instantiated on the device to perform a deeper integrity scan or validate sensor readings. This process allows for non-intrusive, minimally disruptive health assessments of consumer devices, reducing the need for user intervention or physical servicing [26]. Additionally, when a critical vulnerability is identified—either through vendor disclosure or third-party research—the cloud platform can rapidly coordinate a multi-device response across all affected units [27].

Patch delivery is also managed through the cloud, using a secure distribution mechanism that ensures only authorized and validated firmware is deployed. Devices authenticate to the patch server using rotating credentials and digital

certificates issued by a national device registry [28]. Once authenticated, they download and apply the patch in a sandboxed environment before activating it. This cloud-centric design not only enables scale but also ensures uniformity, making it possible to measure national compliance rates, identify outliers, and detect attempts to tamper with update mechanisms [29].

3.3 Governance and Compliance Layer

The governance layer of US-DIF is designed to align technological enforcement with national policy objectives and privacy protections. It introduces a standardized compliance interface that enables regulators, vendors, and third-party auditors to validate device behavior and update status without exposing sensitive user data. This interface operates on principles of minimal disclosure and differential privacy, ensuring that collected telemetry cannot be reverse-engineered to infer individual behavior or identity.

To facilitate nationwide adoption, the framework proposes a regulatory-backed certification process analogous to ENERGY STAR or FCC compliance. Devices that adhere to the core tenets of US-DIF—verified firmware chains, telemetry participation, and patch responsiveness—are granted a compliance mark visible to consumers. This label incentivizes vendors to participate in the framework and assures end-users of minimum protections. Certification would also serve as a prerequisite for government procurement, subsidized distribution programs, or smart device rebates.

Furthermore, the governance layer supports vendor accountability through audit logs, patching histories, and fault response time reports. These logs are cryptographically secured and submitted periodically to a centralized compliance portal managed by a neutral federal agency or approved consortium. This arrangement allows stakeholders to evaluate trends, identify non-cooperative vendors, and enforce corrective actions. Through these mechanisms, US-DIF not only standardizes device integrity but also embeds accountability and transparency into the lifecycle of consumer electronics [30].

4. Implementation Considerations and Case Analysis

4.1 Integration into Existing Device Ecosystems

Integrating US-DIF into existing smart TV and home device platforms requires a dual approach: retrofitting legacy systems and embedding the framework into new products during the design phase. For legacy devices, retrofitting must operate within hardware and software constraints. This may involve deploying lightweight firmware agents capable of minimal telemetry collection, patch monitoring, and basic fault detection. Such agents can be delivered through vendor-provided updates or third-party integration agreements and configured to operate within a device's native operating system environment.

One practical method for integration is the use of containerized microservices that encapsulate US-DIF diagnostic and patching functions. These can be embedded in devices with sufficient processing capacity, such as smart TVs with Linux-based firmware or Android-powered platforms. For resource-constrained devices, a proxy-based approach may be adopted, whereby a nearby gateway device (such as a smart hub) handles most of the computational load for telemetry analysis and firmware coordination [31].

Newer devices offer a more seamless path to integration. Manufacturers can embed US-DIF compliance at the chipset level, leveraging trusted platform modules (TPMs) or secure enclaves that support secure boot, cryptographic verification, and remote attestation. Moreover, integrating with vendor SDKs and middleware platforms during development allows for native support of US-DIF protocols, ensuring compatibility with national registries and compliance dashboards from first release. In both scenarios, coordination with original equipment manufacturers (OEMs) is vital to streamline deployment and minimize friction [32].

4.2 Scalability and Performance Metrics

To be viable on a national scale, US-DIF must demonstrate that it can operate efficiently across millions of devices without significant performance penalties. Several evaluation benchmarks are proposed to measure the framework's effectiveness: telemetry latency, patch success rate, average fault resolution time, and system resource overhead. These metrics provide tangible evidence of impact while also guiding optimizations in deployment strategy.

Latency refers to the time required for telemetry to be transmitted, processed, and acted upon. In pilot environments, acceptable latency thresholds for integrity checks and diagnostics are under 500 milliseconds for non-critical tasks and under 100 milliseconds for fault alerts. Early simulations suggest that cloud-based processing pipelines with regional edge nodes can maintain this latency even under high device load, particularly when telemetry is batched or event-driven.

Patch success rate is another critical measure, reflecting the percentage of targeted devices that successfully install security updates within a specified window (e.g., 72 hours from release). A successful US-DIF deployment would aim for a 95% or higher success rate, compared to the current average of 40–60% for many consumer devices. Automated testing environments and post-patch validation routines can be embedded into the firmware delivery pipeline to support this target.

Finally, system overhead must be minimized to avoid degrading user experience. Monitoring agents and diagnostic engines must consume less than 5% of device CPU cycles and 10MB of RAM on average, based on industry benchmarks for background services. Where such thresholds are unattainable—such as on older or ultra-low-cost devices—US-DIF can delegate responsibilities to companion devices or offload tasks to the cloud. These adaptive mechanisms ensure scalability while accommodating device heterogeneity [33].

4.3 U.S. Policy, Privacy, and Vendor Coordination

The successful nationwide adoption of US-DIF hinges on a well-structured legal and regulatory framework that balances innovation, consumer protection, and vendor autonomy. To that end, policymakers must establish baseline requirements for integrity, fault detection, and patch compliance, particularly for devices entering sensitive environments such as schools, hospitals, and government buildings. These requirements can be codified into procurement standards, digital safety certifications, or interstate data security compacts.

Privacy remains a foundational concern in any system involving telemetry and cloud analytics. US-DIF addresses this by enforcing strict anonymization protocols and by allowing users and regulators to audit the nature and scope of

collected data. Data collection policies must adhere to federal statutes such as the Electronic Communications Privacy Act (ECPA) and the California Consumer Privacy Act (CCPA), while also preparing for anticipated national legislation that governs IoT privacy rights. Consent frameworks and opt-out mechanisms should be standardized across vendors to enhance transparency and consumer trust.

Coordinating with manufacturers is essential to align technical implementation with market incentives. Potential incentives include compliance-based access to federal subsidies, grants for research and development of compliant devices, tax benefits for certified vendors, and preferential listing on government-approved product registries. A public-private governance consortium could oversee versioning of the framework, validate vendor participation, and evolve best practices in response to emerging threats. By embedding legal, financial, and reputational incentives into the framework, US-DIF encourages voluntary industry participation while retaining regulatory leverage where necessary.

5. Conclusion and Future Research

This paper has introduced US-DIF as a conceptual and operational architecture capable of addressing major deficiencies in the current consumer electronics landscape. The framework directly confronts fragmentation by proposing a unified protocol suite that can be embedded into both legacy and next-generation devices. Through its layered structure—comprising core architecture, cloud-based monitoring, and a governance interface—US-DIF fosters consistent enforcement of security baselines and performance standards.

In terms of security, US-DIF incorporates proactive telemetry collection, anomaly detection, and cryptographically secure patch distribution. These elements offer a sharp departure from ad hoc update mechanisms and passive failure detection common in current systems. Furthermore, US-DIF's modular design ensures that security protocols can be evolved incrementally without destabilizing device functionality or disrupting the end-user experience. Finally, the framework scales by design. It is capable of servicing millions of devices through cloud-native data processing pipelines, edge computing enhancements, and standardized compliance templates. These features, coupled with incentives for vendor participation and legal accountability, position US-DIF as a viable national infrastructure for smart device integrity, addressing consumer protection at both the technical and policy levels.

Despite its strengths, US-DIF faces significant hurdles that must be acknowledged. Technically, the diversity of device hardware and operating systems poses integration challenges. Many low-cost devices lack the computational resources or firmware flexibility required to host US-DIF agents, necessitating external workarounds such as companion device proxies or firmware adaptations. Additionally, ensuring real-time fault detection and patch deployment at scale remains a resource-intensive endeavor that may incur cloud infrastructure costs and latency trade-offs.

From a policy perspective, national implementation is complicated by fragmented regulatory authority across states and the absence of a unified federal standard for IoT governance. Privacy concerns, particularly regarding telemetry and diagnostic data collection, require careful navigation to avoid infringing upon user rights or triggering public backlash. Furthermore, industry stakeholders may resist adoption due to perceived cost increases or fears of losing competitive differentiation under standardized protocols.

There are also broader sociopolitical challenges. Cybersecurity has become a geopolitical issue, and the introduction of any national framework may attract opposition from interest groups wary of centralized oversight or increased federal control. Overcoming these challenges will require coordinated action across academic, commercial, and governmental sectors, as well as continuous iteration based on field feedback.

Future research can expand on US-DIF by exploring more intelligent, adaptive mechanisms for security and fault management. One promising direction is the integration of AI-driven fault detection systems that use machine learning to identify subtle behavioral anomalies across device fleets. These systems could operate semi-autonomously, adapting to novel attack vectors or firmware glitches without relying solely on predefined rule sets. Researchers can investigate federated learning models that preserve user privacy while aggregating insights from distributed telemetry.

Another avenue is the use of blockchain and decentralized ledgers for firmware verification and patch distribution. These technologies offer tamper-proof audit trails, enhanced transparency, and a distributed trust model that can reduce reliance on centralized patch servers. Smart contracts could automate compliance checks or revoke non-compliant firmware deployments in near real time, adding another layer of assurance to the update lifecycle. Lastly, cross-disciplinary studies that combine behavioral economics, cybersecurity policy, and systems engineering could help uncover optimal strategies for incentivizing vendor cooperation and consumer participation. Pilot studies involving municipal or state-level deployments of US-DIF-compliant devices could yield empirical data on effectiveness, user acceptance, and cost-benefit trade-offs. These research efforts are critical to ensuring that the framework remains both theoretically robust and practically viable in the evolving landscape of smart consumer technologies.

6. References

1. Talal M, *et al*. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. Journal of Medical Systems. 2019;43:1–34.
2. Khriji S, Benbelgacem Y, Chéour R, Houssaini DE, Kanoun O. Design and implementation of a cloud-based event-driven architecture for real-time data processing in wireless sensor networks. The Journal of Supercomputing. 2022;78(3):3374–401.
3. Karlin B, *et al*. Characterization and potential of home energy management (HEM) technology. 2015.
4. Lies J. Marketing intelligence: Boom or bust of service marketing? 2022.
5. Kesan JP, Hayes CM. Bugs in the market: Creating a legitimate, transparent, and vendor-focused market for software vulnerabilities. Ariz L Rev. 2016;58:753.
6. Leverett E, Clayton R, Anderson R. Standardisation and certification of safety, security and privacy in the 'Internet of Things'. In: Proceedings of the 16th Workshop on the Economics of Information Security (WEIS). 2017.
7. Xenofontos C, Zografopoulos I, Konstantinou C, Jolfaei

A, Khan MK, Choo KK. Consumer, commercial, and industrial IoT (in) security: Attack taxonomy and case studies. IEEE Internet of Things Journal. 2021;9(1):199–221.
8. Albahri AS, Zaidan A, Albahri OS, Zaidan B, Alsalem M. Real-time fault-tolerant mHealth system: Comprehensive review of healthcare services, opens issues, challenges, and methodological aspects. Journal of Medical Systems. 2018;42:1–56.
9. Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials. 2019;22(1):616–44.
10. Mtetwa NS, Tarwireyi P, Abu-Mahfouz AM, Adigun MO. Secure firmware updates in the Internet of Things: A survey. In: 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC). IEEE; 2019. p. 1–7.
11. Vakhter V, Soysal B, Schaumont P, Guler U. Threat modeling and risk analysis for miniaturized wireless biomedical devices. IEEE Internet of Things Journal. 2022;9(15):13338–52.
12. Rizvi S, Pipetti R, McIntyre N, Todd J, Williams I. Threat model for securing Internet of Things (IoT) network at device-level. Internet of Things. 2020;11:100240.
13. Khan A, Ahmad A, Ahmed M, Sessa J, Anisetti M. Authorization schemes for Internet of Things: Requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems. 2022;8(5):3919–41.
14. Ferrag MA, Maglaras L, Derhab A, Janicke H. Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. Telecommunication Systems. 2020;73(2):317–48.
15. Poongodi T, Rathee A, Indrakumari R, Suresh P. IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition. In: Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Springer; 2019. p. 127–51.
16. Alajlan NN, Ibrahim DM. TinyML: Enabling of inference deep learning models on ultra-low-power IoT edge devices for AI applications. Micromachines. 2022;13(6):851.
17. Schizas N, Karras A, Karras C, Sioutas S. TinyML for ultra-low power AI and large-scale IoT deployments: A systematic review. Future Internet. 2022;14(12):363.
18. Capella JV, Campelo JC, Bonastre A, Ors R. A reference model for monitoring IoT WSN-based applications. Sensors. 2016;16(11):1816.
19. El Jaouhari S, Bouvet E. Secure firmware over-the-air updates for IoT: Survey, challenges, and discussions. Internet of Things. 2022;18:100508.
20. Vaniea K, Rashidi Y. Tales of software updates: The process of updating software. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. 2016. p. 3215–26.
21. Maurushat A, Nguyen K. The legal obligation to provide timely security patching and automatic updates. International Cybersecurity Law Review. 2022;3(2):437–65.
22. Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero trust architecture (ZTA): A comprehensive survey. IEEE Access. 2022;10:57143–79.
23. Chinamanagonda S. Zero trust security models in cloud infrastructure-adoption of zero-trust principles for enhanced security. Academia Nexus Journal. 2022;1(2).
24. Tiwari S, Sarma W, Srivastava A. Integrating artificial intelligence with zero trust architecture: Enhancing adaptive security in modern cyber threat landscape. International Journal of Research and Analytical Reviews. 2022;9:712–28.
25. Stafford V. Zero trust architecture. NIST Special Publication. 2020;800(207):800–7.
26. Chen B, Wan J, Shu L, Li P, Mukherjee M, Yin B. Smart factory of Industry 4.0: Key technologies, application case, and challenges. IEEE Access. 2017;6:6505–19.
27. Shuwandy ML, Zaidan B, Zaidan A, Albahri AS. Sensor-based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review. Journal of Medical Systems. 2019;43(2):33.
28. Petrov S. Patch delivery infrastructure in SCADA systems. 2018.
29. Dhakal S, Jaafar F, Zavarsky P. Private blockchain network for IoT device firmware integrity verification and update. In: 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE). IEEE; 2019. p. 164–70.
30. Azad MA, Arshad J, Mahmoud S, Salah K, Imran M. A privacy-preserving framework for smart context-aware healthcare applications. Transactions on Emerging Telecommunications Technologies. 2022;33(8):e3634.
31. Apthorpe N, Shvartzshnaider Y, Mathur A, Reisman D, Feamster N. Discovering smart home Internet of Things privacy norms using contextual integrity. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2018;2(2):1–23.
32. Sicari S, Rizzardi A, Grieco LA, Piro G, Coen-Porisini A. A policy enforcement framework for Internet of Things applications in the smart health. Smart Health. 2017;3:39–74.
33. Stratikopoulos A. Low overhead & energy-efficient storage path for next-generation computer systems. The University of Manchester (United Kingdom); 2019.