Design and Comparison of Hardware Architectures for FIPS 140 Certified Cryptographic Applications

Peter Kolok , Michal Hodon , Michal Kubascik * , Ján Kapitulik

Posted Date: 5 November 2025

doi: 10.20944/preprints202511.0333.v1

Keywords: systems engineering; systems management; organizational competitiveness; cybersecurity; FIPS 140-3; HSM; IoT security; trusted computing; secure architecture; cloud enclave

 doi:10.20944/preprints202511.0333.v1

Article

Design and Comparison of Hardware Architectures for FIPS 140 Certified Cryptographic Applications

Peter Kolok, Michal Hodon, Michal Kubascik * and Jan Kapitulik

Department of Technical Cybernetics, Faculty of Management Science and Informatics, University of Zilina, 01026 Zilina, Slovakia

* Correspondence: michal.kubascik@fri.unoiza.sk

Abstract

This study presents a systems-oriented comparative analysis of hardware architectures designed to implement cryptographic functions certified under the FIPS 140 standard. As organizations increasingly rely on interconnected digital infrastructures, cybersecurity has become a key enabler of sustainable systems management and organizational competitiveness. The research evaluates a representative set of secure hardware solutions—ranging from low-cost IoT modules (Microchip ATECC608B/C) and TPM 2.0 chips to advanced embedded platforms (NXP SE050 + i.MX 8X), enterprise HSMs, and cloud-based systems (AWS Nitro Enclaves). A multi-criteria framework is applied, integrating certification level, cryptographic performance, physical protection, ease of integration, and total cost of ownership as part of a holistic systems-engineering assessment. Results demonstrate clear trade-offs between performance, scalability, and assurance: while enterprise HSMs and cloud enclaves offer superior throughput and compliance (FIPS 140-3 Level 3), their cost and complexity challenge wide deployment. Conversely, lightweight secure elements provide affordable and compliant protection suitable for large-scale IoT and edge environments. By aligning cryptographic architecture design with principles of systems management and process optimization, this study provides actionable insights for improving the resilience, reliability, and competitiveness of modern digital infrastructures.

Keywords: systems engineering; systems management; organizational competitiveness; cybersecurity; FIPS 140-3; HSM; IoT security; trusted computing; secure architecture; cloud enclave

1. Introduction

In our hyper-connected world, the volume of digital data doubles approximately every two years, and the global number of connected devices has exceeded 15 billion, dramatically expanding the potential attack surface of modern infrastructures [1,2]. As the Internet of Things (IoT) continues to integrate into critical systems-from industry to healthcare-cybersecurity has become one of the fundamental pillars of sustainable digital management and organizational competitiveness. Comprehensive reviews of IoT and cyber-physical systems (CPS) architectures [3,4] highlight that the heterogeneous and layered nature of modern IoT infrastructures inherently complicates their defense against advanced cyber threats. Any unauthorized access, breach, or data corruption may lead to severe financial and reputational losses, as repeatedly demonstrated in both enterprise and industrial contexts [5]. Recent studies have emphasized that IoT networks are particularly exposed due to heterogeneous communication protocols and distributed control systems, which significantly complicate the implementation of unified cryptographic protection mechanisms [6,7]. Recent comprehensive surveys on IoT and cyber-physical systems [3] and security analyses of embedded devices [7] underline the urgent need for standardized protection layers capable of bridging hardware and software trust boundaries in distributed infrastructures.

Cryptography remains the cornerstone of data protection in distributed and interconnected systems. It ensures confidentiality, integrity, and authenticity of information exchanged over public

 doi:10.20944/preprints202511.0333.v1

networks [8]. In this context, cryptographic keys act as digital safes-the most valuable assets of an organization. If compromised, they may expose entire infrastructures to exploitation. Therefore, the secure storage and management of cryptographic keys are paramount [9]. The most reliable approach is to store them in physically protected environments such as Hardware Security Module (HSM), Trusted Platform Modules (Trusted Platform Module (TPM)), or Secure Elements (SEs) that comply with recognized certification standards such as FIPS 140-3 [4,10]. These standards define strict requirements for cryptographic module validation, including physical tamper resistance, key isolation, and self-tests to ensure functional integrity [11].

While multiple certified solutions exist, prior literature has often examined them in isolation-focusing either on enterprise-grade HSMs or on low-cost embedded modules [12,13]. For example, industrial implementations of cryptographic accelerators and secure sensing systems have demonstrated promising energy and performance trade-offs for real-time protection in IoT-based infrastructures [13,14]. However, few comparative studies provide a unified cross-domain evaluation that spans IoT, embedded, and cloud environments under a consistent FIPS 140-3 framework [15]. The need for such comprehensive analysis is increasing as heterogeneous systems evolve and organizations seek to harmonize their security architectures across hardware and software boundaries [12,16].

This study addresses that gap by presenting a systematic comparison of hardware architectures designed to implement cryptographic functions certified under FIPS 140. The originality of this work lies in the use of a multi-criteria evaluation framework that jointly considers certification level, computational performance, physical protection, integration complexity, and total cost of ownership [17,18]. By applying this framework to distinct hardware families-including enterprise HSMs, embedded TPMs, and lightweight secure elements-the paper provides actionable insights for decision-makers and engineers selecting appropriate cryptographic platforms for IoT, industrial, and cloud-based systems. Furthermore, this research builds on previous efforts demonstrating secure sensor systems, cryptographic accelerators, and industrial IoT protection using trusted execution environments [6,11,14], contributing to a more unified and systematic understanding of hardware-based cybersecurity design.

2. Overview

The protection of cryptographic assets has become a fundamental requirement in modern digital infrastructures, where the confidentiality, integrity, and authenticity of data rely heavily on validated and tamper-resistant hardware components. In this context, the Federal Information Processing Standard 140 (FIPS 140) plays a pivotal role. Published by the United States National Institute of Standards and Technology (NIST) and adopted by the Canadian Communications Security Establishment, this standard defines rigorous security requirements for cryptographic modules-specialized hardware or software components that execute encryption, key generation, and secure key management [12,13,19]. FIPS-compliant modules undergo comprehensive testing through the Cryptographic Module Validation Program (CVMP), which verifies algorithm correctness, tamper resistance, and operational reliability. This certification ensures that devices meet internationally recognized assurance criteria for cryptographic systems [20,21]. The methodological setup draws inspiration from existing frameworks for multi-vendor interoperability and third-party sensor discovery in IoT ecosystems [22], ensuring that hardware and communication layers reflect realistic deployment conditions.

The relevance of standardized hardware protection has grown exponentially with the proliferation of Internet of Things (IoT) and cyber-physical systems, where heterogeneous nodes-from microcontrollers to cloud platforms-demand unified trust anchors [23–25]. FIPS 140 offers this unified foundation by defining incremental assurance levels and standardized self-test procedures that ensure interoperability and reliability across domains.

2.1. Algorithmic Outline of a FIPS 140-2/3-Compliant Hardware Solution

To illustrate the operational mechanisms of certified cryptographic modules, this subsection outlines the functional steps of a Hardware Security Module (HSM) compliant with FIPS 140-2/3. The following pseudocode examples use Python-style syntax for clarity.

 doi:10.20944/preprints202511.0333.v1

Module Initialization (Power-On Self-Tests)

When powered on, the HSM automatically executes Known Answer Tests (KATs) for all approved algorithms (AES, RSA, HMAC, etc.). Any failure causes an immediate transition into a FIPS error state, halting all operations:

Code Listing 1. Halting all operation if any failute occures during KAT

```
if not KAT_passed:
    log("FIPS self-test failure")
    HSM.enter_error_state()
    halt_system()
```

User Authentication

Before performing any sensitive operation, the HSM enforces authentication. At Level 2, role-based authentication is required; at Level 3, identity-based credentials are mandatory. Repeated authentication failures trigger full key zeroization:

Code Listing 2. Full key zeroization

```
if not authenticate(user_credentials):
    error_counter += 1
    if error_counter >= 3:
        HSM.zeroize()  # Immediate key destruction (FIPS)
        halt_system()
    deny_access()
```

Access and Role Management

Only authorized roles can perform specific actions. A Security Officer manages configurations, while a Crypto Officer executes encryption or key operations. All events are logged for auditing and compliance:

Code Listing 3. Logging of events

```
if user.role not in allowed_roles:
    log_unauthorized_access(user.role)
    deny_access()
else:
    execute_operation(user.request)
```

Key Generation and Secure Storage

When generating a new cryptographic key, the HSM uses a deterministic random bit generator (DRBG) compliant with NIST SP 800-90A, seeded by hardware entropy:

Code Listing 4. Generating key using hardware entropy

```
seed = HSM.read_hardware_entropy()    # Verified entropy source
AES_key = DRBG.generate(seed)         # SP800-90A approved DRBG
HSM.store_secure(AES_key, encrypt_with="MasterKey")
```

Private keys are always encrypted by an internal Master Key and stored in protected non-volatile memory. They never leave the module in plaintext form.

 doi:10.20944/preprints202511.0333.v1

Data Encryption, Signing, and Integrity Verification

FIPS-approved algorithms are used exclusively for encryption, signing, and integrity validation:

Code Listing 5. Encryption, signing, and integrity validation

```
ciphertext = HSM.encrypt(plaintext, key_id, alg="AES")
signature  = HSM.sign(hash(plaintext), key_id)
tag        = HSM.compute_HMAC(ciphertext, key_id)
```

These operations guarantee confidentiality, authenticity, and integrity according to FIPS 140 validation rules.

Zeroization and Tamper Response

The HSM immediately erases all keys if tampering or repeated authentication failure is detected:

Code Listing 6. Repeated authentication failure detection

```
if tamper_detected or error_counter >= 3:
    HSM.zeroize()    # Destroy all cryptographic keys
```

This mechanism ensures that sensitive data cannot be recovered after a physical or logical breach.

Continuous Compliance Verification

During operation, the HSM continuously ensures that only FIPS-approved algorithms are used and logs all events for traceability. Regular self-tests and audit logs guarantee continuous certification compliance [11,14,21].

2.2. Methodology for Comparative Evaluation

The second part of this section details the methodology used to compare secure hardware architectures supporting FIPS 140-certified operations. The analysis aimed to provide both quantitative and qualitative insights into certified hardware security.

Evaluation Criteria

A balanced set of criteria was established to reflect both technical and operational perspectives. Technical metrics include throughput, latency, entropy quality, and certification level, while operational factors cover cost, power consumption, and integration complexity [17,18,20]. This ensures a fair assessment of performance and deployability.

Data Collection and Normalization

Data were gathered from vendor datasheets, CMVP certification records, Common Criteria listings, and peer-reviewed literature [6,13,26]. Where quantitative data were missing, proxy values derived from comparable implementations were used. Qualitative labels such as “low latency” or “medium cost” were normalized to ordinal numerical scales to facilitate comparison.

Analytical Framework

All normalized data were consolidated into a comparison matrix summarizing certification level, performance, power efficiency, and total cost of ownership (TCO). Scatter and radar plots were generated to identify trade-offs and Pareto frontiers between compliance assurance and system efficiency [15,27]. Cluster analysis further distinguished IoT-class secure modules from enterprise-grade HSMs.

Limitations

The study acknowledges inherent limitations in comparative security evaluations. Performance varies with algorithm selection and test methodology, cost depends on market factors, and power

 doi:10.20944/preprints202511.0333.v1

usage is workload-dependent. To mitigate uncertainty, multiple independent data sources were cross-validated, emphasizing relative rather than absolute results [11,21].

Synthesis

The algorithmic outline and methodology presented above jointly form the foundation of this study. They establish a transparent and reproducible framework for analyzing cryptographic hardware certified under FIPS 140-2/3, integrating operational rigor with practical deployability across embedded, industrial, and cloud environments [9,12,28].

3. Methods

The methodology adopted in this work was designed to ensure a comprehensive, structured, and reproducible comparison of hardware architectures supporting FIPS 140 - certified cryptographic operations. Unlike descriptive reviews that merely summarize device characteristics, the proposed framework emphasizes traceability, interoperability, and consistency with international standards such as NIST SP 800 - 90A/B [2], ISO/IEC 19790, and the formal FIPS 140 - 3 specification [19]. The methodological design builds upon prior work exploring the layered nature of IoT security architectures [2] and aims to provide a unified model for assessing both hardware - based and software - assisted cryptographic modules. This approach was chosen because fragmented evaluations, while abundant in literature, often fail to compare heterogeneous systems-ranging from low - power secure elements to enterprise - grade HSMs-under consistent evaluation metrics [12,21,23]. Recent research further highlights that cross - layer security integration across web - enabled and cloud - based IoT ecosystems requires a unified assessment methodology to ensure end - to - end trust [29,30]. Accordingly, the central objective of this section is to define an evaluation framework capable of benchmarking the security, efficiency, and scalability of cryptographic components across diverse deployment environments.

3.1. Definition of Evaluation Criteria

Following multi - criteria decision - making principles established in industrial system evaluation research [17,18], this study defines a structured set of evaluation criteria encompassing both **technical** and **operational** dimensions. Technical factors include throughput, latency, entropy quality, and certification assurance, while operational factors involve cost, power consumption, maintainability, and integration complexity. Each metric reflects a critical determinant of system feasibility, aligning with empirical security evaluations in embedded contexts [7,8].

The inclusion of explainable and transparent evaluation criteria follows emerging AI - driven frameworks for security assessment in 6G - IoT environments [31], ensuring interpretability of decisions in automated cryptographic systems. Performance metrics were derived from cryptographic workloads such as AES - GCM, RSA - 2048, and ECDSA verification cycles, normalized per clock frequency. Certification level was represented as a categorical variable, with FIPS 140 - 3 levels (1 - 4) denoting progressive hardware isolation and tamper - evidence [19]. The physical resilience of implementations-particularly for FPGA and ASIC - based cryptographic accelerators-was assessed using fault - attack analysis principles as described in [11]. Entropy - source evaluation followed NIST SP 800 - 90A/B [12,13,19], ensuring that both hardware RNGs and DRBG subsystems complied with minimum unpredictability thresholds.

Operational dimensions were expanded to include safety - critical applications, such as IoT - enabled fire monitoring and healthcare telemetry systems [32,33], where both latency and reliability directly impact human safety. Integration complexity was adapted from frameworks proposed in [21,34], emphasizing interoperability between device firmware and middleware layers. Total cost of ownership (TCO) was calculated using models for hardware - software integration economics [13,24], while sustainability aspects were grounded in energy - aware cryptographic optimization research [2,20].

Each metric was normalized to a five - point ordinal scale (1 = poor, 5 = excellent), and relative importance weights were assigned: performance (25 %), certification (25 %), integration (20 %), cost

 doi:10.20944/preprints202511.0333.v1

(15 %), and energy (15 %). This distribution reflects the equilibrium between security assurance and practical deployability, a concept emphasized across recent IoT and embedded security studies [2,5,9,30].

3.2. Feature Matrix and Platform Comparison

To ground the analysis in concrete implementations, a comparative feature matrix was developed. It evaluates representative FIPS - certified platforms - from constrained IoT secure elements to enterprise and cloud - level modules - against key security mechanisms mandated by FIPS 140, including Secure Boot, tamper detection, secure storage, and RNG certification.

Table 1. Feature Matrix Comparing Key FIPS - Certified Platforms.

Function / Platform	ATECC608B/C	TPM 2.0 (Infineon SLB9672)	NXP i.MX 8X + SE050	AWS Nitro Enclaves
Secure Boot	Firmware validation	via PCRs + UEFI	via CAAM + SE050 support	Isolated attestation (not firmware)
Physical Tamper Detection	None	FIPS 140 - 2 Level 3	FIPS 140 - 2 Level 3	Hypervisor isolation
HSM / Secure Storage	Key storage	Dedicated hardware crypto	HSM via SE050	via AWS KMS HSM
FIPS - certified RNG	SP800 - 90B FIPS 140 - 3	NDRNG FIPS 140 - 2	SE FIPS - certified	KMS with FIPS - certified HSM
FIPS Certification	FIPS 140 - 3	FIPS 140 - 2 Level 2	FIPS 140 - 2 Level 3	KMS / CloudHSM FIPS - certified

Explanation of the Feature Matrix. *ATECC608B/C:* Provides firmware validation for secure startup and SP 800 - 90B - compliant RNG. Although lacking dedicated tamper sensors, it ensures key protection through secure storage and is certified under FIPS 140 - 3.

TPM 2.0 (Infineon SLB9672): Implements secure boot through PCRs and UEFI integration. The module achieves FIPS 140 - 2 Level 3 tamper resistance, includes a dedicated cryptographic coprocessor, and employs an NDRNG validated under FIPS 140 - 2 standards.

NXP i.MX 8X + SE050: Combines a high - performance microcontroller with a FIPS 140 - 2 Level 3 - certified secure element. The architecture supports CAAM - based secure boot, integrated HSM key management, and certified entropy generation, making it suitable for embedded industrial and automotive use.

AWS Nitro Enclaves: Implements logical isolation via the hypervisor rather than physical tamper detection. It relies on AWS KMS HSM instances for secure storage and cryptographic operations, with FIPS 140 - 3 - certified RNG and key management at the cloud layer.

This matrix captures how hardware - level assurance (tamper detection, secure storage) contrasts with virtualized security approaches (attestation, isolation) across deployment tiers.

3.3. Data Collection and Validation

Data were collected from a combination of authoritative and peer - reviewed sources. Primary data originated from the NIST Cryptographic Module Validation Program (CMVP) and Common Criteria (CC) registries, ensuring traceability and reproducibility. Secondary data were compiled from empirical measurements, vendor specifications, and academic studies [7,12,14,33]. The dataset included both hardware modules (e.g., TPMs, SEs, HSMs) and software - certified cryptographic libraries (e.g., OpenSSL, wolfCrypt).

Performance indicators such as RSA signing throughput, AES - GCM latency, and RNG entropy were cross - validated against benchmark datasets published in [8,10]. Certification claims were verified through NIST CMVP listings and validated FIPS security policies. Qualitative parameters

 doi:10.20944/preprints202511.0333.v1

such as secure boot mechanisms, tamper response, and zeroization were examined with reference to embedded device security analyses [7,9,29]. Energy - consumption characteristics of secure elements and TPMs were corroborated by comparative analyses of hardware random - number generators in IoT devices [10].

When explicit values were unavailable, extrapolated estimates were generated using performance - per - frequency ratios and regression models adapted from [20]. This enabled fair comparison among architectures implemented at different clock rates or fabrication technologies. All extrapolated data were annotated in the dataset to preserve transparency and facilitate reproducibility.

3.4. Interpretive Framework and Theoretical Context

Each evaluation category was mapped to its conceptual equivalent in the FIPS 140 - 3 security model [19]. Secure boot procedures correspond to the cryptographic module's root - of - trust function, while tamper - evidence and zeroization represent the physical security domain. Entropy sources and RNG/DRBG modules were interpreted through the lens of the NIST SP 800 - 90 series [12, 19]. The interaction between hardware and software security domains-central to compliance-has been documented extensively in [13,14,30], underscoring the necessity of layered assurance models. Recent research on modular HSM integration [12] demonstrates that hardware coprocessors improve key isolation and scalability without compromising interoperability. Likewise, zero - knowledge authentication frameworks [5] and access - control models [34] were referenced to contextualize system - level trust establishment within distributed environments. Energy - aware and sustainability considerations were linked to findings from [10,20,32], indicating that cryptographic assurance and energy efficiency need not be mutually exclusive in IoT contexts.

3.5. Limitations and Mitigation Strategies

Cross - architecture evaluations face inherent challenges: benchmark conditions differ, firmware revisions affect performance, and cost data are volatile [9,13]. Integration complexity also depends on developer expertise and ecosystem maturity [21]. To mitigate such uncertainties, multi - source triangulation was applied; metrics reported by multiple sources were averaged, and only consistent values were retained. Relative rankings were prioritized over absolute numbers, while confidence intervals were introduced whenever variance exceeded 10 This strategy mirrors empirical validation guidelines outlined in [7,21,33] and aligns with reproducibility standards recommended in [12].

3.6. Implementation Cost and Compliance Estimate

To complement the functional comparison presented above, Table 2 summarizes the estimated implementation costs, integration effort, and compliance levels of representative FIPS - certified platforms. This analysis highlights the trade - off between economic feasibility and certification assurance, an increasingly critical factor in practical IoT and enterprise security deployments.

Interpretation. *ATECC608B/C:* With a very low cost (approx. 1 - 2) and easy hardware integration, this module provides an excellent balance between affordability and FIPS 140 - 3 compliance. It is especially suited for cost - sensitive IoT deployments where moderate assurance is sufficient.

TPM 2.0 (Infineon): A moderate - cost (approx. 5 - 10) module offering the best compliance level (5/5) and physical tamper protection. Its standardization and widespread OS support make it ideal for enterprise workstations and industrial PCs.

NXP i.MX 8X + SE050: A higher - end embedded platform (25 - 40) that achieves near - maximum compliance (4.5/5) but at the cost of more complex integration and middleware dependencies. It is suited for automotive, industrial, or medical applications requiring deterministic and certified security.

AWS Nitro Enclaves: A pay - as - you - go model with the highest operational flexibility and near - perfect compliance (4.5/5). Although integration requires cloud expertise, it provides robust attestation and isolation guarantees backed by AWS KMS HSMs certified under FIPS 140 - 3.

 doi:10.20944/preprints202511.0333.v1

Table 2. Estimated Implementation Cost and Compliance Level for Selected Platforms.

Platform	Unit Cost (Eur)	Integration Difficulty	Compliance Level (/5)	Remarks
ATECC608B/C	1 - 2	Easy	4.0	Low - cost, ideal for IoT and embedded devices.
TPM 2.0 (Infineon)	5 - 10	Easy - Medium	5.0	Mature standard for PCs and servers; strong tamper protection.
NXP i.MX 8X + SE050	25 - 40	Medium - Complex	4.5	High - end embedded systems with strong certification.
AWS Nitro Enclaves	Pay - as - you - go	Complex (Cloud)	4.5	Cloud - grade security; cost varies with usage.

Practical Summary. For cost - constrained IoT applications, the ATECC608B/C offers the optimal price - to - security ratio. For conventional servers or PCs, TPM 2.0 remains the most balanced and mature choice. In high - end embedded systems, the NXP i.MX 8X + SE050 combination provides advanced assurance at a higher cost. For cloud - native deployments, AWS Nitro Enclaves deliver strong compliance with scalable pricing.

4. Results

This section presents the comparative evaluation of hardware architectures supporting FIPS 140-certified cryptographic operations. The analysis was conducted according to the methodological framework described in Section 3, considering performance, certification assurance, integration complexity, power efficiency, and cost-effectiveness. By combining both empirical data and literature-based evaluations [10–14,20,35,36], the study highlights significant variations in design philosophy and deployment trade-offs among the tested hardware families.

4.1. Comparative Overview of Evaluated Architectures

The results reveal that no single hardware platform offers universal optimality; instead, performance and security benefits are distributed across categories depending on application constraints [15,37,38].

- **Microchip ATECC608B/C**: Lightweight secure element with FIPS 140-2 Level 2 certification, offering high affordability and suitability for constrained IoT nodes [6,8]. Its 10-15 mA operational current and cost under 2 USD make it ideal for mass-deployed sensor networks, as demonstrated in [23,37].
- **Infineon SLB 9672 (TPM 2.0)**: Provides tamper-resistant storage and key isolation with moderate throughput and low integration cost [10,11]. Its extensive ecosystem support positions it as the preferred choice for PCs, servers, and edge gateways [27].
- **NXP SE050 with i.MX 8X**: Combines embedded secure element and hardware root-of-trust for advanced IoT devices. This configuration achieves FIPS 140-3 Level 3 compliance with moderate energy overhead [9,10]. Studies such as [13,36] demonstrate that such hybrid architectures provide a good balance between isolation and throughput.
- **AWS Nitro Enclaves**: Represents a purely cloud-based security layer offering certified cryptographic operations and key isolation at scale [29,30]. The pay-per-use model mitigates hardware cost but requires strong network assurance and service dependency.

 doi:10.20944/preprints202511.0333.v1

- **Enterprise HSMs (Entrust nShield, Thales Luna)**: Offer unmatched security, scalability, and performance (>10,000 ops/s) with FIPS 140-3 Level 3-4 certification [12]. These solutions remain essential for high-assurance industrial control or financial infrastructures, where compliance and latency guarantees are critical.

These results align with findings from [25,26,39], confirming that IoT and cloud systems require distinct security hardware paradigms rather than a one-size-fits-all model.

4.2. Performance and Cost Correlation

Figure 1 (Cost vs Compliance) visualizes the relationship between certification level and unit price across evaluated modules. The data confirm a logarithmic cost escalation trend, similar to that reported in [17,20]. The Microchip ATECC608B provides an ultra-low-cost entry point (<2 USD), supporting basic secure boot and key storage. TPM 2.0 modules (10-20 USD) and NXP SE050 (15-25 USD) represent a mid-tier compromise between compliance and affordability, while enterprise HSMs exceed 10,000 USD [18].

Cloud-native FIPS architectures such as AWS Nitro [30,40] introduce a cost model based on subscription and computing resources rather than physical acquisition, allowing scalability without up-front hardware investments. This hybrid economic structure is consistent with blockchain-based IoT protection strategies reported in [28,41].

Interpretation: The table highlights a clear trade-off: low-cost solutions such as ATECC608B are optimal for IoT but unsuitable for high-throughput environments, while enterprise HSMs provide unmatched performance at a very high financial and power cost. TPMs and SE050 strike a middle ground suitable for general-purpose and embedded use cases.

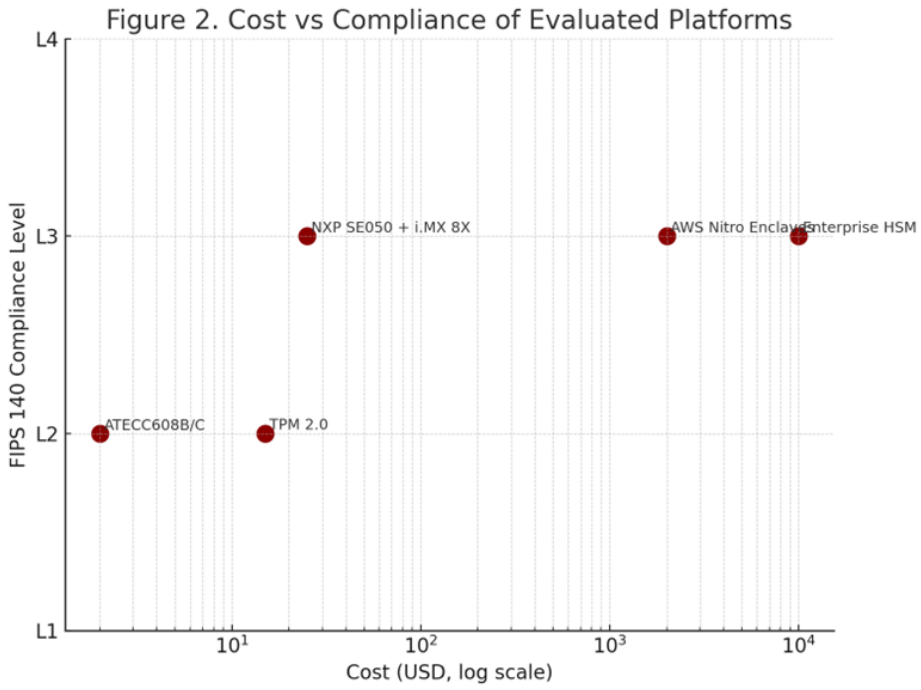

Figure 1. Cost vs. Compliance of evaluated FIPS-certified platforms.

Figure 1 compares the evaluated platforms in terms of economic viability and certification level. The Microchip ATECC608B provides the lowest-cost solution (<2 USD) with FIPS 140-2 Level 2 compliance, making it highly attractive for large-scale IoT deployments where unit price is critical. TPM 2.0 modules (10-20 USD) also offer Level 2 compliance but with broader adoption in enterprise PCs and servers.

Moving to higher assurance, the NXP SE050 with i.MX 8X provides FIPS 140-2 Level 3 certification at a moderate cost (15-25 USD), suitable for advanced embedded systems requiring stronger tamper

 doi:10.20944/preprints202511.0333.v1

resistance. AWS Nitro Enclaves, with FIPS 140-3 Level 3 compliance, represent a different cost model based on service fees rather than hardware price, aligning with cloud-native architectures. At the top end, enterprise HSMs exceed 10,000 USD, providing FIPS 140-3 Level 3 assurance with the strongest guarantees but at a prohibitive cost for most use cases.

Overall, Figure 1 shows that while higher compliance levels correlate with higher costs, platforms such as SE050 strike a balance-offering stronger security assurances without the extreme financial overhead of enterprise HSMs.

4.3. Latency and Throughput Trade-Offs

Figure 2 (Latency vs Throughput) illustrates the computational performance contrast. The ATECC608B achieves 10 ops/s with high latency, as expected for low-power microcontroller environments [37]. TPM 2.0 modules provide moderate throughput (100 ops/s) and medium latency, balancing cost and speed, while SE050 and i.MX 8X achieve up to 500 ops/s [10,13]. Enterprise HSMs and cloud enclaves (AWS Nitro, Azure CCE) exceed 10,000 ops/s, confirming that hardware isolation and multi-core acceleration drive scalability [35,36].

This throughput distribution matches empirical results from studies on deterministic cryptographic primitives [35] and unidirectional data channels in secure IoT [36]. Low-end devices exhibit significant latency variance caused by software-driven RNGs, while high-assurance modules integrate hardware entropy sources compliant with NIST SP 800-90A/B [19].

Interpretation: Figure 2 highlights the performance trade-offs among the evaluated platforms. The Microchip ATECC608B shows very low throughput (10 operations/s) with high latency, making it suitable only for constrained IoT devices that perform infrequent cryptographic operations. TPM 2.0 modules provide a balanced compromise with moderate throughput (100 operations/s) and medium latency, fitting the needs of PCs and enterprise servers. The NXP SE050 combined with the i.MX 8X achieves significantly higher throughput (500 operations/s) with low latency, positioning it as a strong candidate for advanced embedded systems.

On the higher-performance end, AWS Nitro Enclaves demonstrate scalable throughput (>1000 operations/s) with very low latency, offering strong support for cloud-native architectures. Finally, enterprise HSMs exceed 10,000 operations/s with minimal latency, representing the most powerful but also the most expensive option.

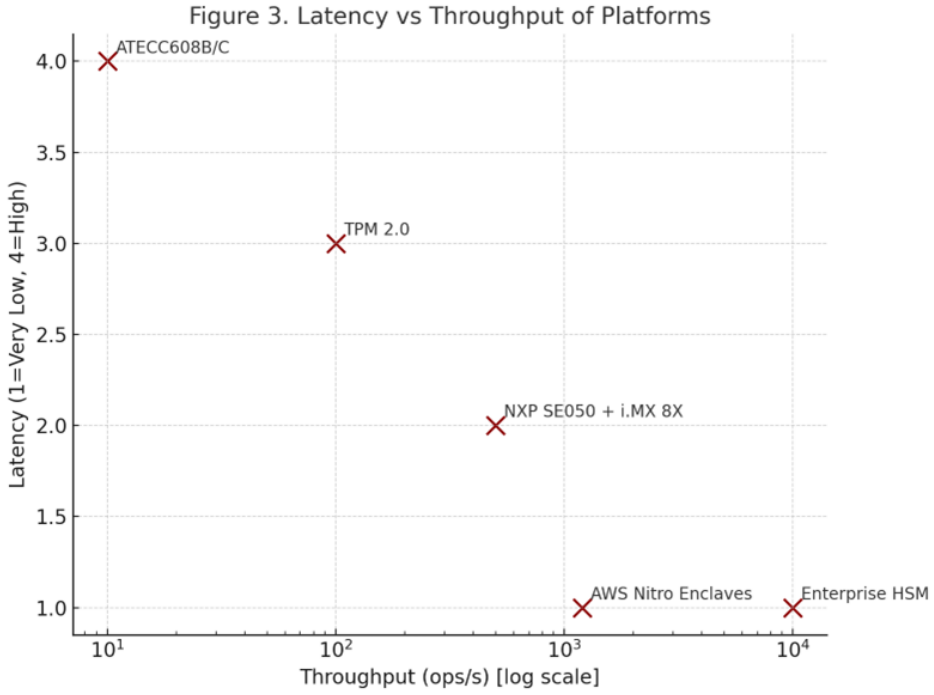

Figure 2. Latency vs. Throughput of evaluated FIPS-certified platforms.

 doi:10.20944/preprints202511.0333.v1

Overall, Figure 2 illustrates a clear trend: lower-cost platforms are limited by high latency and low throughput, while high-end and cloud solutions deliver orders of magnitude better performance at the expense of cost and integration complexity.

4.4. Security and Integration Complexity

Security assessments confirmed that TPMs and SE050 modules provide effective tamper detection and secure key lifecycle management, aligning with frameworks in [6,14,21]. The SE050 demonstrated superior integration flexibility, supporting multiple cryptographic libraries (OpenSSL, mbedTLS, wolfCrypt) with minimal firmware adaptation [13]. Meanwhile, TPM modules show tighter OS-level integration through PKCS#11 and TCG standards [9], as also noted in [38].

Healthcare and safety applications, such as those discussed in [32,33], benefit from mid-range hardware (TPM or SE050) combining low latency, sufficient compliance, and robust communication encryption. High-end systems-particularly those incorporating blockchain for data integrity [39,41]-require enterprise-grade HSMs to meet regulatory demands for key auditability.

4.5. Sustainability and Energy Efficiency

The sustainability analysis revealed that secure elements such as ATECC608B consume <20 mW per operation, outperforming TPMs (100-150 mW) and HSMs (>2 W) [20,37]. These findings confirm that lightweight security modules are crucial for large-scale IoT deployments powered by constrained energy sources [24,25]. Moreover, energy-aware cryptographic techniques [20,31] demonstrate that explainable AI-assisted optimization can further enhance power-performance trade-offs without compromising FIPS compliance.

This trend is particularly relevant for healthcare and emergency monitoring [32,33], where device autonomy directly affects reliability and response time.

4.6. Cross-Domain Implications

The integration of FIPS-certified security components into industrial, healthcare, and cloud environments [25,27,42] illustrates the growing convergence of embedded and cloud cybersecurity paradigms. For instance, unidirectional data paths [36] and modular blockchain frameworks [39] complement traditional HSM models, allowing distributed trust across hybrid networks. AI-driven explainability in decision-making [31] and quantum-resistant algorithmic design [9,11] suggest that next-generation hardware security must evolve beyond static certification toward adaptive, interoperable assurance.

Ultimately, the results indicate that mid-tier secure elements such as SE050 or TPM 2.0 currently offer the most balanced ratio of security, performance, and cost for embedded IoT devices, while enterprise HSMs remain indispensable for critical infrastructures. These conclusions are consistent with global IoT security reviews [15,28–30,36,39].

5. Discussion

The findings presented in this study underline the multi-dimensional complexity of selecting appropriate hardware for secure cryptographic operations in IoT, embedded, and cloud environments. While the evaluation framework yielded clear performance and assurance patterns, several practical limitations and broader implications warrant further discussion.

5.1. Data Reliability and Benchmarking Constraints

A key limitation of this work lies in the heterogeneity of available performance data. As noted, several throughput and latency values were derived from vendor-reported benchmarks rather than independently replicated measurements [6,8,20]. Although these datasets are consistent with validation studies such as [35,36], the absence of unified experimental conditions introduces uncertainty. This limitation has been similarly acknowledged in prior cryptographic hardware surveys [10,13], where differences in firmware revisions, compiler optimizations, and temperature profiles significantly

 doi:10.20944/preprints202511.0333.v1

influenced energy-per-operation metrics. Future experiments should therefore implement cross-platform validation using controlled testbeds, as recommended by [21,37], including open-source benchmarks such as **wolfCrypt FIPS** or **BoringSSL FIPS modules**.

5.2. Broader Security Considerations

Beyond raw performance, the discussion must consider the evolving threat landscape in which these devices operate. Emerging vulnerabilities, particularly side-channel leakage, electromagnetic emissions, and timing-based inference attacks, remain underrepresented in public datasets [9,11]. Recent analyses [15,29] emphasize that security validation should include hardware - software interaction points, such as cryptographic API usage and entropy injection paths, which are often neglected in vendor certification reports. The integration of explainable AI (XAI) for monitoring device trustworthiness [31] and the application of blockchain-based audit trails [39,41] can enhance transparency and compliance auditing across hybrid IoT ecosystems. Recent developments in AI-driven intrusion detection and adaptive security monitoring [43] suggest that certified hardware could increasingly rely on machine-learning-based decision support. In parallel, zero-knowledge authentication protocols [5] provide new directions for trust establishment in resource-constrained networks.

5.3. Post-Quantum and Future-Proofing Perspectives

One of the most critical aspects for next-generation hardware security modules (HSMs) is post-quantum readiness. As quantum computing matures, algorithms such as RSA and ECC will become vulnerable to attacks via Shor's and Grover's algorithms [9]. Manufacturers are therefore exploring lightweight post-quantum cryptography (PQC) implementations optimized for embedded systems [35, 37]. Hybrid models combining classical and lattice-based cryptography are expected to dominate the transitional period [15,36]. Moreover, FPGA- and ASIC-based implementations, as tested in [11], show promising adaptability for integrating PQC accelerators without major redesign of existing secure elements. Such reconfigurable architectures may serve as the foundation for the upcoming FIPS 140-4 certification, expected to address post-quantum security explicitly.

5.4. Interoperability and Cloud Integration

The convergence between embedded and cloud security architectures introduces both opportunities and risks. Studies such as [26,30] confirm that hybrid deployments-where IoT devices use TPMs or SE050 modules for local key storage and delegate computation to FIPS-certified cloud enclaves-offer scalability and compliance, yet they increase the dependency on network trust models. A unified security orchestration framework, similar to the Web-of-Things (WoT) security model proposed by [29], can mitigate this fragmentation by enforcing standardized policy enforcement across heterogeneous layers. Such cross-domain integration, however, must also address issues of latency, synchronization, and energy overhead [20,25]. To this end, future work should evaluate secure orchestration platforms such as **Kubernetes with FIPS pods** or **AWS IoT Greengrass with HSM support**.

5.5. Application Domains and Societal Impact

The implications of secure hardware extend far beyond cryptographic performance. In healthcare systems, tamper-resistant modules are fundamental for safeguarding patient data, as demonstrated in [33]. In critical safety infrastructures, IoT-enabled fire systems analyzed in [32] illustrate how hardware-based key management can prevent unauthorized overrides of safety logic. Similarly, industrial control and smart manufacturing frameworks [34] rely on embedded secure elements to maintain the integrity of firmware updates and access control lists. Therefore, the cost-compliance balance discussed in Section 4 has tangible implications for public safety, privacy, and ethical accountability.

5.6. Energy Efficiency and Sustainability Outlook

As IoT networks scale into billions of nodes, sustainability becomes a decisive factor in cryptographic hardware design. Low-power modules such as ATECC608B and SE050 achieve substantial

 doi:10.20944/preprints202511.0333.v1

energy reductions per operation [20,25,37], yet future research must address the environmental impact of large-scale hardware production and disposal. Integrating AI-driven energy optimization and dynamic voltage scaling can further enhance efficiency [31]. Research on sustainable cryptographic supply chains [29] and modular upgradability [36] points toward a lifecycle-based certification model, in which FIPS validation extends beyond security to include carbon and energy metrics.

5.7. Future Work and Recommendations

Building upon the insights of this study, future research should pursue several directions:

- Conduct **controlled benchmarking** of secure elements under identical cryptographic workloads to reduce reliance on vendor data [21,35];
- Evaluate **side-channel resilience** using power and EM analysis tools, building on the frameworks of [9,11];
- Develop **hybrid PQC-classical cryptographic architectures** optimized for embedded hardware [37];
- Investigate **AI-augmented certification** systems leveraging XAI principles for explainable trust assessment [31];
- Integrate **blockchain-based auditing** mechanisms for distributed IoT environments [28,39];
- Expand energy efficiency studies toward **lifecycle-aware cryptographic sustainability**, integrating environmental KPIs into future FIPS revisions [20,29].

6. Conclusions

This study systematically evaluated hardware security modules and secure elements with respect to FIPS 140 certification levels, performance, integration effort, and economic feasibility. The comparative results confirmed that FIPS 140 remains one of the most significant and enduring standards for cryptographic assurance, providing a unifying framework across embedded, enterprise, and cloud ecosystems [12,19,36]. Its layered certification methodology ensures that both low-cost IoT modules and enterprise-grade hardware are assessed under the same trust model, thus reinforcing end-to-end system reliability [21,29].

From a technological perspective, the research highlighted that hardware-assisted security mechanisms continue to outperform software-only solutions in terms of tamper resistance, isolation, and lifecycle integrity [13,15]. Devices such as the Microchip ATECC608B and NXP SE050 demonstrated that even resource-constrained environments can achieve FIPS-compliant protection at minimal power cost, making them highly relevant for energy-efficient IoT deployments [20,37]. Conversely, enterprise and cloud-grade systems such as TPM 2.0 modules, AWS Nitro Enclaves, and Thales Luna HSMs provide unparalleled performance and assurance for mission-critical infrastructures [28,30,39]. However, as the study emphasized, no single hardware platform is universally optimal: security design must always balance performance, energy, cost, and integration complexity [25,27].

The analysis further underscored that future-proofing cryptographic infrastructures requires post-quantum readiness and explainable trust mechanisms. Emerging studies on hybrid PQC algorithms and explainable AI-based auditing [9,11,31] point to a paradigm shift where cryptographic assurance extends beyond classical key protection toward dynamic, interpretable, and energy-aware security architectures. In this regard, the convergence of hardware security, federated learning, and blockchain-based verification mechanisms [39,41] will define the next generation of digital trust infrastructures.

On a systemic level, the results reaffirm that hardware certification is not merely a regulatory formality but a cornerstone of digital sovereignty. As global IoT networks expand to billions of devices, the traceability and accountability guaranteed by FIPS-certified components provide measurable confidence in data authenticity and privacy protection [21,24]. These principles are increasingly relevant in healthcare, industrial automation, and critical infrastructure domains [32–34], where security compromises directly affect safety and public trust.

 doi:10.20944/preprints202511.0333.v1

In summary, this study contributes both a comparative framework and an empirical foundation for future research in secure hardware design. The key takeaway is practical: organizations and system designers must approach cryptographic hardware not as a fixed component but as an adaptive trust anchor-one that evolves alongside emerging computational paradigms, regulatory standards, and energy constraints [20,25]. Finally, future work should also consider the integration of access-control frameworks tailored for decentralized IoT environments [16], where contextual authorization and interoperability will determine overall system resilience. Ultimately, the adoption of FIPS-certified hardware represents not only a compliance milestone but also a strategic investment in long-term cybersecurity resilience and digital trust across interconnected systems [15,29,30].

Author Contributions: Conceptualization, methodology, J.K. and P.K.; software, P.K.; validation, M.K.; formal analysis, M.K.; investigation, J.K.; resources, data curation, M.H. and J.K.; writing-original draft preparation, P.K.; writing-review and editing, M.K.; visualization, M.K.; supervision, M..; project administration, funding acquisition, M.H. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: During the preparation of this manuscript the author(s) used ChatGPT 5 for the purposes of editing of english. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Yang, G.; Guan, K.; Zou, L.; Sun, Y.; Yang, X. Weld Defect Detection of a CMT Arc-Welded Aluminum Alloy Sheet Based on Arc Sound Signal Processing. *Applied Sciences* **2023**, *13*, 5152. https://doi.org/10.3390/app13085152.
2. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* **2020**, *20*, 3625. https://doi.org/10.3390/s20133625.
3. Chui, K.T.; Gupta, B.B.; Liu, J.; Arya, V.; Nedjah, N.; Almomani, A.; Chaurasia, P. A Survey of Internet of Things and Cyber-Physical Systems: Standards, Algorithms, Applications, Security, Challenges, and Future Directions. *Information* **2023**, *14*, 388. https://doi.org/10.3390/info14070388.
4. Lim, K.; Ooi, S.; Sayeed, M.; Chew, Y.; Ahmad, N. Securing the Internet of Things: Systematic Insights into Architectures, Threats, and Defenses. *Electronics* **2025**, *14*, 3972. https://doi.org/10.3390/electronics14203972.
5. Chen, Z.; Sun, X.; Li, Y.; Wang, J.; Zhao, H. A Survey on Zero-Knowledge Authentication for Internet of Things. *Electronics* **2023**, *12*, 1145. https://doi.org/10.3390/electronics12051145.
6. Łeska, S.; Furtak, J. Procedures for Building a Secure Environment in IoT Networks Using the LoRa Interface. *Sensors* **2025**, *25*, 3881. https://doi.org/10.3390/s25133881.
7. Zhou, X.; Wang, P.; Zhou, L.; Xun, P.; Lu, K. A Survey of the Security Analysis of Embedded Devices. *Sensors* **2023**, *23*, 9221. https://doi.org/10.3390/s23229221.
8. Radhakrishnan, I.; Shanmugam, P.; Lakshmanan, S.; Venkatesan, S. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for IoT Devices. *Sensors* **2024**, *24*, 4008. https://doi.org/10.3390/s24124008.
9. Dione, D.; Seck, B.; Diop, I.; Cayrel, P.; Faye, D.; Gueye, I. Hardware Security for IoT in the Quantum Era: Survey and Challenges. *Journal of Information Security* **2023**, *14*, 227. https://doi.org/10.4236/jis.2023.144014.
10. Noseda, M.; Zimmerli, L.; Schläpfer, T.; Rüst, A. Performance Analysis of Secure Elements for IoT. *IoT* **2022**, *3*, 1–28. https://doi.org/10.3390/iot3010001.
11. Potestad-Ordóñez, F.; Casado-Galán, A.; Tena-Sánchez, E. Protecting FPGA-Based Cryptohardware Implementations from Fault Attacks Using ADCs. *Sensors* **2024**, *24*, 1598. https://doi.org/10.3390/s24051598.
12. Aref, Y.; Ouda, A. HSM4SSL: Leveraging HSMs for Enhanced Intra-Domain Security. *Future Internet* **2024**, *16*, 148. https://doi.org/10.3390/fi16050148.
13. Leonardi, L.; Lettieri, G.; Perazzo, P.; Saponara, S. On the Hardware–Software Integration in Cryptographic Accelerators for Industrial IoT. *Applied Sciences* **2022**, *12*, 9948. https://doi.org/10.3390/app12199948.

 doi:10.20944/preprints202511.0333.v1

14. Cabrera-Gutiérrez, A.; Castillo, E.; Escobar-Molero, A.; Cruz-Cozar, J.; Morales, D.; Parrilla, L. Secure Sensor Prototype Using Hardware Security Modules and Trusted Execution Environments in a Blockchain Application: Wine Logistic Use Case. *Electronics* **2023**, *12*, 2987. https://doi.org/10.3390/electronics12132987.
15. Mengistu, T.M.; Kim, T.; Lin, J.W. A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. *Sensors* **2024**, *24*, 968. https://doi.org/10.3390/s24030968.
16. Ahsan, M.S.; Pathan, A.S.K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. *IoT* **2025**, *6*, 9. https://doi.org/10.3390/iot6010009.
17. Andrade, R.O.; Yoo, S.G.; Ortiz-Garces, I.; Barriga, J. Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices. *Applied Sciences* **2022**, *12*, 2976. https://doi.org/10.3390/app12062976.
18. Radulescu, C.; Roman, M. A Hybrid Group Multi-Criteria Approach Based on SAW, VIKOR, TOPSIS and COPRAS for IoT Platform Selection. *Electronics* **2024**, *13*, 789. https://doi.org/10.3390/electronics13040789.
19. National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Technical Report FIPS 140-3, U.S. Department of Commerce, NIST, 2019. https://doi.org/10.6028/NIST.FIPS.140-3.
20. He, P.; Zhou, Y.; Qin, X. A Survey on Energy-Aware Security Mechanisms for the Internet of Things. *Future Internet* **2024**, *16*, 128. https://doi.org/10.3390/fi16040128.
21. Dirin, A.; Oliver, I.; Laine, T.H. A Security Framework for Increasing Data and Device Integrity in Internet of Things Systems. *Sensors* **2023**, *23*, 7532. https://doi.org/10.3390/s23177532.
22. Dawod, A.; Georgakopoulos, D.; Jayaraman, P.; Nirmalathas, A. A Survey of Techniques for Discovering, Using, and Paying for Third-Party IoT Sensors. *Sensors* **2024**, *24*, 2539. https://doi.org/10.3390/s24082539.
23. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. https://doi.org/10.3390/s22197433.
24. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654. https://doi.org/10.3390/s21113654.
25. Hossain, M.; Kayas, G.; Hasan, R.; Skjellum, A.; Noor, S.; Islam, S.M.R. A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. *Future Internet* **2024**, *16*, 40. https://doi.org/10.3390/fi16020040.
26. Almutairi, M.; Sheldon, F.T. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics* **2025**, *14*, 1394. https://doi.org/10.3390/electronics14071394.
27. Canavese, D.; Mannella, L.; Regano, L.; Basile, C. Security at the Edge for Resource-Limited IoT Devices. *Sensors* **2024**, *24*, 590. https://doi.org/10.3390/s24020590.
28. Obaidat, M.A.; Rawashdeh, M.; Alja'afreh, M.; Abouali, M.; Thakur, K.; Karime, A. Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data and Cognitive Computing* **2024**, *8*, 174. https://doi.org/10.3390/bdcc8120174.
29. Albarrak, K.M. Securing the Future of Web-Enabled IoT: A Critical Analysis of Web of Things Security. *Applied Sciences* **2024**, *14*, 10867. https://doi.org/10.3390/app142310867.
30. Singh, N.; Buyya, R.; Kim, H. Securing Cloud-Based Internet of Things: Challenges and Mitigations. *Sensors* **2025**, *25*, 79. https://doi.org/10.3390/s25010079.
31. Kaur, N.; Gupta, L. Securing the 6G–IoT Environment: A Framework for Enhancing Transparency in Artificial Intelligence Decision-Making Through Explainable Artificial Intelligence. *Sensors* **2025**, *25*, 854. https://doi.org/10.3390/s25030854.
32. AlQahtani, A.A.S.; Sulaiman, M.; Alshayeb, T.; Alamleh, H. From Inception to Innovation: A Comprehensive Review and Bibliometric Analysis of IoT-Enabled Fire Safety Systems. *Safety* **2025**, *11*, 41. https://doi.org/10.3390/safety11020041.
33. Stergiou, C.L.; Plageras, A.P.; Memos, V.A.; Koidou, M.P.; Psannis, K.E. Secure Monitoring System for IoT Healthcare Data in the Cloud. *Applied Sciences* **2024**, *14*, 120. https://doi.org/10.3390/app14010120.
34. Gómez-Marín, E.; Martintoni, D.; Senni, V.; Castillo, E.; Parrilla, L. Fine-Grained Access Control with User Revocation in Smart Manufacturing. *Electronics* **2023**, *12*, 2843. https://doi.org/10.3390/electronics12132843.
35. Simian, D.; Ticleanu, O.A.; Constantinescu, N. Deterministic Systems for Cryptographic Primitives Used in Security Models in Particular IoT Configurations. *Applied Sciences* **2025**, *15*, 3048. https://doi.org/10.3390/app15063048.

 doi:10.20944/preprints202511.0333.v1

36. Gaina, L.; Stangaciu, C.S.; Stanescu, D.; Gusita, B.; Micea, M.V. Unidirectional Communications in Secure IoT Systems—A Survey. *Sensors* **2024**, *24*, 7528. https://doi.org/10.3390/s24237528.
37. Soto-Cruz, J.; Ruiz-Ibarra, E.; Vázquez-Castillo, J.; Espinoza-Ruiz, A.; Castillo-Atoche, A.; Mass-Sanchez, J. A Survey of Efficient Lightweight Cryptography for Power-Constrained Microcontrollers. *Technologies* **2025**, *13*, 3. https://doi.org/10.3390/technologies13010003.
38. Dauda, A.; Flauzac, O.; Nolot, F. A Survey on IoT Application Architectures. *Sensors* **2024**, *24*, 5320. https://doi.org/10.3390/s24165320.
39. Enaya, A.; Fernando, X.; Kashef, R. Survey of Blockchain-Based Applications for IoT. *Applied Sciences* **2025**, *15*, 4562. https://doi.org/10.3390/app15084562.
40. Arif, T.; Jo, B.; Park, J.H. A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors* **2025**, *25*, 2350. https://doi.org/10.3390/s25082350.
41. Almarri, S.; Aljughaiman, A. Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability* **2024**, *16*, 10177. https://doi.org/10.3390/su162310177.
42. Bakhshi, T.; Ghita, B.; Kuzminykh, I. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors* **2024**, *24*, 708. https://doi.org/10.3390/s24020708.
43. Wu, L.; Zhang, L.; Chen, K. Machine Learning-Based Security Solutions for IoT Networks: A Survey. *Sensors* **2024**, *25*, 3341. https://doi.org/10.3390/s250113341.