UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1328

DOI: https://doi.org/10.14483/22487638.23671

REVISIÓN

Advances in the security of embedded systems in electronics: a systematic review of techniques and trends

Avances en la seguridad de los sistemas embebidos en electrónica: una revisión sistemática de técnicas y tendencias

Maria Alejandra Ortiz Salazar [1], Heriberto Fernando Vargas Losada [2], Alejandro G. Jurado Mejía [3]

Fecha de Recepción: 31 de mayo de 2025 **Fecha de Aceptación**: 24 de septiembre de 2026

Cómo citar: M. A. Ortiz-Salazar, H.F, Vargas Losada y A.G. Jurado Mejía, «Advances in the security of embedded systems in electronics: a systematic review of techniques and trends», *Tecnura*, vol. 30, n.° 90, oct. 2026. 4–37. https://doi.org/10.14483/22487638.23671

Abstract

Introduction: Security in embedded systems has become increasingly important owing to their integration into critical applications such as the Internet of Things (IoT), cyber-physical systems (CPS), and industrial infrastructures like smart grids.
Objective: This systematic review aims to provide a comprehensive analysis of recent literature on the security of embedded electronic systems, focusing on the evolution of security techniques, emerging trends in vulnerability mitigation, persistent vulnerabilities, and the impact of resource constraints on the implementation of security mechanisms in domains such as IoT, CPS, automotive systems, medical devices, and telecommunications.
Methodology: A primary search was conducted in Scopus and supplemented by searches in ScienceDirect (Elsevier) and SpringerLink, with inclusion and exclusion criteria applied in accordance with the PRISMA guidelines. After screening, eligibility assessment, and removal of cross-database duplicates, 53 studies were included in the review: 50 from Scopus, 2 from ScienceDirect, and 1 from SpringerLink.
Results: The findings reveal significant growth in the development of defensive methods that balance energy efficiency and resilience against attacks, particularly in resource-constrained environments such as IoT devices and CPS. Furthermore, advances in lightweight cryptography, authentication techniques, and hardware-assisted protection measures, including Physically Unclonable Functions (PUFs) and the integration of Trusted Platform Modules (TPMs), are highlighted.
Conclusions: These findings underscore the critical need for continued innovation in this field to address both cyber and physical threats in increasingly complex applications.
Keywords: Embedded systems, architectures, energy efficiency, industrial applications, development tools, hardware-software integration.

1 Ingeniera de sistemas de Universidad de la Amazonía. Miembro de GIECOM. Email: mariaal.ortiz@udla.edu.co
2 Ingeniero de sistemas y Docente de la Facultad de Ingeniería de la Universidad de la Amazonía. Miembro de GIECOM. Email: heri.vargas@udla.edu.co
3 Ingeniero de alimentos y docente Docente de la Facultad de Ingeniería de la Universidad de la Amazonía. Miembro de GIECOM. Email: a.jurado@udla.edu.co

Resumen

Introducción: La seguridad en los sistemas embebidos ha cobrado creciente importancia debido a su integración en aplicaciones críticas, como el Internet de las Cosas (IoT), los sistemas ciberfísicos (CPS) y las infraestructuras industriales como las redes inteligentes.
Objetivo: Esta revisión sistemática analiza de manera integral la literatura reciente sobre la seguridad en sistemas electrónicos embebidos, con énfasis en la evolución de las técnicas de seguridad, las tendencias emergentes en la mitigación de vulnerabilidades, las vulnerabilidades persistentes y la influencia de las limitaciones de recursos en la implementación de mecanismos de protección en ámbitos como IoT, sistemas automotrices, dispositivos médicos y telecomunicaciones.
Metodología: Se condujo una búsqueda principal en Scopus y búsquedas complementarias en ScienceDirect (Elsevier) y SpringerLink, aplicando criterios de inclusión y exclusión conforme a las directrices metodológicas PRISMA. Tras el cribado, la evaluación de elegibilidad y la depuración de duplicados, se seleccionaron 53 estudios (50 de Scopus, 2 de ScienceDirect y 1 de SpringerLink).
Resultados: Los hallazgos revelan un crecimiento significativo en el desarrollo de métodos defensivos que equilibran la eficiencia energética y la resiliencia frente a ataques, en particular en entornos con restricciones de recursos como dispositivos IoT y CPS. Asimismo, se destacan los avances en criptografía ligera, técnicas de autenticación y medidas de protección asistidas por hardware, tales como las Funciones Físicamente No Clonables (PUF) y la integración de Módulos de Plataforma Confiable (TPM).
Conclusiones: Lo anterior subraya la necesidad crítica de una innovación continua en este campo para mitigar de manera integral las amenazas cibernéticas y físicas en escenarios de aplicación cada vez más complejos.
Palabras clave: Sistemas embebidos, arquitecturas, eficiencia energética, aplicaciones industriales, herramientas de desarrollo, integración hardware-software.

Introduction

Embedded systems have become a fundamental component in various industrial applications, ranging from the automotive sector to medical devices and power grid automation. These systems, operating autonomously and continuously, are essential for the functioning of critical infrastructures and have found fertile ground for expansion in the Internet of Things (IoT) and cyber-physical systems (CPS). However, their connectivity and limited resources make them attractive targets for various attacks, both cyber and physical. The growing reliance on these systems in industry and society poses a significant challenge: how to ensure the security of these devices given their limited processing and storage capacities.

The integration of embedded systems in sensitive applications has increased threats to their security. Among these threats are Advanced Persistent Threats (APT), Laser Fault Injection Attacks (LFIA), and flash memory manipulation, all of which can compromise the integrity and availability of these devices. These threats demand the implementation of innovative security techniques that are not only effective but also compatible with the power and resource constraints of these systems. In this context, extensive research has been conducted to develop solutions ranging from lightweight cryptography and hardware-based authentication to advanced sensors and Physically Unclonable Functions (PUF) for generating unique identities.

The objective of this systematic review is to comprehensively analyze recent literature on security in embedded electronic systems, focusing on the evolution of security techniques, emerging trends in vulnerability mitigation, persistent vulnerabilities, and the influence of resource constraints on the implementation of security mechanisms in applications such as IoT, cyber-physical systems, automotive systems, medical devices, and telecommunications.

This article begins by detailing the search and study selection methodology, followed by the results of the review and a discussion on emerging trends in embedded system protection against cyber threats. Finally, recommendations and conclusions are presented, focusing on the application of these techniques in critical sectors such as IoT, CPS, and industrial infrastructures.

Methodology

Objective: The objective of this systematic review is to comprehensively analyze recent literature on security in embedded electronic systems, focusing on the evolution of security techniques, emerging trends in vulnerability mitigation, persistent vulnerabilities, and the influence of resource constraints on the implementation of security mechanisms in applications such as IoT, cyber-physical systems, automotive systems, medical devices, and telecommunications.

Search Expression: ("embedded system" OR "embedded device") AND ("security" OR "cybersecurity" OR "vulnerab" OR "attack" OR "threat")

Research Questions: The research questions guiding this review are presented in Table 1. They focus on the security techniques used in embedded electronic systems and their evolution, emerging trends in protection against cyber threats, the effect of processing power and memory limitations on the implementation of security mechanisms, and persistent vulnerabilities along with the mitigation strategies reported as effective in the reviewed literature.

Table 1. *Research questions*

Id	Questions
P1	What are some of the security techniques used in embedded systems in electronics, and how have they evolved in recent years?
P2	What emerging trends have been identified in protecting embedded systems against cyber threats?
P3	How do resource limitations (such as processing power and memory) affect the implementation of security techniques in embedded systems?
P4	What common vulnerabilities persist in embedded systems, and which strategies have proven most effective in mitigating them?

Source: authors

Inclusion and Exclusion Criteria:

To ensure the relevance and quality of the studies selected in this review, I established clear inclusion and exclusion criteria. The inclusion criteria, shown in Table 2, focused on ensuring that the articles were relevant to the topic of embedded systems in electronics, published between 2014 and 2024, and available in English or Spanish. This allowed for the incorporation of the most recent and relevant technological advancements in the field.

Table 2. *Inclusion criteria*

Theme	Inclusion
Thematic relevance	Articles focused on embedded systems, architecture, applications, and development in the field of electronics.
Publication date	Studies were published between 2014 and 2024 to ensure the inclusion of current technologies and developments within the defined review period.
Language	Publications in English or Spanish, as these are the predominant languages in scientific and technical literature.
Availability	Studies with full-text access or sufficiently detailed abstracts to assess research quality.

Source: authors

On the other hand, the exclusion criteria, shown in Table 3, were applied to discard studies that did not offer an in-depth analysis of embedded systems, those without peer review, or those from non-scientific sources, as well as research dealing with obsolete technologies. These filters ensure that only high-quality and current sources are included, aligning with the objectives of this review.

Table 3. *Exclusion criteria*

Theme	Exclusion
Lack of thematic focus	Studies that do not specifically focus on embedded systems or only mention the topic superficially without contributing to an in-depth analysis.
Lack of peer review	Studies from blogs, forums, non-peer-reviewed websites, or publications lacking scientific rigor.
Outdated studies	Research presenting obsolete technologies or developments no longer relevant to current embedded systems applications and advancements.

Source: authors

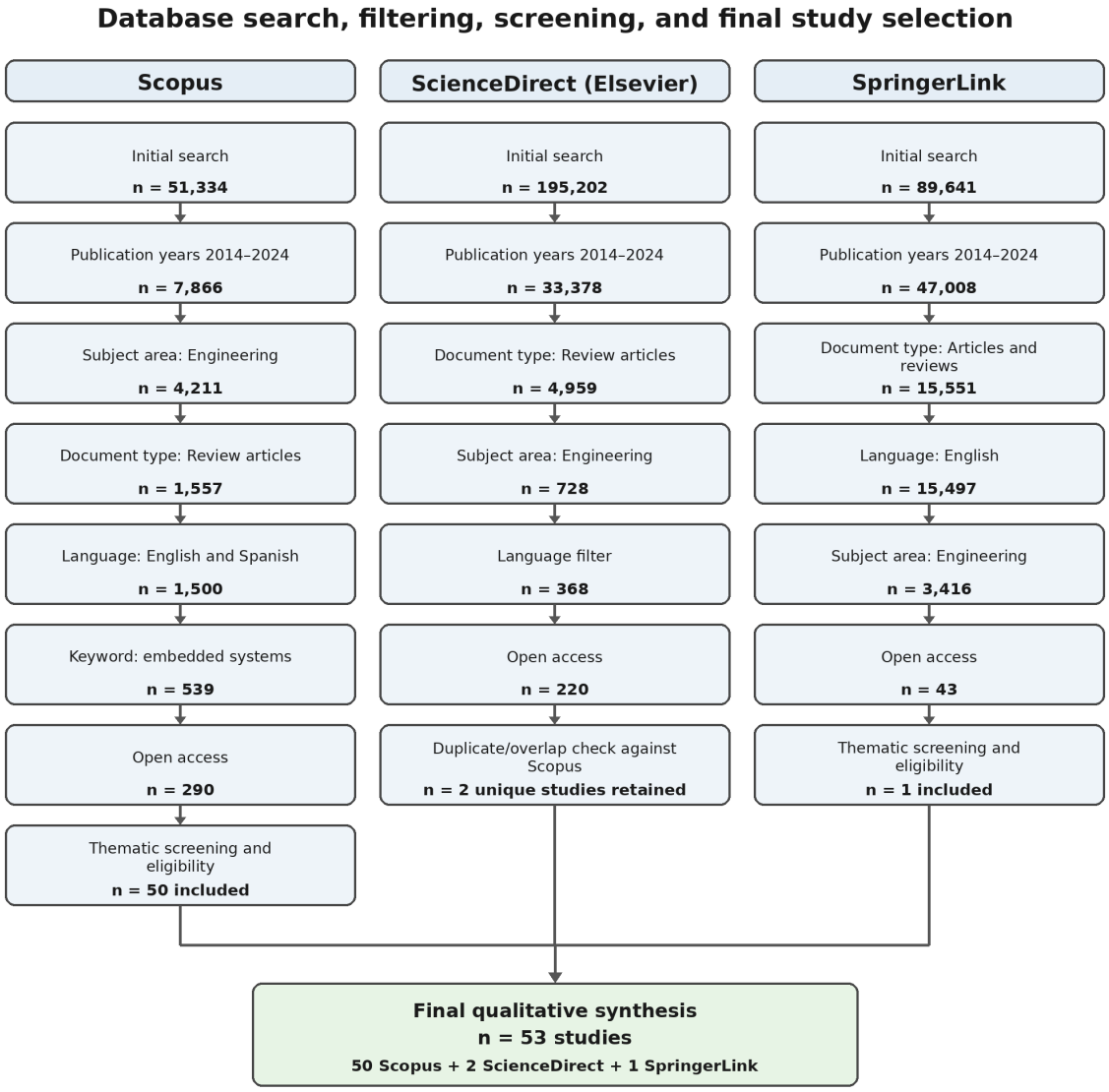
Selection of articles:

The systematic search began in Scopus using the expression ("Embedded system" OR "embedded device") AND ("security" OR "cybersecurity" OR "vulnerab" OR "attack" OR "threat"), which returned 51,334 records. The publication-year filter (2014–2024) reduced this set to 7,866 records. Limiting the results to the Engineering subject area produced 4,211 records, and selecting review articles reduced the total to 1,557. The language filter (English and Spanish) resulted in 1,500 records. The keyword "embedded systems" was then applied, leaving 539 records, and the open-access filter reduced the set to 290. These records were screened according to the inclusion and exclusion criteria in Tables 2 and 3; studies that did not contribute directly to the research topic or did not provide sufficient relevant information were excluded. After this screening and eligibility assessment, 50 Scopus studies were retained.

Complementary searches were conducted in ScienceDirect (Elsevier) and SpringerLink. ScienceDirect initially returned 195,202 results; restricting the period to 2014–2024 reduced the set to 33,378, the review-article filter to 4,959, the Engineering subject-area filter to 728, the language filter to 368, and the open-access filter to 220. After checking for duplication and overlapping with the studies already identified in Scopus, 2 unique studies were retained. In SpringerLink, the search expression returned 89,641 results. Restricting the period to 2014–2024 yielded 47,008 records; selecting articles and review articles reduced the set to 15,551; the English-language filter reduced it to 15,497; the Engineering filter to 3,416; and the open-access filter to 43. After thematic screening, records that did not directly address the research topic were excluded, and 1 study was retained. The final qualitative synthesis therefore comprised 53 studies: 50 from Scopus, 2 from ScienceDirect, and 1 from SpringerLink, as summarized in Graph 1.

290 records remaining after applying database filters in Scopus
263 records identified after applying database filters to complementary sources (220 ScienceDirect + 43 SpringerLink)
53 studies included in the final qualitative synthesis (50 Scopus + 2 ScienceDirect + 1 SpringerLink)

Figure 1. PRISMA



Source: authors

Evolution of Security Techniques in Embedded Systems

In embedded electronic systems, security has evolved significantly to address rising threats across applications such as IoT networks, wireless communication systems, and cyber-physical environments, including 3D printing and modular multilevel converters (M2C) in power grids. In the case of M2C systems, these environments combine a cyber layer for data exchange among sensors and controllers with a physical layer where semiconductor devices are managed. However, this dependence on a cyber-physical system (CPS) structure exposes them to false data injection attacks (FDIA), in which attackers

intercept and manipulate data to send incorrect information to the control system. To counteract this vulnerability, FDIA detectors have been developed using advanced techniques like reinforcement learning, which enables the identification and mitigation of specific attacks on submodules [2].

Another notable evolution in embedded system security is the adoption of hardware-assisted measures to counter code reuse attacks, balancing protection with resource efficiency. A prominent example is the shadow stack mechanism, which validates return addresses in real-time to maintain control flow integrity, significantly reducing the impact on system performance. Additionally, lightweight stream ciphers are used to secure critical data without overloading system resources [3].

The need for secure communication has driven the use of lightweight cryptography, such as the CLEFIA cipher, which is designed for resource-constrained environments. Recognized within ISO/IEC lightweight cryptography standards, CLEFIA provides an efficient and secure structure through a generalized Feistel network, minimizing space requirements and enhancing resilience against attacks. This is particularly effective in IoT and automotive applications [4].

In wireless networks and IoT applications, embedded systems have adopted advanced identification mechanisms to counter pseudobase stations (BS), illegal devices that exploit vulnerabilities in 5G networks to intercept or manipulate communications. New techniques, such as the Signal Echoing Protocol (SEP), allow devices to accurately detect BS imposters regardless of their location, improving detection accuracy for mobile threats [5].

Finally, the convergence of Information Technology (IT) and Operational Technology (OT) in power grids has exposed embedded systems to new threats, especially when using communication protocols like IEC-61850 GOOSE. Although this protocol supports efficient grid operations, its lack of encryption makes it vulnerable to cyberattacks. Recent studies have evaluated the security of GOOSE hardware implementations, emphasizing the importance of response protocols and additional security measures, such as encryption, in future designs [6].

The evolution of security techniques in embedded systems recently reflects the growing complexity and integration of these systems across various applications, from critical infrastructure to consumer devices. Key advancements have centered on enhancing authentication, protecting data integrity, and increasing resilience against potential attacks, particularly in IoT environments where security and efficiency are paramount.

One significant development is the integration of Trusted Platform Module (TPM) technology into IoT devices. In critical infrastructure like smart grids, this hardware-based security approach, exemplified by the "Fortified-Grid" system, uses TPM for attestation and X.509 certificates for authentication and

integrity verification. By embedding TPM, devices can attest to their operational state, reinforcing trust and reducing vulnerabilities to potential grid failures. Formal security verification using the Random Oracle (ROR) model and the AVISPA tool has further validated the effectiveness of these methods, underscoring a trend toward hardware-assisted, formally verified security in interconnected systems like smart grids [7].

Alongside TPM advancements, the increasing adoption of open hardware platforms such as RISC-V is enabling tailored security solutions that address embedded system vulnerabilities with minimal performance trade-offs. RISC-V's customizable architecture supports innovations like pre-execution memory validation, information obfuscation, and post-execution corruption detection, providing a low-overhead, efficient approach to countering software vulnerabilities. This hardware-centric approach is evolving to address complex threats, such as intra-object overflows, with future research focusing on enhancing resilience and standardizing security evaluation [8].

In safety-critical applications like railway systems, where embedded systems often integrate Commercial Off-The-Shelf (COTS) components, new security techniques are adapting to balance the need for safety and cost-effectiveness. Systems like Rete Ferroviaria Italiana's Remote Worker Dashboard (RWD) integrate COTS mobile devices with existing interlocking railway infrastructure, ensuring safety through a controlled cyber-physical environment compliant with CENELEC standards. This approach enables real-time, responsive security while maintaining rigorous safety standards through advanced verification and validation, reflecting a trend in embedded systems where cyber-physical integration is key to secure, functional operations in mixed technology environments [9].

Further addressing IoT security, advancements in lightweight cryptographic processors, such as the RECO-ASCON processor, emphasize low power consumption and adaptability across different hardware platforms. Supporting cryptographic Hash and ASCON algorithms, RECO-ASCON can achieve high operational frequencies and parallel processing capabilities, which are vital for IoT security. This processor's reconfigurable design allows it to balance energy efficiency with robust security, making it suitable for evolving IoT needs where both resource constraints and security threats are significant [10].

Finally, with the rise of 3D printing and additive manufacturing, embedded systems leveraging the Controller Area Network (CAN) have gained popularity for their plug-and-play capabilities. However, this shift has introduced security risks due to CAN's shared communication bus, which is vulnerable to spoofing and unauthorized data access. Recent security strategies to mitigate these vulnerabilities include anomaly detection, CAN packet encryption, and node isolation, which collectively aim to preserve data integrity and prevent unauthorized control, crucial for ensuring safe operation in industrial and consumer applications [11].

Embedded systems have experienced a significant increase in security challenges, driving the development and evolution of various techniques to mitigate both cyber and physical risks. Below are some of the main security techniques that have emerged in recent years and how they have evolved to face the growing threats in this field.

Advanced Persistent Threats (APT), known for their stealthy and targeted approach, represent a considerable threat to critical infrastructures like power grids. Notable examples include the Stuxnet attacks and the manipulation of Ukraine's power grid. To mitigate this type of attack, new defenses have been implemented in electrical substations, extending the kill chain in Industrial Control Systems (ICS) to address both the digital and physical aspects of Cyber-Physical Systems (CPS) [12].

Physical attacks, such as Laser Fault Injection Attacks (LFIA), which allow attackers to manipulate circuits with high precision, have driven the development of advanced digital sensors. New sensors based on time-to-digital converters (TDC) have proven effective in detecting these faults under various conditions, improving the physical security of embedded systems and providing a more efficient solution against physical attacks [13].

The flash memory erasure suppression attack exploits vulnerabilities in microcontrollers by interrupting the memory erasure process, allowing access to protected data. Since it is difficult to implement software solutions once a device is compromised, it is proposed to select microcontrollers with integrated hardware countermeasures to prevent this type of attack and protect critical data [14].

Cyber-physical systems (CPS), which integrate digital and physical systems, require a broader security approach due to their increasing complexity and connectivity. Runtime enforcement (RE) has become a key technique to prevent systems from being compromised. This technique allows multiple security policies to be applied in parallel, reducing reliance on vulnerable software layers and improving the real-time protection of critical industrial systems [15].

This need for enhanced protection has also driven defensive advances against Advanced Persistent Threats (APTs) in power grids, such as extending the ICS kill chain to address both digital and physical components in CPS [12], and physical security improvements using sensors to detect Laser Fault Injection Attacks (LFIA) via time-to-digital converters [13]. To address memory vulnerabilities, microcontrollers with built-in hardware defenses against flash memory erasure suppression attacks are now preferred for safeguarding critical data [14]. In CPS, runtime enforcement allows simultaneous policy enforcement across software layers, reducing compromise risks [15], while in smart grids, IEC 62351 standards, including geometric authentication methods, have enabled encryption without specialized hardware to meet stringent timing requirements [22].

In the context of the Internet of Things (IoT), embedded devices are often vulnerable due to their limited resources. Physically Unclonable Functions (PUFs) have proven to be an effective solution for providing unique and secure identities to these devices. The integration of PUFs into the RIOT operating system enhances the security of IoT devices without requiring additional hardware, efficiently generating secure keys [17].

CAN-based systems (Controller Area Networks), common in industrial applications, present vulnerabilities that allow for data manipulation and the injection of dangerous commands. Techniques used to mitigate these attacks include network traffic authentication and the implementation of security controls. In IoT environments, Physically Unclonable Functions (PUFs) embedded in the RIOT operating system provide device-specific identities and support secure key generation without requiring additional hardware. Furthermore, in deep-learning applications, voltage over scaling techniques offer a lightweight defense against adversarial attacks while reducing energy use without requiring hardware or software modifications [18].

These advances, along with improvements in cryptography and energy efficiency, have been fundamental for the evolution of embedded systems, supporting more complex and secure applications in areas such as healthcare, home automation, and other sensitive sectors.

Emerging Trends in the Protection of Embedded Systems Against Cyber Threats

Currently, embedded systems face a growing number of cyber threats due to their integration into critical infrastructures and increasing connectivity. As threats evolve, so do the protection strategies. Below are some of the most relevant emerging trends in the protection of these systems:

Protection Against Advanced Persistent Threats (APT) Advanced Persistent Threats (APT), such as the attacks on Ukraine's power grids or the Stuxnet virus, represent one of the most serious threats to embedded systems in critical infrastructure. These attacks, which unfold stealthily and in multiple phases, require sophisticated defenses. An emerging approach is the use of Hardware-in-the-Loop (HIL) simulation to test control protocols in electrical substations. This approach helps identify vulnerabilities in control systems (IEC 60870-5-104 and IEC 61850) and improve security in Cyber-Physical Systems (CPS) [12].

Emerging trends in protecting embedded systems against cyber threats include using real-time hybrid neuromorphic frameworks that leverage event-based cameras for object tracking and classification. Given the computationally intensive demands of deep learning at the edge, this solution focuses on enhancing energy efficiency in low-power embedded platforms, such as mobile nodes and remote security applications, which typically face processing limitations.

The proposed approach combines frame-based and event-based processing, enabling energy savings while maintaining high performance. Using a frame-based region proposal method based on the density of foreground events and an object tracking strategy that relies on plain object velocity, this framework optimizes object tracking even in occlusion scenarios. Converting frame-based object tracking inputs into spikes for classification on neuromorphic networks helps maintain energy efficiency without sacrificing accuracy in surveillance applications. Furthermore, the proposed neuromorphic system demonstrates effectiveness compared to standard RGB camera setups in several hours of traffic recordings, underscoring its applicability in real-time embedded environments.

This approach represents a trend toward leveraging neuromorphic vision sensors to reduce latency and enhance processing efficiency without relying on traditional event-by-event methods. It positions embedded systems to better handle security demands in practical surveillance scenarios [19].

Emerging trends in protecting embedded systems against cyber threats focus increasingly on open-source projects like the Open-source programable Logic Controller (OpenPLC), which provides accessible, vendor-neutral solutions for various embedded devices, including Raspberry Pi and Arduino. As OpenPLC gains popularity in research and industry, addressing its security vulnerabilities has become essential to safeguard industrial applications. Key trends include:

Table 4. *Key trends*

Enhanced Threat Modeling and Vulnerability Analysis	**A systematic approach to identifying security gaps—such as unauthorized access—communication protocol weaknesses, and a lack of encryption, helps in understanding and addressing potential threats.**
Control Logic Injection Attack Analysis	Experimentation with attacks, such as stealthy control logic injection attacks that bypass user detection, highlights the real-world risks associated with these vulnerabilities and reinforces the need for proactive countermeasures.
Development of Security-Enhanced Versions	The introduction of enhanced software like OpenPLC Aqua, which includes robust security solutions to counter known vulnerabilities, shows a trend toward creating modified, secure versions of open-source software to better withstand attacks in industrial settings.

Source: authors

Development of Security-Enhanced Versions: The introduction of enhanced software like OpenPLC Aqua, which includes robust security solutions to counter known vulnerabilities, shows a trend toward creating modified, secure versions of open-source software to better withstand attacks in industrial settings.

These trends underscore a shift toward making open-source embedded systems not only affordable but also secure for industrial use by integrating rigorous security analyses and targeted enhancements [20].

Emerging trends in protecting embedded systems against cyber threats increasingly focus on addressing vulnerabilities unique to shared, programable environments, such as multitenant FPGA schemes in cloud computing. Traditionally valued for their programmability and hardware-level parallelism, FPGAs are now being proposed for spatial multitenancy to maximize resource utilization. However, this setup introduces new security challenges, as shared environments expose potential attack surfaces that are not present in single-tenant configurations [21].

Additionally, the increased reliance on smart grid technology for digital substations has heightened cyber vulnerabilities. Recent trends include updates to communication protocols, such as the IEC 62351 standard for the GOOSE protocol. However, practical challenges arise due to conflicting time constraints with traditional security procedures. To address these, an innovative geometric approach for GOOSE message authentication and encryption has been developed, using vector coordinate shifts to ensure efficiency and rapid implementation while meeting strict timing requirements. Notably, this method is hardware-agnostic, requiring no specific components or changes to the GOOSE message format, making it versatile for various infrastructures while ensuring high performance and simplicity [22].

Emerging trends in protecting embedded systems against cyber threats include a growing focus on integrating cyber and physical system monitoring to address the complex, cross-domain behaviors seen in cyber-physical systems (CPS). Traditionally, cyber and physical components have been managed separately, often with distinct tools and analytical approaches. However, the combined security of CPS requires holistic analysis methods to understand and respond effectively to disturbances, whether planned or malicious [23].

To address this need, clustering techniques have been proposed to analyze cyber-physical data, specifically within smart grid systems, to reveal patterns and interdependencies between cyber, physical, and combined cyber-physical disturbances. By leveraging clustering algorithms—commonly used in data science for sorting large datasets based on statistical similarities —researchers can identify meaningful relationships and pathways within CPS, offering insights into which components and connections

are most critical or vulnerable. This approach not only improves situational awareness but also supports decision-making by highlighting strongly or weakly linked cyber-physical components, frequently traversed pathways, and critical nodes or edges within the system. This trend toward cyber-physical graph interdependency analysis underscores a foundational shift toward more integrated security and resilience strategies for embedded systems in CPS environments [23].

Another recent advancement in threat assessment and protection includes the systematic analysis of combined threats, such as FPGA power wasters and "satisfiability don't-care" hardware Trojans. Attacks like the notable X-Attack exploit remote undervolting to manipulate FPGAs, remotely triggering concealed Trojans in victim designs through power manipulation. This vulnerability enables an adversary to activate hardware Trojans by strategically adjusting power levels in shared FPGA instances, potentially compromising security-critical applications.To counter such threats, research has developed lightweight, self-calibrating countermeasures designed to detect and mitigate undervolting-induced Trojan activation, representing a novel protective trend for shared FPGAs. This approach marks a significant step toward securing multitenant FPGA systems against fault-injection attacks on commercially available cloud FPGA environments [21].

Laser Fault Injection Attacks (LFIA) and Detection with Digital Sensors Laser Fault Injection Attacks (LFIA) are becoming more common in embedded systems, allowing attackers to manipulate electronic circuits with precision. Traditional methods to prevent these attacks, such as temporal or spatial redundancy, are costly. In response, a digital sensor based on time-to-digital converters (TDC) has been developed, demonstrating high effectiveness in detecting these faults under a variety of environmental conditions and offering a more efficient protection alternative [13].

Resource limitations, such as processing power and memory, present significant challenges for implementing security techniques in embedded systems. In fields like healthcare, where medical imaging and applications like 3D image registration are critical, these constraints are particularly impactful. 3D image registration is a highly demanding computational task requiring optimal geometric alignment among 3D image stacks. In these situations, achieving real-time, energy-efficient processing becomes crucial. Hardware accelerators offer promising solutions but are complex to design and integrate within software pipelines. The Hephaestus framework demonstrates an effective approach by automating the generation of efficient 3D image registration pipelines that integrate reconfigurable accelerators. By codesigning software-programable accelerators that adjust to image volume dimensions, Hephaestus addresses memory constraints effectively, a major challenge in embedded systems. For instance, Hephaestus applies an approximation mechanism to allow embedded devices with limited memory to handle 3D image registration. This approach helps achieve near high-performance accuracy, even with the limited resources of embedded systems. Ultimately, resource constraints require tailored solutions in both software and hardware. With Hephaestus, improvements such as a 1.85× speedup and 2.35×

efficiency boost over the state of the art illustrate that through carefully designed accelerators, embedded systems can still implement high-performing security and processing techniques despite memory and power limitations [24].

Flash Memory Erasure Suppression and Microcontroller Protection Flash memory erasure suppression is an attack vector that allows attackers to disable debugging interface protection, exposing sensitive data. As embedded systems in microcontrollers face this risk, countermeasures based on selecting secure hardware have been implemented since software alone cannot fully mitigate this type of attack [14].

Cyber-Physical Systems Security and Holistic Analysis: Cyber-Physical Systems (CPS), which combine physical and cyber components, are vulnerable to both physical and digital attacks. An emerging trend to enhance security is the use of clustering techniques on cyber-physical data, allowing for the analysis of similarities in system behavior during cyber and physical disruptions. This analysis provides crucial insights into the relationship between cyber and physical components, enabling better cyber-physical situational awareness [15].

Authentication and Encryption in Smart Grid Networks In smart grid networks, cyber vulnerabilities have increased due to the digitalization of substations. The authentication and encryption of GOOSE messages, in compliance with the IEC 62351 standard, face timing challenges that hinder implementation. An emerging approach uses geometric methods for authentication, allowing time requirements to be met efficiently and without the need for additional hardware, thereby improving security in critical infrastructures [16].

Threat Mitigation in Multitenant FPGA Systems The use of Field-programable Gate Arrays (FPGAs) in cloud computing environments has enabled greater flexibility in hardware programming but has also introduced new attack surfaces. Threats related, to remote undervolting in shared FPGAs can activate hidden hardware Trojans, highlighting the need for specialized countermeasures, such as auto-calibrators to mitigate these attacks without affecting system performance [17].

Vulnerabilities in Open-Source PLCs and Security Improvements OpenPLC—a widely used open-source solution in industrial environments— has drawn the attention of the research community due to vulnerabilities in its communication protocols and a lack of robust encryption mechanisms. In response, OpenPLC Aqua has been developed, an improved version with integrated security solutions, including protection against code injection attacks in logic control systems [11].

Defenses in Neural Network-Based Systems and the Use of VOS Adversarial attacks on deep neural networks (DNNs), which manipulate input data to generate errors, are a growing threat in embedded

systems. An emerging trend is the use of voltage overscaling (VOS) as a lightweight and efficient defense. This approach exploits temporal violations within computing elements to implement a defense that does not require hardware or software modifications, providing a robust mechanism against various attack methods [18].

Fault Injection Attack Detection in Multitenant FPGA Systems Fault injection attacks using undervolting in multitenant FPGAs represent a new threat in cloud computing environments. These attacks activate hidden hardware Trojans in FPGA designs. Research into countermeasures, such as auto-calibration techniques, is crucial to mitigate these threats and ensure security in shared hardware environments [25].

Impact of Resource Limitations on the Implementation of Security Techniques in Embedded Systems

Embedded systems, characterized by their limited processing power and memory, face unique challenges when implementing robust security techniques. Below are some of the ways these limitations affect the implementation of advanced security methods, and the strategies adopted to mitigate these constraints.

Homomorphic Encryption (HE) allows operations to be performed on encrypted data without needing to decrypt it, preserving privacy during data transmission between IoT devices and the cloud. However, its high memory consumption and computational cost make it impractical for embedded devices with limited resources. To address this limitation, SEAL-Embedded, an optimized library, has been developed using memory reuse techniques and specific algorithms to reduce the memory footprint and improve performance on IoT devices. With configurations that can run with as little as 64 KB of RAM, SEAL-Embedded enables efficient encryption in devices with restricted capabilities, demonstrating that with algorithmic optimizations, it is possible to implement advanced security techniques without compromising available hardware resources [26].

An emerging trend in protecting embedded systems against cyber threats is the use of blockchain technologies, due to their versatility across various applications. Blockchain has proven effective in facilitating the transition from a low-trust, centralized ledger maintained by a single third party to a high-trust, decentralized structure managed by multiple entities or "validating nodes."

Despite its potential, many blockchain implementations face significant challenges in terms of performance and security that must be resolved to achieve widespread adoption in embedded systems and IoT applications. Addressing these challenges largely hinges on the consensus algorithm, which is critical for defining both the performance and security of any blockchain system. This work implements

several consensus algorithms in hardware, such as PoS (Proof of Stake), PoW (Proof of Work), and PoA (Proof of Authority), using VHDL (Very High-Speed Integrated Circuit Hardware Description Language) to optimize consensus execution time through IPs (Intellectual Property). Evaluating these methods in terms of security, scalability, and performance provides a foundation for understanding how embedded systems can benefit from enhanced and optimized consensus, allowing blockchain to become an effective defense mechanism against threats in IoT systems [27].

Emerging trends in protecting embedded systems against cyber threats increasingly focus on understanding and securing quantum-safe cryptographic implementations, particularly in response to NIST's selection of Dilithium as the standard for quantum-secure digital signatures. Given Dilithium's randomized (or hedged) signing mode, which was chosen to mitigate vulnerabilities in deterministic signing, research is heavily aimed at evaluating its susceptibility to fault attacks. Notably, new types of key-recovery attacks highlight vulnerabilities in randomized Dilithium, where correcting faulty signatures reveals critical intermediate values, enabling attackers to infer the signing key.

To combat these risks, researchers are developing fault injection techniques and analyzing countermeasures that bypass existing protections with minimal computational cost. For example, recent attacks have exploited instruction-skipping and faults injected into the matrix A within the public key, showing that even countermeasures designed to prevent side-channel attacks may be insufficient. The results indicate a need for more robust analysis and defensive mechanisms to protect against varied fault injection techniques, which may be circumvented with moderate increases in computational requirements and faults. This trend underscores the growing focus on securing embedded systems against quantum threats through deeper vulnerability analysis and stronger, multi-layered countermeasures [28].

Post-Quantum Security and FrodoKEM FrodoKEM and a key encapsulation mechanism based on lattice-based cryptography, is designed to resist quantum attacks. However, the complexity of unstructured lattices involves significant memory usage, making it challenging to implement in embedded systems like smart cards. To overcome these limitations, stack reduction strategies have been explored, reducing memory usage by up to 75% and allowing post-quantum encryption to be more accessible for embedded systems without sacrificing security performance [29].

Adversarial Attacks on Neural Networks Deep neural networks (DNNs) applied in embedded systems are vulnerable to adversarial attacks that exploit limited processing capacity. Black-box attacks, which manipulate processing times, can cause classification errors in these systems. These attacks do not require training data or substitute models, making them particularly difficult to prevent. The proposed countermeasures include adjustments to activation functions to avoid processing time leaks, but these require a careful balance between security and the already limited processing capacity of the devices [30].

Physical Tamper Detection Embedded systems are vulnerable to physical attacks, such as circuit board manipulation or probe insertion into integrated components. Traditional solutions, like tamper-proof enclosures, are often expensive and incompatible with low-cost devices. An effective solution is the characterization of the power distribution network using sensors integrated into FPGAs, which can detect physical tampering by analyzing impedance. This method allows for chip-level attack detection without the need for additional hardware, making it a resource-efficient option [31].

A significant emerging trend in protecting embedded systems against cyber threats involves the development of secure databases specifically tailored for embedded environments, such as BiTDB (Built-in TEE Secure Database). BiTDB focuses on using Trusted Execution Environments (TEE), which offer isolated environments within embedded systems for secure data processing and storage. This design helps safeguard sensitive data from unauthorized access, even if the main system's security is compromised. By integrating a TEE-based secure database, embedded systems can maintain a robust, tamper-resistant framework that not only supports secure data storage but also enables secure execution of critical operations, greatly enhancing resilience against cyber threats [32].

Hardware Encryption Acceleration for Post-Quantum Security The advent of quantum computing poses threats to traditional cryptographic algorithms, driving the development of mechanisms like Crystals-Kyber. To address the computational complexity of these algorithms in embedded systems, Instruction Set Extensions (ISEs) for low-power RISC-V processors have been proposed. These extensions allow for the acceleration of cryptographic operations with minimal impact on chip area and energy consumption, achieving performance improvements of up to 47% in key encapsulation without requiring significant hardware design modifications [33].

The emerging trend in protecting embedded systems against cyber threats focuses on optimizing hardware implementations for real-time, reliable, and resource-efficient processing, particularly in constrained environments. The development of optimized segmentation algorithms, such as those designed for phonocardiogram (PCG) analysis on low-end field-programable gate arrays (FPGAs), exemplifies this trend. By employing strategies that reduce latency, memory usage, and energy consumption, such systems become more resilient to attacks that exploit processing delays or resource bottlenecks. Moreover, the use of fixed-point data types enhances performance consistency, which is crucial for maintaining reliable, low-cost diagnostic responses—especially important in sensitive applications, such as healthcare monitoring in resource-limited settings. This emphasis on resource-constrained optimization also represents a defense mechanism, reducing system exposure to cyber threats that target inefficiencies in computational processes [34].

Resource limitations, such as processing power and memory, significantly impact the implementation of security techniques in embedded systems, particularly given their rising use and increasing

vulnerability to malicious code reuse attacks. Traditional security approaches, whether software-based or hardware-assisted, often struggle to provide effective defense without incurring substantial performance and implementation overhead. However, the lightweight hardware-assisted scheme presented in this paper addresses these limitations by optimizing both the architecture and implementation for constrained environments. The proposed solution includes an on-chip lightweight hardware shadow stack that enhances backward-edge control flow integrity by validating return addresses at runtime, thereby reducing the risk of code reuse attacks. Additionally, a lightweight stream cipher circuit encrypts critical stack data related to control flow, further protecting against unauthorized access and manipulation. By designing these security mechanisms with resource constraints in mind, the solution achieves a low performance overhead of 0.39% and a minimal area footprint (0.316 mm^2) when integrated into the OR1200 processor and tested on the Terasic DE1-SoC FPGA platform. This demonstrates that a carefully optimized approach can effectively secure embedded systems with minimal impact on system resources [3].

Resource limitations, such as processing power and memory, significantly impact the implementation of security techniques in embedded systems. For instance, fault injection attacks are a considerable threat, exploiting faults within the microarchitecture to compromise embedded systems. A recent development to counteract this is the MAFIA microarchitecture protection, which aims to secure pipeline control signals against such attacks using a signature-based mechanism. However, implementing MAFIA comes with notable resource overheads. Two versions—using CBC-MAC/Prince and CRC32—have been analyzed, each with different trade-offs in security and resource demands. The CBC-MAC/Prince variant incurs a 23.8% area overhead and substantial execution overheads of 50% in code size and 39% in execution time. By contrast, the CRC32 variant has lower overheads (6.5% in area, 29.4% in code size, and 18.4% in execution time), but may offer different levels of protection. These overheads highlight the challenge of balancing security effectiveness with limited processing power and memory, as high overheads can strain system resources, potentially reducing efficiency or even making certain protections infeasible in highly constrained environments [35].

Resource limitations, such as processing power and memory constraints, present significant challenges for implementing security techniques in embedded systems. Software obfuscation is often used to protect intellectual property or secret keys within programs, especially in untrusted execution environments where malware or reverse engineering are potential threats. However, state-of-the-art software-only obfuscation techniques, including white-box cryptography, are generally impractical or insecure in real-world applications due to these resource constraints.

This is where frameworks like OBSCURE come into play. OBSCURE is designed to be a practical and cryptographically strong obfuscation framework, leveraging a simple, stateless secure element that can be embedded within protected hardware chips or tokens. This setup allows for provable security while addressing efficiency, which is crucial for constrained environments. Additionally,

OBSCURE's new rectangular universalization technique and support for C-based program inputs make it versatile and suitable for various applications. By benchmarking it on both simple programs and cryptographic primitives, OBSCURE demonstrates its potential as a viable alternative to purely software-based obfuscation methods, providing a more feasible approach for embedded systems with limited resources [36].

An emerging trend in protecting embedded systems against cyber threats is the development of efficient hardware/software (HW/SW) co-designed accelerators for post-quantum cryptography (PQC) schemes, particularly digital signature algorithms (DSAs) like FALCON. In the context of embedded system security, FALCON's distinct task-processing approach—handling multiple tasks with similar execution times—requires a novel optimization strategy, contrasting with traditional methods that accelerate a single dominant task. This research demonstrates that optimizing lower-level operations rather than broad functional segments enhances FALCON's performance while minimizing the silicon area used, a crucial factor for resource-constrained embedded systems. Furthermore, implementing pipelined execution and concurrent processing of FALCON's sampling function across both hardware and software layers significantly reduces latency, showing a 3.58x improvement in clock cycles over traditional accelerators. These innovations highlight a shift toward granularity-focused optimization and parallel execution to achieve both high performance and compact design in PQC for embedded systems, which is especially relevant as the field adapts to the demands of quantum-resistant cybersecurity [37].

Recent trends in protecting embedded systems against cyber threats focus on mitigating vulnerabilities in ARM-FPGA embedded SoCs, which are widely used in fields like 5G wireless, advanced driver-assistance systems (ADAS), and the Industrial Internet of Things due to their performance and design flexibility. These systems face significant security threats, particularly from cross-domain cache-related attacks such as Flush+Reload, Flush+Flush, Meltdown, and specter. Emerging defenses address these threats with a combination of hardware and software measures. However, traditional hardware-based defenses require changes to the core architecture, making them impractical for existing devices. In contrast, software runtime defenses may be easier to implement but often suffer from limited coverage and high performance costs. To tackle these challenges, a notable innovation is SnapMem, a hardware/software cooperative memory solution that employs a "burn-after-reading" mechanism to secure sensitive data. By ensuring that each process can only access its own SnapMem, this approach prevents cross-process data theft. SnapMem can efficiently transfer sensitive data in and out of main memory in real-time, significantly reducing the risk of cache-related attacks without incurring the high performance overhead associated with conventional software defenses [38].

Common Vulnerabilities in Embedded Systems and Effective Strategies for Mitigating Them

Embedded systems, present in a wide range of critical applications such as automotive, healthcare, and the Internet of Things (IoT), are vulnerable to various security threats. These vulnerabilities can compromise the confidentiality, integrity, and availability of systems. Below are some of the most common vulnerabilities and strategies that have proven effective in mitigating them.

Fault Injection Attacks: One of the most common vulnerabilities in embedded systems is exposure to fault injection attacks, including techniques like voltage or clock glitching to bypass protection during the microcontroller boot process. For example, microcontroller bootloaders can be vulnerable to attacks that manipulate system behavior during startup, allowing attackers to disable memory protections and access-sensitive data. Recent studies have used a combination of static and dynamic analysis, along with symbolic execution, to precisely target glitches to specific bootloader instructions. This enables security measures to be bypassed and protected memory to be accessed on real microcontrollers, such as the NXP LPC and STM8. This approach highlights the importance of improving bootloader designs and avoiding vulnerable patterns [39].

Embedded systems face persistent vulnerabilities, particularly regarding secure key exchange methods. Traditional cryptographic algorithms, such as Diffie-Hellman, RSA, and elliptic curve schemes, are susceptible to future quantum computing attacks, which could compromise their ability to protect sensitive data. To address this looming threat, the National Institute of Standards and Technology (NIST) has spearheaded the development of post-quantum cryptographic solutions, such as the Crystals-Kyber algorithm, which was selected for standardization in 2022 as ML-KEM due to its robustness against both classical and quantum-based attacks. Mitigating these vulnerabilities in embedded systems requires not only new cryptographic standards but also hardware acceleration to achieve the necessary performance, efficiency, and scalability in resource-constrained environments. For instance, in the case of Crystals-Kyber, using Instruction Set Extensions (ISEs) in a 32-bit RISC-V core (like Ibex) can enhance performance and reduce energy consumption. Accelerating symmetric primitives like SHA-3 and AES/SHA-2 (Kyber-FIPS202 and Kyber-90s) with specific ISEs has shown a performance gain of up to 42% and an energy reduction of 37% for Kyber-512 encapsulation. Additionally, using novel ISEs like Xkyber, which accelerates polynomial arithmetic and other processes, can further improve both performance and efficiency by approximately 47% and 41%, respectively, while reducing code size. Thus, adopting quantum-resistant algorithms coupled with efficient hardware acceleration is proving effective in strengthening the security and resource efficiency of embedded systems against emerging threats [33].

In embedded systems, common vulnerabilities often arise from constraints on computational power and memory, as well as the need for high-speed processing. These limitations can lead to a reliance on simplified encryption methods that may not offer robust security. Traditional encryption algorithms,

designed primarily for general-purpose computing, often fall short in meeting the dual demands of speed and security in embedded environments.

To address these vulnerabilities, strategies for leveraging Field-programable Gate Arrays (FPGAs) have proven effective, especially in applications requiring secure and high-speed image encryption. For instance, a novel approach using the LTB map—a combination of three 1D chaotic maps (Logistic, Tent, and Bernoulli shift)—demonstrates a solution that is both resource-efficient and secure. The LTB map's expanded key space and complex behavior enhance unpredictability, while the hardware efficiency and parallelism inherent in FPGA implementation enable fast encryption without compromising security. By focusing on streamlined operations like addition, subtraction, and multiplication, this method mitigates resource-related vulnerabilities common in embedded systems, achieving a balanced approach to speed and security [31].

Embedded systems face persistent vulnerabilities, especially as AI and machine learning (ML) become increasingly integrated into these environments. Common vulnerabilities include limited transparency, poor traceability, and insufficiently robust security mechanisms within the embedded software. To address these issues, integrating Capability-based Hierarchical Embedded RISC Instructions (CHERI) with AI Bills of Materials (AI BOMs) has proven effective. CHERI's advanced security features, when combined with AI BOMs, create a more secure foundation by improving the transparency, traceability, and overall reliability of embedded AI systems. This combined approach mitigates threats by allowing detailed assessments of vulnerabilities and exploits in new Software Bills of Materials (SBOMs), and it enhances the trustworthiness and quality of AI systems through systematic threat analysis and AI-driven simulations [40].

Emerging trends in protecting embedded systems against cyber threats focus on addressing the inherent security vulnerabilities of embedded platforms, particularly those used in critical sectors such as manufacturing, smart grids, industrial control systems, and transportation. Since many of these systems, especially those based on ARM Cortex-M microcontrollers, lack built-in security features, they are prone to cyberattacks such as malware injections targeting power distribution systems. A notable threat involves exploiting the clock-gating distribution system, allowing attackers to manipulate subsystem activation, which can compromise the reliability of these systems [41].

To counteract such vulnerabilities, recent advancements include the development of Intrusion Detection Systems (IDSs) specifically designed to detect malware targeting clock-gating mechanisms. Various IDS methodologies—such as K-Nearest Classifier, Random Forest, Logistic Regression, Decision Tree, Naive Bayes, and Stochastic Gradient Descent—have been implemented to identify and categorize different forms of clock-gating malware. These systems leverage data on power consumption under both normal and attack conditions for model training and validation. In simulations, IDS models,

particularly those based on K-Nearest Classifier and Logistic Regression, demonstrated high detection accuracy, with some achieving a 0.99 detection rate, highlighting their effectiveness in defending ARM Cortex-M-based systems against such sophisticated malware threats [41].

Emerging trends in protecting embedded systems against cyber threats include a shift toward distributed, edge-computing architectures, particularly within video surveillance systems. Traditionally, these systems relied on a centralized network of cameras feeding into a single node; however, a more resilient and responsive distributed approach is now being favored. By processing data locally on embedded platforms, these systems enhance security by reducing the data exposure associated with centralized processing. Edge computing also enables real-time analysis for people and event detection at each node, which is essential for minimizing response times in critical scenarios. Leveraging deep learning and segmentation algorithms, as well as recurrent neural networks (such as LSTMs), these systems can perform human action recognition (HAR) efficiently, even in complex environments. Optimized for high performance on lightweight hardware, such architectures make embedded systems both more portable and scalable, creating robust, cyber-secure solutions for real-world surveillance applications [42].

One emerging trend in protecting embedded systems against cyber threats is the development of architecture- and operating-system-agnostic reverse engineering frameworks, such as Incision. Security analysis of embedded devices presents unique challenges due to undocumented peripherals, esoteric instruction sets, and limited tool support, often necessitating extensive reverse engineering. Incision addresses this by reducing the upfront effort needed to analyze complex embedded devices. It uses a feedback loop between static and dynamic analyses, allowing information from each to enhance overall firmware understanding. This approach proves effective across different devices, operating systems, and instruction sets, offering a robust solution that requires minimal manual effort while yielding accurate results. Such frameworks represent a significant step forward in enabling a more efficient and reliable security analysis of embedded systems [43].

Emerging trends in protecting embedded systems against cyber threats, particularly in the automotive industry, focus on adapting to the shift from traditional hardware-defined to software-defined architectures. This evolution, which supports the development of Software-Defined Vehicles (SDVs), requires a service-oriented architecture to manage increasing software complexity, enabling efficient software development, integration, and deployment from cloud or backend systems to vehicles [44].

To address the complexity of managing software updates in highly distributed embedded Electronic Control Units (ECUs), a software-centric approach has emerged as more effective for handling diverse configurations and architectures across platforms. One key innovation is a variability-rich software update scheme based on Merkle tree structures. This approach allows Original Equipment Manufacturers (OEMs) to sign a software module once and verify it across multiple ECU variants, simplifying variant

management while ensuring secure and authenticated updates. The Merkle tree approach, combined with digital signatures, strengthens authentication and verification processes for multiple software variants, offering enhanced security without sacrificing passenger safety. This method not only streamlines software updates but also provides a scalable, secure solution to the challenges of SDV software management, highlighting the importance of cybersecurity in maintaining vehicle integrity as connectivity and autonomy levels increase [44].

Emerging trends in protecting embedded systems against cyber threats include using advanced methods to detect tampering through physical attack signatures, particularly focusing on the impedance characterization of the power distribution network (PDN). Traditional security methods, such as tamper-proof enclosures, are often costly and incompatible with legacy systems, making them impractical for many low-cost applications. As a modern approach, researchers are leveraging on-chip circuit-based network analyzers to detect physical tampering by analyzing changes in the PDN's frequency response. These embedded analyzers can be deployed directly on FPGAs, enabling the detection of various tamper events without modifications to existing systems. By using techniques from power integrity analysis, this method provides a cost-effective and robust solution. The analysis can identify different classes of tamper events, from PCB-level modifications to IC package manipulation. Experiments using commercial FPGA development kits have shown that the frequency response of the PDN is sensitive enough to detect subtle tampering activities, such as the proximity of EM probes or slight modifications to the IC package. Using statistical metrics like the Wasserstein Distance further enhances the accuracy of tamper detection, showing promise as a new standard for embedded system protection against physical attacks [45].

Emerging trends in protecting embedded systems against cyber threats include the use of threshold implementation (TI) as an effective lightweight countermeasure against side-channel attacks, particularly under conditions where glitches are present. For masking schemes, safeguarding the S-box component is central to ensuring security. A new approach, the MiniSat-lightweight-threshold implementation (MS-LW-TI), has been developed as a first-order TI scheme specifically for 4 × 4 S-boxes. This technique leverages the MiniSat tool to optimally decompose an S-box into minimal operations using AND, OR, and XOR gates, and introduces two defined primitives along with extensions that meet stringent security properties [46].

The MS-LW-TI scheme is particularly efficient for implementation on FPGA platforms, such as the Xilinx Spartan-6, where it demonstrates significant reductions in resource usage. For example, it achieves reductions in look-up tables (LUTs), flip-flops (FFs), and slices compared to previous designs, with improvements up to 38% for the PRESENT S-box and substantial reductions for the GIFT and PICCOLO S-boxes as well. This optimization trend in lightweight TI design reflects a focused move toward

efficiency and security, making these methods particularly valuable for resource-constrained embedded systems [46].

The integration of CHERI with AI BOMs has shown effectiveness in identifying and addressing specific vulnerabilities, thereby reducing the risk of exploitation in embedded systems. By establishing a robust, AI-supported framework, this strategy not only secures current AI-enabled embedded systems but also sets a pathway for future advancements in AI and ML security. Through this approach, embedded systems benefit from a multi-faceted defense mechanism, which is essential in an era where security and transparency are critical for trustworthy AI and ML deployments [40].

Mitigation Strategy:

To mitigate these attacks, insecure design patterns should be avoided, and robust fault detection techniques should be applied, such as monitoring for anomalous events during system boot. Flash Memory Attacks: Another vulnerability is flash memory erasure suppression attacks, which exploit a feature of some microcontrollers where the protection of the debugging interface can be disabled when erasing flash memory. By manipulating this process, attackers can gain unlimited access to flash memory without erasing the data, posing a significant threat to intellectual property protection and other sensitive data [47].

Since implementing countermeasures through software is difficult, the careful selection of microcontrollers and hardware designs that does not allow such vulnerabilities is a key approach to mitigating this risk [47].

Hardware Trojans are malicious components inserted into chip designs that aim to sabotage processor performance or introduce vulnerabilities that are difficult to detect during the silicon verification phase. These Trojans can directly affect system functionality or allow unauthorized access to critical resources. Detecting these Trojans after hardware deployment is crucial for ensuring system security. The most effective methods include real-time monitoring of hardware counters for performance anomalies and the use of analytical models that compare expected microarchitectural events with actual ones, enabling the identification of suspicious behavior without requiring specific profiles for each processor [48].

Side-channel attacks and cryptography based on Physically Unclonable Functions (PUFs) is gaining traction as a security strategy in IoT devices for generating unique cryptographic keys based on hardware characteristics. However, physical signals, such as those obtained from ECGs in medical applications, can be subject to instability and noise, complicating reliable key generation. The use of filtering and feature extraction techniques, along with fuzzy extraction mechanisms, can stabilize physical signals and improve the reliability of the generated cryptographic keys. These techniques allow IoT devices to securely handle sensitive data in resource-constrained environments [49].

Cryptography in Resource-Limited Systems The growth of IoT has highlighted the need for lightweight cryptographic solutions due to the processing and memory limitations of embedded devices. Post-quantum cryptography algorithms, such as the Saber key encapsulation mechanism, require complex arithmetic processing, which presents challenges in resource-constrained devices. However, recent improvements in polynomial multiplication efficiency have achieved performance gains of up to 5x on ARM Cortex-M processors without compromising the energy profile. Implementing algorithmic optimizations like Toom-Cook and Karatsuba, along with the efficient use of registers and instruction programming, has proven effective in addressing resource limitations in embedded devices [50].

Cryptographic Systems and RNGs in FPGAs Cryptographic systems implemented in Field-programable Gate Arrays (FPGAs) require the random number generators (RNGs), which, if not properly designed, can be affected by noise generated by other algorithms running on the same reconfigurable logic. This can compromise the quality of random numbers and, ultimately, the security of the system. The implementation of PLL-based True Random Number Generators (TRNGs), which separate the random number generator from the reconfigurable logic, is an effective strategy to ensure the entropy and quality of the generated random numbers, thereby enhancing security in FPGAs [25].

Discussion

Embedded system security has evolved due to increasing threats in IoT applications, wireless communication systems, and industrial environments. Advanced security techniques incorporate hardware-based measures, such as the Trusted Platform Module (TPM), that strengthen trust and reduce risks in critical infrastructures. In addition, open platforms such as RISC-V enable customized security solutions that ensure effective protection without compromising performance.

For IoT devices, lightweight encryption methods such as CLEFIA provide confidentiality in resource-constrained environments, while Physically Unclonable Functions (PUFs) support device identity and secure key generation. Protocol-level mechanisms, such as the Signal Echoing Protocol (SEP), help protect against spoofed base stations in 5G networks. Together, these developments illustrate the combination of cryptographic, hardware-assisted, and communication-level protections used in embedded systems.

In industrial environments, CAN bus-base systems and cyber-physical systems (CPS) have adopted anomaly detection and encryption techniques to protect data and prevent unauthorized access. The integration of holistic analysis in CPSs makes it possible to monitor critical interactions between digital and physical components, improving the system's resilience to disturbances. This trend toward adaptive and robust security remains key to addressing the challenges of embedded systems, balancing efficiency and protection in critical applications and rapidly expanding IoT environments.

As a complement to the original review, Zhong and Gu [51] compare lightweight block ciphers for resource-constrained environments, showing that the choice of a cipher depends not only on security, but also on memory, implementation cost, and platform characteristics.

Khan et al. [52] present a trusted-hardware security framework for IoT edge devices based on TPM support, showing how key protection and cryptographic operations can be strengthened with dedicated hardware.

Alwaisi et al. [53] study lightweight machine-learning methods for anomaly detection in constrained IoT systems, highlighting the need to balance detection capability with memory, energy, model complexity, and deployment location.

Although the review was broadened beyond Scopus through complementary searches in ScienceDirect and SpringerLink, IEEE Xplore and the ACM Digital Library were not included in this search. Therefore, studies indexed exclusively in those databases may not be represented. This source-coverage limitation should be considered when interpreting the scope of the synthesis and can be addressed in future updates of the review.

Table 5. Comparative security characteristics and execution platforms

Technique / mechanism	Security contribution / reported level	Platform / application	Main trade-off	Ref.
CLEFIA	Lightweight symmetric confidentiality. The exact security level not reported in this review.	Resource-constrained IoT and embedded applications	Low implementation footprint; classical rather than post-quantum protection	[4]
RECO-ASCON	Lightweight hashing / reconfigurable protection. The exact security level not reported in this review.	Reconfigurable embedded hardware and IoT	Balances frequency, parallelism, and energy use	[10]
TPM + X.509	Hardware trust, attestation, authentication, and integrity. Not directly comparable as an encryption level.	IoT devices in smart-grid infrastructure	Requires TPM integration and certificate management	[7]

Technique / mechanism	Security contribution / reported level	Platform / application	Main trade-off	Ref.
PUF-based keys	Device-bound identity and key derivation. Not directly comparable as an encryption level.	RIOT OS / IoT and Internet of Medical Things	Reliability can be affected by noise and physical variability.	[17], [49]
Crystals-Kyber / ML-KEM	Post-quantum key encapsulation. The exact parameter/ security level not specified in this review.	32-bit RISC-V embedded cores	Acceleration helps control latency and energy cost	[33]
FrodoKEM	Post-quantum key encapsulation. Exact parameter/ security level not specified in this review.	Embedded / smart-card-class platforms	High memory demand; stack reduction improves feasibility	[29]
Lightweight cipher survey	Security-resource-performance comparison; the reported levels vary by cipher and platform.	Constrained IoT and embedded hardware/software	No single cipher dominates across all platforms	[51]
TPM, trusted hardware	Key protection and trusted hardware support. These are not directly comparable to an encryption level.	IoT edge devices	Needs dedicated trusted hardware and key management	[52]
Lightweight anomaly detection	Resource-aware intrusion and anomaly detection. Not applicable as an encryption-level metric.	Constrained IoT / edge devices	Must balance detection with memory, energy, and model complexity.	[53]

Source: authors

Table 6. Unresolved challenges and future research directions

Research gap	Why it remains unresolved	Future direction	Related evidence
Cross-platform comparability	Studies use different security, latency, energy, and area metrics.	Develop shared benchmarks for security/performance trade-offs.	[3], [10], [35], [37], [51]
Post-quantum efficiency	PQC can exceed the memory and compute budgets of constrained devices.	Co-design algorithms, instruction extensions, and accelerators.	[28], [29], [33], [37], [50]
PUF reliability	Noise, aging, and environmental conditions can affect reproducibility.	Use robust extraction and long-term evaluation on deployed devices.	[17], [49]
Shared FPGA security	Multitenancy introduces undervolting, Trojan, and cross-domain risks.	Strengthen isolation and monitoring for multitenant FPGAs.	[21], [25], [38]
Embedded AI security	DNNs introduce adversarial, timing, and provenance risks.	Combine adversarial robustness with resource-aware runtime defenses.	[18], [30], [40], [53]

Source: authors

Conclusions

1. The security of embedded systems has evolved considerably to address a wide range of threats, driven by their integration into diverse applications such as IoT, cyber-physical systems (CPS), and critical infrastructures like power grids. Key advancements include protection against Advanced Persistent Threats (APTs) through extended attack chains in industrial control systems (ICS) and defenses against physical threats, such as Laser Fault Injection Attacks (LFIA), using advanced digital sensors that enhance CPS resilience against both digital and physical attacks. For IoT and resource-constrained environments, lightweight cryptographic techniques such as CLEFIA encryption and reconfigurable processors like RECO-ASCON have been optimized to balance security and performance. Similarly, hardware-assisted techniques, such as the integration of Trusted Platform Modules (TPMs) in power grids and customizable RISC-V architectures, enable efficient and tailored security solutions, supporting secure attestation and dynamic control flow integrity. Other significant developments include specific defense mechanisms like Real-time Execution (RE) in CPS, which allows multiple security policies to be applied in real-time; Physically Unclonable Functions (PUFs) to provide unique identities to IoT devices; and geometric authentication methods in power grid networks to meet strict synchronization requirements. Additionally, CAN-based systems have advanced network traffic authentication to counter data tampering risks, while Voltage Overscaling (VOS) techniques offer defenses against adversarial

attacks on deep neural networks (DNNs) with improved energy efficiency. These innovations reflect a multifaceted approach to security in embedded systems, balancing protection, performance, and resource constraints to support secure and functional operations in critical and emerging applications such as healthcare, home automation, and industrial automation.

2. The increasing connectivity and critical role of embedded systems in essential infrastructures have heightened cyber threats to these systems, necessitating advanced protection strategies. Advanced Persistent Threats (APTs), such as attacks on power grids, exemplify the high risk and demand sophisticated defenses. Techniques like Hardware-in-the-Loop (HIL) are now used to identify control system vulnerabilities, while neuromorphic vision and hybrid detection systems achieve superior energy efficiency and optimized real-time processing. Furthermore, the security of open-source embedded systems like OpenPLC has become critical, emphasizing the need for improved threat modeling and the development of enhanced versions with integrated security solutions. In shared hardware environments, such as cloud-based FPGAs, spatial multitenancy introduces new security challenges, which are addressed through automatic calibrators that mitigate fault injection attacks. These trends indicate a shift toward holistic solutions that integrate both physical and cyber protections, optimizing critical infrastructure efficiency through innovative authentication approaches and data clustering algorithms. In conclusion, the convergence of advanced technologies and a focus on embedded system security aims not only to mitigate emerging threats but also to strengthen the resilience and sustainability of these critical infrastructures in the current and future landscape.

3. Resource limitations in embedded systems, such as limited processing power and memory, pose unique challenges for implementing advanced security techniques. These constraints restrict the adoption of protection technologies such as homomorphic encryption, blockchain, and post-quantum cryptography, which demand high memory and computational power. However, innovative strategies have been developed to mitigate these issues, such as optimized libraries, specialized consensus algorithms, and hardware accelerators designed to maximize performance with minimal resources. For instance, SEAL-Embedded enables homomorphic encryption on devices with as little as 64 KB of RAM, and SnapMem introduces a "burn-after-reading" mechanism to secure real-time data without significantly impacting performance. Additionally, the use of Trusted Execution Environments (TEEs) in databases and improvements in quantum-safe cryptography are providing accessible and secure solutions even for resource-constrained embedded systems. These trends reflect a shift toward hardware/software co-design and granular optimization to keep embedded systems secure in resource-limited environments. In conclusion, these advancements not only facilitate the implementation of advanced security techniques on limited-resource devices but also strengthen their resilience against emerging cyber threats, adapting to an increasingly complex security landscape.

4. Embedded systems, present in critical applications such as automotive, healthcare, and the Internet of Things (IoT), face security vulnerabilities that can compromise data confidentiality, integrity, and availability. Among the most common threats are fault injection attacks, flash memory attacks, and hardware Trojan attacks, each significantly impacting system security and functionality. To mitigate these vulnerabilities, specific strategies are being developed. For instance, in the case of fault injection attacks, anomaly detection and secure boot design prove effective in preventing the manipulation of sensitive data. Careful selection of microcontrollers without flash memory suppression vulnerabilities is crucial to prevent data exposure and protect intellectual property. In cryptography, the advancement of quantum computing necessitates quantum-resistant solutions, such as the Crystals-Kyber algorithm, along with hardware acceleration to ensure performance in resource-constrained environments. Furthermore, the integration of advanced security systems like FPGAs enables rapid and secure cryptographic implementations through efficient true random number generators, providing robust protection in critical systems.

Lastly, emerging technologies such as Physically Unclonable Functions (PUFs) and lightweight encryption solutions are essential for safeguarding IoT devices with limited processing and memory. These strategies demonstrate a comprehensive and scalable approach that strengthens embedded system security in an increasingly interconnected environment, addressing new and evolving threats.

Across the four research questions, the synthesis also identifies unresolved gaps that limit direct comparison and deployment across platforms. As summarized in Table 6, future work should prioritize shared benchmarks for security-performance trade-offs, more resource-efficient post-quantum implementations, long-term evaluation of PUF reliability, stronger isolation and monitoring for multitenant FPGAs, and resource-aware defenses for embedded AI. These gaps indicate that future progress will depend not only on stronger protection mechanisms, but also on reproducible evaluation criteria that make results comparable across architectures and application domains.

References

[1] M. J. Page *et al*., "Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas," *Rev Esp Cardiol*, vol. 74, no. 9, pp. 790–799, Sep. 2021, doi: https://doi.org/10.1016/j.recesp.2021.06.016.

[2] C. Burgos-Mellado *et al*., "Reinforcement Learning-Based Method to Exploit Vulnerabilities of False Data Injection Attack Detectors in Modular Multilevel Converters," *IEEE Trans. Power Electron.*, vol. 38, no. 7, pp. 8907–8921, Jul. 2023, doi: https://doi.org/10.1109/TPEL.2023.3263728.

[3] Z. An, W. Wang, W. Li, S. Li, and D. Zhang, "Securing Embedded System from Code Reuse Attacks: A Lightweight Scheme with Hardware Assistance," *Micromachines (Basel)*, vol. 14, no. 8, p. 1525, Jul. 2023, doi: https://doi.org/10.3390/mi14081525

[4] A. H. Karode, S. R. Suralkar, and V. B. Patil, "Performance Evaluation of Light Weight Cryptographic CLEFIA Algorithm," *International Journal of Electronics and Communication Engineering*, vol. 10, no. 8, pp. 48–58, Sep. 2023, doi: https://doi.org/10.14445/23488549/IJECE-V10I8P105

[5] Y. Sun, G. Li, H. Luo, Y. Xing, S. Dang, and A. Hu, "Location-Invariant Radio Frequency Fingerprint for Base Station Recognition," *IEEE Wireless Communications Letters*, vol. 12, no. 9, pp. 1583–1587, Sep. 2023, doi: https://doi.org/10.1109/LWC.2023.3283800.

[6] M. Boeding, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, "A flexible OT testbed for evaluating on-device implementations of IEC-61850 GOOSE," *International Journal of Critical Infrastructure Protection*, vol. 42, p. 100618, Sep. 2023, doi: https://doi.org/10.1016/j.ijcip.2023.100618

[7] G. Sharma, A. M. Joshi, and S. P. Mohanty, "Fortified-Grid: Fortifying Smart Grids through the Integration of the Trusted Platform Module in Internet of Things Devices," *Information*, vol. 14, no. 9, p. 491, Sep. 2023, doi: https://doi.org/10.3390/info14090491

[8] M. Brohet and F. Regazzoni, "A Survey on Thwarting Memory Corruption in RISC-V," *ACM Comput Surv*, vol. 56, no. 2, pp. 1–29, Feb. 2024, doi: https://doi.org/10.1145/3604906

[9] T. Zoppi *et al.*, "Safe Maintenance of Railways using COTS Mobile Devices: The Remote Worker Dashboard," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 4, pp. 1–20, Oct. 2023, doi: https://doi.org/10.1145/3607193

[10] M. El-Hadedy *et al.*, "RECO-ASCON: Reconfigurable ASCON hash functions for IoT applications," *Integration*, vol. 93, p. 102061, Nov. 2023, doi: https://doi.org/10.1016/j.vlsi.2023.102061

[11] T. Cultice and H. Thapliyal, "Vulnerabilities and Attacks on CAN-Based 3D Printing/Additive Manufacturing," *IEEE Consumer Electronics Magazine*, vol. 13, no. 1, pp. 54–61, Jan. 2024, doi: https://doi.org/10.1109/MCE.2023.3240849

[12] A. Akbarzadeh, L. Erdodi, S. H. Houmb, and T. G. Soltvedt, "Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation," *Int J Inf Secur*, vol. 23, no. 4, pp. 2739–2758, Aug. 2024, doi: https://doi.org/10.1007/s10207-024-00856-6

[13] M. Ebrahimabadi *et al.*, "DELFINES: Detecting Laser Fault Injection Attacks via Digital Sensors," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 3, pp. 774–787, Mar. 2024, doi: https://doi.org/10.1109/TCAD.2023.3322623.

[14] M. Schink *et al.*, "Unlock the Door to my Secrets, but don't Forget to Glitch," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2024, no. 2, pp. 88–129, Mar. 2024, doi: https://doi.org/10.46586/tches.v2024.i2.88-129

[15] A. Baird, A. Panda, H. Pearce, S. Pinisetty, and P. Roop, "Scalable Security Enforcement for Cyber Physical Systems," *IEEE Access*, vol. 12, pp. 14385–14410, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3357714

[16] T. Hutzelmann, D. Mauksch, A. Petrovska, and A. Pretschner, "Generation of Tailored and Confined Datasets for IDS Evaluation in Cyber-Physical Systems," *IEEE Trans Dependable Secure Comput*, vol. 21, no. 4, pp. 3948–3962, Jul. 2024, doi: https://doi.org/10.1109/TDSC.2023.3341211

[17] P. Kietzmann, T. C. Schmidt, and M. Wählisch, "PUF for the Commons: Enhancing Embedded Security on the OS Level," *IEEE Trans Dependable Secure Comput*, vol. 21, no. 4, pp. 2194–2210, Jul. 2024, doi: https://doi.org/10.1109/TDSC.2023.3300368

[18] M. S. Islam, I. Alouani, and K. N. Khasawneh, "SecureVolt: Enhancing Deep Neural Networks Security via Undervolting," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 42, no. 12, pp. 4922–4933, Dec. 2023, doi: https://doi.org/10.1109/TCAD.2023.3296379

[19] A. Ussa *et al.*, "A Hybrid Neuromorphic Object Tracking and Classification Framework for Real-Time Systems," *IEEE Trans Neural Netw Learn Syst*, vol. 35, no. 8, pp. 10726–10735, Aug. 2024, doi: https://doi.org/10.1109/TNNLS.2023.3243679

[20] W. Alsabbagh, C. Kim, and P. Langendörfer, "Investigating the Security of OpenPLC: Vulnerabilities, Attacks, and Mitigation Solutions," *IEEE Access*, vol. 12, pp. 11561–11583, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3356051

[21] D. G. Mahmoud, B. Shokry, V. Lenders, W. Hu, and M. Stojilović, "X-Attack 2.0: The Risk of Power Wasters and Satisfiability Don't-Care Hardware Trojans to Shared Cloud FPGAs," *IEEE Access*, vol. 12, pp. 8983–9011, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3353134

[22] M. F. Elrawy, C. Fioravanti, G. Oliva, M. K. Michael, and R. Setola, "A Geometrical Approach to Enhance Security Against Cyber Attacks in Digital Substations," *IEEE Access*, vol. 12, pp. 18724–18738, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3361753

[23] N. Jacobs *et al.*, "Leveraging graph clustering techniques for cyber-physical system analysis to enhance disturbance characterisation," *IET Cyber-Physical Systems: Theory & Applications*, Feb. 2024, doi: https://doi.org/10.1049/cps2.12087.

[24] G. Sorrentino, M. Venere, D. Conficconi, E. D'Arnese, and M. D. Santambrogio, "<scp>Hephaestus</scp> : Codesigning and Automating 3D Image Registration on Reconfigurable Architectures," *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 5s, pp. 1–24, Oct. 2023, doi: https://doi.org/10.1145/3607928

[25] V. Fischer, F. Bernard, Q. Dallison, and M. Skórski, "Enhancing Quality and Security of the PLL-TRNG," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 211–237, Aug. 2023, doi: https://doi.org/10.46586/tches.v2023.i4.211-237

[26] D. Natarajan and W. Dai, "SEAL-Embedded: A Homomorphic Encryption Library for the Internet of Things," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 756–779, Jul. 2021, doi: https://doi.org/10.46586/tches.v2021.i3.756-779

[27] J. Ktari, T. Frikha, M. Hamdi, and H. Hamam, "Enhancing Blockchain Consensus With FPGA: Accelerating Implementation for Efficiency," *IEEE Access*, vol. 12, pp. 44773–44785, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3379374

[28] E. Krahmer, P. Pessl, G. Land, and T. Güneysu, "Correction Fault Attacks on Randomized CRYSTALS-Dilithium," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2024, no. 3, pp. 174–199, Jul. 2024, doi: https://doi.org/10.46586/tches.v2024.i3.174-199

[29] J. W. Bos, O. Bronchain, F. Custers, J. Renes, D. Verbakel, and C. Van Vredendaal, "Enabling FrodoKEM on Embedded Devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 74–96, Jun. 2023, doi: https://doi.org/10.46586/tches.v2023.i3.74-96

[30] T. Nakai, D. Suzuki, and T. Fujino, "Timing Black-Box Attacks: Crafting Adversarial Examples through Timing Leaks against DNNs on Embedded Devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 149–175, Jul. 2021, doi: https://doi.org/10.46586/tches.v2021.i3.149-175

[31] M. Yamni, A. Daoui, P. Pławiak, O. Alfarraj, and A. A. A. El-Latif, "A Hardware-Accelerated Approach to Chaotic Image Encryption: LTB Map and FPGA Implementation," *IEEE Access*, vol. 12, pp. 103921–103940, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3432008

[32] C. Ma *et al.*, "BiTDB: Constructing A Built-in TEE Secure Database for Embedded Systems," *IEEE Trans Knowl Data Eng*, vol. 36, no. 9, pp. 4472–4485, Sep. 2024, doi: https://doi.org/10.1109/TKDE.2024.3380367

[33] C. Gewehr, L. Luza, and F. G. Moraes, "Hardware Acceleration of Crystals-Kyber in Low-Complexity Embedded Systems With RISC-V Instruction Set Extensions," *IEEE Access*, vol. 12, pp. 94477–94495, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3416812

[34] D. Enériz *et al.*, "Low-Cost FPGA Implementation of Deep Learning-Based Heart Sound Segmentation for Real-Time CVDs Screening," *IEEE Trans Instrum Meas*, vol. 73, pp. 1–16, 2024, doi: https://doi.org/10.1109/TIM.2024.3392271.

[35] T. Chamelot, D. Couroussé, and K. Heydemann, "MAFIA: Protecting the Microarchitecture of Embedded Systems Against Fault Injection Attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 42, no. 12, pp. 4555–4568, Dec. 2023, doi: https://doi.org/10.1109/TCAD.2023.3276507

[36] D. Mercadier, V. S. Nguyen, M. Rivain, and A. Udovenko, "OBSCURE: Versatile Software Obfuscation from a Lightweight Secure Element," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2024, no. 2, pp. 588–629, Mar. 2024, doi: https://doi.org/10.46586/tches.v2024.i2.588-629

[37] Y. Lee *et al.*, "An Efficient Hardware/Software Co-Design for FALCON on Low-End Embedded Systems," *IEEE Access*, vol. 12, pp. 57947–57958, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3387489

[38] J. Ge and F. Zhang, "SnapMem: Hardware/Software Cooperative Memory Resistant to Cache-Related Attacks on ARM-FPGA Embedded SoC," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 10, pp. 2902–2915, Oct. 2024, doi: https://doi.org/10.1109/TCAD.2024.3392082

[39] J. Van den Herrewegen, D. Oswald, F. D. Garcia, and Q. Temeiza, "Fill your Boots: Enhanced Embedded Bootloader Exploits via Fault Injection and Binary Analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 56–81, Dec. 2020, doi: https://doi.org/10.46586/tches.v2021.i1.56-81

[40] P. Radanliev, O. Santos, and A. Brandon-Jones, "Capability hardware enhanced instructions and artificial intelligence bill of materials in trustworthy artificial intelligence systems: analyzing cybersecurity threats, exploits, and vulnerabilities in new software bills of materials with artificial intelligence," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Aug. 2024, doi: https://doi.org/10.1177/15485129241267919

[41] N. A. Kose, R. Jinad, A. Rasheed, N. Shashidhar, M. Baza, and H. Alshahrani, "Detection of Malicious Threats Exploiting Clock-Gating Hardware Using Machine Learning," *Sensors*, vol. 24, no. 3, p. 983, Feb. 2024, doi: https://doi.org/10.3390/s24030983

[42] A. C. Cob-Parro, C. Losada-Gutiérrez, M. Marrón-Romera, A. Gardel-Vicente, and I. Bravo-Muñoz, "A new framework for deep learning video based Human Action Recognition on the edge," *Expert Syst Appl*, vol. 238, p. 122220, Mar. 2024, doi: https://doi.org/10.1016/j.eswa.2023.122220

[43] S. L. Thomas, J. Van den Herrewegen, G. Vasilakis, Z. Chen, M. Ordean, and F. D. Garcia, "Cutting Through the Complexity of Reverse Engineering Embedded Devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 360–389, Jul. 2021, doi: https://doi.org/10.46586/tches.v2021.i3.360-389

[44] A. Bazzi, A. Shaout, and D. Ma, "A Novel Variability-Rich Scheme for Software Updates of Automotive Systems," *IEEE Access*, vol. 12, pp. 79530–79548, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3409629

[45] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 301–325, Nov. 2022, doi: https://doi.org/10.46586/tches.v2023.i1.301-325

[46] B. Liu and M. Tang, "MS-LW-TI: Primitive-Based First-Order Threshold Implementation for 4 × 4 S-boxes," *IET Inf Secur*, vol. 2024, pp. 1–17, May 2024, doi: https://doi.org/10.1049/2024/8851878

[47] P. Branco, L. Fiolhais, M. Goulão, P. Martins, P. Mateus, and L. Sousa, "ROTed: Random Oblivious Transfer for embedded devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 215–238, Aug. 2021, doi: https://doi.org/10.46586/tches.v2021.i4.215-238

[48] B. Amornpaisannon, A. Diavastos, L.-S. Peh, and T. E. Carlson, "Secure Run-Time Hardware Trojan Detection Using Lightweight Analytical Models," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 2, pp. 431–441, Feb. 2024, doi: https://doi.org/10.1109/TCAD.2023.3316113.

[49] B. Boi and C. Esposito, "Securing the Internet of Medical Things with ECG-based PUF encryption," *IET Cyber-Physical Systems: Theory & Applications*, vol. 9, no. 2, pp. 115–124, Jun. 2024, doi: https://doi.org/10.1049/cps2.12089

[50] H. Becker, J. M. Bermudo Mera, A. Karmakar, J. Yiu, and I. Verbauwhede, "Polynomial multiplication on embedded vector architectures," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 482–505, Nov. 2021, doi: https://doi.org/10.46586/tches.v2022.i1.482-505

[51] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," *Future Generation Computer Systems*, vol. 157, pp. 288–302, Aug. 2024, doi: https://doi.org/10.1016/j.future.2024.03.054

[52] M. Khan, M. Hatami, W. Zhao, and Y. Chen, "A novel trusted hardware-based scalable security framework for IoT edge devices," *Discover Internet of Things*, vol. 4, art. no. 4, Apr. 2024, doi: https://doi.org/10.1007/s43926-024-00056-7

[53] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, "Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention," *Internet of Things*, vol. 28, art. no. 101398, Dec. 2024, doi: https://doi.org/10.1016/j.iot.2024.101398