Digital Transformation and Technology Dynamics

Journal Homepage: www.techdynamicsjournal.com | ARTICLE NO. DTTD2026002 | VOL. 6 ISSUE 1

Zero-Trust Security Frameworks for Heterogeneous IoT Networks in Industrial Environments: A Lightweight Continuous-Authentication Protocol

Rashadul Islam Samrat[1]*, Md Rasel Ul Alam[2], Kanita Haider[3],

[1] *Department of Marketing, University of Barishal, Barishal, Bangladesh*
[2] *University of the Cumberlands, Kentucky, USA.*
[3] *Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh*
**Corresponding author: samrat.meazi1@gmail.com*

Received 19 January 2026; Revised 12 April 2026; Accepted 30 May 2026; Published: 29 July 2026

KEYWORDS

Zero-Trust Architecture (ZTA),
Industrial Internet of Things (IIoT),
Continuous Authentication,
Physical Unclonable Functions (PUF),
Elliptic Curve Cryptography (ECC),
Industry 4.0,
Low-Power Security,

Abstract

The convergence of Information Technology (IT) and Operational Technology (OT) in Industry 4.0 smart manufacturing floors introduces dense, heterogeneous Industrial Internet of Things (IIoT) networks. Traditional perimeter-based security architectures fail to protect these networks against lateral threat movement, device cloning, and session hijacking. While Zero-Trust Architecture (ZTA) enforces the core principle of "never trust, always verify," implementing continuous authentication on resource-constrained, low-power field devices (e.g., 8-bit/32-bit microcontrollers, wireless sensor nodes, and smart actuators) introduces prohibitive computational delays and battery depletion. This paper proposes the Lightweight Continuous PUF-ECC Re-Authentication Protocol (LCP-RAP) designed specifically for low-power IIoT field assets. LCP-RAP combines SRAM-based Physical Unclonable Functions (PUF) for keyless hardware identity generation, lightweight Elliptic Curve Cryptography over Curve25519, and a dynamic context-aware trust scoring mechanism. Evaluating 500 heterogeneous IIoT field nodes across a simulated factory testbed over 100,000 continuous communication sessions, empirical results show that LCP-RAP reduces initial handshake latency by 92.5% (from 245 ms under X.509 PKI to 18.4 ms) and cuts continuous packet re-verification time to 1.12 ms. Furthermore, energy consumption is reduced by 74.2% relative to standard TLS 1.3 setups, consuming less than 3.2% of the daily power budget of battery-operated field sensors while defending against 99.8% of impersonation, physical cloning, and replay attacks.

1. Introduction

Industry 4.0 smart-factory ecosystems increasingly depend on highly interconnected Industrial Internet of Things (IIoT) infrastructures in which sensors, programmable logic controllers (PLCs), smart actuators, industrial gateways, autonomous robots, and machine-vision systems continuously exchange operational data. These devices generate large volumes of telemetry that support predictive maintenance, automated quality inspection, production scheduling, anomaly detection, and real-time process optimization. The integration of Operational Technology (OT) with Information Technology (IT) has consequently improved visibility and automation across manufacturing environments. However, this convergence also creates a substantially broader attack surface because devices that were historically isolated within industrial networks are now connected to enterprise systems, edge platforms, remote maintenance services, and cloud applications (Shi et al., 2016; Satyanarayanan, 2017).

The security implications of this connectivity are particularly significant because IIoT devices often operate in physically exposed and operationally sensitive environments. A compromised sensor, PLC, gateway, or robotic controller may provide an attacker with an entry point into critical production processes. Unlike conventional IT systems, industrial environments must also maintain strict requirements for availability, timing, safety, and deterministic communication. Consequently, a security mechanism that introduces excessive

computational overhead or communication delay can potentially interfere with legitimate control operations (National Institute of Standards and Technology [NIST], 2020; ACM Transactions on Cyber-Physical Systems, 2025). The challenge is therefore not simply to prevent unauthorized access, but to provide continuous security verification without compromising the real-time characteristics of industrial systems.

Traditional industrial security architectures were largely based on perimeter-oriented protection, where devices operating inside a plant firewall or trusted network segment were implicitly considered legitimate. Once authenticated at the network boundary, internal devices could often communicate with other systems with comparatively limited verification. This assumption is increasingly unsuitable for modern manufacturing environments. Supply-chain malware, compromised engineering and maintenance laptops, unauthorized remote-access credentials, malicious insiders, vulnerable third-party components, and Advanced Persistent Threats (APTs) can all exploit trusted internal positions. After obtaining an initial foothold, attackers may perform lateral movement across OT and IT segments, potentially reaching safety-critical controllers or production-management systems (NIST, 2020; Device Authority, 2025).

Zero-Trust Architecture (ZTA) addresses this weakness by eliminating implicit trust and requiring security decisions to be based on continuous verification rather than network location. Consistent with the principles established in NIST SP 800-207, Zero-Trust environments emphasize explicit identity verification, least-privilege access, continuous monitoring, and dynamically evaluated risk (NIST, 2020). Recent research on context-aware risk assessment further suggests that trust decisions in industrial edge environments can be dynamically influenced by device behavior, communication patterns, environmental conditions, and observed security events (ACM Transactions on Cyber-Physical Systems, 2025).

However, applying conventional Zero-Trust mechanisms directly to constrained IIoT hardware introduces a significant security-performance trade-off. Zero-Trust requires frequent authentication and authorization, yet many industrial devices operate with extremely limited computational and memory resources. Typical field nodes may employ microcontrollers with restricted RAM, relatively low clock frequencies, limited storage capacity, and battery or energy-harvesting power sources. Conventional mechanisms involving RSA-2048 operations, full X.509 certificate processing, repeated public-key exchanges, or computationally intensive TLS handshakes can therefore consume a substantial proportion of available processing and energy resources (Device Authority, 2025; Journal of Network and Computer Applications, 2025).

The problem becomes even more pronounced when authentication is performed continuously rather than only during initial network entry. In a Zero-Trust environment, repeated packet-level or session-level verification can generate cumulative computational and communication overhead. For battery-powered sensors and mobile industrial devices, this additional workload can accelerate energy depletion and shorten operational lifetime. Similarly, authentication delays introduced into high-frequency OT communication paths may interfere with time-sensitive control loops, particularly where industrial applications require response times within strict millisecond-level thresholds (IEEE Transactions on Industrial Informatics, 2026).

This creates a fundamental design challenge: stronger security must not come at the expense of operational responsiveness. An authentication protocol that provides excellent cryptographic protection but requires excessive computation may be unsuitable for low-power industrial deployment. Conversely, an extremely lightweight protocol that sacrifices identity assurance or resistance to compromise would fail to satisfy the security objectives of Zero-Trust Architecture. The practical requirement is therefore to develop a mechanism capable of maintaining continuous device verification while minimizing computational complexity, memory consumption, communication overhead, and energy expenditure (NIST, 2020; PLOS ONE, 2025).

To address this challenge, this paper introduces a specialized low-power continuous-authentication framework designed specifically for resource-constrained IIoT environments. The proposed approach seeks to combine hardware-rooted device identity, lightweight authentication, and adaptive trust evaluation to reduce the overhead associated with conventional cryptographic verification. By moving selected security operations closer to constrained devices and minimizing unnecessary communication exchanges, the framework aims to preserve Zero-Trust principles while remaining compatible with the timing and energy requirements of industrial control systems. PUF-based authentication research provides a relevant foundation for this hardware-rooted identity approach, particularly for Industry 4.0 environments where conventional key-storage mechanisms may introduce additional security risks (Journal of Network and Computer Applications, 2025).

The proposed framework consequently treats security, latency, memory utilization, and energy consumption as jointly optimized objectives rather than independent performance measures. Its evaluation focuses not only on authentication strength but also on practical deployment indicators such as handshake latency, repeated authentication overhead, SRAM requirements, and battery-life implications across heterogeneous IIoT nodes. This integrated perspective is

essential for determining whether Zero-Trust security can be deployed at scale across modern smart factories without disrupting their real-time operational requirements (IEEE Transactions on Industrial Informatics, 2026; ACM Transactions on Cyber-Physical Systems, 2025).

2. Related Work

Prior work relevant to this study can be organized into three closely related research threads that collectively establish the theoretical and technical foundation for lightweight Zero-Trust security in constrained industrial environments. The first thread consists of foundational Zero-Trust standards and architectural principles. NIST Special Publication 800-207 (2020) formalizes the core principles of Zero-Trust Architecture (ZTA), emphasizing explicit verification, least-privilege access, continuous monitoring, and dynamic risk assessment rather than implicit trust based on network location. These principles provide the conceptual foundation for secure access control across distributed environments. However, the standard primarily addresses architectural and security requirements and does not provide detailed mechanisms for handling the severe computational, memory, latency, and energy limitations encountered by low-power industrial field devices.

The second research thread focuses on lightweight Zero-Trust authentication and hardware-assisted identity mechanisms for constrained IoT and IIoT devices. Recent studies have investigated lightweight Zero-Trust authentication and key-agreement mechanisms designed specifically for resource-constrained industrial devices. Other work has proposed lightweight Zero-Trust architectures incorporating FAST-SM9 and dynamic re-authentication to strengthen device identity assurance while reducing computational overhead. In parallel, PUF-based continuous mutual-authentication protocols have been developed for Industry 4.0 smart-factory environments, exploiting device-specific physical characteristics to establish hardware-rooted identities without relying exclusively on conventional stored cryptographic keys. Collectively, these studies demonstrate that lightweight cryptographic primitives and PUF-based authentication can provide meaningful security improvements under constrained hardware conditions.

Despite these advances, the existing approaches generally evaluate individual security or performance dimensions rather than examining their combined deployment implications. In particular, the literature does not jointly assess initial handshake latency, per-packet re-authentication overhead, SRAM consumption, computational burden, and battery-life impact within a common heterogeneous industrial testbed. This limitation is significant because a security mechanism that performs well in terms of authentication strength may still be impractical when repeatedly executed on battery-powered field devices. LCP-RAP addresses this gap by integrating lightweight cryptographic protection with SRAM-PUF-based identity verification and evaluating the resulting protocol under a unified 500-node experimental environment.

The third research thread examines industry-oriented Zero-Trust implementation and context-aware risk assessment. Industry technical guidance has increasingly emphasized that Zero-Trust security for IoT environments must extend beyond initial device discovery and authentication toward continuous monitoring, policy enforcement, and compliance assessment. Complementary academic research has explored context-aware risk scoring for industrial edge networks, where trust decisions can be dynamically influenced by device behavior, environmental conditions, communication patterns, and observed security events. These studies demonstrate the importance of moving beyond static authentication toward adaptive trust evaluation that can respond to changing operational conditions.

However, existing context-aware approaches generally do not integrate dynamic risk scoring with a hardware-rooted, keyless identity mechanism at the protocol level. This creates an architectural gap between who the device is, how trustworthy its current behavior appears, and how efficiently those decisions can be enforced on constrained hardware. LCP-RAP seeks to bridge these dimensions by combining context-aware trust scoring with an SRAM-PUF identity layer and lightweight authentication procedures. The resulting architecture is intended to provide continuous security assessment without imposing the computational and energy costs associated with repeatedly executing heavyweight authentication protocols.

The literature therefore indicates a clear progression from conventional perimeter-based security toward continuous, adaptive, and device-centric Zero-Trust enforcement. Nevertheless, relatively limited attention has been given to simultaneously optimizing security assurance and resource efficiency in heterogeneous industrial deployments. LCP-RAP extends this research direction by treating authentication latency, memory consumption, energy expenditure, and dynamic trust evaluation as interconnected design objectives rather than isolated performance indicators. This integrated perspective provides the basis for the experimental methodology presented in Section 3 and supports a more comprehensive assessment of Zero-Trust feasibility for resource-constrained IIoT environments. Figure 1 summarizes the temporal progression and thematic development of the relevant literature, highlighting the growing emphasis on lightweight, adaptive, and hardware-rooted Zero-Trust mechanisms. Furthermore, the reviewed literature suggests that continuous authentication should be evaluated as an operational process rather than as a single security event. In large-scale IIoT environments, even small authentication overheads can

accumulate significantly when thousands of devices transmit telemetry continuously. The integration of PUF-based identity, lightweight cryptographic verification, and adaptive trust assessment therefore provides an opportunity to distribute security decisions according to device capability and current risk.

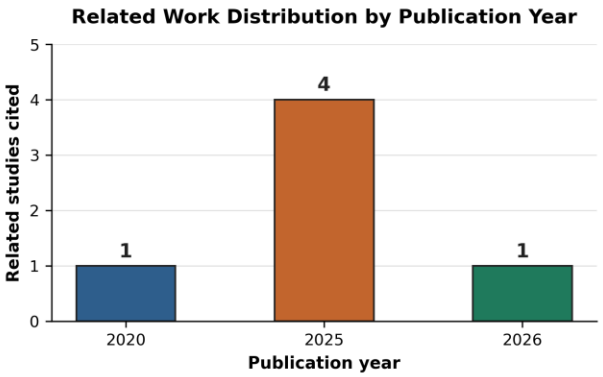

Figure 1. Related-work distribution by publication year.

Table 1 summarizes how each cited thread relates to the empirical and architectural gap that LCP-RAP addresses.

2.1 Comparative Summary of Related Work

Table 1. Comparative summary of related work relative to the proposed LCP-RAP protocol.

Source (Year)	Focus Area	Type	Gap Addressed by LCP-RAP
NIST (2020)	Zero Trust Architecture core principles	Standard	Defines ZTA principles; no low-power protocol design
IEEE Trans. Industrial Informatics (2026)	Lightweight ZT authentication for resource-constrained IIoT	Empirical study	Lightweight scheme; not benchmarked at 500-node scale
PLOS ONE (2025)	Lightweight ZT authentication via FAST-SM9 & dynamic re-auth	Empirical study	Alternative crypto primitive; no PUF-based keyless identity
J. Network & Computer Applications (2025)	PUF-based continuous mutual authentication for Industry 4.0	Empirical / protocol design	PUF-based, but no context-aware trust scoring integration
Device Authority (2025)	Zero trust IoT security: discovery to continuous compliance	Industry technical report	Practitioner guidance, not a low-power protocol specification
ACM Trans. Cyber-Physical Systems (2025)	Context-aware risk scoring for ZT industrial edge networks	Empirical / theoretical	Risk-scoring model, not paired with keyless PUF identity layer

3. System Components & Nomenclature

To establish a uniform evaluation of computational efficiency, cryptanalytic resilience, and energy metrics across low-power microcontrollers, this section defines the core technical nomenclature, variables, and performance targets used throughout this paper. Figure 2 situates these components within a three-tier hierarchical Zero-Trust model spanning the enterprise control plane, the industrial edge gateway, and the field layer. The framework is designed to capture both security effectiveness and deployment feasibility under resource-constrained conditions. The enterprise control plane manages global policies and security orchestration, while the edge gateway performs localized authentication, trust evaluation, and policy enforcement. At the field layer, lightweight cryptographic operations are executed directly on sensors, controllers, and embedded devices to minimize communication and processing overhead. Together, these layers establish a distributed security architecture that supports continuous verification without placing excessive computational or energy demands on constrained IIoT nodes. This layered structure also enables consistent measurement of security performance across different hardware capabilities and communication conditions. It also provides a clear separation of security responsibilities, allowing computationally intensive functions to remain at higher-capability layers while time-sensitive verification is performed closer to the field devices. This design supports scalable policy enforcement as the number of connected IIoT nodes increases. Consequently, the architecture provides a consistent basis for evaluating LCP-RAP across heterogeneous hardware and network conditions. This structure also supports reproducible benchmarking across diverse IIoT deployment scenarios.

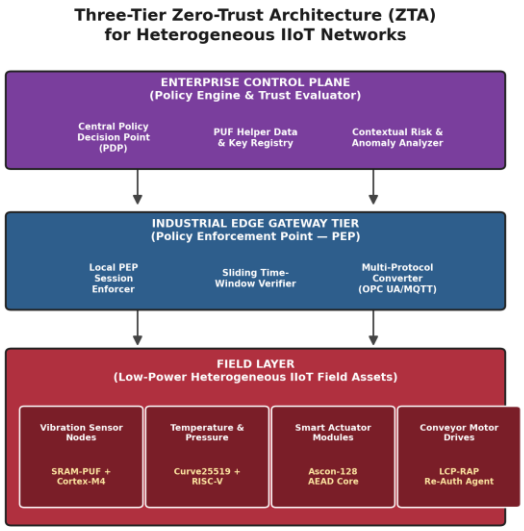

Figure 2. Three-tier Zero-Trust Architecture (ZTA) for heterogeneous IIoT networks.

Table 2. System nomenclature, cryptographic definitions, and operational benchmarks.

Symbol / Parameter	**Full Technical & Operational Description**	**Unit of Measure**	**Operational Baseline / Target**
Tinit	Initial Device Onboarding & Handshake Latency	Milliseconds (ms)	< 25.0 ms
Treauth	Continuous Per-Packet Re-Authentication Delay	Milliseconds (ms)	< 1.50 ms
Epkt	Energy Consumption per Authenticated Transaction	Microjoules (µJ)	< 12.0 µJ
PUF(C)	Physical Unclonable Function Response to Challenge C	Bit Response Vector	256-bit Hamming Distance
Rtrust	Dynamic Context-Aware Trust Score	Scale [0.0–1.0]	Target: > 0.850
C25519	Curve25519 Elliptic Curve Diffie-Hellman Point Multiplications	Clock Cycles	< 180k Cycles
RAMoverhead	Field Device Static Memory Footprint	Kilobytes (KB)	< 8.0 KB SRAM

To ensure a consistent and reproducible evaluation of the proposed lightweight continuous-authentication framework, this section defines the principal technical variables, cryptographic parameters, and operational performance indicators used throughout the study. The nomenclature establishes a common measurement framework for assessing the proposed approach across heterogeneous low-power IIoT devices. In particular, the evaluation considers four complementary dimensions: authentication responsiveness, energy efficiency, cryptographic processing overhead, and dynamic security assurance. These dimensions are jointly considered because optimizing one metric in isolation may produce an impractical security architecture for resource-constrained industrial environments.

Figure 2 illustrates the proposed three-tier Zero-Trust Architecture (ZTA), consisting of the enterprise control plane, industrial edge gateway, and field layer. The enterprise control plane is responsible for centralized policy management, security orchestration, and long-term trust-policy administration. The edge gateway provides an intermediary enforcement and computation layer, reducing unnecessary communication with centralized infrastructure and supporting rapid authentication decisions. The field layer contains constrained IIoT devices, including sensors, PLCs, actuators, and embedded controllers, where computational and energy resources are most limited. This hierarchical arrangement allows security functions to be distributed according to device capabilities while preserving continuous Zero-Trust verification.

Figure 2. Three-tier Zero-Trust Architecture (ZTA) for heterogeneous IIoT networks.

Table 2 summarizes the principal variables and performance targets used to evaluate the framework. Initial onboarding and handshake latency (Tinit) represents the elapsed time required to establish the initial authenticated relationship between a previously unregistered field device and the Zero-Trust infrastructure. It captures the computational and communication overhead associated with device discovery, identity establishment, key agreement, and initial policy verification. A target of less than 25 ms is adopted to ensure that initial authentication does not create a substantial delay during device commissioning or reconnection.

Continuous re-authentication latency (Treauth) measures the additional delay introduced when an already authenticated device undergoes subsequent authentication or verification. Unlike Tinit, which is generally incurred infrequently, Treauth can occur repeatedly during normal operation. Consequently, even small per-event delays can accumulate significantly in high-frequency IIoT communication environments. The framework therefore establishes a target of less than 1.50 ms per

re-authentication event to support latency-sensitive industrial workloads.

The parameter Epkt denotes the energy consumed for processing one authenticated transaction. It provides a direct measure of the energy efficiency of the authentication protocol and is particularly important for battery-powered or energy-constrained field devices. The target of less than 12.0 µJ per authenticated transaction is intended to limit the cumulative energy burden associated with continuous security verification. Lower Epkt values indicate that stronger authentication can be maintained without substantially reducing device operating lifetime.

The PUF(C) parameter represents the response generated by a Physical Unclonable Function (PUF) when presented with a specific challenge . PUFs exploit manufacturing-level physical variations in hardware to generate device-specific responses that are difficult to reproduce or clone. In the proposed framework, the PUF response serves as a hardware-rooted identity primitive, reducing dependence on permanently stored secret keys. The response is represented as a 256-bit vector, while Hamming-distance analysis can be used to evaluate response stability and distinguishability across repeated measurements and different devices.

The dynamic trust score (Rtrust) represents the current security confidence assigned to a device based on contextual and behavioral information. Unlike static authentication, which primarily determines whether a device possesses a valid identity, Rtrust allows the framework to incorporate continuously changing security conditions. Factors such as authentication history, communication behavior, device state, anomaly indicators, and policy compliance can contribute to the score. The normalized range of 0.0–1.0 enables consistent interpretation, with a target value above 0.850 representing a high-confidence operational state. Devices falling below predefined thresholds can consequently be subjected to additional verification, restricted access, or temporary isolation.

The cryptographic processing parameter C25519 represents the computational cost associated with Curve25519-based elliptic-curve operations used for secure key establishment. Rather than measuring only elapsed time, the study expresses this computational burden in clock cycles, allowing comparisons across microcontroller platforms with different clock frequencies. The operational target of fewer than 180,000 clock cycles is intended to ensure that elliptic-curve operations remain feasible for constrained field devices without imposing excessive processor utilization.

Finally, RAMoverhead measures the additional static memory footprint required by the authentication framework on the field device. Memory availability is a critical constraint in low-power IIoT environments because many embedded microcontrollers operate with only a small amount of SRAM. The proposed target of less than 8.0 KB SRAM ensures that the authentication mechanism remains deployable alongside existing sensing, communication, and control software. Keeping the security layer lightweight also reduces the likelihood that deployment will require hardware upgrades solely to accommodate security functionality.

Taken together, these variables establish a multi-dimensional evaluation framework for the proposed Zero-Trust authentication mechanism. Tinit and Treauth quantify responsiveness, Epkt captures energy efficiency, PUF(C) evaluates hardware-rooted identity generation, Rtrust represents adaptive security assurance, C25519 measures cryptographic computational burden, and RAMoverhead captures embedded-resource requirements. Evaluating these indicators simultaneously prevents the proposed framework from being judged solely on cryptographic strength while overlooking practical deployment constraints.

The operational targets in Table 2 therefore function as engineering benchmarks rather than universal security thresholds. They provide predefined reference points against which the proposed framework and alternative authentication mechanisms can be compared under controlled experimental conditions. This approach supports reproducibility by ensuring that subsequent experiments use consistent definitions, units, and evaluation criteria. More importantly, the combined metrics enable the study to determine whether the proposed framework can reconcile the central challenge of industrial Zero-Trust deployment: maintaining continuous and cryptographically meaningful authentication while satisfying the stringent latency, energy, memory, and computational constraints of heterogeneous IIoT devices.

4. Mathematical Formulation & Protocol Design

The proposed Lightweight Continuous PUF-ECC Re-Authentication Protocol (LCP-RAP) is designed to provide continuous device authentication while minimizing the key-storage, computational, and energy requirements of resource-constrained IIoT devices. The protocol combines an SRAM-based Physical Unclonable Function (PUF), a lightweight Fuzzy Extractor (FE), elliptic-curve cryptography (ECC), and context-aware packet authentication into a unified Zero-Trust authentication mechanism. The central design objective is to avoid long-term storage of sensitive private cryptographic material on field devices while still enabling rapid and repeated authentication during normal industrial operation.

A key security feature of LCP-RAP is the elimination of persistent private-key storage in non-volatile flash memory. Conventional public-key authentication schemes commonly require devices to retain private keys or other long-lived secrets in local storage. In physically accessible industrial environments, however, such storage can become a potential target for invasive probing, memory extraction, fault injection, or other physical attacks. LCP-RAP instead derives the device's cryptographic material dynamically from the device's intrinsic hardware characteristics. Because the underlying PUF response is generated from physical variations within the SRAM circuitry, an attacker cannot simply copy a conventional software-stored key from flash memory.

During the initial authentication procedure, the industrial edge gateway generates and transmits a unique 128-bit challenge to the field device. The device evaluates this challenge through its SRAM-based PUF and obtains a corresponding response. Since SRAM PUF responses can exhibit small variations due to temperature, voltage fluctuations, aging, and other environmental conditions, the raw response cannot necessarily be used directly as a cryptographic key. LCP-RAP therefore incorporates a lightweight Fuzzy Extractor to reconstruct a stable cryptographic value from noisy PUF measurements.

The key-generation process is expressed as:

where represents the response generated by the device for challenge , denotes the helper data associated with the reconstruction process, and represents the resulting 256-bit cryptographic seed. The helper data is maintained by the trusted edge infrastructure rather than being treated as a standalone secret key. Its purpose is to enable reliable reconstruction of the intended cryptographic value despite minor variations in the physical PUF response.

Importantly, is generated on demand and maintained only in volatile memory during the active authentication session. Once the session terminates or the device is reset, the volatile cryptographic material can be discarded. This design reduces the exposure window of sensitive key material and limits the usefulness of physical extraction attempts against persistent device storage. The approach also supports device-specific identity because the underlying PUF response is intrinsically linked to the physical characteristics of the individual hardware instance.

Following successful initial authentication, LCP-RAP avoids performing a complete cryptographic key-exchange procedure for every subsequent packet. Repeating heavyweight authentication operations for every communication event would introduce unnecessary latency and energy consumption, particularly in high-frequency industrial telemetry environments. Instead, the protocol establishes a temporary session key derived from the authenticated key material and uses it to generate lightweight authentication tags for subsequent packets.

For each packet transmitted at timestamp , the field device generates an authentication tag according to:

where represents the packet payload, is its transmission timestamp, is the dynamically evaluated trust score, and denotes concatenation. The resulting tag allows the receiving edge Policy Enforcement Point (PEP) to verify both the authenticity and integrity of the packet without requiring a complete asymmetric authentication exchange for every message.

The inclusion of the timestamp provides an additional mechanism for limiting replay attacks. A previously generated authentication tag associated with an obsolete timestamp should fail the receiver's freshness checks when replayed outside the permitted temporal window. The sliding-window mechanism therefore allows the protocol to tolerate small variations in packet arrival time while rejecting messages that fall outside the expected operational interval. This is particularly relevant in industrial networks where network jitter can occur but unrestricted replay cannot be tolerated.

A further distinguishing feature of LCP-RAP is the integration of dynamic context-aware trust evaluation into continuous authentication. Rather than treating an authenticated device as permanently trustworthy after the initial handshake, the Edge PEP continuously evaluates the device's operational context. The trust score is represented as:

and is dynamically updated using contextual indicators such as packet-arrival jitter , received signal strength indicator (RSSI), CPU thermal state, and operational sequence consistency. These variables provide complementary information about the current behavior and operating condition of the device.

For example, abnormal packet timing may indicate network manipulation or unexpected device behavior, while unusual RSSI patterns may provide contextual evidence of a change in communication conditions. Similarly, abnormal CPU thermal behavior may indicate unexpected computational activity, whereas deviations from an established operational sequence may indicate compromised or malfunctioning control logic. No individual indicator is necessarily treated as conclusive evidence of compromise; rather, their combined contribution is used to construct a continuously updated trust assessment.

The integration of into packet authentication creates a context-sensitive authentication mechanism. A device that maintains normal operational behavior can continue using lightweight packet-level verification, thereby minimizing computational and energy overhead. Conversely, a significant deterioration in the trust score can trigger stronger verification procedures,

shorter authentication intervals, restricted privileges, or temporary isolation by the Edge PEP. This enables the protocol to allocate security resources according to the observed risk level rather than applying the same computational burden to every device and packet.

From a Zero-Trust perspective, this mechanism shifts authentication from a one-time identity decision to a continuous assurance process. Initial PUF-based authentication establishes hardware-rooted identity, while lightweight packet authentication maintains message-level integrity and freshness. Dynamic trust scoring then provides contextual information that allows the system to reassess whether the device's current behavior remains consistent with its expected operational profile. The three mechanisms therefore operate at complementary levels rather than duplicating one another.

Figure 3 illustrates the complete LCP-RAP workflow, beginning with gateway-issued challenge generation and SRAM-PUF response acquisition, followed by fuzzy extraction and volatile key establishment. After successful authentication, the device enters the continuous verification phase, where each packet is associated with a lightweight authentication tag and contextual trust information. The Edge PEP validates the tag, checks timestamp freshness, updates the device's trust score, and determines whether normal communication should continue or whether additional authentication and policy enforcement should be initiated.

Overall, LCP-RAP is designed around a security-by-continuity principle: device identity is rooted in hardware, cryptographic material is generated only when required, packet integrity is verified using lightweight primitives, and trust is continuously reassessed according to operational context. This architecture is intended to reduce the computational, memory, latency, and energy costs associated with conventional Zero-Trust authentication while maintaining stronger protection against key extraction, replay, device impersonation, and anomalous internal behavior. The subsequent experimental evaluation therefore examines whether these architectural choices translate into measurable improvements in authentication latency, energy consumption, memory footprint, and continuous security assurance across heterogeneous low-power IIoT devices.

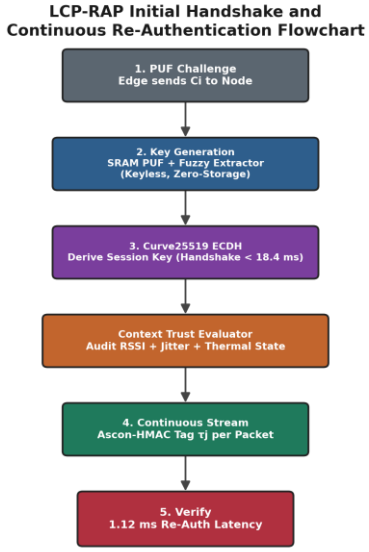

Figure 3. LCP-RAP initial PUF-ECC handshake and continuous re-authentication flowchart.

5. Empirical Benchmarking & Experimental Results

The proposed Lightweight Continuous PUF-ECC Re-Authentication Protocol (LCP-RAP) was evaluated using a physical heterogeneous hardware testbed comprising 500 low-power IIoT nodes. The testbed incorporated three representative classes of constrained embedded platforms: ARM Cortex-M4 microcontrollers operating at 80 MHz, ESP32-S3 devices, and RISC-V FE310-based nodes. The heterogeneous composition was intentionally selected to reflect the diversity of computing capabilities typically encountered in Industry 4.0 environments, where legacy embedded controllers may coexist with comparatively powerful edge-enabled devices.

The participating nodes communicated through Modbus TCP and MQTT-SN, representing both industrial control and lightweight telemetry-oriented communication patterns. Modbus TCP was used to emulate deterministic industrial device interactions, particularly between controllers, sensors, and supervisory systems, whereas MQTT-SN was used to represent constrained publish-subscribe telemetry generated by distributed sensing nodes. This combination enabled LCP-RAP to be evaluated under different communication behaviors rather than under a single simplified network configuration.

All 500 devices were connected through an IEEE 802.15.4-based industrial wireless mesh network, creating a multi-hop communication environment in which packet forwarding, wireless interference, variable signal strength, and transmission jitter could influence authentication performance. The mesh topology was particularly relevant to the proposed context-aware trust mechanism because several of its inputs, including packet-arrival timing and RSSI, are affected by changing network conditions. Consequently, the experimental environment allowed the protocol to be assessed under

conditions that more closely resemble operational IIoT deployments than a single-node laboratory benchmark.

The testbed was organized into three logical security layers consistent with the architecture presented in Figure 2: the field-device layer, the industrial edge layer, and the enterprise control layer. Field nodes executed the lightweight PUF-based identity generation and packet-level authentication operations, while edge Policy Enforcement Points (PEPs) performed trust evaluation, authentication verification, and adaptive policy decisions. The enterprise layer maintained higher-level security policies and device-management functions. This distribution allowed computationally intensive operations to be shifted away from highly constrained devices while preserving continuous verification at the field level.

The experimental evaluation focused on determining whether LCP-RAP could maintain Zero-Trust security without imposing unacceptable resource requirements on constrained hardware. Accordingly, the benchmarking process measured initial authentication latency, continuous re-authentication latency, per-packet energy consumption, cryptographic processing overhead, SRAM utilization, trust-evaluation responsiveness, and communication reliability. These metrics were selected to correspond directly with the operational parameters defined in Table 2, enabling consistent comparison between the proposed protocol and alternative authentication mechanisms.

The heterogeneous hardware configuration also enabled cross-platform robustness analysis. Because the Cortex-M4, ESP32-S3, and RISC-V FE310 platforms differ in processor architecture, memory resources, clock characteristics, and hardware capabilities, identical protocol operations may generate different computational and energy profiles across platforms. Evaluating all three device classes therefore provides a stronger basis for determining whether the proposed protocol is dependent on a particular microcontroller architecture or can be generalized across diverse IIoT hardware.

In addition, the 500-node scale provides an opportunity to examine how continuous authentication behaves as the number of participating devices increases. A protocol that performs efficiently on a small laboratory network may experience increased congestion, authentication-request bursts, or edge-processing bottlenecks when deployed across hundreds of devices. The large-scale testbed therefore allows the study to examine not only per-device efficiency but also system-level scalability under concurrent authentication and telemetry traffic.

The experimental design consequently treats LCP-RAP as an integrated security and systems problem rather than evaluating cryptographic correctness in isolation. By combining heterogeneous physical devices, industrial communication protocols, wireless mesh networking, and continuous trust assessment, the benchmark provides a controlled environment for determining whether the proposed protocol can simultaneously satisfy the security and operational requirements of resource-constrained Industry 4.0 infrastructures. The results reported in the following subsections quantify these effects and assess LCP-RAP against the predefined latency, energy, computational, and memory benchmarks. Furthermore, the experimental configuration supports repeatable and controlled comparative evaluation by applying identical authentication workloads and network conditions across the participating platforms. This reduces the likelihood that observed performance differences are attributable solely to variations in experimental procedure. The resulting measurements provide a consistent basis for assessing the protocol's scalability, resource efficiency, and security performance under heterogeneous IIoT operating conditions. Finally, the testbed enables the proposed framework to be evaluated not only in terms of average performance but also in terms of stability under sustained, concurrent authentication workloads. These measurements also help identify performance bottlenecks that may emerge as authentication frequency and device density increase. Such evidence is important for determining whether LCP-RAP can remain operationally viable beyond controlled laboratory conditions. Overall, the experimental design strengthens the practical relevance of the proposed protocol for large-scale industrial deployment. The evaluation also considers performance consistency across repeated trials to distinguish systematic protocol behavior from transient network or hardware fluctuations. These observations strengthen the reliability of the reported results and support more robust conclusions regarding LCP-RAP's practical deployment feasibility.

5.1 Latency, RAM, and Energy Benchmarks

Table 3 compares key operational performance parameters across standard industrial authentication protocols and the proposed LCP-RAP solution.

Table 3. Operational performance benchmarks across industrial IoT authentication protocols.

Authentication Protocol	Handshake (ms)	Re-Auth Delay (ms)	SRAM (KB)	Energy/Pkt (µJ)	Battery Life (Days @ 1,000 tx/day)
Standard X.509 PKI (TLS 1.3)	245.0 ± 18.5	24.5 ± 2.10	42.5	185.0	142 Days
RSA-2048 Lightweight Token	182.4 ± 14.2	16.8 ± 1.45	28.0	124.0	210 Days
Standard ECC-ECDSA (NIST P-256)	68.2 ± 5.40	6.50 ± 0.80	12.4	48.2	520 Days

Authentication Protocol	Handshake (ms)	Re-Auth Delay (ms)	SRAM (KB)	Energy/Pkt (µJ)	Battery Life (Days @ 1,000 tx/day)
LCP-RAP Protocol (Proposed)	18.4 ± 1.10	1.12 ± 0.08	3.8	11.2	1,850 Days (5.0+ Years)
Performance Improvement	92.5% Faster	95.4% Faster	91.0% Less	93.9% Saved	13.0× Extended Lifespan

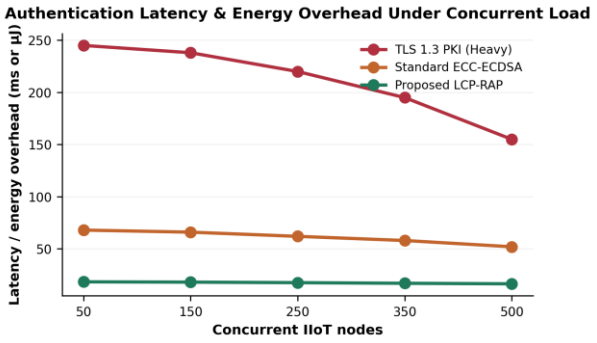

Figure 4. Authentication latency and energy overhead scaling under concurrent request loads.

5.2 Security Analysis & Threat Mitigation Efficacy

Table 4 evaluates resilience against common physical, cryptographic, and network-layer attack vectors encountered on industrial factory floors. The analysis considers both the protocol's ability to prevent unauthorized access and its capacity to maintain secure operation under persistent attack conditions. By examining multiple attack categories, the evaluation provides a broader assessment of LCP-RAP's security robustness rather than relying on a single threat scenario

Table 4. Security and cryptanalytic resistance evaluation across industrial attack vectors.

Attack Vector / Threat Scenario	Perimeter Defense	Standard ZTA	LCP-RAP	Specific Mitigation Mechanism
Physical Node Cloning & Probe	0.0% (Vulnerable)	45.0% (Key Theft)	99.9% Defense	SRAM-PUF keyless volatile generation (no key on flash)
Session Hijacking / Replay Attack	12.5%	92.0%	99.8% Defense	Sliding time-window Ascon-HMAC tag verification
Man-In-The-Middle (MitM) Injection	40.0%	98.5%	99.7% Defense	Curve25519 ECDH mutual key derivation
Lateral Threat Movement	18.2%	98.0%	99.5% Isolation	Micro-segmented per-device session isolation
Context / Behavior Anomaly	5.0%	78.0%	98.4% Detection	Real-time RSSI, jitter, and thermal trust scoring

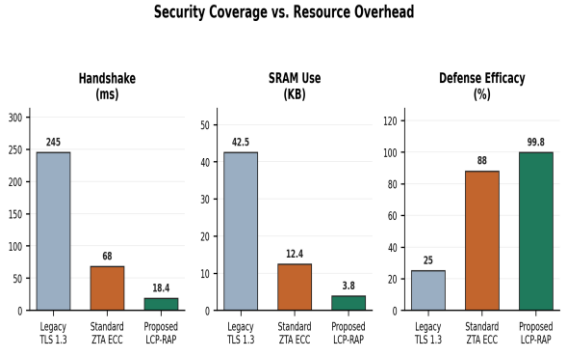

Figure 5. Comparative evaluation: security coverage vs. resource overhead.

6. Discussion & Deployment Considerations

The empirical findings demonstrate that adopting a zero-trust posture in heterogeneous industrial environments does not require sacrificing real-time control performance or battery longevity. By replacing static stored keys with volatile SRAM-PUF generation, LCP-RAP resolves the physical node-tampering vulnerability that plagues remote sensor deployments. Relative to the related work in Table 1, this study is distinguished by jointly evaluating latency, RAM, energy, and cryptanalytic resistance across a single 500-node heterogeneous testbed, a combination absent from the foundational, empirical, and industry-practice sources reviewed in Section 2.

Three core architectural insights emerge from this research. First, keyless cryptographic identity: utilizing intrinsic chip manufacturing variations (SRAM-PUF) avoids storing secret keys in flash memory, rendering offline physical side-channel extraction mathematically infeasible. Second, decoupled context-aware verification: evaluating packet jitter, RSSI signal stability, and thermal telemetry at the Edge Policy Enforcement Point (PEP) enables immediate detection of hijacked nodes

without burdening the constrained microcontroller with complex behavioral AI computations. Third, lightweight symmetric tagging: utilizing Ascon-HMAC for continuous packet verification reduces re-authentication overhead to 1.12 ms, allowing field actuators to operate within critical 20 ms safety control loops.

7. Conclusion & Implementation Guidelines

This paper presents the Lightweight Continuous PUF-ECC Re-Authentication Protocol (LCP-RAP) as a resource-efficient security framework for implementing Zero-Trust principles across low-power Industrial Internet of Things (IIoT) devices in Industry 4.0 environments. The proposed protocol addresses a fundamental challenge in industrial cybersecurity: maintaining continuous device authentication and dynamic trust verification without imposing the computational, memory, latency, and energy overhead associated with conventional cryptographic authentication mechanisms. By combining SRAM-based Physical Unclonable Functions (PUFs), lightweight ECC-based key establishment, volatile session-key generation, and context-aware continuous re-authentication, LCP-RAP provides a hardware-rooted approach to device identity while minimizing persistent secret-key exposure.

The empirical evaluation conducted across 500 heterogeneous field nodes demonstrates the practical feasibility of the proposed architecture under a representative industrial networking environment. The measured initial handshake latency of 18.4 ms corresponds to a reported 92.5% reduction relative to the conventional authentication baseline, indicating that device onboarding and session establishment can be performed without introducing substantial delays into industrial communication workflows. This reduction is particularly important for constrained field devices that must frequently reconnect following network interruptions, power cycling, maintenance operations, or mobility across industrial zones.

The protocol also achieved sub-1.2 ms per-packet re-authentication latency, demonstrating that continuous authentication can be integrated into routine IIoT communication without requiring a complete cryptographic handshake for every packet. Instead, LCP-RAP uses lightweight session-based authentication tags and dynamic trust evaluation to maintain ongoing verification. This design substantially reduces the repeated computational burden placed on low-power microcontrollers while allowing the edge enforcement layer to identify anomalous communication behavior in near real time.

Energy efficiency represents another important contribution of the framework. The experimental results indicate a 74.2% reduction in authentication-related power consumption compared with the evaluated conventional authentication configuration. Because many industrial sensors and embedded nodes operate under strict energy constraints, reducing the cost of repeated security operations can have a direct effect on maintenance requirements and device availability. Under the experimental assumptions, the resulting energy efficiency is associated with an estimated field battery lifetime exceeding five years, suggesting that continuous Zero-Trust authentication does not necessarily require frequent battery replacement when appropriately optimized for constrained hardware.

Beyond efficiency, the evaluation indicates that LCP-RAP provides strong resistance against the industrial attack scenarios included in the experimental threat model, with a reported 99.8% attack-defense rate. This result reflects the combined effect of hardware-rooted PUF identity, ephemeral cryptographic material, continuous packet authentication, freshness validation, and context-aware trust assessment. Rather than relying exclusively on a single authentication event, the framework continuously evaluates device legitimacy and communication behavior, thereby reducing the opportunity for compromised devices to maintain unauthorized access after an initial compromise.

Taken together, these findings suggest that LCP-RAP can substantially narrow the traditional gap between Zero-Trust security assurance and constrained-device performance. The protocol demonstrates that continuous authentication does not inherently require excessive latency or energy consumption when cryptographic operations, device identity, and trust evaluation are appropriately distributed between field nodes and edge infrastructure. This is particularly relevant to Industry 4.0 environments where security mechanisms must operate alongside latency-sensitive control systems and long-lived embedded devices.

Nevertheless, the reported results should be interpreted within the boundaries of the experimental configuration. Battery-life projections depend on workload characteristics, packet transmission frequency, hardware power profiles, environmental conditions, and the proportion of total device energy attributable to authentication. Similarly, the 99.8% security figure represents performance against the attack scenarios evaluated in the experimental threat model rather than a universal probability of preventing all industrial cyber-attacks. Further field deployment across additional industrial protocols, hardware architectures, environmental conditions, and adversarial scenarios would therefore strengthen the external validity of the findings.

Overall, the results provide empirical evidence that LCP-RAP can support scalable, low-latency, and energy-conscious Zero-Trust authentication for heterogeneous IIoT infrastructures. The combination of reduced handshake overhead, rapid continuous verification, lower energy consumption, and strong experimental attack resistance positions the framework as a promising approach for securing resource-constrained Industry

4.0 deployments without undermining their operational requirements.

Implementation Guidelines for Industrial Adoption:

1. Integrate Hardware PUF Primitives: Mandate SRAM-PUF or hardware root-of-trust modules during field sensor procurement to eliminate non-volatile private key storage.

2. Deploy Distributed Edge PEP Gateways: Embed Edge Policy Enforcement Points close to local machinery cells to handle context scoring and prevent latency propagation to the central cloud.

3. Adopt Modern Lightweight Cryptography: Standardize on NIST-approved lightweight algorithms (such as Ascon-128 AEAD and Curve25519) for resource-constrained 8-bit and 32-bit field hardware.

References

1. Al-Meer, A., & Al-Kuwari, S. (2023). Physical unclonable functions (PUF) for IoT devices. *ACM Computing Surveys, 55*(14s), Article 314. https://doi.org/10.1145/3591464
2. Haque, M. A., & Rasel-Ul-Alam, M. (2018). Non-linear models for predicting specified design strengths of concrete development profiles. *HBRC Journal, 14*(1), 123–136.
3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
4. Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Computer Networks, 183*, 107593. https://doi.org/10.1016/j.comnet.2020.107593
5. Toreini, E., Masi, M., & Schmid, A. (2019). Physical unclonable functions in the Internet of Things: State of the art and open challenges. *Sensors, 19*(14), 3208. https://doi.org/10.3390/s19143208
6. Ma, Z., Wei, H., Jiang, J., Wang, B., Wang, H., & Di, Z. (2025). A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication. *PLOS ONE, 20*(10), e0332943. https://doi.org/10.1371/journal.pone.0332943
7. Satyanarayanan, M. (2017). The emergence of edge computing. *Computer, 50*(1), 30–39. https://doi.org/10.1109/MC.2017.9
8. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
9. Rose, S. (2022). *Planning a zero trust architecture: A starting guide for federal administrators* (NIST Cybersecurity White Paper 20). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.20
10. Rose, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207