International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V6I4P124
Eureka Vision Publication | Volume 6, Issue 4, 159-162, 2025

Original Article

Zero-Trust in Connected Physical Systems: A Security Blueprint for Smart Homes and Industrial IoT

Vignesh Alagappan
Sr. Manager, Ecosystem Engineering, Rheem Manufacturing, Roswell, GA,USA.

Received On: 07/11/2025 ***Revised On: 29/11/2025*** ***Accepted On: 06/12/2025*** ***Published On: 15/12/2025***

Abstract - The rapid expansion of connected physical systems (CPS) from smart homes and connected water heaters to industrial HVAC ecosystems has intensified the need for security frameworks that operate under the assumption that no entity is inherently trustworthy. Traditional perimeter models fail in distributed IoT topologies characterized by heterogeneous devices, multi-protocol radios, global supply chains, and cloud-driven control surfaces. This paper proposes a Zero-Trust Security Blueprint for connected Physical Systems, integrating identity-first device authentication, robust PKI and mTLS frameworks, secure boot and runtime attestation, BLE/Wi-Fi/Thread/Matter-based commissioning, and end-to-end software supply chain integrity. The blueprint outlines architectural principles, implementation pathways, and governance models required to operationalize Zero-Trust across smart homes and industrial IoT ecosystems.

Keywords - *Zero-Trust, Connected Physical Systems, Iot Security, PKI, Mtls, Device Identity, BLE Commissioning, Thread, Matter, Runtime Attestation, Secure OTA, Supply Chain Security, Connected Water Heaters, HVAC, Smart Homes.*

1. Introduction

Connected physical systems (CPS) increasingly form the backbone of residential, commercial, and industrial operations. From connected HVAC systems to demand-response enabled water heaters and grid-interactive equipment, modern CPS environments are distributed, interoperable, and cloud-orchestrated. However, this connectivity introduces a broader attack surface [3]. Devices operate across multiple RF interfaces, authenticate through multiple gateways, and often rely on outsourced manufacturing for hardware, firmware, and provisioning. These complexities undermine traditional trust assumptions.

The Zero-Trust paradigm offers a fundamental shift: trust no device, no subsystem, and no network, always verify identity, integrity, and context [1]. This paper builds a practical blueprint for implementing Zero-Trust in CPS environments, emphasizing:

- Identity-based trust rooted in immutable cryptographic anchors
- End-to-end PKI with lifecycle-aware certificate management
- Interoperable commissioning across BLE, Wi-Fi, Thread, and Matter
- Secure OTA and continuous integrity verification
- Strong supply chain governance from silicon to cloud

2. Background and Motivation

2.1. Connected Physical Systems Are No Longer Perimeter-Bound

CPS ecosystems operate in hybrid spaces: part physical, part digital. Devices often:

- Communicate locally (BLE/Thread/BLE-Mesh/NFC) [8], [9]
- Communicate via cloud through Wi-Fi, LTE-M, NB-IoT, Sidewalk
- Exchange data between gateways and mobile apps
- Integrate with energy/grid service providers

This matrix creates dynamic trust boundaries, making perimeter-based security models obsolete [1].

2.2. Key Challenges

- Device identity fragmentation across radios, serial numbers, MAC addresses, and ecosystem-specific identifiers
- Weak commissioning flows, particularly in BLE-based or QR-code-based onboarding [5]
- High-risk global supply chains, including CM/OEM-based key provisioning
- Inconsistent OTA pipelines, risking firmware tampering [3]
- Limited runtime integrity checks, allowing post-deployment compromise

2.3. Why Zero-Trust is Necessary

Zero-Trust extends beyond enterprise IT [1]. In CPS:

- Physical tampering is common
- Devices live 10–15 years on the field
- Gateways may change across homeowners
- Firmware evolves constantly
- Multiple vendors share responsibility across the device-to-cloud chain

This necessitates a continuous, identity-first, context-aware trust model [1], [3].

3. Zero-Trust Architecture for Connected Physical Systems

Zero-Trust in CPS is anchored in five core pillars [1]:

- Strong, immutable device identities
- Continuous authentication and encrypted communication (mTLS)
- Contextual authorization (least privilege)
- Continuous verification (runtime attestation)
- Full lifecycle governance (secure supply chain → EoL)

The following sections detail the components of this architecture.

4. Identity-Based Device Trust

Identity is the foundation of Zero-Trust [1], [3]. In CPS systems, a device identity must be:

- Cryptographically anchored (e.g., ECC key in secure element or silicon root-of-trust) [4]
- Immutable across hardware lifecycle
- Recognizable by all trust participants cloud, mobile, gateway, commissioning protocols

4.1. Identity Construction

A device identity typically includes:

- Device Key Pair (DKP) Generated inside a secure element or MCU-internal TRNG [4]
- Device Attestation Certificate (DAC) Signed by the OEM or ecosystem CA [2]
- Identity Metadata Product type, region, hardware revision, commissioning capabilities

4.2. Multi-Radio Identity Alignment

Devices often use BLE for commissioning [9], Wi-Fi for cloud, Thread for ecosystem-level messaging [8]. A unified identity ensures:

- BLE pairing ties to the same identity used in cloud mTLS
- Thread/Matter fabric certificates map to device attestation identity [2], [8]
- OEM-level PKI coexists with ecosystem PKIs (Matter, OpenThread, proprietary cluster models)

5. Pki Hierarchy and Mtls

5.1. PKI for CPS

A multi-tier PKI hierarchy is essential [1], [6]:

- Root CA (offline, OEM-controlled)
- Intermediate CAs
- Device attestation
- Operational certificates
- OTA signing
- Leaf certificates
- Device identity
- Gateway/client identities

5.2. Mtls for All Communication

All device-to-cloud traffic must use mTLS to guarantee [6], [7]:

- Confidentiality
- Authenticity
- Replay protection
- Identity-bound sessions

This reduces reliance on shared secrets, tokens, or cloud-generated credentials [1].

5.3. Certificate Lifecycles

Devices must support:

- Certificate renewal
- Revocation
- Ownership transfer
- Multi-gateway coexistence
- Fabric membership for Matter/Thread [2], [8]

6. Commissioning Flows across Ble, Wi-Fi, Thread, Matter

Commissioning is a high-risk phase [5]. Zero-Trust requires:

- Proof of device authenticity
- Proof of installer/homeowner authority
- Binding to the correct cloud, fabric, or ecosystem

6.1. BLE → Wi-Fi Commissioning

Key principles [9]:

- Verify DAC during BLE handshake [2]
- Use ECDH to derive session keys
- Never expose Wi-Fi credentials unencrypted [5]
- Persist identity before network association

6.2. Thread / Matter Commissioning

Matter introduces [2]:

- PASE (Password Authenticated Session Establishment)
- CASE (Certificate Authenticated Session Establishment)
- DAC/NOC chain validation

Zero-Trust alignment requires:

- OEM verifies DAC origin [2]
- Cloud validates NOC ownership
- Runtime attestation ensures firmware integrity before fabric onboarding [4]

7. Supply Chain Security

7.1. Contract Manufacturers (CM/OEM)

Risks include [3], [5]:

- Unauthorized key generation
- Counterfeit boards
- Firmware flashing outside secure process
- Debug interfaces left open

7.2. Secure Key Injection

Zero-Trust requires [3], [4]:

- On-device key generation (preferred)
- Verified secure element presence
- CM sites audited for HSM-driven certificate programming

- Chain-of-custody records sent to OEM cloud

7.3. Firmware Provenance

Ensure [3]:

- Reproducible builds
- Signed firmware artifacts
- Read-only bootloader roots [4]
- Tamper-evident manufacturing logs

8. Secure Ota Update Pipeline

OTA is the most critical element of post-deployment security [3], [5].

8.1. OTA Pipeline Requirements

- Firmware must be double signed (OEM + optional ecosystem) [6], [7]
- Delta updates must validate block-level signatures
- Manifest files must include firmware lineage
- Device must verify signature before install [4]

8.2. Cloud Governance

- Role-based signing controls [6], [7]
- Build → Scan → Sign → Publish pipeline
- Evidence logs retained for compliance [10]

8.3. Failure Handling

- Banked firmware slots
- Automatic rollback [4]
- Revocation lists for compromised keys

9. Runtime Attestation and Continuous Verification

Zero-Trust requires devices to continuously prove that their software and state remain trustworthy [1], [4].

9.1. Types of Attestation

- Secure Boot Attestation [4]
- Firmware Hash Attestation
- Memory Integrity Checks
- Sensor/Actuator Behavior Anomaly Detection

9.2. Cloud-side Verification

Cloud platform should [6], [7]:

- Maintain golden reference firmware hashes
- Track unexpected module changes
- Flag devices operating outside expected telemetry bounds

9.3. Integration with Digital Twins

Runtime attestation becomes more powerful when combined with digital twins:

- State anomalies trigger remediation
- Behavioral deviations feed ML models for threat detection
- Maintenance prediction integrates security + performance insights

10. Threat Model

10.1. Primary Threat Actors

- Nation-state attackers
- Rogue contractors/field technicians
- Compromised gateways/mobile apps
- Malicious tenants or homeowners
- Insider threats inside ODM/CM
- Botnet operators targeting IoT fleets [5]

10.2. Attack Surfaces

- BLE pairing hijacks [9]
- Thread fabric takeover [8]
- Wi-Fi credential injection [5]
- OTA tampering [3]
- Supply chain firmware swaps
- Local serial/JTAG tampering
- Sensor spoofing
- Cloud API abuse [6], [7]

10.3. Security Objectives

- Prevent unauthorized onboarding [1], [5]
- Prevent unauthorized cloud access
- Ensure firmware authenticity [3], [4]
- Prevent local tampering
- Detect compromised behavior
- Maintain trust across device lifetime

11. Zero-Trust Blueprint: End-To-End Architecture

11.1. Components

- Device Layer - Secure elements [4], DAC [2], mTLS client, bootloader, attestation engine
- Local Connectivity Layer - BLE [9], Wi-Fi, Thread [8], Matter clusters [2], Local Commissioning
- Gateway / Mobile Layer - Commissioning app, ownership transfer, NOC issuance [2]
- Cloud Layer - Certificate authority, identity registry, OTA service, telemetry validation [6], [7]
- Governance Layer - Audit logs, supply chain records, runtime decision engine [10]

11.2. Blueprint Principles

- Identity over network location [1]
- Encrypt everything, authenticate every session
- Integrity checks at every lifecycle step [3]
- Context-aware authorization
- Continuous anomaly monitoring
- Hardware-software-cloud co-validation

12. Implementation Strategy for Oems and Cps Operators

12.1. Phase 1 - Identity Foundation

- Standardize secure elements [4]
- Create OEM-level PKI [1]
- Unify identities across radios
- Create device identity registry [3]

12.2. Phase 2 - Secure Commissioning and Connectivity

- Harden BLE flows with DAC verification [2], [9]
- Adopt Matter/Thread for fabric-level standardization [2], [8]
- Implement mTLS on all cloud links [6], [7]

12.3. Phase 3 - Secure OTA and Supply Chain

- Build reproducible firmware pipelines [3]
- Establish HSM-backed key injection [4]
- Digitally sign all artifacts

12.4. Phase 4 - Continuous Verification

- Deploy attestation [4]
- Deploy behavioral monitoring
- Tie into digital twin models

13. Governance and Compliance

Zero-Trust is not only technical it is procedural [1], [10].

OEMs must adopt:

- Secure development lifecycles (SDLC) [3]
- Vulnerability disclosure policies [5]
- CM/ODM audit frameworks
- Periodic certificate/key rotation
- Privacy and data minimization practices [5]

14. Impact on Smart Homes and Industrial Iot

14.1. Smart Homes

- Prevent rogue onboarding [5]
- Protect homeowners across device ownership changes
- Enable demand response and grid programs securely
- Reduce botnet vulnerability

14.2. Industrial IoT

- Protect HVAC/WH/DHW deployments across large fleets [10]
- Secure contractor/installer workflows
- Enable safe digital twin integration
- Reduce downtime from compromised firmware

15. Conclusion

Zero-Trust for cyber-physical systems is no longer aspirational it is foundational [1]. Each layer of the CPS stack must participate in a continuous cycle of verification, enforcement, and validation. By unifying identity, enforcing cryptographic trust, securing the supply chain, and embedding runtime attestation, OEMs and operators can build durable, scalable, and resilient IoT ecosystems [3], [6], [7]. As the physical world becomes more connected and software-defined, Zero-Trust becomes the only viable security paradigm for ensuring safety, reliability, and long-term resilience in smart homes and industrial IoT [1], [5].

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, NIST SP 800-207, Aug. 2020.

[2] Connectivity Standards Alliance, "Matter 1.4 Specification," CSA, 2024.

[3] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, "Foundational Cybersecurity Activities for IoT Device Manufacturers," National Institute of Standards and Technology, NISTIR 8259, May 2020.

[4] Arm Limited, "PSA Certified: Security Model," ARM, 2021. [Online]. Available: https://www.psacertified.org/

[5] European Telecommunications Standards Institute, "Cyber Security for Consumer Internet of Things: Baseline Requirements," ETSI EN 303 645 V2.1.1, Jun. 2020.

[6] Google Cloud, "IoT platform product architecture on Google Cloud" Available: https://docs.cloud.google.com/architecture/connected-devices/iot-platform-product-architecture

[7] Amazon Web Services, "AWS IoT Security Best Practices," AWS Documentation, 2024. [Online]. Available: https://docs.aws.amazon.com/iot/

[8] Thread Group, "Thread 1.3.0 Specification," Thread Group, 2022.

[9] Bluetooth SIG, "Bluetooth Core Specification v5.4," Bluetooth SIG, 2023.

[10] International Electrotechnical Commission, "IEC 62443: Security for Industrial Automation and Control Systems," IEC, 2018.