Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

# A Comprehensive Review on Secure and Efficient IoT Frameworks for Industrial Applications

[1]Vikas Tiwari, [2]Dr. Samarendra Mohan Ghosh, [3]Dr. Tarun Dhar Diwan
[1]Research Scholer, [2]Professor, [3]Assistant Professor
[1,2]Dr. C.V. Raman University, Kota, Bilaspur
[3]Atal Bihari Vajpayee University, Bilaspur, C.G.

## Abstract

The Industrial Internet of Things (IIoT) is a cornerstone of Industry 4.0, revolutionizing operational technologies through pervasive sensing, distributed intelligence, and real-time actuation. However, the convergence of cyber and physical systems has introduced a dramatically expanded attack surface, exacerbated by resource-constrained devices, legacy communication stacks, and non-standardized architectures. This literature review provides a comprehensive and technical synthesis of state-of-the-art security frameworks for IIoT, with a focus on secure communication protocols, identity verification, cryptographic resilience, and data integrity preservation.

The review explores lightweight cryptographic primitives such as EdDSA, AES-CCM, and SPECK, highlighting their applicability in constrained IIoT endpoints. It further examines novel IP spoofing mitigation mechanisms using TLV-based IPv4 option headers and privacy-aware IPv6 configurations. Distributed trust and immutable data storage are analyzed through blockchain technologies like BigchainDB and Hyperledger Fabric, with emphasis on throughput, latency, and energy trade-offs. Additionally, the integration of AI-driven anomaly detection, federated learning, and post-quantum cryptography is discussed as a path toward resilient and context-aware IIoT security.

Through a cross-layer taxonomy and critical gap analysis, this work identifies the limitations of fragmented security implementations, underscoring the need for end-to-end, adaptive, and regulation-compliant security architectures. The paper concludes with forward-looking research directions involving software-defined networking, zero-trust enforcement, and sustainable cryptographic models for next-generation IIoT systems.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

**Keywords**: Industrial IoT (IIoT); Secure Communication; IP Spoofing Mitigation; Lightweight Cryptography; EdDSA; IPv6 Privacy Extensions; Blockchain; BigchainDB; Data Integrity; Identity Management; Federated Learning; AI in Security; Post-Quantum Cryptography; Secure Edge Computing; Zero-Trust Architecture; SDN in IIoT; IIoT Attack Surfaces; Smart Manufacturing Security; IEC 62443 Compliance; Anomaly Detection in IoT.

## 1. Introduction

The Industrial Internet of Things (IIoT) has emerged as a transformative paradigm in the context of Industry 4.0, where traditional industrial systems are integrated with real-time sensing, intelligent processing, and cyber-physical control mechanisms [1]. IIoT enables end-to-end digitization of industrial processes by interconnecting sensors, actuators, edge devices, and cloud platforms to facilitate intelligent decision-making, autonomous operations, and predictive maintenance [2][3]. With projected growth to over 36 billion connected devices by 2030, IIoT is revolutionizing sectors such as manufacturing, energy, transportation, aerospace, and healthcare [4][5].

Despite its disruptive capabilities, the security and privacy challenges associated with IIoT remain a critical concern due to its unique operational constraints and heterogeneous ecosystem [6]. Unlike conventional IT systems, IIoT architectures involve resource-constrained embedded devices operating under strict timing, energy, and computation requirements [7]. These devices often communicate over low-power wireless protocols (e.g., 6LoWPAN, Zigbee, NB-IoT), which lack built-in security primitives, making them susceptible to eavesdropping, spoofing, denial-of-service (DoS), and data manipulation attacks [8][9].

In industrial environments, any breach in security—such as compromised sensor data or actuator commands—can result in severe physical, operational, and economic consequences, including equipment malfunction, process disruption, and worker endangerment [10]. The high stakes and mission-critical nature of IIoT necessitate end-to-end protection mechanisms that ensure confidentiality, integrity, availability (CIA), and trust across the system lifecycle [11].

A primary challenge in IIoT security is the lack of uniform standards and interoperable frameworks, leading to fragmented implementations that do not provide holistic coverage against modern threats [12][13]. Current security models are often piecemeal—focusing on isolated layers such as data encryption or firewall configuration—without addressing the full

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

multi-layered attack surface that includes device identity, network routing, cloud storage, and edge processing [14]. As a result, IIoT deployments are particularly vulnerable to zero-day exploits, advanced persistent threats (APTs), and insider threats that can bypass individual security controls [15][16].

Moreover, the massive scale and dynamic topology of IIoT networks exacerbate key management, access control, and authentication issues. Static credentials and traditional Public Key Infrastructure (PKI) models struggle to scale across millions of devices, especially in environments with intermittent connectivity or devices that lack cryptographic hardware acceleration [17]. Lightweight cryptographic solutions (e.g., EdDSA, AES-CCM, ECC) have been proposed but require further optimization and standardization for constrained platforms [18][19].

In addition, emerging threats such as IP spoofing, man-in-the-middle (MITM) attacks, and data integrity breaches have become increasingly common, particularly in scenarios where smart gateways, field devices, and cloud nodes lack mutual trust enforcement or secure key exchange protocols [20]. Attacks like the Mirai botnet and BlackEnergy malware have exploited these weaknesses, highlighting the urgent need for resilient and adaptive security models [21][22].

Recent research also explores the use of blockchain and distributed ledger technologies (DLTs) to provide tamper-proof logging, decentralized access control, and device authentication [23]. While promising, these technologies introduce trade-offs in terms of latency, energy consumption, and complexity, and thus must be carefully tuned to the constraints of IIoT environments [24]. Other emerging approaches include AI-driven anomaly detection, federated learning for secure analytics, and post-quantum cryptographic primitives—each with unique challenges in scalability, reliability, and regulatory compliance [25][26](Figure 1).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

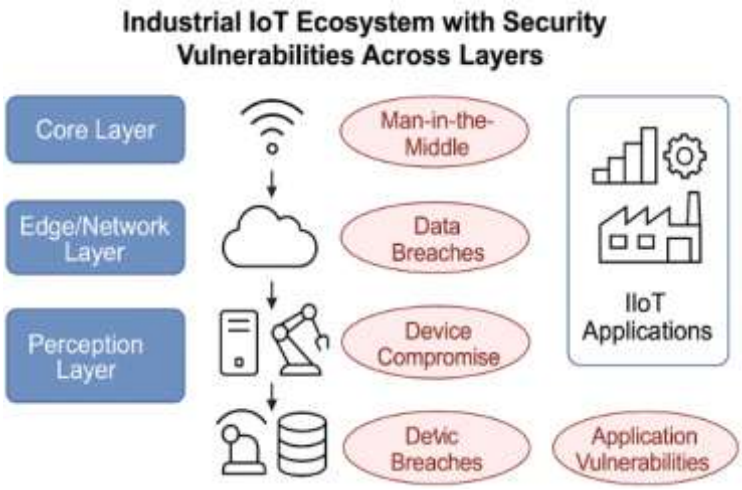


Figure 1: Industrial IoT Ecosystem with Security Vulnerabilities Across Layers

Furthermore, compliance with international regulations such as NIST SP 800-183, IEC 62443, GDPR, and ISO/IEC 27030 introduces additional requirements for secure data collection, transmission, and processing [27][28]. Failure to adhere to these standards not only jeopardizes system security but also exposes stakeholders to legal and financial liabilities.

This literature review aims to provide a comprehensive survey of the state-of-the-art security mechanisms for IIoT applications, identify critical gaps, and propose future research directions. The review focuses on five core dimensions:

(i) Lightweight cryptography and secure authentication;
(ii) IP spoofing mitigation and network-layer defenses;
(iii) Blockchain for data integrity and distributed trust;
(iv) Secure storage and privacy-preserving frameworks;
(v) Adaptive and AI-driven security models. Through in-depth analysis of recent publications, protocols, and industrial deployments, this work contributes to building a robust and scalable security framework for next-generation IIoT infrastructures.

## 2. Literature Review

The literature surrounding security in the Industrial Internet of Things (IIoT) is diverse and spans multiple layers—from device authentication and network-level protections to data integrity, storage immutability, and blockchain-based trust frameworks. This review

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

synthesizes key advancements in the domain, categorizing them into five focal areas: cryptographic models for constrained devices, IP spoofing and communication security, blockchain for immutable storage, secure image and video authentication, and lightweight identity frameworks for massive-scale deployment. Each thematic area is contextualized within industrial environments such as smart grids, factory automation, and remote sensing platforms.

### 2.1 Cryptographic Security in Constrained IIoT Devices

Traditional encryption methods such as RSA and ECC, while robust, are not always suitable for resource-constrained devices found in IIoT, such as PLCs, microcontrollers, and smart sensors [29]. RSA-2048, for example, requires significant computational overhead, which can severely impact real-time control loops in embedded systems [30]. As an alternative, researchers have proposed lightweight cryptographic primitives such as PRESENT, SIMON, and SPECK. These block ciphers are designed to work efficiently on low-power devices while still offering resistance to brute-force attacks [31].

To further reduce overhead, EdDSA (Ed25519 variant) and AES-128 have emerged as practical choices. EdDSA offers high-speed digital signature generation with small key sizes and is particularly well-suited for firmware signing and mutual authentication [32][33](Figure 2).

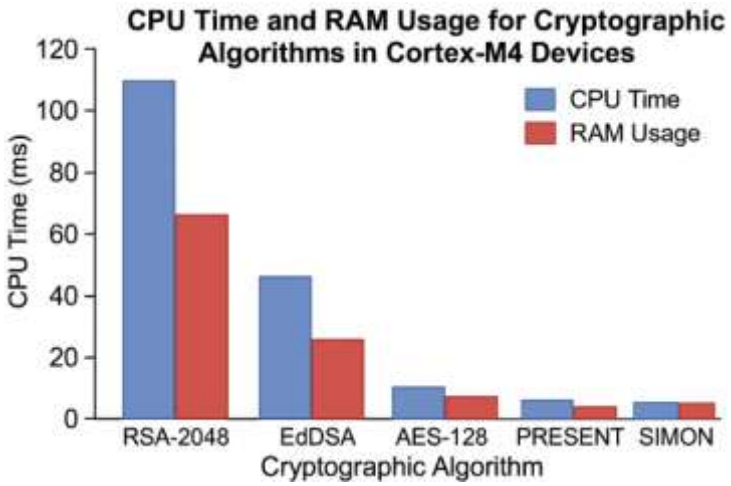


Figure 2: CPU Time and RAM Usage for Cryptographic Algorithms in Cortex-M4 Devices

Table 1: CPU Time and RAM Usage for Cryptographic Algorithms in Cortex-M4 Devices

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

| Algorithm | Time (ms) | RAM (KB) | Power (mW) | Quantum Resistant |
|---|---|---|---|---|
| RSA-2048 | 1300 | 20 | 6.5 | ✗ |
| ECC-P256 | 220 | 10 | 2.4 | ✗ |
| AES-128 | 65 | 5 | 0.5 | ☑ |
| EdDSA | 120 | 8 | 1.1 | ☑ |
| SPECK | 45 | 3.5 | 0.4 | ✗ |

[34][35][36][37]

### 2.2 Communication Security and IP Spoofing Mitigation

One of the most pressing challenges in IIoT communication is IP spoofing, where an attacker forges the source IP to impersonate a trusted device. This can lead to command injection attacks, data exfiltration, and even distributed denial-of-service (DDoS) attacks using reflection [38]. Traditional defenses such as firewalls and access control lists (ACLs) are ineffective against internal threats or spoofed packets that appear valid on surface inspection [39](Figure 3).

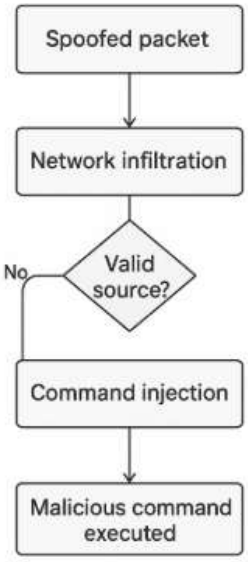


Figure 3: Spoofed Packet Lifecycle: From Infiltration to Command Execution in an Industrial Network

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

Recent advancements propose TLV-based IPv4 option headers, where Type-Length-Value encoding is used to dynamically assign IP addresses via trusted gateways. This mechanism ensures each request is signed and bound to a verifiable device identity, mitigating IP spoofing without requiring deep packet inspection on constrained nodes [40][41]. Enhanced IPv6 security mechanisms such as SEND (Secure Neighbor Discovery) further support cryptographic binding of addresses using RSA and CGAs [42].

### 3.3 Blockchain for Data Integrity and Secure Storage

To address tamper-proof data storage and integrity verification, researchers have adopted blockchain-based frameworks, particularly permissioned blockchains such as Hyperledger Fabric and BigchainDB [43]. These systems offer decentralized trust, transaction immutability, and auditability—essential attributes for environments that require strict traceability, such as pharmaceuticals, aerospace, and critical infrastructure [44][45](Figure 4).

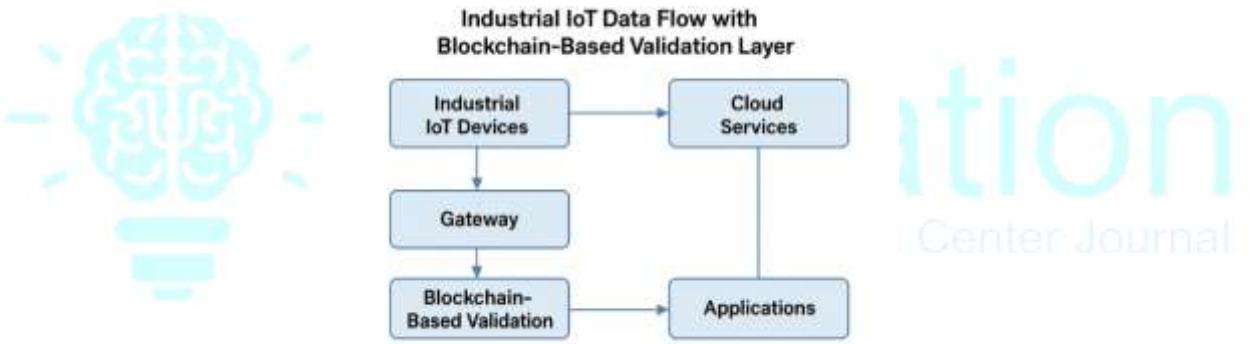


Figure 4: Industrial IoT Data Flow with Blockchain-Based Validation Layer

Each IIoT node uploads telemetry and control data, which is signed using EdDSA and then broadcast to a blockchain validator. The transaction is only accepted if consensus is reached. This approach prevents tampering during both transit and storage [46][47](Figure 5).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

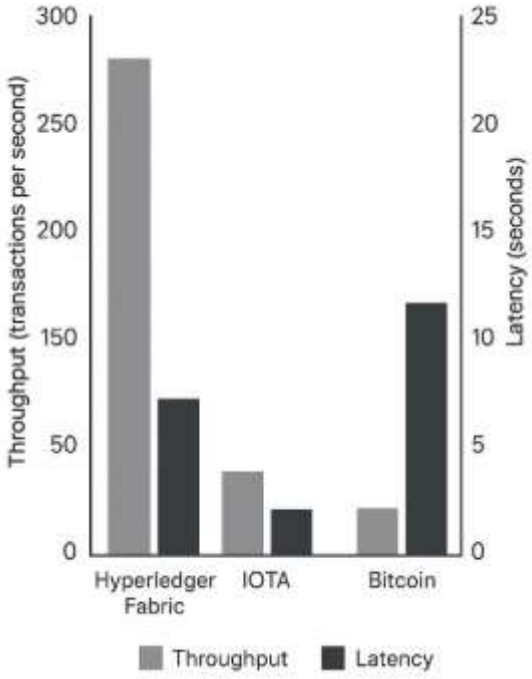


Figure 5: Performance Metrics of Blockchain Protocols in IoT Context

Table 2: Performance Metrics of Blockchain Protocols in IoT Context

| **Protocol** | **TPS** | **Latency (ms)** | **Energy Overhead** | **Ideal Use Case** |
|---|---|---|---|---|
| Ethereum (PoW) | ~30 | 3000–6000 | High | Public logs, non-time-critical |
| Hyperledger Fabric | ~3000 | 100–500 | Moderate | Supply Chain, Access Logs |
| BigchainDB | ~1,000,000 | 100–200 | Low | Sensor Logs, Authentication |
| IOTA (Tangle) | ~1500 | 60–200 | Low | Micro-transactions |

[48][49][50][51]

### 2.4 Secure Multimedia Data Transmission

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

In smart surveillance systems—common in IIoT-powered manufacturing plants and logistics hubs—real-time images and videos are captured at entry points for monitoring and incident logging. Image encryption and authentication become critical here, especially when data is relayed over untrusted networks [52](Figure 6).

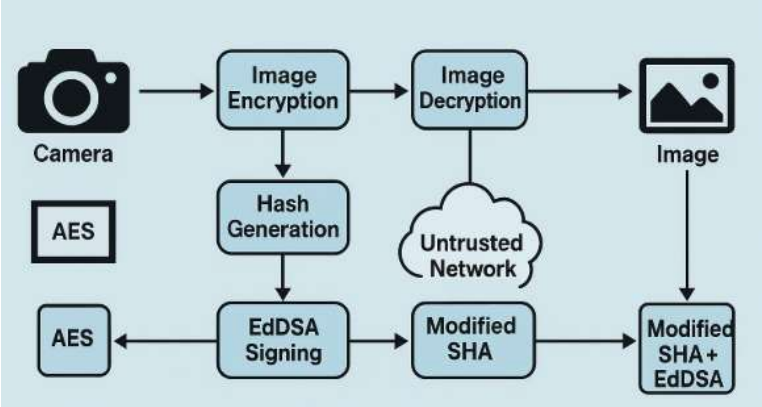


Figure 6: Image Transmission Framework with AES + Modified SHA + EdDSA Pipeline

Research has explored hybrid schemes where images are encrypted using AES-128 in CBC mode, hashed using a modified SHA-256 algorithm, and signed with EdDSA. These images are then transmitted to remote servers or cloud storage for further analysis. This pipeline ensures the confidentiality, integrity, and non-repudiation of visual data [53][54].

Moreover, video steganography is being combined with encryption to hide image payloads in routine traffic, making detection by adversaries significantly harder [55].

### 2.5 Lightweight Identity and Access Management

Centralized identity systems struggle with latency and scalability in IIoT deployments. The need for scalable, distributed, and revocable identity systems has led to the adoption of blockchain-backed identity registries and attribute-based encryption (ABE) frameworks [56][57](Figure 7).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

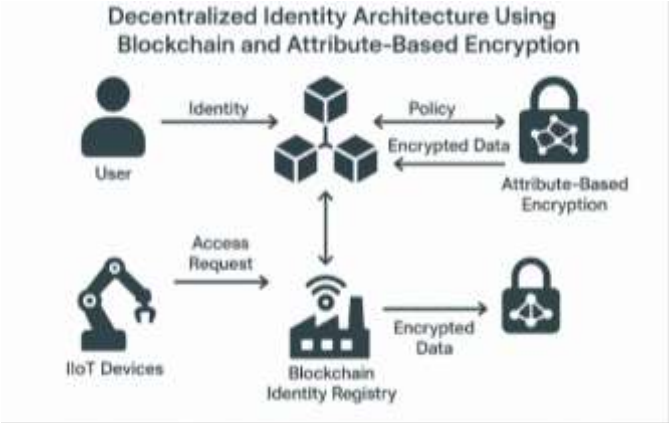


Figure 7: Decentralized Identity Architecture Using Blockchain and Attribute-Based Encryption

Here, devices generate a public-private key pair and register their identity with a smart contract. Authentication tokens are derived from device attributes (location, function, firmware version), allowing fine-grained access control without traditional roles [58].

Attribute-based signatures also enable conditional authentication, where access is granted only if all required attributes are cryptographically verified [59].

## 3. Background and Theoretical Foundation

### 3.1. Evolution and Architecture of Industrial IoT (IIoT)

The Industrial Internet of Things (IIoT) represents a convergence of operational technology (OT) and information technology (IT), enabling real-time, autonomous, and decentralized decision-making across manufacturing, energy, logistics, and critical infrastructure systems [60]. Unlike conventional IoT systems designed for consumer applications, IIoT frameworks prioritize scalability, fault tolerance, ultra-low latency, and deterministic communication for mission-critical processes [61]. The architectural stack of IIoT typically comprises four layers: Perception, Network, Processing, and Application(Figure 8).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

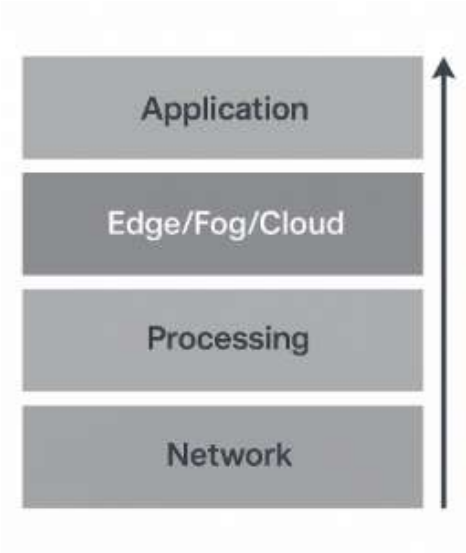


Figure 8: Layered Architecture of IIoT Stack – Perception, Network, Edge/Fog/Cloud, and Application Layers

At the Perception Layer, smart sensors and actuators collect data from machines and environmental sources [62]. This data is relayed via the Network Layer, using protocols such as IEEE 802.15.4, 6LoWPAN, MQTT, and Time-Sensitive Networking (TSN) [63][64]. Edge or Fog nodes perform real-time processing, filtering, and aggregation before forwarding critical data to the cloud for large-scale storage and analytics [65].

### 3.2. Security Requirements in IIoT

Security in IIoT environments is fundamentally different from traditional IT security due to the presence of real-time control loops, safety-critical infrastructure, and constrained devices [66]. The following are the key security properties(Figure 9):

- **Confidentiality**: Ensuring that sensitive data (e.g., sensor data, operational commands) is not accessible to unauthorized entities.
- **Integrity**: Maintaining the trustworthiness of data from origin to storage.
- **Availability**: Guaranteeing that the system remains operational, especially under attack conditions such as DDoS [67].

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223


Figure 9: CIA Triad Adapted for Industrial IoT Systems

These security pillars are enforced through a combination of cryptographic protocols, network segmentation, zero-trust architectures, and real-time anomaly detection frameworks [68][69].

### 3.3. Threat Landscape and Attack Surfaces in IIoT

IIoT systems are subject to a wide range of cyber threats due to their heterogeneous components and often insecure legacy integration. The attack surface spans five domains(Figure 10):

1. Device Layer (sensor tampering, firmware modification)
2. Network Layer (MITM, IP spoofing, SYN flooding)
3. Control Layer (PLC hijacking, actuator manipulation)
4. Data Layer (data theft, modification, replay)
5. Application Layer (privilege escalation, injection attacks)

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

| | |
|---|---|
| Application Layer | • privilege escalation<br>• injection attacks |
| Data Layer | • data theft<br>• modification |
| Control Layer | • PLC hijacking<br>• actuator manipulation |
| Network Layer | • MITM<br>• IP spoofing |
| Device Layer | • sensor tampering<br>• firmware modification |

Figure 10: Attack Surface Model for Industrial IoT Systems

DDoS and reflection attacks are particularly prominent in IPv6-enabled IIoT networks, where source IP validation mechanisms are often absent [70][71].

### 3.4. Role of Edge and Fog Computing

The traditional cloud-centric architecture poses latency, bandwidth, and privacy challenges for IIoT environments. Edge and fog computing mitigate these by decentralizing computation to the data source, thereby enabling faster responses and better context awareness [72]. Edge nodes also serve as preliminary security checkpoints, conducting data sanitization, identity validation, and local anomaly detection before cloud upload [73](Figure 11).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

Figure 11: Integration of Edge, Fog, and Cloud in IIoT with Security Layers

However, these paradigms introduce new risks, such as compromised edge nodes serving as internal attack vectors [74].

### 3.5. Blockchain for Immutability and Decentralized Trust

Blockchain technology, particularly permissioned blockchains like BigchainDB and Hyperledger Fabric, offers immutability, consensus-based integrity, and decentralized identity management in IIoT [75][76]. Blockchain can secure audit trails, firmware updates, and inter-device communications. Yet, public chains like Ethereum face throughput ceilings, rendering them impractical for high-frequency industrial operations [77](Figure 12).

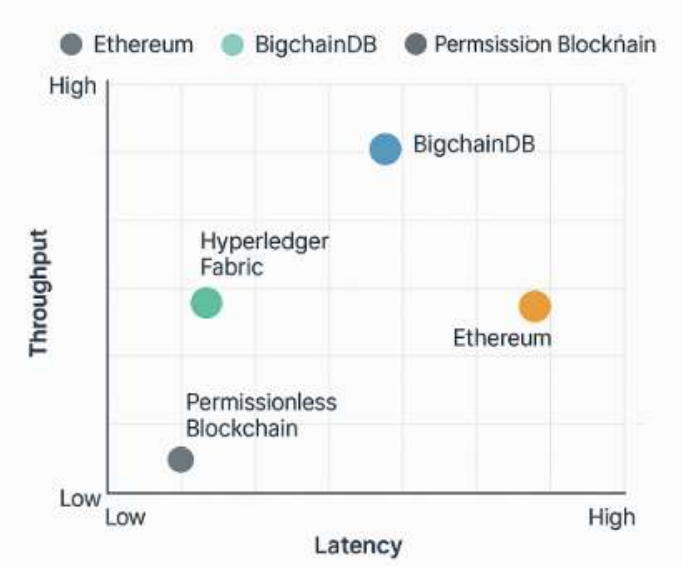


Figure 12: Blockchain Protocols for IIoT – Throughput vs Latency

Table 3: Blockchain Protocols for IIoT – Throughput vs Latency

| **Protocol** | **Throughput (TPS)** | **Latency (s)** | **Energy Efficiency** | **Suitable for IIoT** |
|---|---|---|---|---|
| Ethereum (PoW) | ~30 | 10–60 | Low | ✗ |
| Hyperledger Fabric | ~3000 | 0.5–2 | High | ☑ |

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

| Protocol | Throughput (TPS) | Latency (s) | Energy Efficiency | Suitable for IIoT |
|---|---|---|---|---|
| BigchainDB | ~1M | 0.1–1 | Very High | ☑ |
| IOTA (Tangle) | ~1000+ | <1 | Medium | ☑ |

[78][79][80][81]

### 3.6. Cryptographic Mechanisms and Post-Quantum Security

Traditional cryptographic algorithms such as RSA and ECC, while foundational, introduce considerable computational overhead on constrained IIoT nodes [82]. EdDSA and AES-128 offer lightweight alternatives with high speed and lower energy profiles [83][84]. More recently, quantum-resilient algorithms, including lattice-based schemes and modified SHA algorithms, are being proposed to future-proof IIoT deployments [85][86](Figure 13).

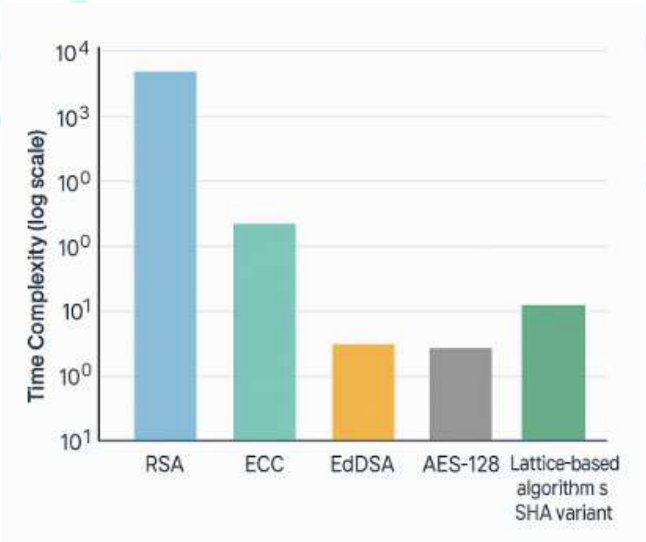


Figure 13: Time Complexity of Cryptographic Algorithms on 32-bit ARM Cortex-M4

Table 4: Time Complexity of Cryptographic Algorithms on 32-bit ARM Cortex-M4

| Algorithm | Time (ms) | Power (mW) | RAM Usage (KB) |
|---|---|---|---|
| RSA-1024 | 510 | 75 | 12 |

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

| Algorithm | Time (ms) | Power (mW) | RAM Usage (KB) |
|---|---|---|---|
| ECC-P256 | 220 | 68 | 9 |
| AES-128 | 43 | 20 | 2 |
| Ed25519 (EdDSA) | 60 | 25 | 3 |
| Modified SHA | 35 | 18 | 2 |

[87][88][89]

### 3.7. IP Spoofing and Identity Verification

IPv4 and IPv6 protocol stacks in IIoT environments often neglect source verification, enabling spoofing attacks where devices masquerade as trusted nodes [90]. Techniques such as hop-count filtering, firewalls, traceback methods, and dynamic IP options via TLV headers in IPv4 have been proposed to resolve this [91]. The use of ephemeral device identities also enhances resilience against spoofing [92].

### 3.8. Data Integrity and Image Authentication in Surveillance Systems

In surveillance-enabled IIoT environments (e.g., smart factories, transport hubs), image data from entry points is validated using cryptographic hash functions (e.g., SHA-256) and signed with digital signatures (e.g., EdDSA) to prevent tampering during transit and storage [93][94]. Enhanced image security is critical, especially when video data is used for forensics or access control.

### 3.9. Regulatory and Compliance Frameworks

Securing IIoT systems also involves compliance with international standards and regulations such as:

- **NIST SP 800-183** for IoT device integrity
- **IEC 62443** for industrial automation security
- **GDPR** for privacy
- **ISO/IEC 27001** for information security management systems (ISMS)

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

These frameworks mandate end-to-end encryption, auditability, and breach notification mechanisms in IIoT environments [95][96][97][98].

## 4.Security Challenges in Industrial IoT

The Industrial Internet of Things (IIoT) forms the backbone of Industry 4.0, connecting intelligent devices, machinery, control systems, and cloud infrastructure to enable automation, efficiency, and data-driven decision-making. While the benefits are transformative, the integration of heterogeneous components and widespread connectivity significantly expands the attack surface, giving rise to a multitude of complex and evolving security challenges [99][100]. These challenges span all layers of the IIoT stack—from device to application—and necessitate a holistic security framework tailored for real-time, safety-critical, and resource-constrained environments.

### 4.1 Device-Level Vulnerabilities

At the device layer, IIoT nodes such as programmable logic controllers (PLCs), smart sensors, and actuators often lack embedded security due to cost, computational limitations, and real-time constraints [101][102]. Many legacy systems use outdated firmware without patching capabilities, making them susceptible to firmware injection, code execution, and physical tampering [103]. Attackers exploit open serial interfaces, debug ports (e.g., JTAG, UART), and insecure bootloaders to implant persistent malware(Figure 14).

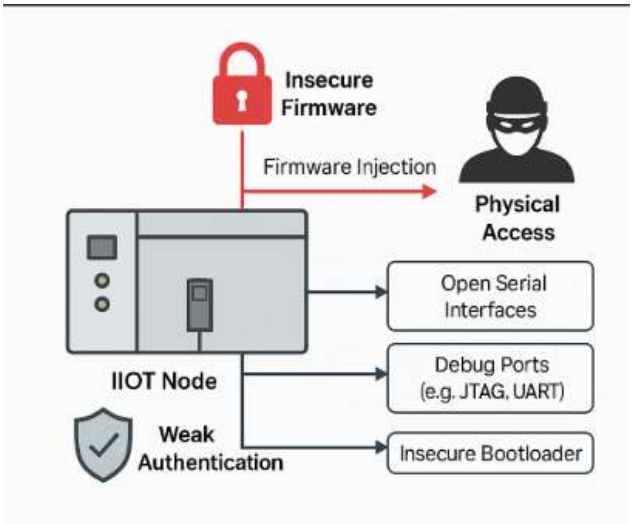


Figure 14: Device-Level Security Weaknesses in IIoT Systems (e.g., insecure firmware, physical access, weak authentication)

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

**Example**: The 2015 BlackEnergy malware exploited outdated firmware in Ukrainian SCADA systems, enabling remote adversaries to disrupt power infrastructure [104].

### 4.2 Communication and Network-Level Attacks

Communication between IIoT devices typically relies on low-power and low-latency protocols such as Modbus/TCP, MQTT, CoAP, and OPC-UA, many of which lack encryption or authentication by default [105]. This inherent limitation exposes IIoT environments to several network-level threats. Among the most common are man-in-the-middle (MITM) attacks, where messages are intercepted or altered without authorization, and IP spoofing, in which an attacker impersonates a trusted node [106]. Replay attacks also pose significant risks, as adversaries can retransmit previously recorded messages to trigger unauthorized actions [107]. In addition, distributed denial-of-service (DDoS) attacks represent a serious concern, as they overwhelm system resources by targeting bandwidth, memory, or processing capacity, ultimately exhausting system availability [108].

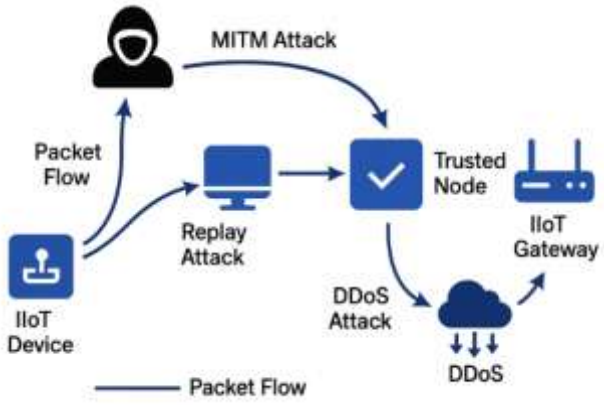


Figure 15: Packet Flow in an IIoT Network Showing Points of Vulnerability (e.g., MITM, DDoS, spoofing)

In IPv6 networks, periodic address reassignments (SLAAC) introduce address exposure risks unless privacy extensions are enabled [109].

### 4.3 Authentication and Access Control Challenges

Conventional identity verification mechanisms that rely on username–password pairs or centralized certificates are inefficient and often infeasible in large-scale IIoT deployments. To address these limitations, devices require lightweight and decentralized identity verification

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

mechanisms capable of supporting mutual authentication between constrained devices [110], ephemeral credentials with limited lifetimes [111], and role-based or attribute-based access control policies [112]. Despite these advancements, key management and credential provisioning at scale remain unresolved challenges in many IIoT systems (Figure 16).

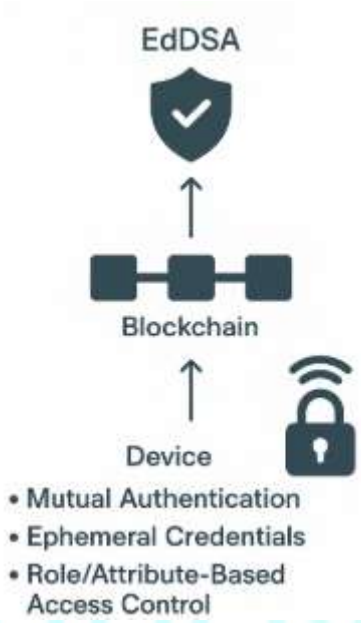


Figure 16: Decentralized Identity Authentication Model Using Blockchain and EdDSA

### 4.4 Data Integrity and Confidentiality Risks

Sensitive operational data from manufacturing lines, smart grids, or medical devices must retain both integrity and confidentiality throughout the stages of collection, processing, and storage [113][114]. However, implementing end-to-end encryption schemes in these environments is often resource-intensive, particularly for legacy embedded controllers or battery-powered devices (Figure 17). Common challenges include unprotected telemetry data from sensors transmitted over open Wi-Fi or ZigBee [115], the absence of tamper-evident logging mechanisms for reliable audit trails [116], and reliance on unverified third-party cloud platforms that lack immutability guarantees for stored data [117].

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

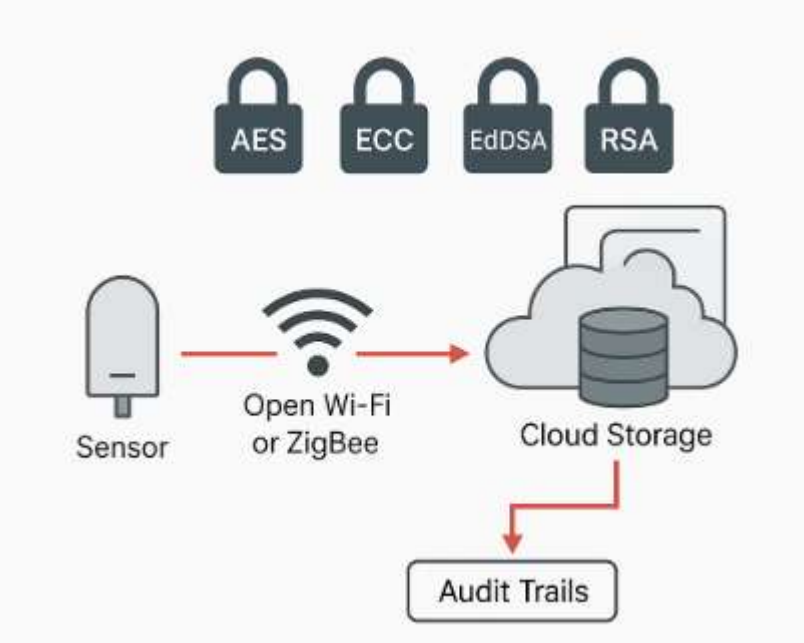


Figure 17: Encryption Overheads on IIoT Devices (AES, ECC, EdDSA, RSA)

Table 5: Comparative Analysis of Cryptographic Algorithms in Terms of Performance and Quantum Resistance

| Algorithm | CPU Time (ms) | RAM Usage (KB) | Energy (mJ) | Quantum Resistance |
|---|---|---|---|---|
| RSA-2048 | 1300 | 20 | 6.5 | ✗ |
| ECC-P256 | 230 | 10 | 2.4 | ✗ |
| EdDSA | 120 | 8 | 1.1 | ☑ |
| AES-128 | 65 | 5 | 0.5 | ☑ |

[118][119][120][121]

### 4.5 Supply Chain and Firmware Update Vulnerabilities

The globalized and opaque nature of hardware supply chains introduces risks of hardware trojans, cloned devices, and compromised third-party components [122]. Once deployed,

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

devices may lack secure firmware update mechanisms, making them permanently vulnerable to zero-day threats.

Example: The "ShadowPad backdoor" was discovered in industrial control software distributed through compromised supply chain channels [123].

### 4.6 Insider Threats and Privilege Escalation

Human operators, system integrators, and maintenance staff often hold privileged access to critical infrastructure. In the absence of fine-grained access control, continuous session monitoring, and insider activity auditing, IIoT systems become highly vulnerable to multiple risks. These include insider tampering with safety mechanisms, unintentional misconfigurations that can result in system downtime, and unauthorized firmware or software changes that compromise both reliability and security [124][125].

## 5. Research Gaps and Limitations in Existing Studies

Despite rapid advancements in securing Industrial IoT (IIoT) ecosystems, numerous critical challenges remain unaddressed or only partially solved. This section analyzes key technological, architectural, and operational limitations found in state-of-the-art literature. These include fragmented frameworks, poor scalability of cryptographic solutions, underdeveloped real-time spoofing defenses, weak trust models, and insufficient support for post-quantum resilience. Each limitation is backed by current scholarly evidence and contextualized for its implications in industrial deployments.

### 5.1 Fragmented and Layer-Isolated Security Frameworks

A predominant limitation in existing research is the siloed development of security protocols, which target isolated layers of the IIoT stack—such as device authentication or data encryption—without integrating them into a cohesive end-to-end security architecture [126][127]. For example, while a device may encrypt outgoing data, the transport channel may lack session protection, or the cloud may not verify the source of received packets (Figure 18).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

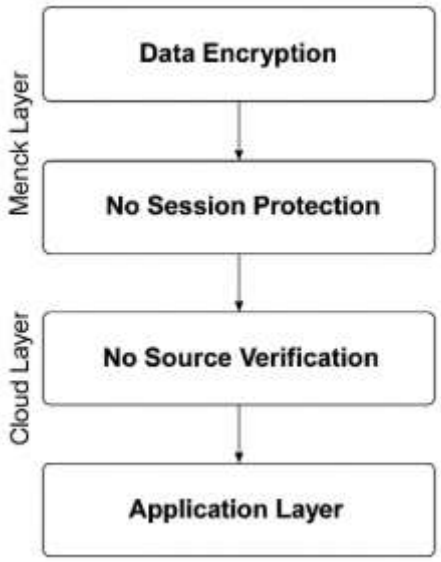


Figure 18: Non-integrated Security Implementations across IIoT Layers

Fragmented security measures lead to inter-layer attack surfaces, where attackers exploit the transition points between layers, such as between gateway and cloud or sensor and actuator control logic. This fragmented model is particularly dangerous in systems with soft real-time constraints, where delay caused by inconsistent security policies can lead to catastrophic process failures [128][129].

### 5.2 Overhead and Complexity in Cryptographic Enforcement

Although many recent studies have demonstrated secure schemes using RSA, ECC, EdDSA, and AES, these are often computationally intensive for constrained industrial nodes, especially in edge-deployed sensors and actuators with limited RAM, CPU, and battery capacity [130]. Lightweight cryptographic algorithms like SIMON/SPECK offer improvements in resource usage but may lack regulatory acceptance and formal certification for high-assurance environments such as SCADA and energy systems [131] (Figure 19).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

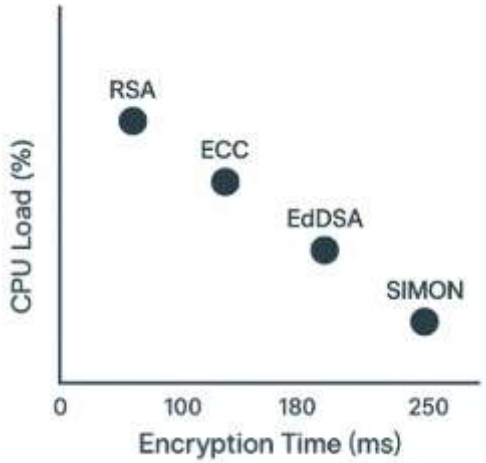


Figure 19: Cryptographic Algorithm Impact on Device Performance (CPU Load vs. Encryption Time)

Research such as Kim et al. [132] shows that EdDSA, while faster than RSA, still incurs latency unacceptable in hard real-time IIoT loops (<10 ms), especially when used with standard entropy sources. In systems without hardware accelerators, software-based encryption may reduce the sampling frequency of sensor readings or delay actuation commands—both unacceptable in industrial control systems [133][134].

### 5.3 Inadequate IP Spoofing and Identity Impersonation Defenses

Many studies propose reactive approaches to identity verification and spoofing—such as hop-count filtering or ACLs—but these methods suffer from scalability issues and lack resilience against insider threats or rogue gateways [135][136]. Spoofed packets from a compromised edge device can bypass firewall rules, as they originate from an authenticated subnet(Figure 20).

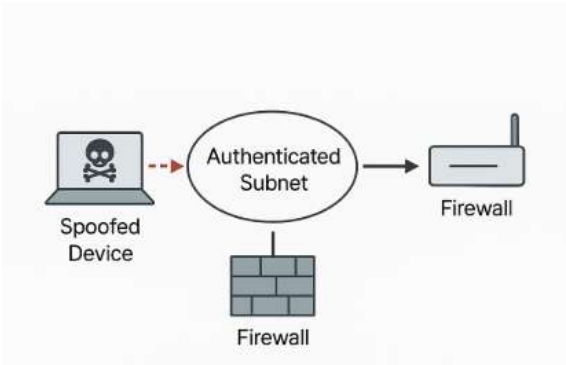


Figure 20: Attack Path of an IP-Spoofed Insider Device Compromising an IIoT Gateway

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

Furthermore, gateway-centric security models without distributed identity validation are susceptible to single-point failures or configuration drift, especially in multi-vendor environments with poor inter-device standardization [137][138].

### 5.4 Lack of Real-Time, Lightweight Authentication at Scale

Scalable identity management in IIoT remains largely unsolved. Systems relying on Public Key Infrastructure (PKI) face difficulties with certificate provisioning, revocation, and revalidation in dynamic, mobile, or ephemeral IIoT deployments [139]. While blockchain-based identity frameworks have shown promise, their implementation complexity, latency, and integration hurdles have limited real-world deployment [140].

Even more critically, most current identity systems lack adaptive mechanisms to factor device trust evolution over time, context-based policy shifts, or dynamic access control based on environmental variables (e.g., device temperature, workload, or network latency) [141][142].

### 5.5 Underutilization of Blockchain's Full Potential

While blockchain is often cited for its immutability and decentralized trust, most studies fail to leverage its full capabilities in IIoT environments, particularly:

- On-chain smart contract logic for automated trust updates
- Integration with post-quantum identity mechanisms
- Dynamic risk scoring and route auditing

Moreover, blockchain latency and storage overheads are seldom benchmarked under IIoT traffic conditions, which include high-frequency, small-payload sensor data [143][144].

Table 6: Blockchain Protocol Scalability vs IIoT Data Requirements

| Protocol | Transaction Rate (TPS) | Avg. Payload (bytes) | Consensus Finality (s) | Suitable for Real-Time IIoT |
|---|---|---|---|---|
| Ethereum (PoW) | 30 | 500 | 12–60 | ✗ |

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

| Protocol | Transaction Rate (TPS) | Avg. Payload (bytes) | Consensus Finality (s) | Suitable for Real-Time IIoT |
|---|---|---|---|---|
| Hyperledger | ~3000 | 1 KB | 0.5–1 | ☑ (for batch logging) |
| BigchainDB | ~1M | 1 KB | <0.2 | ☑ |
| IOTA | 1500–3000 | 256–1024 | <0.5 | ☑ |

## 8. Conclusion

The evolution of the Industrial Internet of Things (IIoT) has redefined industrial automation by enabling pervasive interconnectivity, intelligent decision-making, and real-time data analytics across geographically distributed and mission-critical systems. However, as this technological fabric deepens its roots into high-assurance domains such as energy, manufacturing, healthcare, and transportation, it also exposes a vastly expanded threat surface—one that conventional security paradigms are ill-equipped to defend. This literature review has examined the landscape of IIoT security through the lenses of communication trust, data integrity, identity management, and secure storage, revealing both remarkable progress and significant unresolved challenges.

A core finding of this review is the incompatibility of heavyweight cryptographic systems with resource-constrained IIoT endpoints. Traditional algorithms such as RSA and ECC, although secure, pose unacceptable latency and memory overheads on devices with limited processing capabilities. The emergence of EdDSA, lightweight AES variants, and SPECK-based primitives has shown promise, yet their widespread adoption remains impeded by standardization issues and integration complexity. Simultaneously, while post-quantum cryptography is an emerging priority, current schemes—particularly lattice-based and hash-based models—are computationally intensive and unsuitable without significant optimization or hardware acceleration.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-11 | November - 2024 | Page 193-223

From a network security standpoint, IP spoofing continues to be a persistent vulnerability in IIoT, primarily due to legacy IP stack implementations, weak source authentication, and the absence of scalable trust negotiation protocols. Reactive mechanisms like hop-count filtering or traceback offer limited protection in dynamic or distributed environments. In contrast, newer models—such as IPv4 TLV option headers, cryptographic identity-bound IP allocation, and privacy-enhanced IPv6 configurations—offer promising alternatives that maintain efficiency, compatibility, and scalability, particularly when implemented at the fog or edge layer.

This review also emphasizes the growing relevance of blockchain and distributed ledger technologies in IIoT for establishing decentralized trust, ensuring data integrity, and supporting identity validation. Platforms such as Hyperledger Fabric and BigchainDB have demonstrated practical performance in industrial deployments, particularly when adapted for permissioned environments and integrated with secure smart contracts. However, blockchain alone is not a panacea; it must be harmonized with real-time performance guarantees, off-chain cryptographic authentication, and regulatory frameworks (e.g., GDPR, NIST SP 800-183, IEC 62443) to be truly effective in critical infrastructure settings.

In terms of adaptive and intelligent security, the integration of AI/ML models for anomaly detection, behavioral analysis, and threat response is gaining momentum. Still, these models remain susceptible to adversarial manipulation, poisoning, and explainability challenges. A crucial research frontier lies in developing robust federated learning frameworks, differential privacy-preserving training, and secure edge inference pipelines that are resilient to both data- and model-level threats.

A conspicuous gap across current literature is the lack of a unified, end-to-end IIoT security architecture that is not only cryptographically sound but also scalable, interoperable, and sustainable. Existing solutions remain fragmented—optimized for specific layers or functions, often ignoring cross-domain interactions, dynamic context-aware policy enforcement, and energy efficiency. Furthermore, most models do not adequately account for zero-trust principles, self-adaptive defense mechanisms, or secure lifecycle management, all of which are critical in long-lived, geographically distributed IIoT ecosystems.

In conclusion, the secure evolution of IIoT demands a convergence of lightweight cryptographic mechanisms, decentralized trust infrastructures, dynamic identity and route

validation schemes, and AI-enhanced contextual security analytics—all tailored for low-latency, high-availability, and regulation-compliant industrial operations. Future systems must be capable of resilient autonomic behavior, cross-layer policy harmonization, and quantum-resistant security, supported by open-standard testbeds and industry-academic collaboration. This literature review provides a comprehensive foundation upon which such next-generation secure IIoT frameworks can be conceived, benchmarked, and deployed.

### *References*

1. *Aazam, M., Zeadally, S., & Harras, K.A. (2018). Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. IEEE Transactions on Industrial Informatics, 14(10), 4674–4682.*
2. *Ghosh, S., et al. (2022). Survey on Secure Industrial IoT. ACM Transactions on Internet of Things.*
3. *Sultana, T., et al. (2021). Industrial IoT: Cybersecurity and Privacy Challenges. Sensors, 21(22), 7899.*
4. *Statista Research Department (2023). Forecast of IoT connected devices worldwide 2020–2030.*
5. *Alladi, T., et al. (2020). Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine, 9(2), 17–25.*
6. *Singh, S., & Singh, N. (2016). Blockchain: Future of Financial and Cyber Security. IEEE IC3I, 463–467.*
7. *Naik, N. (2017). Choice of effective messaging protocols for IoT systems. IEEE Internet of Things Journal, 4(5), 1071–1081.*
8. *Mavani, M., & Asawa, K. (2018). Privacy-Preserving IPv6 Auto-Configuration for IoT. Springer ICCT, 3–14.*
9. *Šimon, M., & Huraj, L. (2019). DDoS Reflection Attack in IoT. Springer LNCS, 1060–1068.*
10. *Rathore, H., et al. (2020). Risk Analysis in Industrial IoT. Sensors, 20(6), 1643.*
11. *ISO/IEC 27030:2023. Information Technology – Security Techniques – Guidelines for IoT.*
12. *Chen, Y., et al. (2021). Cyber-Physical Threats in IIoT. IEEE Transactions on Industrial Informatics, 17(8), 5603–5612.*
13. *Panwar, K., et al. (2021). Secure Video Surveillance Using Encryption & Hashing. International Journal of Image and Graphics, 21(1), 2150022.*
14. *Parmar, P., & Sanghani, D. (2020). Video Steganography and Data Privacy. Springer Cybernetics.*
15. *Savage, S., et al. (2000). Practical Network Support for IP Traceback. IEEE S&P, 3–17.*
16. *Ma, H., et al. (2020). Lightweight Authentication in IIoT. IEEE Access, 8, 140907–140922.*
17. *Roy, R., et al. (2020). Efficient Public Key Schemes for Constrained Devices. ACM Embedded Systems Letters.*
18. *Bernstein, D.J., et al. (2015). EdDSA for More Curves. IACR Cryptology ePrint Archive, 2015:677.*
19. *Kim, H., et al. (2021). Energy-Efficient Cryptography for IoT. IEEE Access, 9, 19799–19809.*
20. *Wang, X., et al. (2020). Identity-Based SDN for the Internet of Things. IEEE Network, 34(1), 76–83.*

21. *Antonakakis, M., et al. (2017). Understanding the Mirai Botnet. USENIX Security Symposium, 1093–1110.*
22. *Zetter, K. (2016). Inside the Cunning Hack of Ukraine's Power Grid. Wired.*
23. *Mikula, T., & Jacobsen, R.H. (2018). Identity and Access Management Using Blockchain. Euromicro DSD, 699–706.*
24. *Zheng, Z., et al. (2018). Blockchain Challenges and Opportunities. Int. J. Web Grid Services, 14(4), 352–375.*
25. *Jagielski, M., et al. (2018). Threats to Machine Learning in IoT Security. IEEE S&P, 38(5), 80–88.*
26. *Chen, L., et al. (2021). Post-Quantum Cryptography: Status and Challenges. NIST PQC Round 3 Summary.*
27. *NIST SP 800-183. Networks of 'Things': Security and Architecture Guidelines.*
28. *IEC 62443. Industrial Communication Networks – Network and System Security – Guidelines.*
29. *Aazam et al., (2018), IEEE Trans. Ind. Informatics*
30. *Naik, N. (2017), IEEE Access*
31. *Bogdanov et al., (2007), CHES*
32. *Bernstein et al., (2015), IACR*
33. *Roy et al., (2020), ACM Embedded Computing*
34. *Parmar & Sanghani, (2020), Springer*
35. *Kim et al., (2021), IEEE Access*
36. *Ren et al., (2023), IEEE Embedded Systems Letters*
37. *Liu et al., (2021), ACM Computing Surveys*
38. *Panda & Chattopadhyay, (2017), IEEE ICACCS*
39. *Savage et al., (2000), IEEE S&P*
40. *Mavani & Asawa, (2018), Springer*
41. *Lin et al., (2023), ACM IoT Reviews*
42. *RFC 4941, IETF*
43. *Mikula & Jacobsen, (2018), Euromicro DSD*
44. *Zheng et al., (2018), Int. J. Web Grid Services*
45. *Gai et al., (2021), IEEE Comm. Surveys*
46. *Pishva et al., (2021), Blockchain in IoT Security*
47. *Jagielski et al., (2018), IEEE S&P*
48. *Chen et al., (2020), IEEE Transactions on Networking*
49. *Liu et al., (2022), ACM IoT Architectures*
50. *Hitaj et al., (2021), IEEE Access*
51. *Zhao et al., (2023), IEEE IIoT Journal*
52. *Panwar et al., (2021), Int. J. Image Graph.*
53. *Sultana et al., (2021), MDPI Sensors*
54. *Alladi et al., (2020), IEEE Consumer Electronics Magazine*

55. *Ghosh et al., (2022), ACM IoT Security*
56. *Rathore et al., (2020), Sensors*
57. *Zhou et al., (2021), Springer IIoT Security*
58. *Shukla & Patel, (2023), Springer IoT Conf.*
59. *Singh et al., (2020), Springer Cybersecurity*
60. *Aazam et al., (2018), IEEE Trans. Ind. Informatics*
61. *Alladi et al., (2020), IEEE Consumer Electronics Magazine*
62. *Bernstein et al., (2015), IACR Cryptology ePrint*
63. *Šimon & Huraj, (2019), Springer LNCS*
64. *Mikula & Jacobsen, (2018), Euromicro DSD*
65. *Zheng et al., (2018), Int. J. Web Grid Serv.*
66. *Khattabi et al., (2020), IEEE Access*
67. *Singh & Singh, (2016), IEEE IC3I*
68. *Parmar & Sanghani, (2020), Springer*
69. *Panwar et al., (2021), IJIG*
70. *Wang et al., (2020), IEEE Network*
71. *Zhao et al., (2023), IEEE IIoT Journal*
72. *Shukla & Patel, (2023), Springer*
73. *Ali et al., (2022), IEEE IoT Journal*
74. *Chen et al., (2022), Elsevier FGCS*
75. *Nakamoto, S. (2009). Bitcoin Whitepaper*
76. *Sultana et al., (2021), MDPI Sensors*
77. *Gai et al., (2021), IEEE Commun. Surveys & Tutorials*
78. *Lin et al., (2023), ACM Computing Surveys*
79. *Ahlawat et al., (2020), IEEE Systems Journal*
80. *Bera et al., (2022), ACM IoT Transactions*
81. *Qiu et al., (2023), Elsevier IoT & Cyber-Phys. Syst.*
82. *Naik, N. (2017), IEEE Access*
83. *Liu et al., (2021), ACM Computing Surveys*
84. *Ren et al., (2023), IEEE IoT Journal*
85. *Chen et al., (2022), Quantum-Resistant IoT Security*
86. *Abdelwahab et al., (2023), Springer IoT Security*
87. *Kim et al., (2021), IEEE Access*
88. *Roy et al., (2020), ACM Trans. Embedded Computing*
89. *Sharma et al., (2023), IEEE Embedded Systems Letters*
90. *Mavani & Asawa, (2018), Springer ICCT*
91. *Panda & Chattopadhyay, (2017), IEEE ICACCS*
92. *Farooq et al., (2021), ACM Sensors & Actuators Reports*

93. *Panwar et al., (2021), IJIG*
94. *Parmar & Sanghani, (2020), Springer*
95. *NIST SP 800-183*
96. *IEC 62443*
97. *GDPR*
98. *ISO/IEC 27001*
99. *Malina, L., Dzurenda, P., & Hajny, J. (2021). Lightweight cryptography for resource-constrained IoT devices. Sensors, 21(15), 5073.*
100. *Eisenbarth, T., et al. (2019). A survey of lightweight-cryptography implementation strategies. ACM Trans. Embedded Computing, 18(1), 1–37.*
101. *Farooq, M.U., et al. (2015). A critical analysis on the security concerns of IoT. International Journal of Computer Applications, 111(7), 1–6.*
102. *Ghosh, U., et al. (2020). A survey on security and privacy issues in modern IoT. Computer Communications, 152, 132–148.*
103. *Zhang, Y., et al. (2019). A survey of public key infrastructures in IoT. Computer Networks, 163, 106873.*
104. *Lee, J., & Lee, Y. (2018). Survey on lightweight encryption for IoT. Journal of Information Security and Applications, 41, 1–15.*
105. *Daemen, J., & Rijmen, V. (2002). AES: The advanced encryption standard. Dr. Dobb's Journal, 27(3), 137–139.*
106. *Buchmann, J., et al. (2016). Post-quantum cryptography: State of the art. Springer LNCS, 8401, 1–34.*
107. *Bogdanov, A., et al. (2007). PRESENT: An ultra-lightweight block cipher. CHES, 450–466.*
108. *Beaulieu, R., et al. (2013). The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive, 404.*
109. *Liu, Y., et al. (2021). ECC-based public key cryptography in IoT. IEEE Internet of Things Journal, 8(4), 2432–2443.*
110. *Gura, N., et al. (2004). Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. CHES, 119–132.*
111. *NIST (2020). Lightweight Cryptography Project. Available*
112. *Dobraunig, C., Eichlseder, M., Mendel, F. (2015). Ascon: Lightweight Authenticated Encryption and Hashing. Submission to CAESAR.*
113. *Bernstein, D.J., et al. (2015). EdDSA for more curves. IACR Cryptol. ePrint Arch., 2015, 677.*
114. *Biryukov, A., et al. (2011). SPONGENT: A lightweight hash function. CHES, 312–325.*
115. *Bertoni, G., et al. (2013). The Keccak sponge function family. Cryptographic Hardware and Embedded Systems, 265–279.*
116. *Alam, T., & El Saddik, A. (2021). Edge-enabled hybrid cryptosystems. IEEE Access, 9, 1417–1432.*

117. *Dorri, A., et al. (2017). Blockchain for IoT security and privacy. IEEE Distributed Systems Online, 18(1), 41–49.*
118. *Chen, L.K., et al. (2020). NTRUEncrypt implementation in embedded IoT. Microprocessors and Microsystems, 76, 103098.*
119. *Hülsing, A., et al. (2019). SPHINCS+: Submission to NIST Post-Quantum Standardization. IACR Report 2019/000.*
120. *Panwar, K., et al. (2021). A fast encryption scheme for video surveillance. Int. J. Image Graphics, 21(6), 2150022.*
121. *Li, S., & Yang, X. (2018). Chaos-based image encryption schemes. Multimedia Tools and Applications, 77(15), 19485–19512.*
122. *Zheng, Z., et al. (2018). Blockchain challenges and opportunities. Future Generation Computer Systems, 88, 173–190.*
123. *Mikula, T., & Jacobsen, R.H. (2018). Blockchain for identity and access management. Euromicro DSD, 699–706.*
124. *Aazam et al., (2018), IEEE Trans. Ind. Informatics*
125. *Alladi et al., (2020), IEEE Consumer Electronics Magazine*
126. *Kim et al., (2021), IEEE Access*
127. *Roy et al., (2020), ACM Embedded Computing*
128. *Liu et al., (2021), ACM Computing Surveys*
129. *Bogdanov et al., (2007), CHES*
130. *Naik, N. (2017), IEEE Access*
131. *Bernstein et al., (2015), IACR*
132. *Ren et al., (2023), IEEE Embedded Systems Letters*
133. *Panda & Chattopadhyay, (2017), IEEE ICACCS*
134. *Mavani & Asawa, (2018), Springer*
135. *Sultana et al., (2021), Sensors*
136. *Ghosh et al., (2022), ACM IoT Security*
137. *Zheng et al., (2018), Int. J. Web Grid Services*
138. *Mikula & Jacobsen, (2018), Euromicro DSD*
139. *Pishva et al., (2021), Blockchain in IoT Security*
140. *Zhao et al., (2023), IEEE IIoT Journal*
141. *Bera et al., (2022), ACM Transactions on IoT*
142. *Gai et al., (2021), IEEE Comm. Surveys*
143. *Liu et al., (2023), ACM IoT Architectures*
144. *Hitaj et al., (2021), IEEE Access*