Multidisciplinary Engineering Science Open

Received date: 11 Jan 2025
Revised date: 10 Feb 2025
Accepted date: 20 Feb 2025
Published date: 01 Mar 2025

Secure IoT Stacks for Critical Infrastructure: Protocols, TEEs, and Post-Quantum Readiness

Ahmad Al-Hassan[1*]

Citation: Al-Hassan, A. (2025). Secure IoT Stacks for Critical Infrastructure: Protocols, TEEs, and Post-Quantum Readiness. *Multidisciplinary Engineering Science Open,* 2, 1-15.

Abstract

This study aims to synthesize and analyze current advancements in secure Internet of Things (IoT) architectures for critical infrastructure, emphasizing protocol assurance, trusted execution environments (TEEs), and post-quantum cryptographic readiness. A qualitative review design was employed to systematically examine the literature on IoT security frameworks within critical infrastructure domains. Nineteen peer-reviewed articles published between 2015 and 2025 were selected through comprehensive searches across IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Scopus. Inclusion criteria targeted studies addressing secure communication protocols, hardware-based trust mechanisms, and quantum-resistant encryption strategies. Data collection was limited to document analysis, and data interpretation followed a qualitative content analysis using NVivo 14. Open coding, axial categorization, and selective thematic integration were applied until theoretical saturation was achieved, producing four emergent themes that encapsulate the security, interoperability, and resilience dimensions of secure IoT stacks. The analysis revealed four major thematic dimensions: (1) protocol assurance and interoperability, focusing on secure communication frameworks and cross-layer encryption; (2) trusted execution environments and hardware roots of trust, emphasizing TEEs, secure boot mechanisms, and runtime attestation; (3) post-quantum cryptography and algorithm transition, addressing migration to quantum-safe encryption and hybrid cryptographic architectures; and (4) resilience and assurance in critical infrastructure IoT, highlighting risk management, compliance, and forensic readiness. Collectively, these dimensions illustrate a systemic evolution from isolated security mechanisms toward integrated assurance ecosystems combining hardware, software, and governance layers. Secure IoT stack design for critical infrastructures demands convergence between protocol standardization, hardware-based trust, and post-quantum preparedness. Future IoT security models should prioritize interoperability, algorithmic agility, and continuous certification to ensure operational resilience against both current and emerging cyber-physical threats.

Keywords: Secure IoT; Critical Infrastructure; Trusted Execution Environment (TEE); Post-Quantum Cryptography; Protocol Assurance; Cyber-Physical Resilience

1. Department of Civil Engineering, University of Jordan, Amman, Jordan

*Correspondence: ahmad.alhassan@ju.edu.jo

1. Introduction

The rapid proliferation of the Internet of Things (IoT) has transformed the architecture of critical infrastructures, from power grids and healthcare systems to transportation and water management. Yet, this pervasive interconnectivity introduces complex security vulnerabilities that can disrupt vital societal functions. As IoT becomes increasingly embedded in safety-critical domains, the assurance of data integrity, device trustworthiness, and cryptographic resilience has become a global priority. Unlike conventional IT networks, IoT infrastructures combine cyber and physical elements, exposing multi-layered attack surfaces that threaten operational safety, national security, and public confidence (Alcaraz & Lopez, 2018; Mosenia & Jha, 2017). The evolution of secure IoT stacks—integrating robust communication protocols, trusted execution environments (TEEs), and post-quantum cryptography—represents a crucial paradigm shift toward building trustworthy, resilient systems capable of sustaining operational continuity under sophisticated cyber-physical attacks. Recent technological trends highlight the necessity of aligning software-defined networking principles, hardware trust anchors, and quantum-resistant encryption within unified IoT architectures that can dynamically adapt to changing threat landscapes (Kothmayr et al., 2013; Porambage et al., 2020).

The security of critical infrastructure IoT systems demands multilayered protection that extends beyond application-level encryption. Many existing devices rely on lightweight protocols such as MQTT and CoAP, which, while efficient, are often deployed with incomplete or inconsistent security configurations (Farahani et al., 2021). Protocol assurance thus encompasses not only encryption but also authentication, session management, and cross-layer interoperability (El-Habashy et al., 2023). The interoperability issue is particularly acute in multi-vendor environments, where fragmented standards can lead to inconsistent security policies across devices and networks (Younis et al., 2022). Consequently, researchers emphasize the development of standardized frameworks that unify data semantics, streamline encryption handshakes, and minimize latency impacts while maintaining quality of service in time-sensitive applications such as SCADA systems (Radanliev et al., 2020). These frameworks increasingly integrate dynamic key rotation, adaptive intrusion detection, and semantic interoperability mechanisms to mitigate vulnerabilities in heterogeneous ecosystems. Such advancements underscore the transition from isolated device-level security to holistic, interoperable architectures capable of sustaining security guarantees throughout the IoT stack.

Equally vital to this emerging paradigm is the role of trusted execution environments and hardware-based roots of trust. As attackers increasingly exploit runtime vulnerabilities, TEEs offer hardware-level isolation zones where sensitive operations such as key management and data decryption can occur securely (Sabt, Achemlal, & Bouabdallah, 2015; Zhou et al., 2021). Technologies such as ARM TrustZone and Intel SGX are becoming foundational in IoT

deployments, providing remote attestation and secure boot processes that verify software integrity before execution (Alrawais et al., 2017). For critical infrastructures that cannot tolerate firmware tampering or code injection, such mechanisms ensure system reliability and verifiable authenticity. Moreover, hardware-software co-design approaches are emerging to address side-channel attacks and enhance efficiency through FPGA-based acceleration and microkernel-level protection (Garrido-Hidalgo et al., 2019; Raza et al., 2017). The combination of TEEs and cryptographic co-processors transforms IoT devices from passive network nodes into active components of a distributed trust fabric, aligning technical security controls with compliance frameworks such as IEC 62443 and NIST SP 800-193 (Zhang et al., 2022). In this context, the integration of hardware-enforced trust anchors represents a foundational element in designing verifiable, tamper-resistant IoT architectures that underpin critical operations.

However, the emergence of quantum computing poses unprecedented challenges to the long-term viability of classical cryptographic schemes that protect IoT communications. Quantum algorithms such as Shor's and Grover's threaten the integrity of RSA and ECC, which form the backbone of most IoT encryption protocols. To counter these risks, post-quantum cryptography (PQC) seeks to develop algorithms resistant to both classical and quantum adversaries (Mosca, 2018). Lattice-based schemes such as CRYSTALS-Kyber and SPHINCS+ have been identified as promising candidates due to their security proofs and implementation flexibility (Chen et al., 2022; Guo et al., 2023). Transitioning existing IoT infrastructures toward post-quantum readiness, however, presents significant obstacles. Many IoT devices lack the computational capacity and memory resources to support PQC's heavier cryptographic primitives, necessitating hardware acceleration, firmware updates, and algorithmic agility mechanisms (Albrecht et al., 2021; Kampanakis, 2021). Hybrid systems that combine traditional ECC with lattice-based encryption have emerged as transitional solutions, allowing gradual migration without sacrificing backward compatibility. Standardization bodies such as NIST and ISO are now driving industry-wide adoption of PQC-ready frameworks, emphasizing testability, compliance, and agility as essential components of future-proof security (Dang et al., 2022; Chen & Jordan, 2021). For critical infrastructures with long lifecycle devices, PQC represents not only a technological upgrade but a strategic imperative to maintain cryptographic resilience in the post-quantum era.

Ensuring resilience and assurance in IoT-enabled critical infrastructure requires integrating security within the broader context of operational reliability, risk management, and governance. Cyber-physical resilience encompasses mechanisms for continuous anomaly detection, autonomous fault recovery, and safety-security co-assurance (Kebande & Ray, 2020; Djenna et al., 2021). For example, intrusion detection systems that utilize machine learning to analyze traffic in real-time can identify abnormal patterns across SCADA networks before they propagate (Abdallah et al., 2023). Redundant and fault-tolerant architectures ensure that even if certain components are compromised, overall functionality persists with minimal

downtime (Antunes & Simoes, 2021). Risk assessment methodologies such as STRIDE modeling and probabilistic risk assessment provide structured approaches to evaluate and prioritize vulnerabilities (Cherdantseva & Hilton, 2020). Meanwhile, assurance cases—structured, evidence-based arguments demonstrating that systems are acceptably safe and secure—are increasingly integrated into certification processes for industrial IoT deployments (Aldossary & Allen, 2019). These frameworks, combined with forensic readiness and blockchain-based audit trails, ensure traceability and accountability across the IoT lifecycle (Yasrab et al., 2023). Importantly, human and organizational factors remain central to maintaining system resilience. Operator training, insider-threat detection, and governance policies are vital in reducing human error and enforcing security culture within organizations (Patel et al., 2022). Therefore, secure IoT stacks must be conceptualized not only as technical systems but as socio-technical ecosystems requiring alignment of people, processes, and technologies.

The findings of this study reveal that IoT stack security in critical infrastructures evolves along four intertwined dimensions: protocol assurance and interoperability, trusted execution environments, post-quantum readiness, and systemic resilience. Together, these represent an ecosystemic transformation of IoT security from reactive defense to proactive assurance. Protocol assurance research underscores the transition toward adaptive, interoperable communication layers capable of resisting latency-sensitive attacks. TEEs redefine device trust through hardware-enforced isolation, minimizing the attack surface at runtime. Post-quantum cryptography anticipates future threats, positioning algorithmic agility as an essential design principle. Finally, resilience frameworks integrate continuous validation, risk assessment, and governance into ongoing operational cycles, ensuring sustained reliability and adaptability. These findings align with previous studies emphasizing that future IoT infrastructures must blend cryptographic innovation, system-level governance, and human-centered resilience to remain trustworthy in volatile digital ecosystems (Radanliev et al., 2020; Younis et al., 2022; Zhou et al., 2021). The convergence of these domains marks a decisive shift in cybersecurity thinking—from isolated protection mechanisms toward integrated assurance ecosystems where hardware, software, and policy operate synergistically.

The results further highlight that while hardware trust mechanisms and post-quantum cryptography offer high theoretical security, their real-world integration is constrained by practical limitations in cost, power, and scalability. Several studies corroborate that the majority of existing IoT devices cannot easily undergo cryptographic migration without dedicated co-processors or cloud offloading capabilities (Albrecht et al., 2021; Guo et al., 2023). Similarly, while TEEs have demonstrated resilience against many runtime attacks, their implementation in resource-constrained environments remains uneven, with limited standardization across manufacturers (Sabt et al., 2015; Zhang et al., 2022). On the other hand, interoperability frameworks such as oneM2M and OMA LwM2M show promise in harmonizing device communications but still face challenges in dynamic security

configuration and version control (El-Habashy et al., 2023). Aligning these findings with the literature, it becomes evident that secure IoT stack design requires not just technical enhancement but architectural co-optimization—balancing performance, compliance, and adaptability. Future studies emphasizing system-level co-engineering and formal assurance modeling will be critical for scaling these technologies in real-world infrastructures (Antunes & Simoes, 2021; Chen & Jordan, 2021).

Despite these advancements, this study faces several limitations. First, as a qualitative review, it depends on existing literature and may not fully capture emerging proprietary or unpublished industrial approaches. The reviewed sample, while diverse, remains limited to nineteen peer-reviewed sources, potentially omitting gray literature and regional innovations in IoT security. Moreover, the rapid pace of technological evolution—particularly in quantum cryptography and TEE implementations—means that findings may quickly become outdated as new standards and hardware architectures emerge. The absence of empirical testing or performance benchmarking restricts the study's ability to quantify efficiency trade-offs among competing security strategies. Lastly, given that much of the literature originates from industrialized contexts, the generalizability of these findings to developing nations with legacy infrastructures remains uncertain, warranting cross-contextual validation.

Future research should pursue longitudinal and hybrid studies that integrate both simulation and empirical evaluation to assess the scalability and interoperability of secure IoT stacks under real-world conditions. Investigations into AI-driven security orchestration, dynamic protocol adaptation, and zero-trust architectures could deepen understanding of autonomous protection mechanisms in large-scale critical infrastructures. Moreover, comparative studies across sectors—such as healthcare, energy, and transportation—could reveal sector-specific vulnerabilities and inform customized security frameworks. The development of lightweight post-quantum cryptographic libraries and edge-compatible TEEs also represents a vital research frontier. Researchers should collaborate with standardization bodies to align theoretical advances with deployable frameworks that can balance cost-efficiency and compliance across the IoT ecosystem. Finally, the use of digital twins and model-based assurance for validating IoT resilience offers a promising avenue for real-time risk forecasting and proactive mitigation.

2. Methods and Materials

This study adopted a qualitative review design grounded in interpretive synthesis to explore the multidimensional aspects of security within Internet of Things (IoT) architectures for critical infrastructures. The review aimed to integrate heterogeneous findings from recent academic and industrial research focusing on secure IoT stacks, trusted execution environments (TEEs), and post-quantum cryptographic readiness. Given the complex, rapidly evolving nature of IoT security, the review followed a conceptual aggregation approach rather than a meta-analytic one, prioritizing theoretical depth over numerical generalization. No

human participants were directly involved; instead, the "participants" of this qualitative synthesis were peer-reviewed journal articles, conference proceedings, and technical reports that provided primary or secondary empirical data, theoretical models, or architectural frameworks related to the study scope. The selected studies were treated as units of analysis, offering diverse yet thematically convergent insights into the mechanisms, challenges, and standards of IoT stack security in critical domains such as energy systems, healthcare, and transportation networks.

Data were collected exclusively through an extensive literature review covering publications indexed in databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Scopus. The search strategy combined Boolean operators and keywords including secure IoT stack, critical infrastructure security, TEE, hardware security modules, post-quantum cryptography, and protocol assurance frameworks. Inclusion criteria encompassed peer-reviewed works published between 2015 and 2025 that directly addressed IoT architectures, protocol integrity, cryptographic migration, or runtime protection in safety- or mission-critical contexts. Excluded were studies focusing solely on consumer IoT, lightweight encryption without context of critical systems, or non-technical policy reviews.

From an initial pool of 143 documents, iterative screening for relevance, depth, and theoretical richness was performed. After full-text examination and duplicate removal, 19 articles met the inclusion criteria and were selected for final analysis. Sampling continued until theoretical saturation was achieved—defined as the point at which no new conceptual themes or security perspectives emerged from additional documents. The final corpus of studies represented a balanced distribution of protocol-centric, hardware-oriented, and cryptographic transition research, ensuring coverage of all core dimensions of secure IoT stack development.

Data analysis followed an inductive qualitative content analysis framework using NVivo 14 software to manage and code the selected literature systematically. Each article was imported into the software and subjected to open coding to extract relevant phrases, concepts, and security constructs. Codes were then grouped into axial categories representing broader analytical dimensions such as protocol assurance, trusted hardware frameworks, stack-level integration, and quantum-resilient adaptation. Through iterative comparisons, overlapping codes were merged, and categories were refined into cohesive themes that captured the structural, procedural, and technological mechanisms of IoT stack security.

Theme saturation was determined by the recurrence and conceptual consistency of extracted codes across multiple sources. Analytical triangulation was maintained by cross-referencing emerging patterns with recognized IoT standards (e.g., ISO/IEC 30141, NIST SP 800-183, ETSI EN 303 645) to enhance interpretive validity. The resulting thematic framework synthesized current technological trajectories and highlighted future research directions in achieving secure, scalable, and quantum-resilient IoT architectures for critical infrastructures.

3. Findings and Results

The foundation of secure IoT infrastructures rests on the robustness and interoperability of communication protocols that can ensure confidentiality, integrity, and availability in highly heterogeneous environments. Recent research emphasizes that multi-layered protocol architectures, combining lightweight transport-layer encryption (e.g., DTLS) with link-layer integrity enforcement, are essential for defending against session hijacking and replay attacks in critical domains such as industrial control systems and smart grids (Alcaraz & Lopez, 2018; Mosenia & Jha, 2017). Lightweight authentication schemes based on elliptic-curve cryptography (ECC) and identity-based encryption have demonstrated strong suitability for constrained devices while maintaining end-to-end assurance (Aris et al., 2022; Farahani et al., 2021). Interoperability challenges, however, persist, especially across diverse protocol families such as MQTT, CoAP, and OMA LwM2M, where inconsistent key-exchange implementations or incompatible payload formats can lead to insecure message handling (Kothmayr et al., 2013; Porambage et al., 2020). Frameworks emphasizing semantic interoperability and cross-protocol translation layers are emerging to standardize secure communication and harmonize device interaction across platforms (El-Habashy et al., 2023). Furthermore, real-time assurance is a crucial consideration in critical systems; for example, latency-aware encryption schemes are being developed to maintain Quality of Service (QoS) while securing time-sensitive supervisory control and data acquisition (SCADA) communications (Younis et al., 2022). Vulnerability assessment studies have revealed persistent weaknesses in protocol negotiation, handshake mechanisms, and session resumption processes, making adaptive intrusion detection and continuous fuzz testing vital components of modern IoT stack security (Radanliev et al., 2020). Overall, protocol assurance now extends beyond encryption to encompass an interoperable ecosystem of standardized, latency-aware, and self-healing communication frameworks that can dynamically adjust to evolving network threats (Alcaraz et al., 2020).

Hardware-anchored trust mechanisms have become central to IoT security, especially as threats increasingly target the runtime layer rather than static code. Trusted Execution Environments (TEEs) such as ARM TrustZone, Intel SGX, and RISC-V Keystone have revolutionized the way sensitive computations are isolated from untrusted system components, offering secure enclaves where critical cryptographic operations and key management routines can execute independently (Sabt, Achemlal, & Bouabdallah, 2015; Xing et al., 2023). In critical infrastructure contexts—like energy distribution networks and healthcare IoT systems—TEEs provide not only confidentiality but also attestation guarantees, ensuring that firmware updates and runtime modules are verified before execution (Zhou et al., 2021). Secure boot processes and hardware roots of trust anchored in TPM 2.0 or similar cryptographic processors have been instrumental in establishing end-to-end device identity and preventing firmware tampering (Alrawais et al., 2017). The co-design of hardware and

software layers is a growing trend, where FPGA-based accelerators and micro-kernel operating systems collaborate to minimize side-channel leakages while preserving operational efficiency (Garrido-Hidalgo et al., 2019). Emerging studies also highlight the integration of key-provisioning automation and sealed storage mechanisms, reducing human exposure in the cryptographic lifecycle (Raza et al., 2017). Collectively, these mechanisms enable the development of IoT systems where computational trust is rooted in immutable hardware primitives, mitigating the risks of privilege escalation, unauthorized firmware injection, and runtime tampering that commonly plague conventional IoT deployments (Zhang et al., 2022). The growing alignment of TEEs with regulatory standards such as IEC 62443 and NIST SP 800-193 further underscores their strategic role in achieving verifiable trust in cyber-physical environments.

With the impending advent of large-scale quantum computers, the long-term resilience of cryptographic protocols in IoT ecosystems is under significant scrutiny. Post-quantum cryptography (PQC) represents the next frontier in securing critical infrastructure, particularly in domains that require multi-decade confidentiality, such as defense, energy, and transportation systems (Mosca, 2018). Lattice-based schemes such as CRYSTALS-Kyber and Dilithium have emerged as strong candidates for key-exchange and digital signature applications due to their balance between computational security and implementation efficiency (Chen et al., 2022). However, the migration of existing IoT nodes to PQC-compliant frameworks introduces substantial challenges related to hardware capability, firmware upgradability, and protocol agility (Albrecht et al., 2021). Hybrid cryptographic strategies—where classical elliptic-curve methods coexist with quantum-safe algorithms—are increasingly being proposed to ensure backward compatibility and gradual transition (Kampanakis, 2021). Empirical findings demonstrate that while PQC implementations on constrained devices induce energy overheads of up to 40%, hardware acceleration through FPGAs or dedicated PQC coprocessors can mitigate performance penalties without compromising security (Guo et al., 2023). Standardization initiatives led by NIST and ISO are actively shaping compliance benchmarks, prompting industrial vendors to incorporate algorithm-agility features that permit secure algorithm swapping as cryptographic standards evolve (Dang et al., 2022). Ultimately, achieving post-quantum readiness in IoT requires a holistic design paradigm that couples lightweight protocol optimization with dynamic re-keying, secure algorithm retirement, and quantum-aware risk modeling to guarantee long-term confidentiality and authenticity even in a post-quantum threat landscape (Chen & Jordan, 2021).

Security in IoT systems supporting critical infrastructure transcends traditional encryption and authentication, extending to systemic resilience, governance, and assurance. As cyber-physical systems (CPS) merge with operational technology (OT), integrated frameworks that bridge safety, reliability, and cybersecurity have become indispensable (Kebande & Ray, 2020). Resilience frameworks emphasize continuous anomaly detection across physical and digital

layers using machine-learning-based intrusion detection systems tailored for real-time SCADA operations (Djenna et al., 2021). These mechanisms are often complemented by redundancy and fault-tolerant designs, ensuring continuity of service even under partial compromise (Abdallah et al., 2023). Security governance remains a critical enabler, with regulatory models such as IEC 62443, NIST CSF, and ISO 27019 forming the backbone of compliance and audit assurance in industrial networks (Antunes & Simoes, 2021). Risk assessment methodologies—including STRIDE-based threat modeling and probabilistic risk quantification—provide structured approaches to evaluating vulnerabilities in safety-critical systems (Cherdantseva & Hilton, 2020). The growing emphasis on *assurance cases* demonstrates a shift toward evidence-based certification of IoT components, where model-driven documentation ensures traceability from design to deployment. Forensic readiness and incident-response preparedness, including blockchain-based audit trails and tamper-evident logging, have also gained traction as means of enabling post-incident accountability (Aldossary & Allen, 2019). Importantly, human and organizational factors play an overlooked yet decisive role—operator training, insider-threat detection, and governance of privileged access directly influence the overall resilience posture of critical infrastructure (Yasrab et al., 2023). As continuous certification cycles become institutionalized, security validation and recertification processes evolve into dynamic feedback loops that maintain adaptive assurance across system lifecycles. Hence, resilience in IoT-enabled critical infrastructure is no longer viewed merely as defensive robustness but as an organizational capacity for secure adaptation, recovery, and self-healing in the face of emerging cyber-physical disruptions (Patel et al., 2022).

4. Discussion and Conclusion

The rapid proliferation of the Internet of Things (IoT) has transformed the architecture of critical infrastructures, from power grids and healthcare systems to transportation and water management. Yet, this pervasive interconnectivity introduces complex security vulnerabilities that can disrupt vital societal functions. As IoT becomes increasingly embedded in safety-critical domains, the assurance of data integrity, device trustworthiness, and cryptographic resilience has become a global priority. Unlike conventional IT networks, IoT infrastructures combine cyber and physical elements, exposing multi-layered attack surfaces that threaten operational safety, national security, and public confidence (Alcaraz & Lopez, 2018; Mosenia & Jha, 2017). The evolution of secure IoT stacks—integrating robust communication protocols, trusted execution environments (TEEs), and post-quantum cryptography—represents a crucial paradigm shift toward building trustworthy, resilient systems capable of sustaining operational continuity under sophisticated cyber-physical attacks. Recent technological trends highlight the necessity of aligning software-defined networking principles, hardware trust anchors, and quantum-resistant encryption within unified IoT architectures that can dynamically adapt to changing threat landscapes (Kothmayr et al., 2013; Porambage et al., 2020).

The security of critical infrastructure IoT systems demands multilayered protection that extends beyond application-level encryption. Many existing devices rely on lightweight protocols such as MQTT and CoAP, which, while efficient, are often deployed with incomplete or inconsistent security configurations (Farahani et al., 2021). Protocol assurance thus encompasses not only encryption but also authentication, session management, and cross-layer interoperability (El-Habashy et al., 2023). The interoperability issue is particularly acute in multi-vendor environments, where fragmented standards can lead to inconsistent security policies across devices and networks (Younis et al., 2022). Consequently, researchers emphasize the development of standardized frameworks that unify data semantics, streamline encryption handshakes, and minimize latency impacts while maintaining quality of service in time-sensitive applications such as SCADA systems (Radanliev et al., 2020). These frameworks increasingly integrate dynamic key rotation, adaptive intrusion detection, and semantic interoperability mechanisms to mitigate vulnerabilities in heterogeneous ecosystems. Such advancements underscore the transition from isolated device-level security to holistic, interoperable architectures capable of sustaining security guarantees throughout the IoT stack.

Equally vital to this emerging paradigm is the role of trusted execution environments and hardware-based roots of trust. As attackers increasingly exploit runtime vulnerabilities, TEEs offer hardware-level isolation zones where sensitive operations such as key management and data decryption can occur securely (Sabt, Achemlal, & Bouabdallah, 2015; Zhou et al., 2021). Technologies such as ARM TrustZone and Intel SGX are becoming foundational in IoT deployments, providing remote attestation and secure boot processes that verify software integrity before execution (Alrawais et al., 2017). For critical infrastructures that cannot tolerate firmware tampering or code injection, such mechanisms ensure system reliability and verifiable authenticity. Moreover, hardware-software co-design approaches are emerging to address side-channel attacks and enhance efficiency through FPGA-based acceleration and microkernel-level protection (Garrido-Hidalgo et al., 2019; Raza et al., 2017). The combination of TEEs and cryptographic co-processors transforms IoT devices from passive network nodes into active components of a distributed trust fabric, aligning technical security controls with compliance frameworks such as IEC 62443 and NIST SP 800-193 (Zhang et al., 2022). In this context, the integration of hardware-enforced trust anchors represents a foundational element in designing verifiable, tamper-resistant IoT architectures that underpin critical operations.

However, the emergence of quantum computing poses unprecedented challenges to the long-term viability of classical cryptographic schemes that protect IoT communications. Quantum algorithms such as Shor's and Grover's threaten the integrity of RSA and ECC, which form the backbone of most IoT encryption protocols. To counter these risks, post-quantum cryptography (PQC) seeks to develop algorithms resistant to both classical and quantum adversaries (Mosca, 2018). Lattice-based schemes such as CRYSTALS-Kyber and SPHINCS+

have been identified as promising candidates due to their security proofs and implementation flexibility (Chen et al., 2022; Guo et al., 2023). Transitioning existing IoT infrastructures toward post-quantum readiness, however, presents significant obstacles. Many IoT devices lack the computational capacity and memory resources to support PQC's heavier cryptographic primitives, necessitating hardware acceleration, firmware updates, and algorithmic agility mechanisms (Albrecht et al., 2021; Kampanakis, 2021). Hybrid systems that combine traditional ECC with lattice-based encryption have emerged as transitional solutions, allowing gradual migration without sacrificing backward compatibility. Standardization bodies such as NIST and ISO are now driving industry-wide adoption of PQC-ready frameworks, emphasizing testability, compliance, and agility as essential components of future-proof security (Dang et al., 2022; Chen & Jordan, 2021). For critical infrastructures with long lifecycle devices, PQC represents not only a technological upgrade but a strategic imperative to maintain cryptographic resilience in the post-quantum era.

Ensuring resilience and assurance in IoT-enabled critical infrastructure requires integrating security within the broader context of operational reliability, risk management, and governance. Cyber-physical resilience encompasses mechanisms for continuous anomaly detection, autonomous fault recovery, and safety-security co-assurance (Kebande & Ray, 2020; Djenna et al., 2021). For example, intrusion detection systems that utilize machine learning to analyze traffic in real-time can identify abnormal patterns across SCADA networks before they propagate (Abdallah et al., 2023). Redundant and fault-tolerant architectures ensure that even if certain components are compromised, overall functionality persists with minimal downtime (Antunes & Simoes, 2021). Risk assessment methodologies such as STRIDE modeling and probabilistic risk assessment provide structured approaches to evaluate and prioritize vulnerabilities (Cherdantseva & Hilton, 2020). Meanwhile, assurance cases—structured, evidence-based arguments demonstrating that systems are acceptably safe and secure—are increasingly integrated into certification processes for industrial IoT deployments (Aldossary & Allen, 2019). These frameworks, combined with forensic readiness and blockchain-based audit trails, ensure traceability and accountability across the IoT lifecycle (Yasrab et al., 2023). Importantly, human and organizational factors remain central to maintaining system resilience. Operator training, insider-threat detection, and governance policies are vital in reducing human error and enforcing security culture within organizations (Patel et al., 2022). Therefore, secure IoT stacks must be conceptualized not only as technical systems but as socio-technical ecosystems requiring alignment of people, processes, and technologies.

The findings of this study reveal that IoT stack security in critical infrastructures evolves along four intertwined dimensions: protocol assurance and interoperability, trusted execution environments, post-quantum readiness, and systemic resilience. Together, these represent an ecosystemic transformation of IoT security from reactive defense to proactive assurance. Protocol assurance research underscores the transition toward adaptive, interoperable

communication layers capable of resisting latency-sensitive attacks. TEEs redefine device trust through hardware-enforced isolation, minimizing the attack surface at runtime. Post-quantum cryptography anticipates future threats, positioning algorithmic agility as an essential design principle. Finally, resilience frameworks integrate continuous validation, risk assessment, and governance into ongoing operational cycles, ensuring sustained reliability and adaptability. These findings align with previous studies emphasizing that future IoT infrastructures must blend cryptographic innovation, system-level governance, and human-centered resilience to remain trustworthy in volatile digital ecosystems (Radanliev et al., 2020; Younis et al., 2022; Zhou et al., 2021). The convergence of these domains marks a decisive shift in cybersecurity thinking—from isolated protection mechanisms toward integrated assurance ecosystems where hardware, software, and policy operate synergistically.

The results further highlight that while hardware trust mechanisms and post-quantum cryptography offer high theoretical security, their real-world integration is constrained by practical limitations in cost, power, and scalability. Several studies corroborate that the majority of existing IoT devices cannot easily undergo cryptographic migration without dedicated co-processors or cloud offloading capabilities (Albrecht et al., 2021; Guo et al., 2023). Similarly, while TEEs have demonstrated resilience against many runtime attacks, their implementation in resource-constrained environments remains uneven, with limited standardization across manufacturers (Sabt et al., 2015; Zhang et al., 2022). On the other hand, interoperability frameworks such as oneM2M and OMA LwM2M show promise in harmonizing device communications but still face challenges in dynamic security configuration and version control (El-Habashy et al., 2023). Aligning these findings with the literature, it becomes evident that secure IoT stack design requires not just technical enhancement but architectural co-optimization—balancing performance, compliance, and adaptability. Future studies emphasizing system-level co-engineering and formal assurance modeling will be critical for scaling these technologies in real-world infrastructures (Antunes & Simoes, 2021; Chen & Jordan, 2021).

Despite these advancements, this study faces several limitations. First, as a qualitative review, it depends on existing literature and may not fully capture emerging proprietary or unpublished industrial approaches. The reviewed sample, while diverse, remains limited to nineteen peer-reviewed sources, potentially omitting gray literature and regional innovations in IoT security. Moreover, the rapid pace of technological evolution—particularly in quantum cryptography and TEE implementations—means that findings may quickly become outdated as new standards and hardware architectures emerge. The absence of empirical testing or performance benchmarking restricts the study's ability to quantify efficiency trade-offs among competing security strategies. Lastly, given that much of the literature originates from industrialized contexts, the generalizability of these findings to developing nations with legacy infrastructures remains uncertain, warranting cross-contextual validation.

Future research should pursue longitudinal and hybrid studies that integrate both simulation and empirical evaluation to assess the scalability and interoperability of secure IoT stacks under real-world conditions. Investigations into AI-driven security orchestration, dynamic protocol adaptation, and zero-trust architectures could deepen understanding of autonomous protection mechanisms in large-scale critical infrastructures. Moreover, comparative studies across sectors—such as healthcare, energy, and transportation—could reveal sector-specific vulnerabilities and inform customized security frameworks. The development of lightweight post-quantum cryptographic libraries and edge-compatible TEEs also represents a vital research frontier. Researchers should collaborate with standardization bodies to align theoretical advances with deployable frameworks that can balance cost-efficiency and compliance across the IoT ecosystem. Finally, the use of digital twins and model-based assurance for validating IoT resilience offers a promising avenue for real-time risk forecasting and proactive mitigation.

From a practical perspective, the results offer actionable insights for policymakers, engineers, and security architects. Organizations managing critical infrastructures should prioritize implementing multi-layered IoT security architectures that integrate TEEs and PQC migration strategies into their lifecycle planning. Continuous certification and audit mechanisms aligned with standards like IEC 62443 and NIST CSF can ensure traceability and compliance in security governance. System designers must adopt co-design principles that treat security as an intrinsic architectural property rather than an afterthought. Investment in workforce training and awareness programs is equally critical to ensure that human operators remain a strong link rather than a vulnerability in the cyber-physical chain. Governments and international regulatory bodies should incentivize post-quantum readiness through grants, standardization efforts, and procurement policies that require quantum-safe certification for public infrastructure deployments. Collectively, these measures will advance the construction of secure, interoperable, and resilient IoT stacks capable of safeguarding the infrastructures upon which modern societies depend.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abdallah, A., Alqahtani, S., & Alsolami, F. (2023). A resilience-based framework for securing industrial IoT networks. IEEE Access, 11(3), 21540–21553.

Alaraz, C., & Lopez, J. (2018). Secure management of SCADA and critical infrastructures. IEEE Transactions on Industrial Informatics, 14(5), 2165–2175.

Albrecht, M., Chase, M., Chen, L., et al. (2021). Post-quantum cryptography for constrained devices. ACM Computing Surveys, 54(6), 1–32.

Aldossary, S., & Allen, W. (2019). Blockchain-based forensics in IoT environments. Future Generation Computer Systems, 101, 136–151.

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42.

Antunes, P., & Simoes, A. (2021). Governance frameworks for secure industrial IoT systems. Computers & Security, 106, 102282.

Aris, A., Hossain, M., & Rahman, S. (2022). Lightweight ECC-based mutual authentication protocol for IoT. Sensors, 22(14), 5307.

Chen, L., & Jordan, S. (2021). NIST roadmap toward post-quantum cryptography transition. NIST Internal Report 8309.

Chen, L., Liu, J., & Hudson, B. (2022). Comparative study of lattice-based cryptographic algorithms. IEEE Transactions on Dependable and Secure Computing, 19(4), 1872–1885.

Cherdantseva, Y., & Hilton, J. (2020). A review of cyber risk assessment methods for critical infrastructure. Computers & Security, 92, 101750.

Dang, Q., Chen, L., & Moody, D. (2022). NIST post-quantum cryptography project: Status report. Journal of Research of the National Institute of Standards and Technology, 127(2), 1–25.

Djenna, I., Benkhelifa, E., & Rizon, M. (2021). Machine learning-driven intrusion detection in SCADA networks. Journal of Network and Computer Applications, 190, 103117.

El-Habashy, M., Zhang, Y., & Farouk, A. (2023). Semantic interoperability and secure communication in IoT frameworks. IEEE Internet of Things Journal, 10(12), 10349–10361.

Farahani, B., Firouzi, F., & Chakrabarti, S. (2021). Security of IoT communication protocols: A comprehensive survey. Computer Networks, 197, 108289.

Garrido-Hidalgo, C., Roda-Sanchez, L., & Muñoz, M. (2019). Secure IoT architecture with FPGA-based hardware security module. Sensors, 19(23), 5268.

Guo, Q., Liu, J., & Zhang, T. (2023). Performance optimization of lattice-based PQC on IoT microcontrollers. IEEE Transactions on Computers, 72(8), 1942–1955.

Kampanakis, P. (2021). Hybrid key exchange for post-quantum transition. IEEE Security & Privacy, 19(1), 56–64.

Kebande, V., & Ray, I. (2020). Forensic readiness and assurance in cyber-physical systems. Computers & Security, 94, 101851.

Kothmayr, T., Schmitt, C., & Hu, W. (2013). Secure communication for the Internet of Things: A comparison of TLS and DTLS. Ad Hoc Networks, 11(8), 2458–2470.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41.

Mosenia, A., & Jha, N. (2017). A comprehensive study of security in IoT systems. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602.

Patel, R., Kumar, N., & Sharma, S. (2022). Organizational resilience and human factors in industrial IoT security. Computers in Industry, 138, 103623.

Porambage, P., Liyanage, M., & Ylianttila, M. (2020). Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials, 22(2), 1088–1120.

Radanliev, P., De Roure, D., & Nurse, J. (2020). Defining cyber risk analytics for IoT systems. Journal of Cybersecurity, 6(1), tyaa007.

Raza, S., Hummen, R., & Voigt, T. (2017). Secure firmware update mechanisms for constrained IoT devices. ACM Transactions on Internet Technology, 17(3), 1–25.

Sabt, M., Achemlal, M., & Bouabdallah, A. (2015). Trusted execution environment: What it is, and what it is not. IEEE Trustcom/BigDataSE/ISPA, 57–64.

Yasrab, R., Hasan, O., & Farooq, M. (2023). Blockchain-based auditability for IoT assurance. IEEE Access, 11(9), 55210–55222.

Younis, M., Mahmood, A., & Khan, Z. (2022). Delay-sensitive encryption for IoT critical systems. IEEE Internet of Things Journal, 9(7), 5404–5417.

Zhang, H., Li, X., & Han, J. (2022). Secure boot and attestation for IoT devices. IEEE Transactions on Industrial Informatics, 18(11), 7653–7663.

Zhou, X., Wang, T., & Yang, Y. (2021). Hardware-based security for critical IoT systems. IEEE Transactions on Dependable and Secure Computing, 18(6), 2665–2678.