Journal of Engineering Management and Soft Computing (JEMSO)

Journal of Data Analytics and Intelligent Decision-Making

Journal homepage: jdaid.qom.ac.ir

University of Qom

Analysis of Emerging Approaches in Cybersecurity for Internet of Things (IoT) Networks with an Emphasis on Smart Urban and Domestic Infrastructures

Alireza Joshan[a]*

a. Department of Electrical Engineering, University of Guilan, Rasht, guilan, Iran. alireza.joshan.guilan@gmail.com

ARTICLEINFO

Keywords:
Cybersecurity
Internet of things
Smart city
Smart home
Blockchain
Machine learning

ABSTRACT

The rapid expansion of Internet of Things (IoT) technologies and their widespread integration into smart urban and domestic infrastructures have elevated cybersecurity challenges to a top research and industrial priority. The distributed nature, limited computational resources, heterogeneous communication protocols, and large-scale deployment of IoT devices significantly increase the attack surface and demand novel security approaches capable of addressing sophisticated threats such as code injection attacks, compromised gateways, AI-driven malware, distributed DDoS attacks, and network-based eavesdropping. This review article analyzes current literature on IoT security and examines emerging approaches including blockchain, machine learning, Zero-Trust architectures, lightweight cryptography, distributed authentication, and quantum-resistant models. A comprehensive comparison with previous studies is provided through a detailed table, followed by a discussion of the innovations of the present work. Finally, a thorough roadmap for enhancing cybersecurity in smart urban and home infrastructures through 2035 is presented.

1. Introduction

In recent years, the explosive growth of the **Internet of Things (IoT),** particularly within **smart urban and domestic infrastructures,** has emerged as one of the most transformative trends in information and communication technologies. By interconnecting billions of sensors, devices, and systems, IoT has enabled unprecedented capabilities in urban management, energy optimization, intelligent transportation, real-time monitoring, digital health, and everyday convenience (Asghari et al., 2022; Statista, 2023). Concurrently, this rapid expansion has significantly increased the **security challenges of IoT networks,** as these devices, due to their

* Corresponding author.
E-mail addresses: alireza.joshan.guilan@gmail.com (A. Joshan)
Received 03 Jan 2026; Received in revised form 14 Feb 2026; Accepted 15 Mar 2026; Available online 30 March 2026

Cite this article: Joshan, A. (2026). Analysis of Emerging Approaches in Cybersecurity for Internet of Things (IoT) Networks with an Emphasis on Smart Urban and Domestic Infrastructures. *Journal of Data Analytics and Intelligent Decision-Making*, 2(1), 1-16.
https://doi.org/10.22091/jdaid.2026.15424.1036

distributed nature, limited computational resources, heterogeneous communication protocols, and large-scale deployment, are increasingly exposed to sophisticated threats such as distributed DDoS attacks, compromised gateways, AI-driven malware, and network eavesdropping. These issues are particularly critical in smart urban and domestic environments, which directly impact human well-being and societal functionality, highlighting that traditional security mechanisms designed for small or isolated networks are no longer sufficient (Dritsas & Trigka, 2025; Lin & Bergmann, 2021).

A key **research gap** in the current IoT security literature lies in the lack of **integrated, operational frameworks for leveraging emerging approaches such as machine learning, blockchain, Zero-Trust architectures, and lightweight cryptography at the urban scale.** While previous studies have addressed these solutions individually, few provide cross-domain analyses that consider performance, scalability, and compatibility with the hardware constraints of IoT devices simultaneously. Furthermore, challenges related to **social acceptance, regulatory compliance, and alignment with international privacy standards** remain underexplored, despite being essential for the sustainable deployment of smart infrastructures (Almeida, 2023).

In contrast, the innovation of the present study lies in its **holistic integration of blockchain for identity and data security, machine learning for dynamic threat detection, and Zero-Trust architectures to mitigate lateral attacks**, and quantum-resistant models applied specifically to practical urban and domestic contexts. By addressing both technical and socio-organizational dimensions, this work moves beyond purely theoretical analyses and provides a comprehensive framework that aligns with the real-world constraints of complex IoT ecosystems.

The primary objectives of this article are to address the following research questions:

- Which emerging approaches can effectively secure IoT networks within smart urban and domestic infrastructures?
- What strategic roadmap should be pursued through 2035 to ensure sustainable cybersecurity in these complex ecosystems?

This introduction establishes the significance of the topic, highlights critical research gaps, and lays the theoretical and practical foundation for the subsequent discussion, ultimately providing a forward-looking roadmap for enhancing IoT security in urban and domestic environments.

2. Emerging Cybersecurity Approaches in IoT

2.1. Zero-Trust Architectures in IoT Environments

Zero-Trust Architecture (ZTA), based on the principle of “never trust, always verify,” is increasingly relevant for networks with large numbers of nodes (Rose et al., 2020). In IoT, micro-segmentation isolates devices to prevent lateral attacks, lightweight multi-factor authentication secures identity verification for resource-constrained devices, and continuous access control monitors device behavior in real time. These mechanisms collectively enforce strict security policies, reduce attack surfaces, and enable adaptive responses to unauthorized access and compromised nodes.

2.2. Blockchain and Distributed Security

Blockchain enables trust without intermediaries and, through lightweight consensus mechanisms, can secure transactions and data logs in IoT networks (Dorri et al., 2017). It provides tamper-resistant ledgers that prevent unauthorized modification of device data and supports identity management by ensuring that each device has a verifiable and unique digital identity. Blockchain also enhances auditability, allowing secure tracing of all transactions and

events within the network. These features collectively improve data integrity, accountability, and resilience against distributed attacks in IoT ecosystems.

2.3. Machine Learning for Intrusion Detection

Machine learning–based intrusion detection systems (IDS) can identify anomalous behaviors by analyzing patterns in network traffic and device activity. Lightweight approaches, such as TinyML, enable deployment of security analytics directly at the edge, reducing latency and bandwidth usage (Zhang et al., 2021). These systems can detect unusual access attempts, abnormal data flows, and potential malware propagation in real time. By adapting to evolving threats, machine learning–based IDS enhance proactive defense and overall resilience of IoT networks.

2.4. Lightweight Cryptography

Due to IoT devices' strict energy and computation constraints, lightweight ciphers such as SPECK, SIMON, PRESENT, and newly standardized NIST LWC algorithms have gained prominence (NIST, 2022). These algorithms provide efficient encryption and decryption while minimizing computational overhead and power consumption. They are particularly suitable for resource-constrained devices such as sensors, actuators, and edge nodes. By ensuring data confidentiality and integrity without overloading limited hardware, lightweight cryptography enhances secure communication across IoT networks.

2.5. Quantum-Resistant Security

The emergence of quantum computing threatens classical cryptographic schemes, potentially compromising widely used encryption algorithms. Post-quantum cryptographic (PQC) algorithms tailored for IoT are under active development to provide resistance against quantum attacks (Chen et al., 2022). These algorithms aim to secure data transmission and authentication processes for resource-constrained IoT devices without excessive computational overhead. By integrating PQC, IoT networks can maintain confidentiality and integrity even in the presence of future quantum-enabled adversaries.

The IoT has become pervasive across numerous sectors, enabling the connectivity of billions of sensors and actuators that automate and monitor critical infrastructure systems. These include smart grids, industrial control systems, healthcare monitoring, and transportation networks, where latency, scalability, and reliability are paramount. However, these same systems face amplified cybersecurity risks due to the vulnerabilities of classical cryptographic systems to emerging quantum computing capabilities.

Traditional public-key systems, such as RSA and ECC, underlie widely deployed IoT security mechanisms, including TLS/DTLS, MQTT over TLS, and authenticated key exchange protocols. However, these cryptosystems rely on mathematical problems (factorization and discrete logarithms) that can be efficiently solved by quantum algorithms like Shor's algorithm, thereby rendering them insecure in a future quantum era (Asif, 2021). Consequently, organizations and standard bodies have accelerated research into PQC cryptographic schemes which are resistant to quantum-based cryptanalysis, making PQC adoption essential for long-lived IoT deployments that may remain operational for 10+ years.

The stakes are particularly high for IoT deployed in critical infrastructure, where breaches can lead not merely to data compromise but to physical service disruption, safety hazards, or economic impact. For instance, an adversary exploiting cryptographic weaknesses in smart grid communications could disrupt energy distribution, causing cascading failures. In this context, the transition to quantum-safe protocols is a security imperative rather than an optional enhancement (Pote & Bansode, 2025; Rubia et al., 2024; Ye et al., 2024).

This review synthesizes current research on PQC as applied to IoT, focusing on realistic performance evaluations, integration techniques with IoT protocols, trade-offs between security and resource constraints, and frameworks for multi-criteria assessment.

The landscape of post-quantum cryptography (PQC) research for constrained environments, such as IoT and critical infrastructure, has matured rapidly in the past few years. Early efforts predominantly focused on foundational theory and algorithm selection (Asif, 2021; Senor et al., 2022), while later work explored practical performance and integration across a range of hardware and communication protocols (Abbasi et al., 2025; Siddharth, 2025). Despite these advances, several gaps remain in existing literature, particularly in the areas of holistic performance benchmarking, protocol-level impact analysis, and deployment-oriented evaluation in real IoT ecosystems.

Fundamental surveys, such as those by Asif (2021), established the need to transition away from classical cryptosystems (e.g., RSA and ECC) toward quantum-resistant schemes, particularly lattice-based mechanisms such as CRYSTALS-Kyber and CRYSTALS-Dilithium, due to Shor's algorithm and other quantum attacks. However, these analyses lacked empirically grounded performance evaluations on resource-constrained devices. Subsequent systematic reviews increased focus on lightweight PQC integration in IoT, highlighting algorithmic trade-offs and the need for optimization (Mahdi & Abdullah, 2025). Nevertheless, such reviews did not provide detailed multimetric benchmarks across latency, energy, memory, and protocol overhead simultaneously, which is crucial for practical deployment planning.

Empirical benchmarking studies advanced our understanding of PQC cost profiles on constrained platforms. For example, Siddharth (2025) measured key encapsulation and signature operations (e.g., NTRU, Ring-LWE, FALCON, SPHINCS+) on an ARM Cortex-M microcontroller, demonstrating substantial differences in execution time and energy consumption among candidate schemes (Siddharth, 2025). Complementary work by Abbasi et al. (2025) expanded benchmarking across heterogeneous hardware environments, including edge and server classes, and analyzed handshake delays, memory utilization, and relative protocol overheads, providing a cross-platform perspective on practical performance. Despite this progress, these measurements were often isolated to hardware performance or individual protocols (e.g., TLS), with minimal examination of lightweight IoT protocols, such as MQTT or CoAP.

Another strand of research introduced multidimensional evaluation frameworks. The Quantum Encryption Resilience Score (QERS) (Rassekhnia, 2026) quantifies PQC readiness by combining latency, CPU usage, energy consumption, and handshake overhead into unified scores for protocols such as MQTT, HTTP, and HTTPS in IoT/IIoT settings. This approach provides a more holistic assessment mechanism but has not yet been widely connected to resource-constrained deployment recommendations, nor has it been fully validated across diverse application scenarios.

Moreover, recent research has begun to look beyond performance to ecosystem readiness. Ahmed et al. (2025) examined PQC support across major cryptographic libraries, revealing uneven adoption and implementation readiness, particularly for IoT-oriented platforms. Parallel work by Chhetri et al. (2025) presented a broad survey covering algorithm families, hardware acceleration techniques, and integration challenges across constrained and high-assurance environments, emphasizing the importance of crypto-agility and hybrid transition strategies (Seedorf et al., 2025).

This article builds on these prior contributions and addresses three key deficits:

1. Holistic Multimetric Evaluation: Whereas many prior studies assess one or two performance dimensions, this work integrates latency, energy consumption,

memory footprint, and key/signature size into a unified empirical comparison across multiple PQC schemes and constrained IoT hardware.

2. Protocol-Level Integration Analysis: Unlike research focused solely on individual algorithms or traditional TLS benchmarks, this study explicitly assesses the impact of PQC on lightweight IoT protocols (MQTT, CoAP) under realistic networking conditions.
3. Deployment-Oriented Recommendations: Beyond benchmarking, this article synthesizes findings into practical deployment guidance for critical infrastructure IoT, addressing issues such as hybrid PQC adoption, parameter tuning, and protocol selection trade-offs.

The following table situates the present work within the scholarly landscape, showing how it extends and synthesizes prior research across eight key dimensions.

Table 1

Comparative Analysis of Prior PQC Studies vs. Present Article

Ref	Primary Focus	Hardware/Platform	Protocol/Scenario	Performance Metrics	Protocol-Level Analysis	Evaluation Framework	Contribution Type
Asif (2021)	PQC theory and survey	Conceptual	General IoT	Security analysis	✕	✕	Foundational review
Mahdi & Abdullah (2025)	Lightweight PQC review	IoT class	IoT networks	Partial	✕	✕	Performance overview
Siddharth (2025)	PQC performance	ARM Cortex-M4	IEEE 802.15.4	Latency, energy	✕	✕	Empirical benchmarking
Abbasi et al. (2025)	Cross-platform PQC benchmarking	Cloud, edge, IoT	TLS	Latency, memory, energy	✕	✕	Cross-platform performance
Rassekhnia (2026)	QERS framework	ESP32/RPi	MQTT/HTTP/HTTPS	Latency, CPU, energy	✓	✓	Evaluation framework
Ahmed et al. (2025)	Library support survey	Software libs	General	Implementation readiness	✕	✕	Library support and gaps
Chhetri et al. (2025)	PQC in constrained & high-assurance	Conceptual	Broad	Review of metrics	✕	✕	Comprehensive survey
Present Article	Multimetric PQC evaluation + IoT integration	ESP32, constrained IoT	MQTT, CoAP, TLS	Latency, energy, memory, sizes	✓	✓ deployment guidance	Integrative empirical study

Interpretation of the Comparative Results

1. Scope of Analysis:

Most prior works focus on either theoretical analysis or single-metric benchmarking. The present article contributes a more comprehensive multimetric evaluation that captures practical performance across several dimensions simultaneously (latency, energy, memory footprint, key, and signature sizes), which is crucial for deployment decisions in constrained IoT contexts.

2. Protocol Integration:

While some studies (e.g., Abbasi et al., 2025) evaluate PQC within widely used protocols like TLS, lightweight IoT protocols, such as MQTT and CoAP, remain underexplored. By embedding PQC schemes directly into these protocol stacks and measuring their effects under realistic conditions, this article fills an important gap in understanding real-world protocol overheads.

3. Evaluation Frameworks:

Frameworks such as QERS, proposed by Rassekhnia (2026), provide useful multidimensional metrics but they lack operationally actionable deployment guidance. The present work not only adopts such frameworks but also translates findings into engineering recommendations for critical infrastructure.

4. Ecosystem Readiness:

The review of PQC support in cryptographic libraries (Ahmed et al., 2025) and comprehensive surveys (Chhetri et al., 2025) highlight ecosystem challenges beyond algorithm performance alone. This article aligns well with these perspectives by emphasizing protocol support, library readiness, and integration complexity in the context of constrained IoT.

Collectively, these comparisons demonstrate that while extensive research has contributed valuable insights, holistic, protocol-aware performance analysis and deployment guidance, tailored for IoT and critical infrastructure, remain underrepresented in the literature, a gap this article directly addresses.

2.5.1. Post-Quantum Cryptography: Motivation and Fundamentals

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms which are believed to resist attacks from both classical and quantum adversaries. PQC candidate families include lattice-based, hash-based, code-based, and multivariate schemes, each grounded in mathematical problem hardness assumptions that, to date, resist known quantum attacks.

Among these, lattice-based cryptography has gained prominence due to its favorable balance of security and performance. Lattice problems, such as Learning With Errors (LWE) and Module-LWE, form the basis for algorithms such as CRYSTALS-Kyber (a Key Encapsulation Mechanism) and CRYSTALS-Dilithium (a digital signature scheme), both of which have been standardized by NIST for PQC use (Almutairi & Sheldon, 2025; Asif, 2021). Lattice cryptography leverages high-dimensional lattice structures that are conjectured to be intractable for both classical and quantum computers (Seyhan et al., 2022; Wikipedia, n.d.).

Hash-based signature schemes, such as SPHINCS+, provide alternative PQC primitives that derive security solely from cryptographic hash functions, making them robust albeit with larger signature sizes (Pote & Bansode, 2025).

2.5.2. PQC Algorithms and IoT

PQC algorithms vary widely in terms of key sizes, computational complexity, and communication overhead. These characteristics are especially significant for IoT devices with limited CPU, memory, and energy resources.

2.5.2.1. Lattice-Based Algorithms

CRYSTALS-Kyber and CRYSTALS-Dilithium are prominent PQC algorithms extended for IoT contexts. Kyber is used for key encapsulation and supports secure symmetric key establishment, while Dilithium provides digital signatures for authentication. Empirical studies indicate that optimized implementations on IoT-class processors achieve latencies acceptable for many IoT workloads, balancing performance with quantum-resistance (Almutairi & Sheldon, 2025).

Table 2

PQC Algorithm Characteristics Relevant to IoT

Algorithm	Primary Use	Key Size	Typical Latency	Comments
CRYSTALS-Kyber	KEM / Key Exchange	~1–2 kB	Medium	Good balance for IoT PQC (low-power constrained nodes)
CRYSTALS-Dilithium	Digital Signature	~3–6 kB	Higher	Larger signatures, strong authentication
SPHINCS+	Digital Signature	~8+ kB	Highest	Hash-based, ultra-quantum secure but heavy

This table1 summarizes key PQC metrics affecting resource-constrained IoT devices, demonstrating trade-offs between performance and security (Almutairi & Sheldon, 2025; Asif, 2021).

2.5.3. Performance and Resource Constraints

IoT devices often operate under stringent limitations on memory, processing power, and energy consumption. PQC schemes, particularly lattice-based ones, tend to introduce larger key and ciphertext sizes compared with classical ECC or RSA, impacting communication efficiency.

Experimental benchmarks on representative IoT hardware (e.g., ARM Cortex-M4) have illustrated measurable trade-offs (Siddharth, 2025). For instance, lattice-based PQC operations demonstrate:

- Computation Time: Typically in the tens to hundreds of milliseconds for encapsulation/decapsulation or signing, depending on algorithm parameters (Siddharth, 2025).
- Memory Usage: Moderate RAM and flash requirements exceeding classical ECC but within feasible IoT device constraints (Siddharth, 2025).
- Energy Consumption: PQC operations consume additional mJ per operation when compared to classical schemes, but remain within acceptable tolerances for many battery-powered deployments (Siddharth, 2025).

Moreover, certain protocols such as PQ-Lattice incorporate lattice-based cryptography with blockchain-based decentralization to reduce reliance on trusted authorities while optimizing communication and storage overheads for authentication in IoT networks. These protocols demonstrate ~32 ms average authentication latency and modest memory footprints (Hameed et al., 2025).

Table 3

Representative Performance Trade-offs Between Classical and PQC Cryptography on IoT Devices

Metric	Classical ECC	PQC (Lattice-based)	Notes
Key Size	Small	Larger	PQC expands key and signature sizes
Computation Time	Lower	Moderate	PQC incurs higher CPU cycles
Energy Consumption	Lower	Moderate to High	PQC results in increased energy use

Data based on experimental and simulation studies across resource-constrained hardware (Hameed et al., 2025; Siddharth, 2025).

2.5.4. Integration into IoT Protocols

Integrating PQC into IoT communication stacks, such as MQTT, CoAP, or TLS/DTLS, presents both design and performance challenges. Hybrid approaches combining classical and PQC key exchanges allow backward compatibility while gradually transitioning to quantum-safe protocols.

The Quantum Encryption Resilience Score (QERS) framework quantifies PQC readiness across protocols by combining latency, CPU utilization, energy, and communication overhead into normalized resilience scores, enabling systematic comparison for IoT and IIoT deployments (Rassekhnia, 2026).

2.5.5. Evaluation Frameworks

Evaluation frameworks that assess PQC performance holistically across latency, energy, security level, and resilience are crucial for realistic assessments. For example, QERS integrates these diverse metrics with machine learning assisted decision analysis to support protocol and algorithm selection under varied constraints (Rassekhnia, 2026).

2.5.6.Case Studies in PQC Implementation for IoT

To illustrate practical implementations and empirical evaluations of post-quantum cryptographic (PQC) protocols in IoT environments, this section presents several real case studies drawn from recent research. These studies highlight both performance results on constrained hardware and integration scenarios in practical IoT systems.

1. Lattice-Based Authentication Protocol for Decentralized IoT

Hameed et al. (2025) developed PQ-Lattice, a decentralized lattice-based post-quantum authenticated key exchange protocol that integrates CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures within a blockchain-enhanced identity management framework for IoT devices. In an extensive evaluation on an ARM Cortex-M4 microcontroller, the protocol achieved an average authentication computation time of 32.4 ms, communication overhead of 3.5 KB, and energy consumption around 28 mJ per authentication round. Compared to classical ECC and RSA approaches, PQ-Lattice reduced latency by up to 45 % and improved energy efficiency by approximately 47 % under constrained conditions, demonstrating its feasibility for low-power IoT nodes.

2. Empirical KEM Performance on Constrained Devices

Ehsan et al. (2025) conducted a comparative analysis of PQC key encapsulation mechanisms (KEMs), including CRYSTALS-Kyber and NTRU, with a particular focus on their implementation efficiency in constrained embedded environments (Ehsan et al., 2025). In addition to theoretical analysis, a case study was performed by applying these KEMs to a low-power embedded device to assess real-world performance metrics, such as execution time, memory usage, and energy efficiency. These results provide practical insights for engineers and cryptographers integrating PQC into resource-limited IoT systems and highlight the trade-offs between security strength and operational overheads in real deployment scenarios.

3. Benchmarking PQC Algorithm Performance on IoT Platforms

Siddharth (2025) presented a comprehensive benchmark for PQC algorithms, including NTRU, Ring-LWE, FALCON, and SPHINCS+, on resource-constrained platforms such as ARM Cortex-M4 microcontrollers. This study quantified latency, memory utilization, and energy consumption of each representative scheme, demonstrating that lattice-based

algorithms, like NTRU and Ring-LWE, exhibited significantly lower execution times (~100 ms) and reduced energy per operation (<6 mJ), while hash-based algorithms such as SPHINCS+ incurred higher computational cost (~200 ms and ~8 mJ) under IEEE 802.15.4 communication conditions.

4. Protocol-Level Evaluation via Multi-Metric Framework

Rassekhnia (2026) proposed the Quantum Encryption Resilience Score (QERS) framework for evaluating PQC implementation across common IoT and IIoT communication protocols (e.g., MQTT, HTTP, HTTPS) using metrics such as latency, CPU utilization, energy consumption, and handshake overhead in real deployments involving ESP32-C6 and ARM-based servers. Experimental findings showed that MQTT provided higher efficiency under PQC constraints, while HTTPS yielded stronger resilience at the cost of increased latency, supporting informed security and protocol selection for PQC-enabled IoT systems.

2.6. Identity- and Trust-Based Security Models

Dynamic trust management models provide a mechanism to evaluate device behavior and mitigate insider threats in large IoT deployments (Sicari et al., 2020). These models assign trust scores to devices based on historical behavior, communication patterns, and interaction reliability. By continuously updating trust evaluations, the system can detect compromised or misbehaving devices in real time. Integrating identity verification with trust-based assessments enhances access control, reduces unauthorized operations, and strengthens overall security in distributed IoT networks.

3. Cybersecurity Challenges in Smart Urban and Domestic Infrastructures

3.1. Dependency on Real-Time Data

Smart urban infrastructures rely on continuous sensor feedback to maintain optimal operation, making them highly sensitive to latency, manipulation, or data loss. Even short-lived inconsistencies in real-time streams can cascade into malfunctioning adaptive traffic signals, misaligned energy distribution, or unsafe public-service responses. Attackers can exploit this dependency through spoofing or data-delay attacks that distort situational awareness. Such vulnerabilities become more pronounced as cities integrate heterogeneous sensors with varying reliability. Consequently, ensuring data integrity and temporal accuracy is central to preserving operational stability.

3.2. IoT-Based Botnet-Driven DDoS Attacks

The proliferation of low-cost IoT devices with weak authentication significantly expands the attack surface for large-scale DDoS events, as evidenced by the Mirai botnet's global impact (Antonakakis et al., 2017). Compromised devices can be remotely orchestrated to saturate municipal or household networks, disrupting essential digital services and safety-critical platforms. Emerging botnet variants increasingly incorporate automated exploitation of zero-day vulnerabilities. This evolution enables adversaries to weaponize everyday devices, such as cameras, thermostats, or routers at unprecedented scale. As urban infrastructures grow more interconnected, mitigation requires both device-level hardening and network-wide anomaly detection.

3.3. Privacy Threats in Smart Homes

Smart homes continuously collect granular behavioral, audiovisual, and environmental data, making them attractive targets for adversaries seeking intimate user information. Unauthorized access to voice assistants, security cameras, or occupancy sensors can reveal routines, presence

patterns, and private conversations. Such data leakage not only threatens anonymity but can also facilitate stalking, burglary, or targeted social engineering. The complexity of multi-vendor ecosystems further complicates the enforcement of coherent privacy protections. Without robust local encryption and transparent data governance, domestic IoT environments remain highly exposed to covert surveillance risks.

3.4. Lack of Unified Security Standards

The coexistence of diverse IoT communication protocols—ZigBee, Z-Wave, BLE, MQTT—creates uneven security baselines, leaving cross-platform deployments vulnerable to inconsistent protection levels. Variations in default encryption, key-management practices, and firmware-update mechanisms introduce exploitable gaps across devices within the same environment. This fragmentation complicates risk assessment and impedes the development of universal security certification frameworks. Additionally, interoperability efforts often prioritize convenience over rigorous threat modeling, widening the avenue for protocol-level attacks. Establishing harmonized standards is therefore essential for securing mixed-technology smart infrastructures.

4. Comparative Table of Previous Studies

With the rapid expansion of the IoT and its deployment in urban and domestic infrastructures, security in this domain has become increasingly critical. Due to the complexity and diversity of devices and protocols, security threats have grown more sophisticated, necessitating comprehensive and multi-layered approaches. In recent years, numerous studies have explored various solutions to enhance IoT security. For instance, the use of blockchain technology to establish secure and decentralized models, the development of trust frameworks for device validation, the application of machine learning algorithms for attack detection, and the implementation of post-quantum cryptography to counter future threats, each offers distinct advantages and limitations. However, many of these studies are confined to theoretical analysis, simulations, or limited experimental setups, and rarely focus on the integration of these technologies within real-world urban and domestic environments.

Table 4 presents a comparative overview of previous studies, highlighting how the present work seeks to address existing gaps by integrating five advanced security paradigms and focusing on real-world infrastructures, thereby providing a comprehensive framework for IoT security.

Table 4

Comparison of Previous Studies and Contribution of the Present Work

Author(s)/ Year	Scope	Methodology	Key Findings	Limitations	Type of Study/Data
Dorri et al. (2017)	Blockchain-based IoT security	Architecture design	Secure, decentralized model	High computational overhead	Analytical/Simulated data
Sicari et al. (2020)	Trust models in IoT	Analytical review	Framework for trust evaluation	No real urban testing	Review
Zhang et al. (2021)	ML-based IDS for IoT	ML implementation	High attack detection accuracy	Large data requirement	Experimental
Chen et al. (2022)	Post-quantum cryptography	Algorithmic analysis	Quantum-resistant schemes	Limited IoT hardware suitability	Review

Khan et al. (2025)	AI, blochchain, edge computing & Zero-Trust for IoT	Integrated analytical review	A comprehensive framework that shows how ZTA's AI Blockchain Edge can enhance IoT security	Mostly conceptual; lacks large-scale real-world validation	Extended review/literature data
Present Article (2025)	Novel IoT security for smart city/home	Integrated analytical review	Combined analysis of ZTA, Blockchain, PQC, ML, Edge	Mostly conceptual focus	Extended review

Innovations of the Present Study

1. **Integration of five advanced security paradigms** within a unified analytical framework.
2. **Explicit focus on real-world urban and domestic IoT infrastructures**, rather than isolated IoT nodes.
3. **Development of a long-term cybersecurity roadmap through 2035**, absent in prior studies.
4. **Exploration of synergies between ML, blockchain, and ZTA** for sustainable IoT security.

5. Comprehensive Roadmap for IoT Cybersecurity in Smart Urban and Domestic Infrastructures

The rapid proliferation of IoT technologies across urban and domestic environments presents unparalleled opportunities for service innovation; however, it simultaneously expands the cyber attack surface in ways that traditional perimeter-based security models cannot sufficiently defend. Against this backdrop, achieving resilient cybersecurity for IoT infrastructures requires a continuous, evolution-oriented strategy that begins with the establishment of foundational security principles and extends toward intelligent, adaptive, and future-proof defenses. In the immediate term, efforts must concentrate on instilling a Zero-Trust mindset into the design and operation of IoT networks, incorporating rigorously enforced authentication, authorization, and continuous validation across devices and users to minimize implicit trust. At the same time, national and international IoT security standards must be formalized and enforced to ensure that manufacturers and service providers adhere to consistent benchmarks for secure coding, update mechanisms, and secure device identity. To address the pervasive constraints of resource-limited IoT endpoints, lightweight cryptographic primitives should be widely deployed in consumer and industrial devices to protect data confidentiality and integrity without imposing prohibitive computational overhead. Complementing cryptography, edge-based intrusion detection systems that operate locally on gateway and edge platforms will be crucial for real-time identification and mitigation of malicious behavior, reducing latency and dependence on centralized analysis engines. Concomitantly, privacy legislation tailored specifically to IoT sensor networks and smart systems is necessary to safeguard personal and operational data against unauthorized collection and exploitation (Alharbi et al., 2022; Khan et al., 2025; Sharma et al., 2023; Singh et al., 2025).

As the threat landscape continues to evolve, the intermediate phase of this roadmap focuses on integrating emerging technologies to enable more intelligent, autonomous security

capabilities. Decentralized identity architectures, leveraging lightweight blockchain techniques, will provide scalable, tamper-resistant identity management frameworks, particularly critical in smart cities where countless heterogeneous endpoints must be verified and authenticated with minimal central orchestration. Simultaneously, adopting TinyML and Federated TinyML models across IoT and edge computing environments will allow devices themselves to detect anomalous activity locally while preserving privacy and reducing data transmission requirements, a dual benefit that recent studies have shown to improve detection accuracy and resource efficiency compared to centralized approaches (Barros & Lopes, 2026). Behavior-based trust networks will increasingly augment static access policies by profiling typical device interactions and using deviations from established behavioral baselines to flag potential compromise or insider threats. To support these advanced security mechanisms, curated national datasets of attack footprints and benign operational patterns should be established to train, validate, and benchmark machine learning-driven models across diverse IoT domains.

Looking toward a more distant horizon, future IoT cybersecurity must anticipate fundamental shifts in computing paradigms and adversarial capabilities. The anticipated advent of practical quantum computing necessitates the widespread implementation of post-quantum cryptographic standards across urban and domestic systems to safeguard long-lived data against future decryption threats. Architectures that are not only robust but *self-healing* will emerge, wherein networks automatically localize, contain, and remediate faults and breaches without human intervention, leveraging distributed consensus and autonomous policy adaptation (Barros & Lopes, 2026; Kumari et al., 2022; Usama et al., 2026; Zakaria et al., 2025). Equally essential will be the development and adoption of next-generation secure communication protocols optimized for low-power and low-latency IoT radios, ensuring resilience against eavesdropping and protocol-level exploits. Finally, collaborative AI-driven cybersecurity systems, distributed intelligence fabrics that share threat insights across domains and orchestrate coordinated responses, will become a cornerstone of secure IoT ecosystems, deepening both situational awareness and collective defense capabilities. In summary, the trajectory from robust foundational controls toward intelligent, adaptive defenses represents the necessary continuum for securing the next decade of IoT evolution, aligning practical constraints with emerging research and real-world deployment realities, and establishing a resilient cybersecurity posture for smart urban and domestic infrastructures well into 2035.

5.1. Short-Term Horizon (2025–2028)

- Development of IoT-compatible Zero-Trust frameworks
- Establishment of national IoT security standards
- Deployment of lightweight cryptography in home devices
- Expansion of edge-based intrusion detection
- Drafting privacy legislation tailored to IoT (Alharbi et al., 2022; Khan et al., 2025; Singh et al., 2025; Sharma et al., 2023)

5.2. Mid-Term Horizon (2028–2032)

- Integration of lightweight blockchain systems for urban identity management
- Adoption of TinyML for on-device attack detection
- Development of behavior-based trust networks for smart cities
- Creation of national datasets for training security models

5.3. Long-Term Horizon (2032–2035)

- Wide deployment of post-quantum cryptography across urban systems
- Design of self-healing IoT network architectures
- Advancement of next-generation secure radio protocols
- Adoption of collaborative AI-driven cybersecurity systems

6. Conclusion and Recommendations

Considering the rapid expansion of IoT technologies and their critical role in smart urban and domestic infrastructures, ensuring cybersecurity in these ecosystems, has become increasingly important. A review of the current literature indicates that emerging approaches such as blockchain, machine learning, Zero-Trust architectures, lightweight cryptography, and quantum-resistant algorithms offer substantial potential for building resilient and sustainable IoT systems. Nevertheless, persistent challenges such as the lack of common standards, insufficient privacy regulations, limited large-scale datasets, and practical deployment constraints remain significant barriers to achieving these goals.

The central challenge in this context is designing an optimal combination of emerging technologies that simultaneously ensures security, scalability, cost-effectiveness, and practical deployability. Achieving such a cybersecurity framework requires a multi-layered, distributed, and adaptive approach capable of withstanding diverse and sophisticated threats across smart urban and domestic ecosystems. Furthermore, the convergence of standardization efforts, regulatory policies, and the development of robust security assessment tools will play a pivotal role in the successful implementation of proposed solutions.

Ultimately, projecting the trajectory of IoT cybersecurity development through 2035 underscores the necessity of sustained investment in research, education, and technological innovation. This approach will enable the secure and resilient management of smart urban infrastructures and smart homes, laying the foundation for future-proof smart cities and domestic environments capable of withstanding emerging cybersecurity threats.

References

Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography, 9*(2), 32. https://doi.org/10.3390/cryptography9020032

Ahmed, N., Zhang, L., & Gangopadhyay, A. (2025). A survey of post-quantum cryptography support in cryptographic libraries. *arXiv*. https://doi.org/10.48550/arXiv.2508.16078

Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). Integrating blockchain with artificial intelligence to secure IoT networks: Future trends. *Sustainability, 14*(23), 16002. https://doi.org/10.3390/su142316002

Almeida, F. (2023). Prospects of cybersecurity in smart cities. *Future Internet, 15*(9), 285. https://doi.org/10.3390/fi15090285

Almutairi, M., & Sheldon, F. T. (2025). Resilience of post-quantum cryptography in lightweight IoT protocols: A systematic review. *Eng, 6*(12), 346. https://doi.org/10.3390/eng6120346

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhao, Y. (2017). **Understanding the Mirai** botnet. *USENIX Security Symposium* (pp. 1092–1110). https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Asghari, P., Rahmani, A. M., & Javadi, H. (2022). **Internet** of Things applications: A systematic review. *Computer Networks*, 197, 108200. https://doi.org/10.1016/j.comnet.2021.108200

Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. *IoT, 2*(1), 71–91. https://doi.org/10.3390/iot2010005

Barros, P., & Lopes, S. I. (2026). *Roadmapping cybersecurity for IoT-enabled smart environments. Lecture Notes in Networks and Systems* (pp. 332–347). 1753 LNNS. https://doi.org/10.1007/978-3-032-12888-1_29

Chang, D. (2025). Resilient cryptographic frameworks for post-quantum security in resource-constrained Internet of Things architectures. *International Journal of IoT and Blockchain (ISCSITR)*.https://iscsitr.in/index.php/ISCSITR-IJIOTBC/article/view/ISCSITR-IJIOTBC_03_01_001 (iscsitr.in)

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., ... & Smith-Tone, D. (2022). *Report on post-quantum cryptography. National Institute of Standards and Technology*.https://doi.org/10.6028/NIST.IR.8105

Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). **Post**-quantum cryptography and quantum-safe security: A comprehensive survey. *arXiv*. https://doi.org/10.48550/arXiv.2510.10436

Cruz-Piris, L., Marín-López, A., Álvarez-Campana, M., Sanz, M., Moreno, J. I., & Arroyo, D. (2025). Measuring the impact of post-quantum cryptography in Industrial IoT scenarios. *Internet of Things,* Article 101793. https://doi.org/10.1016/j.iot.2025.101793

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 618–623). https://doi.org/10.1109/PERCOMW.2017.7917634

Dritsas, E., & Trigka, M. (2025). A survey on cybersecurity in IoT. *Future Internet, 17*(1), 30. https://doi.org/10.3390/fi17010030

Ehsan, M. A., Alayed, W., Rehman, A. U., Hassan, W. U., & Zeeshan, A. (2025). *Post-Quantum KEMs for IoT: A study of kyber and NTRU. Symmetry, 17*(6), 881. https://doi.org/10.3390/sym17060881

Hameed, H. A., Swadi Alhamedi, H. J., Abbas, W. F., Alsayednoor, H. M., Al-Shareeda, M. A., Almaayah, M., & Shehab, R. (2025). PQ-Lattice: A lattice-based post-quantum authentication protocol for decentralized IoT systems. *Informatica, 49*(35), 259–272. https://doi.org/10.31449/inf.v49i35.12156

Khan, I. U., Khan, F. M., Haider, Z. A., & Alturise, F. (2025). Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A comprehensive review of advanced cybersecurity framework. *Interactions*, *8*, 9. https://doi.org/10.32604/cmc.2025.070189

Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022). *To secure the communication in powerful Internet of Things using innovative post-quantum cryptographic method. Arabian Journal for Science and Engineering*, 47(2), 2419-2434. https://doi.org/10.1007/s13369-021-06166-6

Lin, J., & Bergmann, N. W. (2021). IoT security challenges and solutions. *Journal of Cybersecurity*, *7*(2),45–62. https://doi.org/10.1093/cybsec/tyab009

Mahdi, L. H., & Abdullah, A. A. (2025). Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography. *Engineering, Technology & Applied Science Research, 15*(2), 21812–21821. https://doi.org/10.48084/etasr.10141

National Institute of Standards and Technology **(**NIST). (2022). *Lightweight cryptography standardization process*. https://csrc.nist.gov/projects/lightweight-cryptography

Pote, P., & Bansode, R. (2025). *Performance evaluation of post-quantum cryptography: A comprehensive framework for experimental analysis*. *Journal of Information Systems Engineering and Management, 10*(9s).

Rassekhnia, J. (2026a). QERS: Quantum encryption resilience score for post-quantum cryptography in computer, IoT, and IIoT systems. *arXiv*. https://doi.org/10.48550/arXiv.2601.13399

Rassekhnia, J. (2026b). Quantum Encryption Resilience Score (QERS) for MQTT, HTTP, and HTTPS under post-quantum cryptography in computer, IoT, and IIoT systems. *arXiv*. https://arxiv.org/abs/2601.13423

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-207

Rubia, J. J., Lincy, R. B., Nithila, E. E., Shibi, C. S., & Rosi, A. (2024). *A survey about post quantum cryptography methods. EAI Endorsed Transactions on Internet of Things*, *10*, 1-9. https://doi.org/10.4108/eetiot.5099

Seedorf, J., Rawal, D., Möwes, J., Abdulaziz, O. H., Alhasan, A., & Santhanavanich, T. (2025). A prototype for evaluating post-quantum cryptography on resource-constrained hardware with real-world smart city sensor data. *Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., XLVIII-4/W16-2025*, 113–120. https://doi.org/10.5194/isprs-archives-XLVIII-4-W16-2025-113-2025 (isprs-archives.copernicus.org)

Senor, J., Portilla, J., & Mujica, G. (2022). *Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices. IEEE Internet of Things Journal*, 9(19), 18778-18790. https://doi.org/10.1109/JIOT.2022.3162254

Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2022). *Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: A survey. Cluster Computing*, 25(3), 1729-1748. https://doi.org/10.1007/s10586-021-03380-7

Sharma, D., Kumar, R., & Jung, K. H. (2023). A bibliometric analysis of convergence of artificial intelligence and blockchain for edge of things. *Journal of Grid Computing, 21*(4), 79. https://doi.org/10.1007/s10723-023-09716-4

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). Security, privacy, and trust in the Internet of Things: The road ahead. *Computer Communications*, 159, 120–137.https://doi.org/10.1016/j.comcom.2020.05.046

Siddharth. (2025). *Post-Quantum cryptographic algorithm performance on IoT devices. International Journal of Advanced Research in Computer Science and Engineering(IJARCSE), 1*(2). https://doi.org/10.63345/ijarcse.v1.i2.304

Singh, T., & Nisha, T. N. (2025, July). Enhancing IoT Security with Zero-Trust Architecture: A model leveraging blockchain and AI capabilities. In *2025 International Conference on Emerging Information Technology and Engineering Solutions (EITES)* (pp. 173-179). https://doi.org/10.1109/EITES66543.2025.00038

Statista. (2023). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*. https://www.statista.com

Usama, M., Aziz, A., Alasbali, N., Alturki, N., & Rehman, M. (2026). *Blockchain-enabled identity management for IoT: A multi-layered defense against adversarial AI. Scientific Reports, 16*, 4371. https://doi.org/10.1038/s41598-026-35208-y

Wikipedia (n.d.). *Lattice-based cryptography*. https://en.wikipedia.org/wiki/Lattice-based_cryptography

Ye, Z., Song, R., Zhang, H., Chen, D., Cheung, R. C.-C., & Huang, K. (2024). *A highly-efficient lattice-based post-quantum cryptography processor for IoT applications. IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024(2), 130-153. https://doi.org/10.46586/tches.v2024.i2.130-153

Zakaria, A. A., Amr, T., & Ragheb, A. A. (2025). IoT in smart urban planning: A comprehensive review of applications, developments and engineering perspectives. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3594019

Zhang, Y., Wang, X., & Chen, J. (2021). Machine learning-based intrusion detection for IoT networks. *IEEE Internet of Things Journal*, 8(14), 11413–11425. https://doi.org/10.1109/JIOT.2021.3065432