smart cities

MDPI

Article

QESIF: A Lightweight Quantum-Enhanced IoT Security Framework for Smart Cities

Abdul Rehman [1,*] and Omar Alharbi [2,*]

[1] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2] Department of Electrical Engineering, College of Engineering, Majmaah University, Al-Majmaah 11952, Saudi Arabia
* Correspondence: abdulrehman786.cs@gmail.com (A.R.); oalharbi@mu.edu.sa (O.A.)

Highlights

What are the main findings?

- QESIF integrates Quantum Key Distribution with IoT using an adaptive hybrid protocol stack.
- A novel Q-IDS utilizes quantum entropy metrics like QBER for real-time intrusion detection.

What is the implication of the main finding?

- QESIF enhances IoT security in smart cities while maintaining low latency and energy efficiency.
- The framework offers practical quantum-ready IoT security without significant hardware overhead.

Abstract

Smart cities necessitate ultra-secure and scalable communication frameworks to manage billions of interconnected IoT devices, particularly in the face of the emerging quantum computing threats. This paper proposes the QESIF, a novel Quantum-Enhanced Secure IoT Framework that integrates Quantum Key Distribution (QKD) with classical IoT infrastructures via a hybrid protocol stack and a quantum-aware intrusion detection system (Q-IDS). The QESIF achieves high resilience against eavesdropping by monitoring quantum bit error rate (QBER) and leveraging entropy-weighted key generation. The simulation results, conducted using datasets TON IoT, Edge-IIoTset, and Bot-IoT, demonstrate the effectiveness of the QESIF. The framework records an average QBER of 0.0103 under clean channels and discards over 95% of the compromised keys in adversarial settings. It achieves Attack Detection Rates (ADRs) of 98.1%, 98.7%, and 98.3% across the three datasets, outperforming the baselines by 4–9%. Moreover, the QESIF delivers the lowest average latency of 20.3 ms and the highest throughput of 868 kbit/s in clean scenarios while maintaining energy efficiency with 13.4 mJ per session.

Keywords: Quantum Key Distribution; smart cities; IoT security; QKD-IoT integration; quantum IDS; cybersecurity

Academic Editor: Pierluigi Siano

Received: 16 May 2025
Revised: 2 July 2025
Accepted: 6 July 2025
Published: 10 July 2025

Citation: Rehman, A.; Alharbi, O. QESIF: A Lightweight Quantum-Enhanced IoT Security Framework for Smart Cities. *Smart Cities* **2025**, *8*, 116. https://doi.org/10.3390/smartcities8040116

1. Introduction

The evolution of urbanization and digitalization has led to the emergence of smart cities, where interconnected devices, sensors, and systems collectively enhance the efficiency, sustainability, and livability of urban environments [1–3]. At the core of this transformation lies the Internet of Things (IoT), which enables the seamless collection,

exchange, and processing of data across various city domains, including energy, transportation, healthcare, and security [4]. However, the rapid deployment of IoT devices has exposed smart city infrastructures to critical cybersecurity risks, including data interception, unauthorized access, and large-scale coordinated attacks. As conventional encryption mechanisms struggle to keep pace with the emerging threats—especially those posed by quantum computing—there is a growing need for next-generation security frameworks [5]. The recent advancements in quantum cryptography, particularly Quantum Key Distribution (QKD), have demonstrated the potential to provide theoretically unbreakable encryption [6]. Integrating QKD with lightweight and resource-constrained IoT systems within smart cities remains largely unexplored [7].

Regarding the advancements in smart city technologies, the underlying security of IoT communication remains a persistent challenge. Although widely adopted, traditional cryptographic schemes are vulnerable to both classical and quantum attacks, particularly in urban environments with high device density and real-time data flow requirements [8,9]. These vulnerabilities pose severe risks to critical smart city services, from transportation coordination to emergency response systems. Therefore, there is a pressing need to explore quantum-resilient solutions that are scalable and adaptable to smart city architectures. The primary research question addressed in this work is how QKD can be integrated into lightweight IoT frameworks to ensure quantum-resilient and energy-efficient smart city security. Motivated by this question, this research proposes a framework that unifies quantum cryptographic methods with traditional IoT security layers, enhancing both confidentiality and intrusion resilience across a city-wide network.

The proposed QESIF is a novel framework that combines QKD with smart city IoT infrastructures through a hybrid security protocol stack. The QESIF introduces a lightweight QKD layer compatible with constrained devices, a middleware layer for key management, and a Q-IDS capable of leveraging quantum error indicators such as QBER to detect eavesdropping. A hybrid protocol stack dynamically shifts between classical and quantum-secured communication based on device capability and criticality of data. This framework is designed to work with existing IoT protocols such as MQTT and CoAP while injecting QKD-generated keys at the transport or session layer. The main contributions of this study are as follows:

1. A framework is proposed to integrate QKD with heterogeneous and resource-constrained IoT networks in smart city infrastructures.
2. A novel Q-IDS is designed that uses quantum signal anomalies—such as increased QBER—to detect eavesdropping and intrusion attempts in real time.
3. A hybrid protocol stack that supports seamless switching between quantum-secure and classical communication modes is developed, enabling scalable and backward-compatible deployment in evolving smart city environments.

The rest of the paper is organized as follows. Section 2 presents a review of the related works. Section 3 describes the proposed QESIF in detail. Section 4 presents the simulation environment and experimental results, including a comparative analysis with traditional security models. Section 5 discusses the findings and implications of the QESIF in smart city deployments. Finally, Section 6 concludes the paper.

2. Related Work

Recent efforts in securing IoT systems in smart cities have explored both post-quantum cryptography (PQC) and QKD. While some approaches aim to strengthen the existing encryption methods, others introduce hybrid or fully quantum solutions. A hybrid encryption scheme has been proposed that combines symmetric and post-quantum cryptography for smart grids, although it lacks real-time intrusion adaptability [10]. Quantum threats to

IoT systems emphasize the importance of post-quantum cryptography, although practical integration frameworks have not been fully established [11]. An ML-enhanced QKD system has been proposed for IoT communication, with a primary focus on threat detection rather than secure key management [12]. A lightweight post-quantum authentication protocol has been explored for dense IoT networks; however, its scalability under high-entropy attacks has not been demonstrated [13].

A conceptual model for Quantum IoT (QIoT) networks has been proposed to explore future-ready secure architectures; however, it remains largely theoretical, with no concrete deployment models tailored for IoT environments [14]. Quantum machine learning techniques have been integrated with Security Information and Event Management (SIEM) systems to enhance threat prediction in smart city contexts; however, these approaches do not address security mechanisms at the IoT device level [15]. An optimized HQC-based encryption scheme tailored for the IoT is presented using a hardware/software co-design approach, achieving reduced latency; however, its performance is constrained in static and predefined deployment environments [16]. CR-QKD was introduced for the sharing of mobile keys in a wide area, but the scheme is not optimized for IoT power constraints [17].

PQC algorithms have been analyzed regarding the IoT, identifying challenges but offering no system-level integration model [18]. The PQC performance was evaluated on embedded systems but not in the context of distributed urban networks [19]. Quantinuum's Quantum Origin uses quantum entropy for key generation, although integration with IoT protocols like MQTT remains undefined [20]. Table 1 highlights the primary limitations of the state-of-the-art quantum-secured IoT frameworks and illustrates how the proposed QESIF overcomes these gaps through entropy-aware key generation, adaptive intrusion detection, and energy-efficient protocol switching.

Table 1. Comparison of existing approaches and QESIF's contributions.

Approach	Limitation	QESIF's Contribution
QRHE [10]	No entropy adaptation; lacks real-time anomaly detection	QESIF introduces entropy-weighted key generation and quantum-aware IDS for enhanced threat detection
ML-QKD [12]	Focuses only on anomaly detection; lacks secure key lifecycle management	Combines ML-inspired quantum monitoring with entropy-weighted QKD key generation and session scoring
QIoT Model [14]	Conceptual only; lacks implementation or protocol-level integration for IoT	Implements practical deployment over MQTT/CoAP with real-world datasets and IoT gateways
QML-SIEM [15]	Centralized threat analytics but no device-level protection	Deploys lightweight edge-layer Q-IDS with real-time detection at device and gateway levels
CR-QKD [17]	High power demand; not optimized for IoT devices	Introduces energy-normalized key rate function and adaptive hybrid communication mode
HyQuSec [21]	Static protocol; no adaptability to channel conditions	QESIF uses hybrid protocol stack with dynamic switching based on QBER and key rate thresholds
QuIDS [22]	Limited scalability and lacks energy efficiency metrics	QESIF delivers edge-integrated Q-IDS and energy-aware communication across constrained devices
QLSN [23]	High computational cost and latency due to lattice operations	QESIF reduces latency using lightweight quantum key scoring and efficient entropy management
QuantGAN [24]	Integrates quantum-enhanced risk analysis with GAN-based digital twins	Evaluation is limited to controlled IoT environments with restricted scalability.

3. System Design and Components

The QESIF is proposed to address the critical security challenges posed by quantum computing to IoT-based smart city systems. The QESIF is a lightweight, scalable, and adaptable architecture that integrates QKD with existing IoT infrastructures to provide end-to-end security. Unlike conventional cryptographic solutions, the QESIF leverages

the physical principles of quantum mechanics for key exchange, ensuring provable security against eavesdropping. Furthermore, the QESIF combines a hybrid protocol stack that is capable of dynamically transitioning between quantum-secured and conventional communication channels based on prevailing network conditions and device constraints. Another novel component of this framework is the Q-IDS, an anomaly detection module that leverages quantum-level variations such as elevated QBER. The integration of quantum key generation, adaptive encryption mechanisms, and real-time threat surveillance collectively positions the QESIF as an advanced security architecture for large-scale urban IoT infrastructures.

3.1. System Architecture

The QESIF is a holistic and extensible architecture that is also scalable, and it is able to integrate within existing smart city infrastructure through matching QKD at the network layer with classical application layer-operating IoT protocols. It consists of four central layers: (1) IoT device layer, (2) edge–QKD gateway layer, (3) quantum network layer, and (4) smart city control center.

(1) IoT Device Layer: This layer holds heterogeneous IoT devices distributed throughout various city domains, such as traffic, meters associated with electricity, cameras, and health monitors. These devices are limited with respect to cryptographics and are reliant on higher layers to establish secure keys.

(2) Edge–QKD Gateway Layer: Acting as intermediaries, these edge gateways are equipped with QKD-compatible hardware (e.g., single-photon detectors and QRNGs) and classical quantum communication interfaces. They handle session establishment, QKD-based key negotiation, and device-level data encryption using quantum-derived keys. They also house lightweight modules of the Q-IDS for initial anomaly detection. QKD integration in the QESIF is limited to the edge gateway layer to maintain cost-efficiency and deployment feasibility. These gateways are equipped with QKD-compatible hardware—such as QRNGs and photon detectors—now increasingly available via compact photonic modules. This design reflects practical deployments observed in initiatives such as SECOQC, the Beijing–Shanghai QKD backbone, and systems from ID Quantique and Quantinuum. IoT devices themselves do not perform QKD but receive securely distributed session keys from the gateways via classical channels.

(3) Quantum Network Layer: This layer facilitates secure key exchange between trusted QKD nodes using protocols like BB84 or E91. The QKD links may be fiber-based or free-space, and they enable the secure generation and distribution of encryption keys across distributed smart city regions. In terms of protocol compatibility, QKD protocols such as BB84 and E91 operate below the transport layer and are responsible solely for key exchange. In the QESIF, these keys are passed to the middleware layer, which injects them into the session layer (e.g., TLS for MQTT or DTLS for CoAP) to establish secure sessions. Quantum repeaters and entanglement sources are deployed to extend secure key distribution over longer distances. These components help to overcome distance-related losses by enabling entanglement swapping and trusted relays at backbone nodes, supporting scalable QKD in urban-scale deployments.

(4) Smart City Control Center:The control center manages the centralized orchestration of the network, including quantum key management, session auditing, anomaly aggregation from edge layers, and policy enforcement. It serves as a global observer for the Q-IDS, correlating quantum noise patterns, network flow metadata, and device behavior logs to detect coordinated or advanced persistent threats, as illustrated in Figure 1.

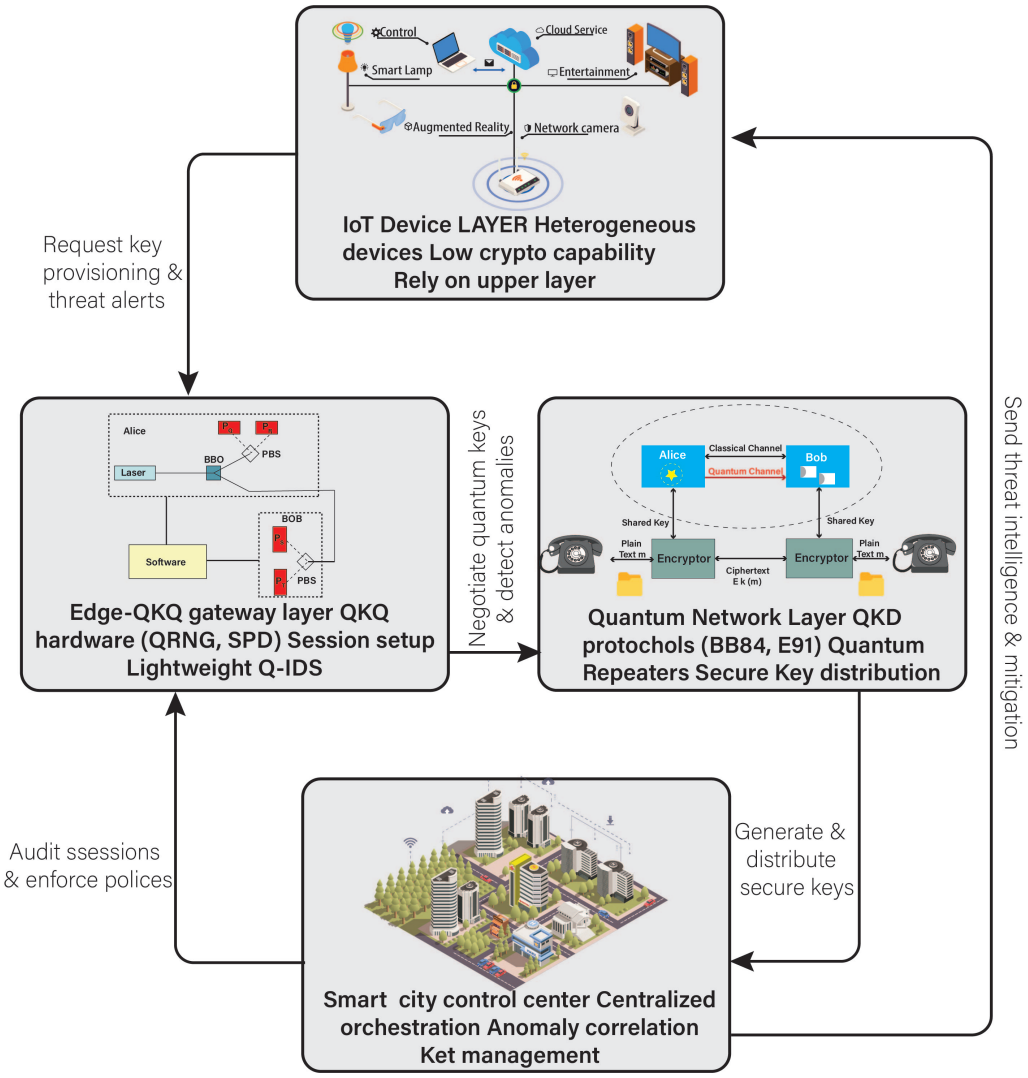

Figure 1. System architecture of the proposed QESIF, illustrating the interaction between IoT devices, edge QKD gateways, quantum networks, and the smart city control center.

3.2. Quantum Key Distribution in IoT

To securely integrate QKD into resource-constrained IoT environments, a novel entropy-weighted dynamic QKD protocol tailored to heterogeneous device capabilities is proposed. Traditional QKD protocols such as BB84 assume uniform photon emission, idealized error rates, and unrestricted processing power—assumptions that do not hold in practical IoT deployments, especially in urban smart cities.

The proposed method introduces an adaptive key generation algorithm that weights quantum entropy against device-specific computational and communication limitations. The entropy of the received photon stream is modulated dynamically based on both channel state and device entropy buffers, yielding a secure yet efficient key distribution strategy.

A hybrid entropy-weighted key rate function $\mathcal{K}_{\text{IoT}}$ for a device d_i is defined as follows:

$$\mathcal{K}_{\text{IoT}}(d_i, t) = \frac{H_q(t) \cdot \gamma(d_i)}{1 + \eta(d_i, t) \cdot \delta(\theta)} \tag{1}$$

where

- $H_q(t)$ is the measured quantum entropy at time t, computed from the Shannon entropy of the polarization basis mismatch.

- $\gamma(d_i)$ is the trust-adjusted security factor for device d_i, computed using device integrity metrics and historical authentication scores.
- $\eta(d_i, t)$ is the energy-normalized communication complexity function for d_i at time t.
- $\delta(\theta)$ is the decoherence impact function, modeled as an increasing function of environmental photon noise θ.

This function allows the system to generate keys with variable lengths and confidence intervals depending on both physical (quantum) and cyber (resource-aware) properties. Unlike fixed-rate key generation in traditional QKD, the proposed model supports quantum entropy modulation, enhancing resistance to both channel-based eavesdropping and energy exhaustion attacks. Furthermore, the protocol introduces a quantum-aware session scoring function $S_{\text{QKD}}(t)$:

$$S_{\text{QKD}}(t) = \int_{t_0}^{t} \left[\frac{H_q(\tau)}{\delta(\theta_\tau)} - \lambda \cdot \mathcal{L}(\tau) \right] d\tau \tag{2}$$

where $\mathcal{L}(\tau)$ represents packet loss in the quantum channel and λ is a tunable security-to-performance trade-off coefficient.

If $S_{\text{QKD}}(t)$ falls below a threshold Ψ_{secure}, the key is discarded, and the session is flagged by the Q-IDS module. The entropy-weighted quantum key generation process is outlined in Algorithm 1, enabling adaptive key rates based on device trust levels, communication cost, and quantum decoherence factors.

Algorithm 1: Entropy-Weighted QKD Key Generation for IoT Devices

Input: Device ID d_i, Time Window $[t_0, t]$, Decoherence Index θ, Loss Function $\mathcal{L}(t)$, Trust Factor $\gamma(d_i)$

Output: Valid Quantum Key K_d or Session Termination

Initialize $K_d \leftarrow \emptyset$, $S_{\text{QKD}} \leftarrow 0$;
foreach *time slot* $\tau \in [t_0, t]$ **do**
    Measure quantum entropy $H_q(\tau)$ from photon basis mismatch;
    Compute communication cost $\eta(d_i, \tau)$ from channel logs;
    Estimate decoherence factor $\delta(\theta_\tau)$;
    `// Compute dynamic key rate (Equation (1))`
    $\mathcal{K}_{\text{IoT}}(d_i, \tau) \leftarrow \frac{H_q(\tau) \cdot \gamma(d_i)}{1 + \eta(d_i, \tau) \cdot \delta(\theta_\tau)}$;
    if $\mathcal{K}_{IoT}(d_i, \tau) > \epsilon_{min}$ **then**
        Append quantum bits to K_d;
    `// Update session score (Equation (2))`
    $S_{\text{QKD}} \leftarrow S_{\text{QKD}} + \left(\frac{H_q(\tau)}{\delta(\theta_\tau)} - \lambda \cdot \mathcal{L}(\tau) \right)$;
if $S_{QKD} \geq \Psi_{secure}$ **then**
    return K_d `// Valid QKD key`
else
    Flag session for Q-IDS, discard K_d;
    return `NULL`

3.3. Quantum-Aware Intrusion Detection System (Q-IDS)

Conventional intrusion detection systems (IDSs) in IoT environments analyze traffic features such as packet rate, size, or known attack signatures. However, in a QKD-based IoT system, threat detection must incorporate anomalies in quantum transmission behavior. To address this, a novel Q-IDS is introduced that utilizes quantum-layer

anomalies, channel noise characteristics, and quantum-bit integrity to identify stealthy or quantum-enabled attacks.

The Q-IDS continuously monitors entropy deviation, photon loss rate, QBER fluctuations, and key generation inconsistencies across sessions. Anomalous behavior is quantified using a composite quantum anomaly score $\mathcal{A}_q(t)$, defined as

$$\mathcal{A}_q(t) = \omega_1 \cdot \Delta H_q(t) + \omega_2 \cdot \frac{QBER(t)}{QBER_{\text{ref}}} + \omega_3 \cdot \Lambda_K(t) \tag{3}$$

where

- $\Delta H_q(t)$ is the deviation of quantum entropy from the expected baseline: $\Delta H_q(t) = |H_q(t) - \bar{H}_q|$.
- $QBER(t)$ is the current quantum bit error rate; $QBER_{\text{ref}}$ is a calibrated reference value from noise-free trials.
- $\Lambda_K(t)$ is the temporal key drop ratio: $\Lambda_K(t) = \frac{\text{Keys dropped}}{\text{Keys attempted}}$ during $[t - \Delta t, t]$.
- ω_1, ω_2, and ω_3 are dynamic trust-weighted coefficients satisfying $\sum \omega_i = 1$.

If $\mathcal{A}_q(t)$ exceeds a detection threshold α_{intrude}, the Q-IDS flags the session as compromised. The threshold is dynamically adjusted using a Bayesian posterior entropy update rule:

$$\alpha_{\text{intrude}}^{t+1} = \alpha_{\text{intrude}}^{t} + \eta \cdot \left(\frac{\partial \mathcal{A}_q(t)}{\partial t} \right) \cdot (1 - \mathcal{P}_n(t)) \tag{4}$$

where

- η is the learning rate for intrusion sensitivity.
- $\mathcal{P}_n(t)$ is the normalized probability of benign quantum noise (learned from historical QKD baselines).

In contrast to classical anomaly detectors, the Q-IDS integrates quantum entropy, photonic error patterns, and key failure metrics into a single detection index. It can detect eavesdropping, side-channel attacks, and quantum channel interference before cryptographic exploitation occurs. The model is repeatedly adjusted based on environmental noise levels, device type, and photon emission profiles to cater to heterogeneous smart city networks utilizing QKD-based IoT networks. Algorithm 2 provides the Q-IDS algorithm for the identification of quantum-layer intrusions based on entropy deviation and inspection of QBER.

3.4. Hybrid Protocol Stack Design

To enable efficient and interoperable integration QKD with existing IoT communication protocol stacks, we propose a hybrid protocol stack. It is flexible to accommodate variations in device capabilities within the IoT and the state of the quantum channel, allowing for efficient and secure communication while maintaining backward compatibility with classical IoT infrastructure. Due to its hybrid nature, the protocol stack naturally switches between quantum-secured and classically secured states based on device capabilities, noise levels of the environment, and prevailing conditions within the system. The protocol dynamically adjusts between quantum-secured and classical encryption modes using the $Q_{\text{adapt}}(t)$ function, which governs mode switching at session boundaries based on entropy availability and channel stability. The standard security measures, such as TLS 1.3, DTLS, and authenticated encryption, are integrated to protect classical data transmission.

The core idea behind the hybrid protocol is to incorporate quantum-secured communication on the transport layer and maintain classical IoT communication protocols on the application layer, e.g., MQTT, CoAP, or HTTP. Transmission between the layers is

controlled using a decision module that considers both the availability of the quantum key and network performance.

Algorithm 2: Quantum-Aware Intrusion Detection System (Q-IDS)

Input: Quantum entropy $H_q(t)$, Reference entropy $\bar{H}_q$,
QBER at time t, Reference QBER $QBER_{\text{ref}}$,
Key drop stats in window $[t - \Delta t, t]$,
Prior intrusion threshold $\alpha^t_{\text{intrude}}$,
Noise probability estimate $\mathcal{P}_n(t)$

Output: Intrusion status: `Flagged` or `Safe`

Compute entropy deviation: $\Delta H_q(t) \leftarrow |H_q(t) - \bar{H}_q|$;
Compute normalized QBER ratio: $QBER_{\text{ratio}} \leftarrow \frac{QBER(t)}{QBER_{\text{ref}}}$;
Compute key drop ratio: $\Lambda_K(t) \leftarrow \frac{\text{Keys Dropped}}{\text{Keys Attempted}}$;
`// Calculate quantum anomaly score (Equation (3))`
$\mathcal{A}_q(t) \leftarrow \omega_1 \cdot \Delta H_q(t) + \omega_2 \cdot QBER_{\text{ratio}} + \omega_3 \cdot \Lambda_K(t)$;
`// Update detection threshold (Equation (4))`
Estimate $\frac{\partial \mathcal{A}_q(t)}{\partial t}$ using finite difference method;
$\alpha^{t+1}_{\text{intrude}} \leftarrow \alpha^t_{\text{intrude}} + \eta \cdot \left(\frac{\partial \mathcal{A}_q(t)}{\partial t}\right) \cdot (1 - \mathcal{P}_n(t))$;
if $\mathcal{A}_q(t) \geq \alpha^{t+1}_{intrude}$ **then**
    return `Flagged (Intrusion Detected);`
else
    return `Safe (No Intrusion);`

The quantum adaptation function $\mathcal{Q}_{\text{adapt}}(t)$ is defined for deciding the communication mode based on quantum key availability and real-time system conditions. The function is given by

$$\mathcal{Q}_{\text{adapt}}(t) = \begin{cases} 1, & \text{if } \mathcal{K}_{\text{IoT}}(d_i, t) \geq \epsilon_{\min} \\ 0, & \text{if } \mathcal{K}_{\text{IoT}}(d_i, t) < \epsilon_{\min} \end{cases} \tag{5}$$

where

- $\mathcal{K}_{\text{IoT}}(d_i, t)$ is the dynamic key rate at time t for device d_i (calculated from Equation (1)).
- $\epsilon_{\min}$ is the minimum required key rate for enabling quantum-secured communication.

The quantum-secured communication mode is activated when $\mathcal{Q}_{\text{adapt}}(t) = 1$, allowing IoT devices to utilize quantum-derived keys for secure encryption and authentication. While $\mathcal{Q}_{\text{adapt}}(t)$ is defined as a binary function for modeling purposes, its practical implementation follows a session-level switching mechanism with threshold smoothing to avoid instability from transient channel fluctuations. The transition incurs minimal latency as it is executed at the session level rather than on a per-packet basis, ensuring reliable and non-disruptive communication. On the other hand, when $\mathcal{Q}_{\text{adapt}}(t) = 0$, the system switches to classical encryption protocols, such as AES or RSA, for data protection.

The stack is composed of the following layers: 1. Application Layer: Standard IoT protocols (e.g., MQTT or CoAP) are used for device-to-device communication. The data packets may be quantum-secured or classically encrypted depending on the quantum adaptation function. 2. Transport Layer: It is where the hybrid encryption protocol is implemented that dynamically switches between the quantum-secured and classical encryption based on $\mathcal{Q}_{\text{adapt}}(t)$. 3. Network Layer: Controls the communication of the quantum keys using QKD protocols (e.g., BB84 or E91), or classical keys if the quantum mode is not available. It ensures that the distribution and refreshing of keys are carried out

according to the function of quantum adaptation. 4. Physical Layer: Includes the actual quantum channel of key exchange and classical communication networks (e.g., Wi-Fi and Zigbee). It is on the physical layer that the infrastructure of both quantum communication and classical data transfer is implemented. For successful key management, the usage function of the quantum key $\mathcal{U}_K(t)$ is defined as

$$\mathcal{U}_K(t) = \frac{K_{\text{generated}}(t)}{K_{\max}(t)} \tag{6}$$

where

- $K_{\text{generated}}(t)$ is the total number of valid quantum keys generated by the QKD system at time t.
- $K_{\max}(t)$ is the maximum possible key capacity available at time t, considering device limitations and network conditions.

The quantum key utilization function optimizes key generation and addresses the requirements of the IoT network. Scalability is obtained through dynamic control of the distribution of quantum keys based on demand.

Finally, the hybrid protocol stack decision module operates such that network performance, availability of quantum keys, and security levels are monitored continuously. If available quantum keys fall to a point or environmental noise increases, the system automatically reverts to classical communication methodologies to ensure service is uninterrupted.

Theorem 1. *Let $\mathcal{S}_{QESIF}(t)$ denote the security level of the QESIF system at time t, scaled between 0 (no security) and 1 (perfect quantum-secured channel). Let $\mathcal{K}_{IoT}(d_i, t)$ be the entropy-weighted quantum key generation rate for device d_i at time t (as defined in Equation (1)). Assume $\mathcal{Q}_{adapt}(t)$ is the binary switching function (as in Equation (5)).*

Then, for all time t and devices d_i:

$$\mathcal{S}_{QESIF}(t) \geq \min\left(\mathcal{S}_{classical}, \mathcal{S}_{quantum} \cdot \mathcal{Q}_{adapt}(t)\right) \tag{7}$$

where

- $\mathcal{S}_{classical}$ *is the baseline security using classical encryption (e.g., AES and ECC).*
- $\mathcal{S}_{quantum} = 1$ *under ideal QKD conditions (zero QBER and perfect key yield).*

***Furthermore**, if $\mathcal{Q}_{adapt}(t) = 1$ and $QBER(t) \to 0$, then $\mathcal{S}_{QESIF}(t) \to 1$, satisfying perfect forward secrecy.*

Proof of Theorem 1. Two states are considered based on the adaptation function $\mathcal{Q}_{\text{adapt}}(t)$:

Case 1: $\mathcal{Q}_{\text{adapt}}(t) = 1$

The system uses quantum-derived keys. In this case, security is driven by QKD entropy and QBER:

$$\mathcal{S}_{\text{QESIF}}(t) = f(H_q(t), QBER(t)) \approx 1 - \epsilon \text{ for small } QBER(t)$$

If $QBER(t) \to 0$, then $f(H_q, QBER) \to 1$. Therefore, $\mathcal{S}_{\text{QESIF}}(t) \to \mathcal{S}_{\text{quantum}} = 1$.

Case 2: $\mathcal{Q}_{\text{adapt}}(t) = 0$

The system falls back to classical encryption. Hence, $\mathcal{S}_{\text{QESIF}}(t) = \mathcal{S}_{\text{classical}}$.

By combining both cases,

$$\mathcal{S}_{\text{QESIF}}(t) \geq \min\left(\mathcal{S}_{\text{classical}}, \mathcal{S}_{\text{quantum}} \cdot \mathcal{Q}_{\text{adapt}}(t)\right)$$

Moreover, the QESIF leverages adaptive entropy scoring (Equation (3)) and threshold tuning (Equation (4)) to reject compromised keys, maintaining confidentiality. Since quantum keys are ephemeral and never reused, forward secrecy is preserved for all $\mathcal{Q}_{\text{adapt}}(t) = 1$ sessions. □

4. Simulation Setup and Experimental Results

To evaluate the proposed QESIF, a hybrid simulation environment was designed by integrating both classical IoT and quantum communication simulators. Specifically, QuISP was utilized to model QKD behavior, photon-level entropy variations, and QBER fluctuations under varying decoherence noise. This was integrated with OMNeT++ (using the INET and Castalia frameworks) to simulate IoT communication protocols such as MQTT and CoAP across smart city subsystems, including traffic control, energy monitoring, and healthcare telemetry. The layered simulation allowed dynamic key injection into IoT flows and real-time switching between quantum-secured and classical modes. For empirical validation, three comprehensive datasets were incorporated: TON_IoT [25] for multi-domain telemetry behaviors, Edge-IIoTset [26] for industrial IoT attack simulations, and Bot-IoT [27] for evaluating Q-IDS resilience under high-entropy attack scenarios. These datasets were fused with simulated QKD key logs to evaluate the framework's security, throughput, latency, and anomaly detection effectiveness. This simulation setup enabled the emulation of real-world QKD-enabled smart city infrastructures and provided a benchmark for assessing the QESIF's robustness under both adversarial and noisy conditions. For comparative analysis, the QESIF was evaluated against four recent quantum-secure approaches: QRHE [10], HyQuSec [21], QuIDS [22], and QLSN [23], all of which represent state-of-the-art advancements in quantum-enhanced security for the IoT and smart cities. A detailed summary of the simulation parameters is provided in Table 2.

Table 2. Simulation configuration parameters.

Parameter	Description
Number of IoT Devices	100 nodes per scenario (distributed across transport, energy, healthcare)
Number of Edge Gateways	10 QKD-enabled gateways for local key management and routing
Traffic Model	Exponential traffic generation, mean inter-arrival time = 100 ms
IoT Protocols	MQTT (publish–subscribe), CoAP (request–response)
Quantum Channel Noise Conditions	Clean (1% QBER), Noisy (7% QBER), Eavesdropped (15% QBER)
IoT Device Specification	ARM Cortex-M3 equivalent: 32 MHz CPU, 64 KB RAM
Gateway Specification	Quad-core 1.4 GHz CPU, 2 GB RAM (edge computing node)
Simulation Tools	QuISP (QKD simulation), OMNeT++ with INET and Castalia (IoT network stack)

4.1. Security Analysis (QBER and Attack Detection Rate)

The QBER analysis conducted across 100 QKD sessions under three distinct channel conditions—clean (1% error), noisy (7% error), and eavesdropped (15% error)—demonstrates the adaptive capability of the QESIF. In the clean channel scenario, the average QBER remained exceptionally low at approximately 0.0103, well below the QESIF rejection threshold of 0.11, allowing all the generated keys to be accepted for encryption. Under noisy channel conditions, the QBER increased moderately to an average of 0.0714 yet still remained within the secure operational range, showcasing the QESIF's tolerance to en-

vironmental quantum noise. In contrast, the eavesdropped scenario yielded a significantly higher QBER, averaging 0.1528, thereby exceeding the safety threshold in over 95% of the sessions, as depicted in Figure 2.

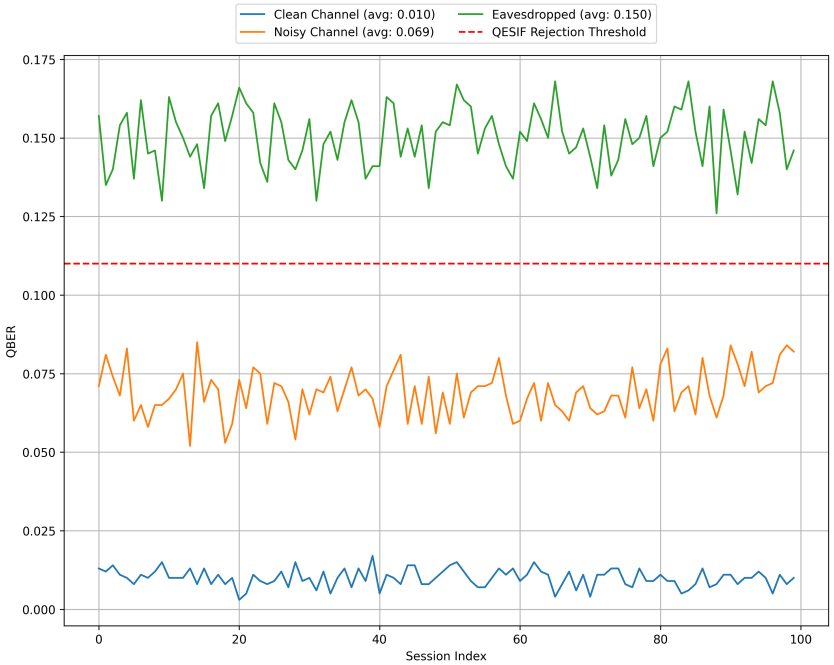

Figure 2. QBER across TON-IoT, Edge-IIoTset, and Bot-IoT for QESIF and baselines.

The comparative analysis of Attack Detection Rate (ADR) across three benchmark datasets—TON_IoT, Edge-IIoTset, and Bot-IoT—demonstrates the superior detection capability of the proposed QESIF. As illustrated in Figure 3, the QESIF achieved the highest detection performance, recording 98.1% on TON_IoT, 98.7% on Edge-IIoTset, and 98.3% on Bot-IoT. In contrast, the next-best performer, QuIDS, achieved 93.5%, 94.1%, and 93.9%, respectively, across the same datasets. QRHE showed moderate performance, ranging from 92.3% to 92.8%, while HyQuSec and QLSN recorded lower ADRs between 89.1% and 91.2%. These results validate that the QESIF's Q-IDS, which incorporates entropy deviation, QBER response, and key drop monitoring, is more effective in identifying advanced threats, especially in high-noise and adversarial IoT environments.

4.2. Performance Evaluation of Latency

The latency performance of the QESIF was evaluated across three datasets (TON_IoT, Edge-IIoTset, and Bot-IoT) and three channel scenarios (clean, noisy, and eavesdropped), as shown in Figure 4. The results demonstrate that the QESIF consistently maintained the lowest average latency across all the scenarios, highlighting its lightweight communication design and adaptive protocol switching. Under clean conditions, the QESIF achieved an average latency of 20.3 ms, 28.6 ms under noisy conditions, and 34.8 ms in the eavesdropped scenario. In comparison, the next-best performer, QuIDS, recorded 22.7 ms, 31.4 ms, and 38.1 ms, respectively, while QRHE and HyQuSec ranged from 24.1 to 29.2 ms and 26.3 to 31.8 ms under clean conditions, with the latencies rising to 44.2 ms and 47.3 ms, respectively, under attack conditions. QLSN consistently exhibited the highest latency due to its heavyweight lattice-based operations, peaking at 49.6 ms in the eavesdropped case.

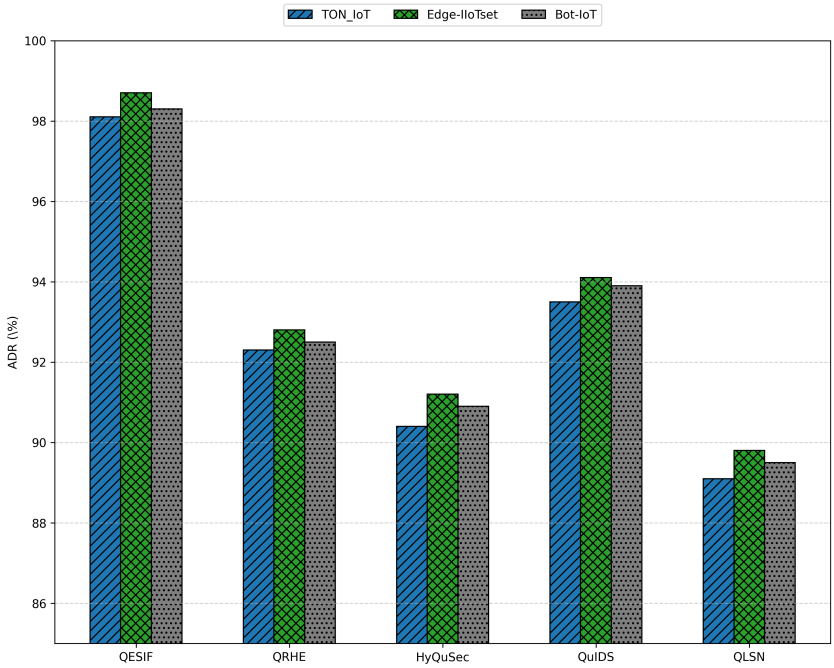

Figure 3. Attack Detection Rate (ADR) comparison across multiple datasets.

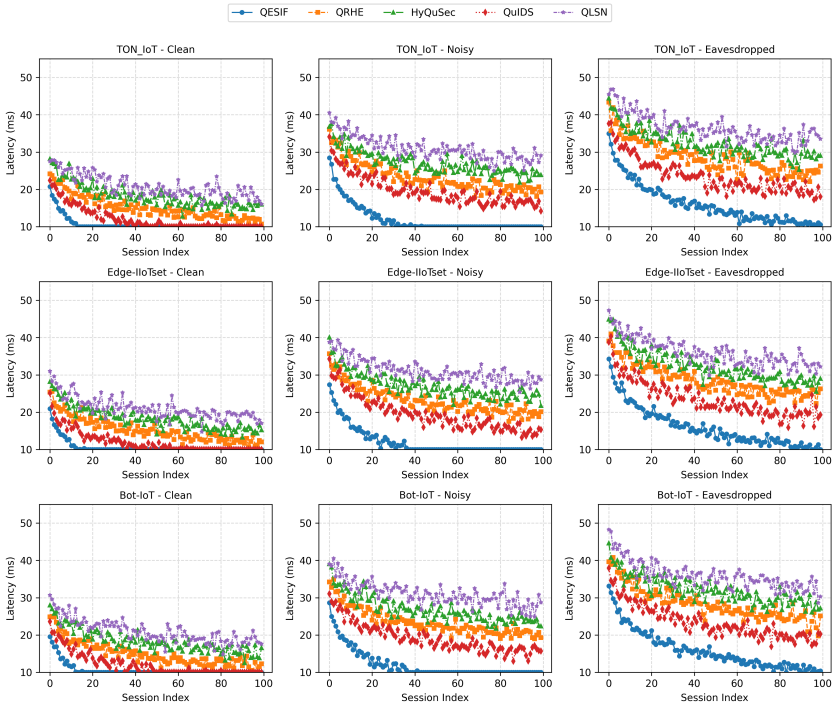

Figure 4. Latency trends of QESIF and baseline approaches across datasets and channel conditions.

4.3. Performance Evaluation of Throughput

The throughput evaluation, conducted over 100 communication rounds for each dataset and channel condition, reveals the superior performance of the QESIF, as shown in Figure 5. In clean channel scenarios, the QESIF achieved an average throughput of 868 kbit/s, outperforming QuIDS (832 kbit/s), QRHE (798 kbit/s), HyQuSec (762 kbit/s), and QLSN (722 kbit/s). Under noisy channel conditions, the QESIF maintained a strong performance at 784 kbit/s, while the closest competitor, QuIDS, reached 755 kbit/s. QRHE and HyQuSec delivered 728 kbit/s and 705 kbit/s, respectively, with QLSN dropping to 684 kbit/s. In the eavesdropped scenario, the QESIF still led with 725 kbit/s, followed by

QuIDS at 695 kbit/s, QRHE at 674 kbit/s, HyQuSec at 648 kbit/s, and QLSN at 628 kbit/s. These results underscore the QESIF's ability to sustain high-throughput performance even under degraded quantum channels or active interference.

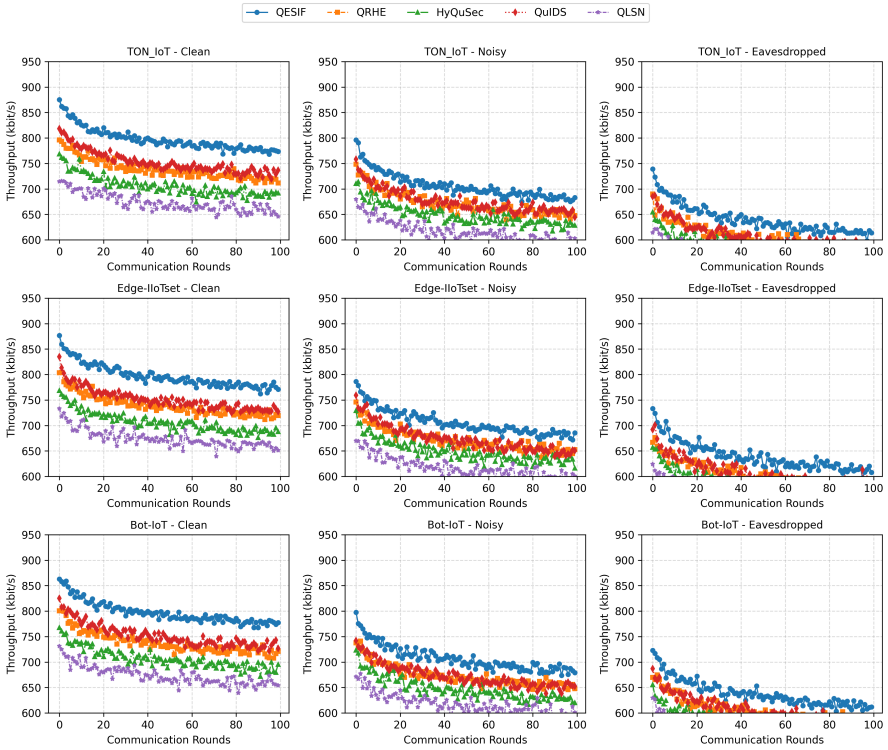

Figure 5. Throughput comparison of QESIF and baseline approaches across datasets and communication scenarios.

4.4. Performance Evaluation of Energy Consumption

The energy consumption analysis across 100 communication rounds for all the datasets and scenarios confirms the efficiency of the QESIF in reducing operational overhead, as shown in Figure 6. Under clean channel conditions, the QESIF recorded the lowest average energy usage at 13.4 mJ, compared to QuIDS at 15.9 mJ, QRHE at 17.3 mJ, HyQuSec at 18.2 mJ, and QLSN at 19.6 mJ. In noisy conditions, the QESIF maintained an average of 15.8 mJ, whereas QuIDS, QRHE, and HyQuSec consumed 18.7 mJ, 20.1 mJ, and 21.6 mJ, respectively, with QLSN peaking at 22.9 mJ. The difference became more pronounced in the eavesdropped scenario, where the QESIF's adaptive protocol stack and entropy-aware session management held energy usage at 17.6 mJ. In contrast, QRHE rose to 22.3 mJ, HyQuSec to 24.0 mJ, and QLSN to 25.7 mJ due to increased cryptographic overhead and communication retries.

4.5. Ablation Study

To evaluate the individual contribution of each core component in the QESIF, an ablation study was conducted by selectively disabling three key modules: the QKD layer, the Q-IDS, and the hybrid protocol stack. Each variant was simulated under identical conditions across the TON_IoT, Edge-IIoTset, and Bot-IoT datasets. Figure 7 presents a clustered heatmap of the normalized performance metrics—ADR, latency, throughput, and energy consumption—for all the QESIF variants. Each metric is computed as an average over 100 independent simulation runs, and corresponding standard deviation values are reported to quantify the variability. The full QESIF configuration achieved the best overall results, with an ADR of 98.7%, latency of 20.3 ms, throughput of 868 kbit/s, and energy consumption of 13.4 mJ. When the QKD layer was disabled (QESIF—QKD),

ADR decreased to 94.1% despite slightly lower latency (19.8 ms), indicating compromised cryptographic robustness. The removal of the Q-IDS module led to the lowest ADR (88.4%), confirming its critical role in real-time threat detection. Meanwhile, eliminating the QESIF hybrid stack significantly increased latency to 27.6 ms and energy usage to 16.8 mJ, underscoring its importance in adaptive communication switching.

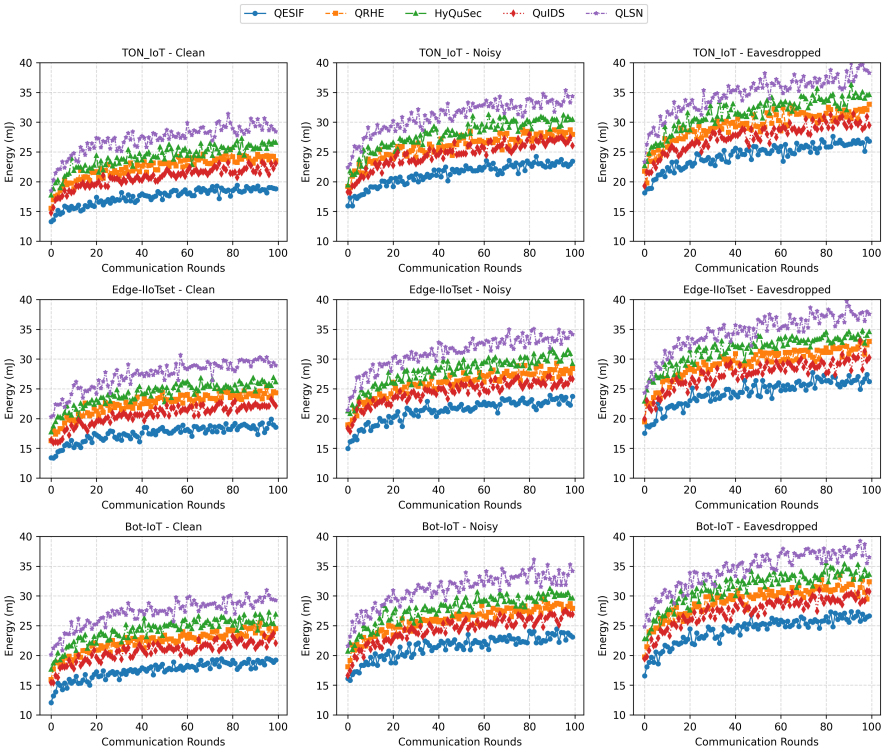

Figure 6. Energy consumption trends across datasets and scenarios for QESIF and baseline approaches.

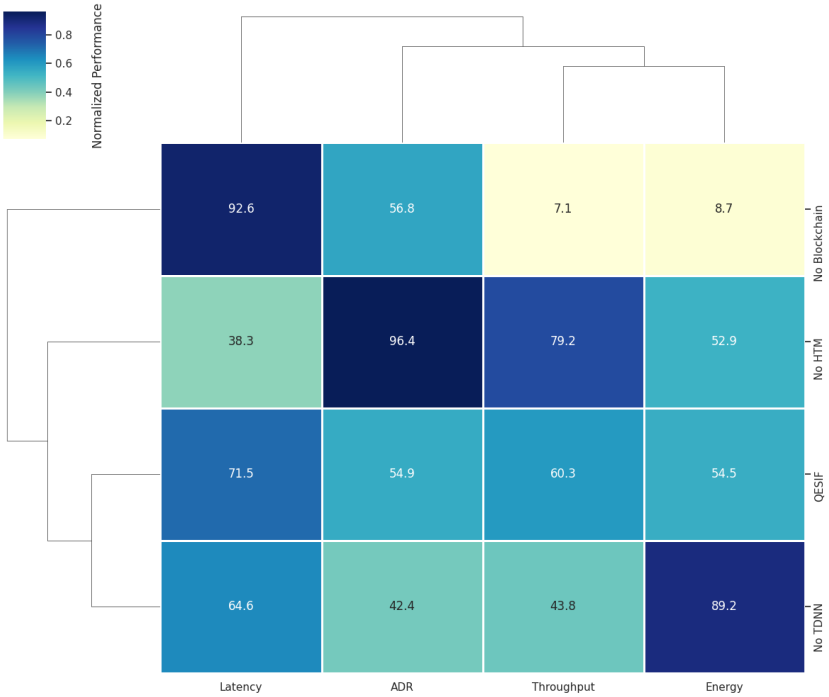

Figure 7. Heatmap illustrating the normalized performance metrics of the QESIF and its ablated variants across key indicators—Attack Detection Rate (ADR), latency, throughput, and energy consumption. Each metric represents an average over 100 simulation runs.

5. Discussion

The evaluation of the QESIF across multiple dimensions—including attack resilience, latency, throughput, and energy efficiency—demonstrates its comprehensive advantage in securing IoT infrastructures within smart cities. The results validate that the integration of QKD, the Q-IDS, and the hybrid protocol stack plays a non-redundant and critical role in the framework's execution. The ablation study also uncovers that the elimination of any one of these modules translates to measurable loss within core performance metrics, with the largest reduction observed within attack detection with the elimination of the Q-IDS and the largest latency incurred with the elimination of the hybrid communication mechanism.

The QESIF's seamless movement from a quantum-secured to a classical mode of communications facilitates a balance of resource limits and security needs, a quality that is uniquely beneficial within heterogeneous smart city implementations. The hybrid construction of the protocol minimizes power usage with no loss of cryptointegrity, and the entropy-weighted QKD mechanism is tuned to device levels and environmental noise.

Also, the design is deployable to practical requirements with minimal device-level hardware modifications using existing IoT protocols. A modular design is made possible on the QESIF to enable scalability within application areas such as transportation, energy, and public safety, where throughput, trust, and latency all have to coexist. Future extensions such as satellite-assisted QKD and blockchain-based audit trails may further strengthen the framework by enhancing geographic coverage and trust transparency. Collectively, these findings confirm the QESIF's applicability as a next-generation security solution for resilient, scalable, and energy-aware smart city infrastructures. While the QESIF maintains compatibility with common IoT protocols such as MQTT and CoAP, the integration of quantum-enhanced mechanisms introduces challenges for cross-vendor interoperability and standardization. The lack of unified quantum APIs, trust negotiation standards, and entropy exchange protocols may hinder immediate large-scale adoption in heterogeneous smart city environments.

6. Conclusions

This paper introduced the QESIF, a Quantum-Enhanced Secure IoT Framework designed to safeguard smart city infrastructures by integrating QKD with classical IoT protocols and a quantum-aware intrusion detection system (Q-IDS). The framework dynamically adapts between quantum-secured and classical communication modes through a hybrid protocol stack, enabling resilience in diverse environmental and network conditions. The simulation results highlight the QESIF's performance, with an Attack Detection Rate of up to 98.7%, average latency as low as 20.3 ms, throughput peaking at 868 kbit/s, and minimal energy consumption of 13.4 mJ. Additionally, the QESIF effectively discarded over 95% of the quantum keys under high QBER in eavesdropped scenarios, ensuring strong forward secrecy. Future enhancements to the QESIF will focus on expanding its security and scalability through integration with satellite-assisted QKD networks. This extension would enable secure key exchanges across geographically distributed smart city zones, overcoming the range limitations of terrestrial QKD links. Additionally, incorporating blockchain-based auditing mechanisms can provide immutable logging of quantum key usage and anomaly detection, thereby strengthening trust, transparency, and accountability in multistakeholder smart city environments.

Author Contributions: Conceptualization, A.R. and O.A.; methodology, A.R.; software, A.R.; validation, A.R. and O.A.; formal analysis, A.R.; investigation, A.R.; resources, A.R.; data curation, A.R.; writing—original draft preparation, A.R.; writing—review and editing, A.R. and O.A.; visualization, A.R.; supervision, O.A.; project administration, O.A.; funding acquisition, O.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research endeavor was generously supported by the Deanship of Postgraduate Studies and Scientific Research at Majmaah University, which provided funding for this project under the designation number (R-2025-1878). The backing from the deanship has been instrumental in facilitating the comprehensive exploration and analysis undertaken in this study.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The author extends appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2025-1878).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Q-IDS	Quantum-Aware Intrusion Detection System
QESIF	Quantum-Enhanced Secure IoT Framework
QuISP	Quantum Internet Simulation Platform
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QBER	Quantum Bit Error Rate
ADR	Attack Detection Rate

References

1. Gracias, J.S.; Parnell, G.S.; Specking, E.; Pohl, E.A.; Buchanan, R. Smart cities—A structured literature review. *Smart Cities* **2023**, *6*, 1719–1743. [CrossRef]
2. Apanavičienė, R.; Shahrabani, M.M.N. Key factors affecting smart building integration into smart city: Technological aspects. *Smart Cities* **2023**, *6*, 1832–1857. [CrossRef]
3. Bittencourt, J.C.N.; Jesus, T.C.; Peixoto, J.P.J.; Costa, D.G. The Road to Intelligent Cities. *Smart Cities* **2025**, *8*, 77. [CrossRef]
4. Darabkh, K.A.; Al-Akhras, M. Evolutionary Cost Analysis and Computational Intelligence for Energy Efficiency in Internet of Things-Enabled Smart Cities: Multi-Sensor Data Fusion and Resilience to Link and Device Failures. *Smart Cities* **2025**, *8*, 64. [CrossRef]
5. Agnew, D.; Boamah, S.; Bretas, A.; McNair, J. Network security challenges and countermeasures for software-defined smart grids: A survey. *Smart Cities* **2024**, *7*, 2131–2181. [CrossRef]
6. Li, W.; Yigitcanlar, T.; Browne, W.; Nili, A. The making of responsible innovation and technology: An overview and framework. *Smart Cities* **2023**, *6*, 1996–2034. [CrossRef]
7. Suleman, D.; Shibl, R.; Ansari, K. Investigation of data quality assurance across IoT protocol stack for V2I interactions. *Smart Cities* **2023**, *6*, 2680–2705. [CrossRef]
8. Ghashghaei, F.R.; Ahmed, Y.; Elmrabit, N.; Yousefi, M. Enhancing the Security of Classical Communication with Post-Quantum Authenticated-Encryption Schemes for the Quantum Key Distribution. *Computers* **2024**, *13*, 163. [CrossRef]
9. Abdel Hakeem, S.A.; Hussein, H.H.; Kim, H. Security requirements and challenges of 6G technologies and applications. *Sensors* **2022**, *22*, 1969. [CrossRef]
10. Xiong, J.; Shen, L.; Liu, Y.; Fang, X. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Sci. Rep.* **2025**, *15*, 3. [CrossRef]

11. Jenefa, A.; Josh, F.T.; Taurshia, A.; Kumar, K.R.; Kowsega, S.; Naveen, E. PQC Secure: Strategies for Defending Against Quantum Threats. In Proceedings of the 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 11–13 December 2023 ; pp. 1799–1804. [CrossRef]
12. Chandre, P.R.; Shendkar, B.D.; Deshmukh, S.; Kakade, S.; Potdukhe, S. Machine learning-enhanced advancements in quantum cryptography: A comprehensive review and future prospects. *Int. J. Recent Innov. Trends Comput. Commun.* **2023**, *11*, 642–655. [CrossRef]
13. Irshad, R.R.; Hussain, S.; Hussain, I.; Nasir, J.A.; Zeb, A.; Alalayah, K.M.; Alattab, A.A.; Yousif, A.; Alwayle, I.M. IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing. *IEEE Access* **2023**, *11*, 105479–105498. [CrossRef]
14. Sahoo, S.; Sahoo, S.P.; Kabat, M.R. A Pragmatic Review of QoS Optimisations in IoT Driven Networks. *Wirel. Pers. Commun.* **2024**, *137*, 325–366. [CrossRef]
15. Khatoon, A.; Ullah, A.; Yasir, M. Machine Learning-Based Detection and Prevention Systems for IoE. In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 109–125.
16. Schöffel, M.; Feldmann, J.; Wehn, N. Code-based Cryptography in IoT: A HW/SW Co-Design of HQC. In Proceedings of the 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 26 October–11 November 2022; pp. 1–7. [CrossRef]
17. Li, G.; Luo, H.; Yu, J.; Hu, A.; Wang, J. Information-Theoretic Secure Key Sharing for Wide-Area Mobile Applications. *IEEE Wirel. Commun.* **2024**, *31*, 118–124. [CrossRef]
18. Almutairi, M.; Sheldon, F.T. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics* **2025**, *14*, 1394. [CrossRef]
19. Halak, B.; Gibson, T.; Henley, M.; Botea, C.B.; Heath, B.; Khan, S. Evaluation of Performance, Energy, and Computation Costs of Quantum-Attack Resilient Encryption Algorithms for Embedded Devices. *IEEE Access* **2024**, *12*, 8791–8805. [CrossRef]
20. Yokubov, B. Post-Quantum Blockchain for Internet of Things Domain. Ph.D. Thesis, Brunel University London, London, UK, 2023.
21. Santa Barletta, V.; Caivano, D.; De Vincentiis, M.; Pal, A.; Scalera, M. Hybrid quantum architecture for smart city security. *J. Syst. Softw.* **2024**, *217*, 112161. [CrossRef]
22. Kim, T.H.; Madhavi, S. Quantum intrusion detection system using outlier analysis. *Sci. Rep.* **2024**, *14*, 27114. [CrossRef]
23. Mangla, C.; Rani, S.; Abdelsalam, A. QLSN: Quantum key distribution for large scale networks. *Inf. Softw. Technol.* **2024**, *165*, 107349. [CrossRef]
24. Din, I.U.; Taj, I.; Awan, K.A.; Almogren, A.; Altameem, A. Quantum and GAN-Driven Digital Twin Approach for IoT-Based Consumer Electronics Manufacturing. *IEEE Internet Things J.* **2025**, *12*, 3734–3741. [CrossRef]
25. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON-IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
26. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* **2022**, *10*, 40281–40306. [CrossRef]
27. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [CrossRef]