Enhancing Security in Low-power Wide-area (LPWA) IoT Environments: The Role of HSM, Tamper-proof Technology, and Quantum Cryptography

Hyung-Sub Han, Tae-hyuk Choi and Jong-Seong Yoon*

SAMIN Geomatics Co., Ltd., Seoul, Korea
E-mail: mukkaby@hanmail.net; xogur111@hanmail.net; yjs353@gmail.com
**Corresponding Author*

Received 23 June 2024; Accepted 13 July 2024

Abstract

Low-power wide-area (LPWA) networks are integral to expanding Internet of Things (IoT) applications, offering extensive coverage with low power consumption. However, these networks face significant security challenges due to their widespread deployment and inherent constraints. In order to provide secure services in an LPWA IoT environment, important information stored in IoT devices (encryption keys, device unique numbers, etc.) must be safely protected from external hacking or theft by physical access, and it is necessary to develop tamper-proof technology to enhance physical security. Meanwhile, with so many ruggedized IoT devices processing and transmitting sensitive information, security systems are essential to protect the integrity and privacy of IoT data. This paper explores the critical role of hardware security modules (HSMs), tamper-proof technology, and quantum

Journal of Web Engineering, Vol. 23_6, 787–800.
doi: 10.13052/jwe1540-9589.2363

cryptography in enhancing the physical, network, and data security of LPWA IoT environments. We propose operational strategies for HSMs, tamper-proof technology in ruggedized LPWA IoT settings, and a quantum key distribution (QKD)-based IPsec solution for robust network and data security.

Keywords: Web-based LPWA security framework, ruggedized IoT, HSM, tamper-proof.

1 Introduction

The proliferation of IoT has driven the development of LPWA networks, which support long-range communication with minimal energy requirements. Technologies such as LoRa, Sigfox, and NB-IoT enable applications ranging from smart metering to industrial automation. Despite their advantages, LPWA networks face substantial security risks, including physical tampering and cyber-attacks. Enhancing physical and data security is crucial to ensure the integrity, confidentiality, and availability of information transmitted across these networks [1, 2].

A hardware security module (HSM) is a specialized hardware device that manages cryptographic keys and performs secure cryptographic operations. HSMs provide a secure environment for sensitive cryptographic processes by being designed to be tamper-resistant. HSMs play a critical role in securing LPWA IoT networks [3–5]. First, HSMs securely generate, store, and manage cryptographic keys, minimizing the risk of key exposure. HSMs also securely perform encryption, decryption, digital signing, and other cryptographic processes, mitigating the risk of data breaches. Finally, engineers build HSMs to resist physical tampering attempts, ensuring that cryptographic keys and operations remain secure even under physical attack [6–8].

Implementing HSMs in ruggedized LPWA IoT environments involves placing them in physically secure and monitored locations to prevent unauthorized access. Organizations also conducts periodic security audits and maintenance to ensure the HSMs remain secure and functional. HSMs can also be embedded within IoT gateways to manage cryptographic functions locally, thereby reducing latency and improving security [9, 10].

2 Enhancing Security in LPWA IoT Environments

The proliferation of IoT devices has accelerated the adoption of low power wide area (LPWA) networks. LPWA networks are characterized by their

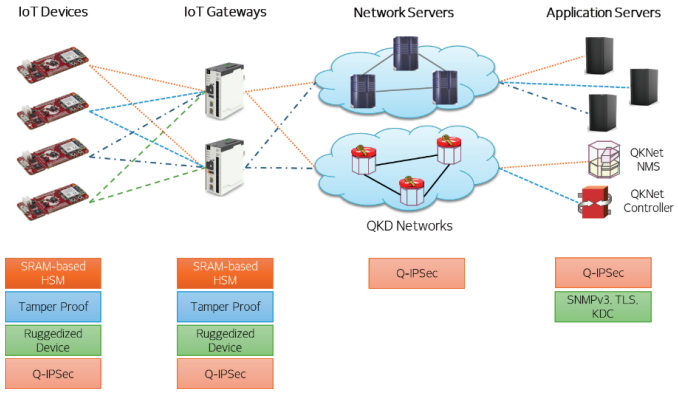


Figure 1 QKD-based IoT target network architecture.

ability to support long-distance communication while consuming low power, making them suitable for many IoT applications. However, the rapid expansion of LPWA networks introduces significant security challenges in ensuring data integrity and confidentiality [11].

Firstly, IoT devices often need more processing power, memory, and battery life, which constrains the implementation of robust security protocols. These devices are frequently deployed in unprotected or remote locations, making them susceptible to physical tampering, theft, or environmental damage. Moreover, IoT gateways play a crucial role as aggregation points. An attack on the IoT gateway can disrupt communication for multiple IoT devices. Since IoT devices relay sensitive data, inadequate protection can result in intercepting data during transmission.

Network servers act as central hubs for data and control messages. Compromising the network server can lead to extensive consequences, such as data loss and service denial. It is crucial to ensure data integrity during transmissions over the network, as alterations or damage to the data can lead to incorrect decisions and actions.

Application servers handle sensitive data, including personal and industrial information. Inadequate privacy measures can result in data breaches and regulatory compliance issues. Furthermore, application servers interact with various external systems, which can introduce vulnerabilities if not properly secured.

To address the security challenges in LPWA IoT networks, we propose integrating quantum key distribution (QKD) into them, as illustrated in Figure 1. In the proposed solution, IoT devices and gateways perform various

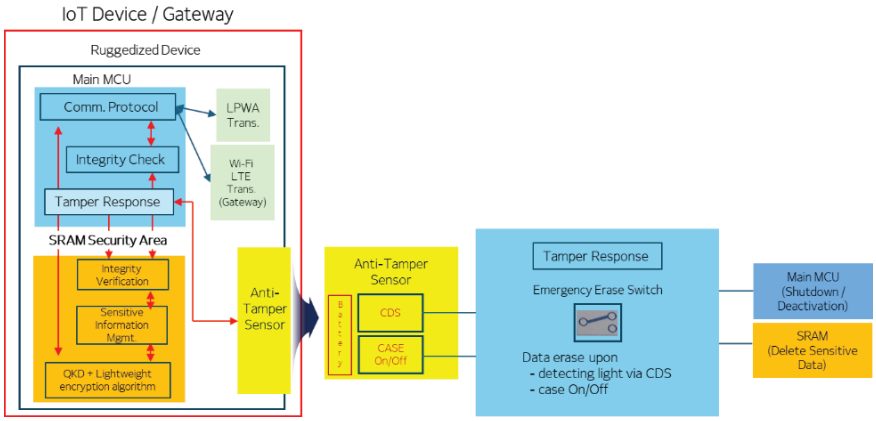


Figure 2 Proposed IoT device and gateway structure.

lightweight encryption methods, including IPsec, based on keys provided by QKD. Additionally, implementing SRAM-based hardware security modules (HSMs) and tamper-proof technologies further strengthens security.

Figure 1 presents the QKD-based IoT network architecture proposed in this paper. This architecture utilizes QKD to generate encryption keys, which IoT devices and gateways use to secure communications. The integration of HSM and tamper-proof features ensures that the devices are protected against physical and environmental threats, thereby enhancing the overall security of the LPWA IoT network. Figure 2 also presents the proposed IoT device and gateway structure.

2.1 SRAM Secure Zone

The SRAM secure zone storage method divides the SRAM into regions of 0×100 bytes, with a hash value applied to each region. When data from a specific region is accessed, the first 28 bytes represent the hash value, followed by a 2-byte length field that indicates the size of the stored data. The system reads the data according to the length specified and then compares it with the hash value to verify the integrity of the data stored in the SRAM.

This paper proposes a method for storing and managing keys within the SRAM secure zone in IoT devices and gateways (Figure 3). The system utilizes the lightweight secure hash (LSH) function and the Q-IPSec encryption algorithm to ensure the confidentiality and integrity of transmitted data. By employing these cryptographic techniques, the proposed method ensures that

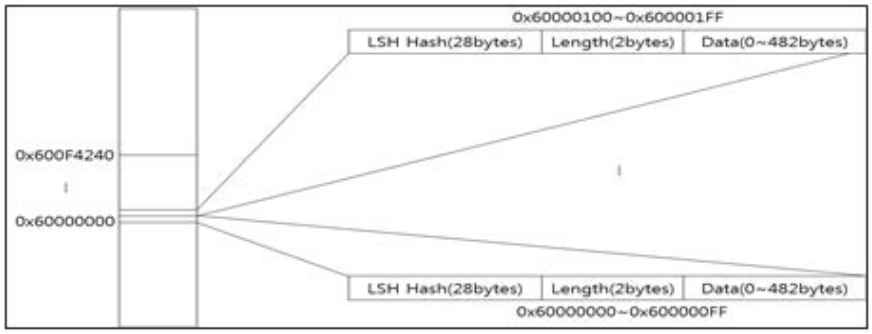


Figure 3 SRAM secure zone storage format.

data sent and received by the IoT devices and gateways remains secure and tamper-proof.

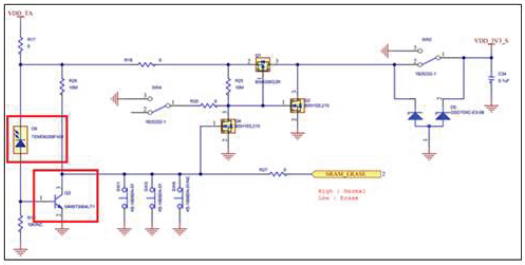
2.2 Tamper Detection

Hardware-based tampering detection technologies enhance system physical security by using various methods to maintain hardware integrity and detect unauthorized access or tampering attempts.

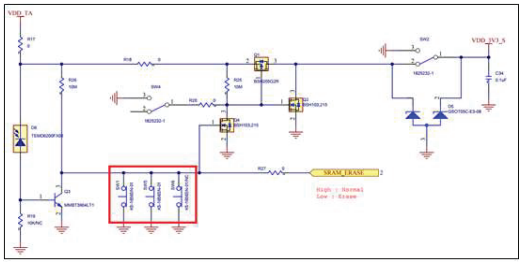
This paper proposes an IoT device and gateway that utilizes physical sensors to detect changes in the hardware's physical state, as illustrated in Figure 4. The system incorporates pressure, photo, and temperature sensors. Pressure sensors detect variations in pressure, allowing the system to recognize when external force is applied. Such pressure changes indicate potential tampering attempts. Photo sensors detect changes in light exposure, enabling the system to monitor whether the device is opened or closed. If light suddenly exposes a sensor to darkness, the system considers it a tampering attempt. Temperature sensors monitor abnormal temperature changes. For instance, they can detect the use of cooling sprays or heat treatments to alter the hardware. If tampering is detected, the system deletes SRAM data to protect sensitive information.

2.3 Quantum Key-based IPSec

This section describes extending the existing IKEv2 protocol performed on Q-IPSec devices based on quantum keys. Q-IPSec devices can receive quantum keys through QKD, so these quantum key values can also be reflected in IKE (internet key exchange).



(a) Detection of changes in light intensity



(b) Detection of pressure changes

Figure 4 Hardware-based tamper detection types.

In terms of performance, Diffie–Hellman (DH) key generation is slow and computationally intensive. The outcome of this step is the IKE SA (security association), which is the contract for the keys and methods of IKE phase 2. IKE Phase 2 is encrypted based on the keys and methods agreed upon in IKE phase 1. During IKE phase 2, the exchanged key materials are used to build IPsec keys. The result of step 2 is IPsec SA. IPsec SA is a contract for the key and method for IPsec, so IPsec is performed according to the key and method agreed upon in IKE phase 2. Finally, as illustrated below, quantum keys obtained through QKD can be used as part of the key materials that form the Q-IPSec SA, and their hash values can also be utilized. The peers accomplish this part through agreement.

Q-IPSec IKE phase incorporating quantum keys:

- Peers authenticate through certificates or pre-shared secret values.
- Each peer generates a DH private key from a random bits pool.
- Each peer derives a DH public key from the private key.
- Exchange of public keys.
- Peers generate a shared secret from their private key and the other's public key.

- The shared secret serves as the DH key.
- DH key is used to exchange random bits and other mathematical data.
- Agreement on encryption and integrity methods for IKE phase 2.
- Each side generates symmetric keys based on the DH key and exchanged key materials for IKE phase 2.
- Agreement on encryption and integrity methods for IPSec.
- Exchange of additional key materials.
- Combine DH key and key materials to generate IPSec symmetric keys.
- Add a quantum key or quantum key hash value at this stage as key materials.
- Use IPSec keys for data transmission.

3 QKD-based IoT Network Structure and Service Scenarios

3.1 Proposed QKD Network Architecture

Figure 5 illustrates the network architecture for QKD-based IoT secure services. The QKD-based research network comprises four layers: the transport layer, the QKD layer, the control layer, and the application layer, which includes the network management system (NMS).

3.1.1 Application layer

The application layer consists of applications requesting end-to-end QE (quantum encryption) services, the NMS, and related service elements. In the QKD-based IoT network, there are two types of end-to-end QE services:

- Q-IPSec-based IP layer VPN
- Transmission equipment-based segment encryption.

End-to-end QE service requests in the QKD-based IoT network can be made in two ways: on-demand and batch. The integrated operations management system provides a RESTful API for on-demand requests. It offers basic FCAPS functionalities of the NMS and performs connection, policy, and discovery management, including key relay management. Connection management offers protection and restoration functions to counter failures in QKD or optical links.

3.1.2 Control layer

The control layer comprises the QKNet controller and a logical set of KPs (key pools). The QKNet controller communicates with the agents of the

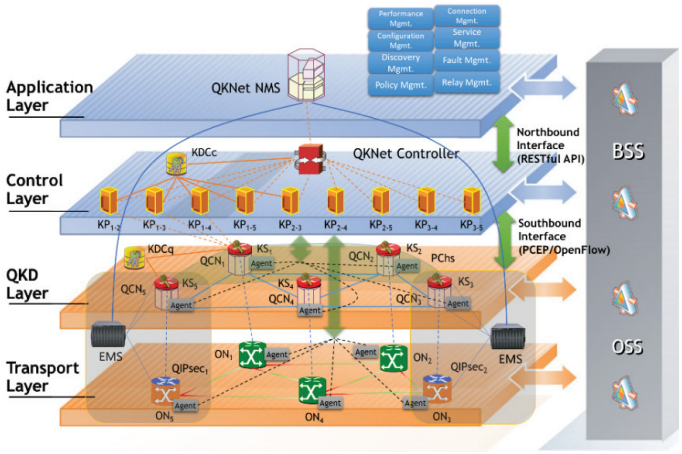


Figure 5 QKD network layer architecture.

QKD layer and the transport layer based on an extended PCEP (path computation element protocol). The control layer transmits commands from the application layer to the agents of the QKD and transport layers.

3.1.3 QKD layer

The QKD layer consists of a set of QCNs (quantum communication nodes), KSs (key servers), and PCE/PCC (path computation client) agents. From an overall security perspective, quantum keys cannot leave the QKD layer. As shown in Figure 6, the KS records the quantum key information received from the QCN, generates a hash value of the quantum key, and stores it along with the key index. Since quantum keys cannot leave the QKD layer, the KS transmits the key index and hash value to the KP.

Given that the QKD key generation rate is significantly lower than the data transmission rate, the KS/KP/EMS/NMS provides key reuse functionality to account for potential QKD errors. A multi-layer interworking interface is provided to support this. The KP is implemented in an overlay network regardless of physical location and manages quantum keys received from two KSs. The KS manages the quantum keys generated in the QKD layer, while only the key ID, hash value, and related information are delivered to the KP. The QKD-based IoT network inherently supports relay nodes. The QKD layer not only generates quantum keys but also facilitates the delivery of these keys to Q-IPsec equipment or transmission equipment with encryption capabilities via a secure channel in coordination with the NMS/EMS.

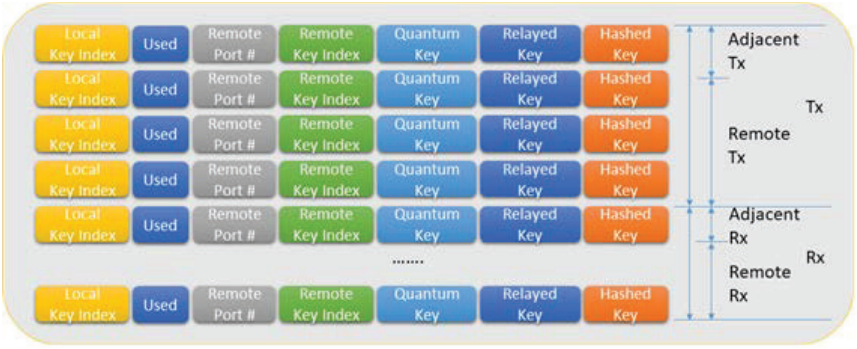


Figure 6 Example of KS_5 configuration in QCN_5.

3.1.4 Transport layer

The transport layer consists of devices providing QE functionality, namely Q-IPSec and Ons (optical nodes) providing cryptographic capabilities. QE delivers encryption services; KS delivers encryption keys through a secure channel. The creation of encryption channels in the transport layer occurs in real-time through interaction with the application layer and element management system (EMS) or in batch mode via pre-configured setup files.

Q-IPsec is a device that provides quantum key-based IPsec functions. Unlike IPsec equipment, Q-IPsec equipment uses a modified IKEv2 protocol and provides tunnel mode encryption services by generating an encryption key that reflects the quantum key. Tunnel creation in the Q-IPSec layer is performed in real time through the service management layer or in batch mode via pre-configured files. The EMS integrates with the NMS of the service management layer to manage QCNs, Q-IPSec, and transmission equipment. EMS specifically provides redundancy and synchronization features to ensure the resilience of QCNs and KS.

3.2 QKNet Operation Interface and Scenarios

3.2.1 NMS-EMS interface

In QKNet, the EMS is aware of the configuration of the devices it manages across the QKD and transport layers. It can integrate the management of up to four devices, such as the KS, QCN, Q-IPSec, and ON (optical node). The NMS-EMS interface protocol typically uses SNMP, TL1, CLI, XML, and CORBA. However, depending on QKNet's security requirements, as shown in Figure 7, the NMS-EMS interface (1) can have the following communication interfaces.

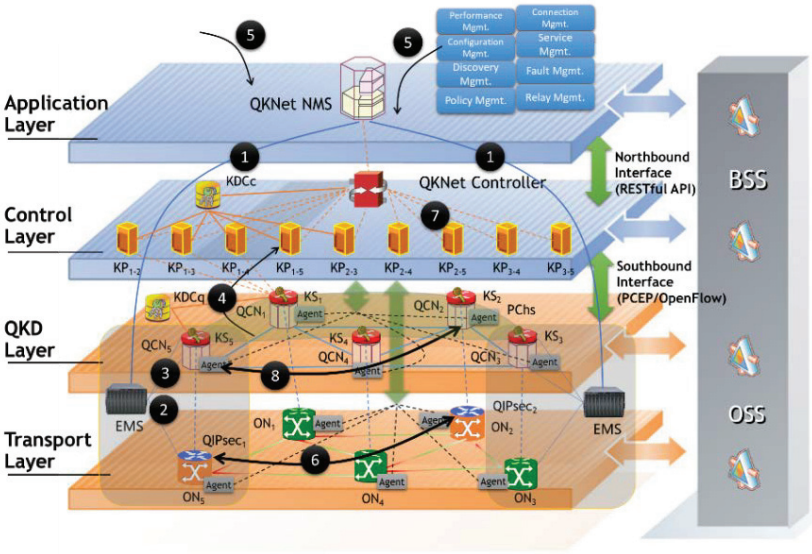


Figure 7 QKNet interfaces and scenarios – 1.

- SNMPv3-based communication
- TLS (transport layer security)-based communication
- KDC (key distribution centre)-based communication.

The interface between EMS and KS, QCN, ON, and Q-IPSec ((2) in Figure 7) employs TLS-based encrypted communication.

3.2.2 QKNet service scenarios

(1) As shown in Figure 7 (3), the EMS managing the QCN/KS operates in a manner that ensures the QCN's functionality is not impacted even if the connection to the NMS is lost or if the connection to the NMS has not yet been established.

(2) The KS generates a hash value from the keys the QCN produces and stores.

(3) As illustrated in Figure 7 (4), adjacent QCN/KS pairs store the <QCN ID, Key Index, Hash Value> in the corresponding KP according to the 'Adjacent TX/RX #' parameter.

(4) For non-adjacent QCN/KS pairs, this information is stored in the KP after establishing the connection.

(5) In QKNet, there are two types of security connection requests: one for setting up tunnels using Q-IPSec and another for establishing encrypted

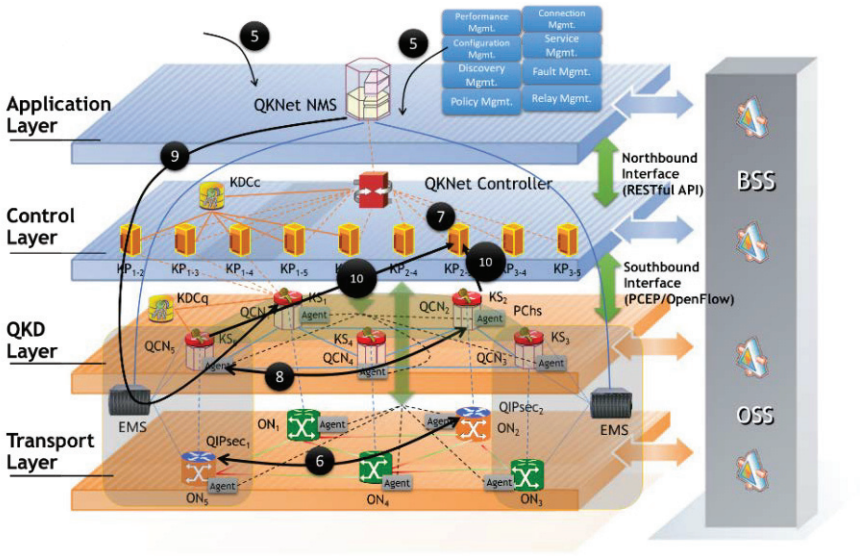


Figure 8 QKNet interfaces and scenarios – 2.

channels between ONs. As shown in Figure 7 (5), a secure connection request between Q-IPSec1 and Q-IPSec2, originating from external applications or internal management functions, is communicated to meet security requirements (Figure 7 (6)).

(6) As shown in Figure 7 (6), to establish a connection between QIPSec_1 and QIPSec_2, KP_{2-5} is checked first (Figure 7 (2)).

(7) If KP_{2-5} is empty, quantum signaling between KS_5 and KS_2 is required, as depicted in Figure 7 (8). In this case, KS_1 performs the relay function.

(8) As shown in Figure 8 (9), the NMS configures the relay function of the respective KS through the EMS.

(9) KS_2 receives the relay information (parity announcements) and stores it in the relay key, as illustrated in Figure 8.

(10) KS_5 and KS_2 store the key information in KP_{2-5}, as depicted in Figure 8 (10).

(11) The QKNet Controller establishes a secure tunnel between Q-IPSec_1 and Q-IPSec_2 through the SBI, as shown in Figure 9 (11). Optionally, the secure tunnel path can also be provided.

(12) As illustrated in Figure 9 (12), QIPSec_1 and QIPSec_2 receive the quantum key values required for the Q-IPSec SA setup process from KS_5 and KS_2.

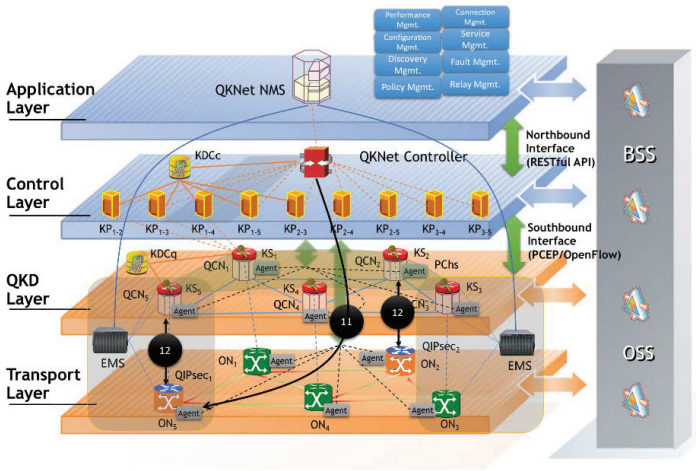


Figure 9 QKNet interfaces and scenarios – 3.

4 Conclusion

The security of LPWA networks is paramount, given their widespread use in critical and sensitive applications. Integrating HSMs, tamper-proof technology, and quantum cryptography provides a comprehensive security framework that addresses physical and cyber threats. HSMs ensure secure key management and cryptographic processing, tamper-proof technology protects devices from physical attacks, and quantum cryptography offers maximum security for data transmission. Together, these technologies enhance the overall security posture of LPWA networks, ensuring their resilience and trustworthiness in an increasingly connected world. The proposed operational strategies in this paper for HSMs and tamper-proof technology in ruggedized LPWA IoT environments, along with the QKD-based IPsec solution, offer practical approaches to securing these networks against emerging threats. As LPWA networks evolve, adopting these advanced security measures will be essential to safeguard against evolving threats and ensure IoT deployments' long-term security and reliability.

References

[1] Stoyanova Maria et al., "A survey on the internet of things (IoT) forensics: challenges approaches and open issues", IEEE Communications Surveys Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020.

[2] Ammar Mahmoud, Giovanni Russello and Bruno Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
[3] Hassija Vikas et al., "A survey on IoT security: application areas security threats and solution architectures", IEEE Access, vol. 7, pp. 82721–82743, 2019.
[4] I. Atov, K. C. Chen, A. Kamal and S. Yu, "Data Science and Artificial Intelligence for Communications", IEEE Communications Magazine, vol. 58, no. 1, pp. 10–11, 2020.
[5] L Wawrowski, A. Bialas, A. Kajzer, A. Kozlowski, R. Kurianowicz, M. Sikora, et al., "Anomaly detection module for network traffic monitoring in public institutions", Sensors, vol. 23, no. 6, 2023.
[6] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things", IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, Oct. 2017.
[7] P. M. Chanal and M. S. Kakkasageri, "Preserving data confidentiality in Internet of Things", SN Computer Science, vol. 2, no. 1, pp. 53, 2021.
[8] P. Panahi, C. Bayılmış, U. Çavuşoğlu and S. Kaçar, "Performance evaluation of lightweight encryption algorithms for IoT-based applications", Arabian Journal for Science and Engineering, vol. 46, pp. 4015–4037, 2021.
[9] A. U. Mentsiev and T. R. Magomaev, "Security threats of NB-IoT and countermeasures", IOP Conference Series: Materials Science and Engineering, vol. 862, no. 5, pp. 052033, May 2020.
[10] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali and A. A. Khan, "A review and state of art of Internet of Things (IoT)", Archives of Computational Methods in Engineering, pp. 1–19, 2021.
[11] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?", IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, Sept. 2018.

Biographies

Hyung-Sub Han received a master's degree in geospatial information engineering from the University of Seoul in 2022 and is currently serving as a vice president at SAMIN Geomatics Co., Ltd.

Tae-hyuk Choi is currently serving as the CEO at SAMIN Geomatics Co., Ltd. and is currently pursuing an MBA master's degree at Kyung Hee University.

Jong-Seong Yoon earned his PhD degree in civil engineering from Inha University in 2008. He is Director of Research Institute at Samin Geomatics Co., Ltd.