International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Communication Model for Constrained Internet of Things Devices

Omar Reyad*[1,2]

Submitted: 26/01/2024 **Revised**: 04/03/2024 **Accepted**: 12/03/2024

Abstract: Internet of Things (IoT) devices are rapidly on the way to becoming a necessary component of our daily life. These tools are efficient at accomplishing a particular task because of their specialized abilities. The IoT platform involves a variety of devices, from less resource-constrained to wireless sensors. These devices are vulnerable to network and hardware/software assaults. Securing communication with constrained IoT devices is crucial to maintaining the privacy of user sensitive information. This study suggested an approach for data protection and secure connectivity that can be deployed as an IoT security system. A symmetric approach is used to encrypt plaintext data devices before storing, and an asymmetric cryptosystem is used for protecting the cloud services and IoT service gateway. The encrypted data can be stored/retrieved based on cloud service requests. Also, plain-text data appears on the client interface whenever needed. Performance measurement of Message Queue Telemetry Transport (MQTT) and Hyper Text Transfer Protocol (HTTP) are illustrated. The outcomes indicate the way the framework works to reduce security threats and guarantee the integrity of the presented IoT model.

Keywords: *Security, Communications, Internet of Things, Symmetric cryptosystem, Asymmetric cryptosystem*

1. Introduction

Several decades recently, the Internet transformed our world by instantaneously linking users all over the world in real-time. The Internet of Things (IoT), also referred to as the Internet of Everything or the Industrial Internet, is a technology paradigm that is envisioned as a network that connects machines and devices globally and enables them to interact with one another and the physical world on their own within the current Internet infrastructure [1]. In order to improve our life, these devices handle private personal information and carry out microtransactions. Privacy is a concern that comes along with this benefit. We really must have a means of securely communicating with such devices. It has been demonstrated achieved to establish adaptive secure communication through a number of advancements. The rapid development of Internet networks, digital communication channels, and gadgets, as well as the ongoing decline in the price of computer power and data storage, have all encouraged these trends [2,3]. Parallel to this, hardware devices have decreased in size, grown more accessible, and developed real-time communication capabilities. These days, practically every organization can measure and collect data in real time at low cost. Theoretically and practically, utilizing software robots, cloud services, and a wide range of IoT devices, it is feasible to monitor and control all business activities [4]. All gadget kinds, however, may not be compatible with these improvements. Devices like sensors or radio-frequency identification (RFID) tags, for instance, might not have enough central processing unit (CPU) power to handle adaptive implementation or to combine a number of security mechanisms that can provide sufficient security levels for communication needs [5]. In the meanwhile, secure communication may be impossible to achieve even with flexibility due to fundamental asymmetries in the availability of security functions at the endpoints. If the intermediate network does not support security functions at the end, the same result is inevitable [6].

The intelligent, diverse equipment that makes up the IoT platform is linked together via the internet. The network layer, application layer, and perception layer formulated the Internet of Things' tiered infrastructure. The most frequent security breaches in the perception layer include radio frequency interruption, hardware tampering, fraudulent node injection, jamming of nodes, and rest deprivation [7]. In the network layer, man-in-the-middle, spoofing, sinkhole, and Sybil attacks are also commonplace. In the application layer, denial-of-service (DoS), malicious script, and phishing assaults are prevalent. Every stage of the device's lifetime, from the original design to the operating environment, requires consideration of security. The main obstacles that IoT solutions must overcome are communication power limitations and finding ways to provide cutting-edge IoT solutions with a little more battery life. IoT environments are susceptible to cyberattacks due to a lack of strong security measures, which might have serious consequences. Data encryption is one of the most important components of IoT communication security. This guarantees the confidentiality of sensitive data transferred

[1] *Department of Information Systems, College of Computing and Information Technology, Shaqra University, 11961 Shaqra, Saudi Arabia ORCID ID : 0000-0003-3479-6986*
[2] *Faculty of Computers and Artificial Intelligence, Sohag University, 82524 Sohag, Egypt*
** Corresponding Author Email: oreyad@su.edu.sa*

between devices and prevents unwanted parties from intercepting it. Transport layer security (TLS), which offers a secure channel for data transit over networks, is a well-liked encryption innovation used in IoT environments [8]. Authentication methods are essential to IoT security in addition to encryption. Mutual authentication guarantees that communication is occurring with legitimate and authorized devices and contributes to the establishment of trust between devices and servers [9].

Fig. 1 presents a general IoT model architecture which includes a network of devices, a gateway, and a web and client servers. These IoT devices can record data and communicate over the Internet. Web or mobile applications that allow users to interact with the IoT system, sending commands to actuators or configuring devices for more control on the application layer. This architecture provides a comprehensive view of an IoT system, highlighting the interaction between devices, communication protocols, cloud infrastructure, and user applications, ensuring a robust and scalable solution. This work presents the following main contributions:

- Examines and describe generic IoT architecture.
- Identify several challenges regarding IoT communication.
- Provide robust authentication mechanisms for IoT communication devices.

The rest of this paper is organized as follows. Section 2 reviews state-of-the-art studies in the area of secure communication for constrained IoT devices. Section 3 addresses the main security challenges of IoT based communication. The suggested security protocol for IoT communication is described in Section 4 with a practical example. Finally, the conclusions and future directions of this research work are given in Section 5.

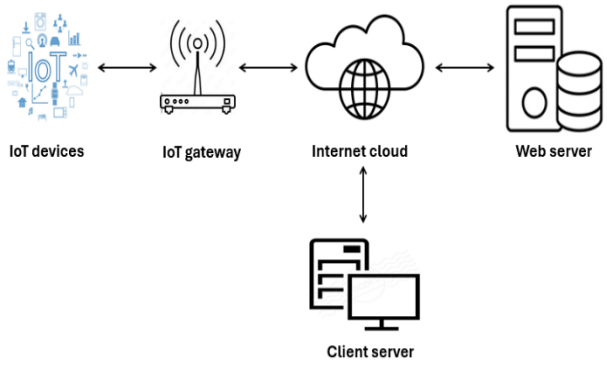

Fig. 1. General IoT model architecture.

2. Related Work

There is a lot of research being done in the area of secure communication for constrained IoT devices, with the goal of addressing the particular challenges brought about by the constrained processing, energy, and communication capabilities of these devices [10]. The authors in [2] presented an innovative streamlined framework for securing IoT connectivity. This method is used in the P3 connection architecture to safely establish a secret key for the parties to exchange messages. By using these keys, the command execution model confirms the parties' identities for each request and answer. The model outlined offers a comprehensive framework for securely interacting with these smart devices in a cloud-based architecture while taking into account their resource constraints. A distributed security method specifically designed for IoT devices is presented in [4]. The suggested method offers a layered security approach between the device and the gateway by combining native wireless security with symmetric encryption for data items. The IoT gateways in the proposed solution secure data using transport layer security, adding an extra layer of safety. Experiments conducted in real time have shown that the suggested mechanism is applicable in terms of the target Class-0 IoT devices' resource consumption and security assurance. In order to help secure communications for resource-constrained IoT instances and devices, authors in [5] looked into the use of security resource-aiding entities. They found that aggressive behavior on the adaptation control is observed when the requesting entity is given the adaptation control, resulting in variations in the message exchange latency. Therefore, it seems that aiders are a better place to conduct adaptation control. In an IoT system based on wireless sensor networks (WSN) [11], a challenge-response mutual authentication mechanism is suggested to improve security. The indicated protocol has the lowest transaction costs, time complexity, end-to-end delays, and energy usage, according to the simulation findings. It is also resistant to attacks such as dictionary, side channel, cloning, denial of service (DoS), man-in-the-middle (MitM), and future password prediction. In [12], an intelligent security framework for Internet of Things devices is presented. The provided approach uses Lattice-based cryptography to secure the Broker devices/Gateway and cloud services. Also, lightweight asymmetric cryptography is used to secure the End-To-End devices, which safeguard the low power sensor nodes and the IoT service gateway. In addition to increasing performance and lowering bandwidth usage, this strategy offers protection against quantum attacks. A suggested algorithm is presented in [13] to verify and control access when a new device is connected to the network. The approach generates keys at the application layer. These keys were produced using JSON and REST format. Since these methods are based on elliptic curve cryptography (ECC), they can be used to minimize communication threats and preserve other elements such as memory space and lifetime during the network's construction. In [14], a security model for IoT as well as an overview, analysis, and taxonomy of

security and privacy issues in IoT have been presented. The access information needed to approve or deny requests for access on the IoT is not just composite but also sophisticated. The direct cause of such structure is the tremendous degree of interconnection between objects, services, and people. The application that encrypts the data determines how much of the software settings are displayed. This makes it possible for a third party to confirm that the software hasn't been altered. Using the trusted platform module (TPM) endorsement key, a special Rivest, Shamir and Adleman (RSA) key burned into the chip during manufacture, or another reliable key derived from it, "binding" encrypts data. To guarantee end-to-end security from an IoT application to IoT devices, a secure IoT framework is suggested in [15]. The IoT devices, an IoT broker, and an IoT application make up the suggested IoT architecture. Sensitive data is encrypted using the suggested framework using both attribute-based and symmetric encryption to reduce computation and communication costs. The defined framework offers protection against malicious IoT brokers and eavesdropping. In [16], the researchers developed an architecture of the intelligent IoT common service platform and executed its core functionalities. In order to apply a basic intelligence-based IoT service, they created a prototype service platform and IoT Broker. Through the user interface, users can easily operate the devices or services that are integrated on the platform. Users must register their IoT Broker at home in order to access the IoT service. Consequently, the effectiveness of the suggested IoT common service platform was validated. In order to improve performance in threat prevention, detection, and mitigation, the work in [17] combines the ECC approach with logistic regression machine learning. The goal of that study is to transmit data using an intelligent transmitter, which reduces packet losses and ensures that the receiver receives secure data in the wireless sensor network (WSN). This method generates and distributes security keys using the ECC algorithm. Because ECC is a lightweight key, the routing overhead is reduced. By verifying the sensor nodes, this cryptography method improves network security. Additionally, route nodes work with IoT to reduce latency.

3. IoT Communication Security Challenges

Through data exchange amongst IoT devices, gateways, and the cloud, these apparatuses can coordinate actions and share information with the aid of IoT communications. To guarantee the availability, integrity, and confidentiality of IoT systems, it is essential to address the security issues raised by the communication channels that IoT devices deploy [7,18]. Here are some of the major IoT communication security challenges:

1. Interception and Eavesdropping: Unauthorized parties may be possible to intercept data that is transmitted between IoT devices. This may result in the disclosure of private or confidential organization information, threatening both competitive advantage and privacy.

2. Data Integrity: It is essential to guarantee the integrity of the data being transferred. Data can be altered while being transmitted, which could result in the receiving and use of false information. This could have harmful consequences particularly in essential systems such industrial control systems and healthcare systems.

3. Replay Attacks: A replay attack occurs when a hacker intercepts a valid transmission and sends it back later. If systems do not have security features in place to identify and stop the replay of previous messages, this could result in unlawful actions.

4. Man-in-the-Middle (MitM) Attacks: In a MitM attack, a third party illegally transmits and may modify communication between two parties that believe they are speaking with each other individually. This enables data intended for another person to be intercepted, sent, and received by the attacker without the original sender or receiver being aware of it.

5. Authentication Challenges: To avoid unwanted access and guarantee that data is shared between reliable parties, it is crucial to correctly identify and authenticate the devices involved in communication. Because many IoT devices do not hold strong authentication features, they are susceptible to fraud and illegal access.

6. Encryption Overhead: Although encryption is an essential security measure for securing data while it is in transit, it comes with computational overhead. Since many IoT devices have limited energy and computing capacity, it might be difficult to install robust encryption techniques without compromising the functionality or life span of the device.

7. Vulnerabilities in Protocols: IoT devices employ several types of communication protocols, some of which were not constructed with robust security measures in the forefront. Attackers may use weaknesses in these protocols to compromise IoT communications.

8. Denial of Service (DoS) Attacks: Attackers can use DoS assaults against IoT communication networking by flooding devices or networks with malicious traffic, which prevents the devices or networks from processing valid requests. Important IoT applications as well as services could be disrupted because of this.

A comprehensive strategy involving the application of cutting-edge cryptographic methods, secure communication protocols, and reliable authentication and authorization systems is needed to address these issues. In order to mitigate these problems, industry supporters have to collaborate together to establish and preserve security

standards and best practices.

4. IoT Security Gateways

IoT security gateways play a crucial role in safeguarding IoT networks by acting as intermediaries between IoT devices and the wider internet or enterprise networks. These gateways are designed to address the unique security challenges posed by IoT devices, which often lack the computational resources to implement robust security measures on their own. IoT gateways enable centralized control and automation in smart environments by connecting a variety of smart devices which in some cases shortage in security conditions. Using IoT security gateways provides the following benefits:

1. Enhanced security: By centralizing security functions, gateways provide a robust layer of protection for IoT devices that might otherwise be vulnerable to attacks.

2. Resource efficiency: Offloading computationally intensive tasks to gateways allows constrained IoT devices to function more efficiently, conserving their battery life and processing power.

3. Simplified management: Gateways provide a centralized point for managing and monitoring IoT devices, making it easier to enforce security policies and update configurations.

4. Scalability: As the number of IoT devices grows, gateways can scale to handle increased traffic and manage more devices without compromising security.

5. Integrated IoT Security Protocol

Developing a framework that provides data confidentiality, integrity, authentication, and availability across a range of possibly constrained IoT devices and networks is a key step in proposing a security protocol for IoT communication. In order to meet the inherent challenges presented by the IoT environment, a well-designed protocol should be lightweight, scalable, and adaptable to various IoT applications and technologies [19,20]. Protecting cloud services and IoT resource gateways with both the advanced encryption standard (AES) [21] and elliptic curve cryptography (ECC) [22] protocols is a very effective security strategy. This approach combines the reliability of ECC for secure communications and key management with the effectiveness and strength of AES for data encryption.

5.1. The Integrated Protocol Components

The Integrated Protocol main components are as follows:

- Initial Key Exchange: To securely transfer AES keys between IoT devices and services, the presented protocol utilized pseudorandom Weierstrass curves defined over P-256 prime fields. ECC's robust security features and effectiveness are advantageous to this process, particularly when operating over potentially insecure networks.

- Data Encryption: Make use of AES with a 128-bit key length to encrypt the intended data once the AES keys have been successfully transferred. This makes use of AES's security and speed to encrypt large information and to meet real-time data encryption requirements.

- Continuous Security: To increase security, periodically exchange or renew current keys and use ECC for continuous authentication. This is important because IoT and cloud services devices may join or exit networks regularly in dynamic situations.

- Efficiency and Scalability: This enables security mechanisms that are both efficient and scalable, making them adaptable to a range of requirements, from resource-constrained IoT devices to large-scale cloud applications.

5.2. Secure Communication Algorithm for Constrained IoT

The following is an explanation of the suggested algorithm for secure communication for constrained IoT. The algorithm contains multiple inputs such as an IoT deviceID, gatewayID, IoT devicePublicKey, and gatewayPublicKey credentials. Numerous data formats, including JSON and extensible markup language (XML), are used in a variety of applications to exchange keys.

Step 1. Key Exchange and Establishment:

deviceSecret = ECC(devicePrivateKey, gatewayPublicKey)

gatewaySecret = ECC(gatewayPrivateKey, devicePublicKey)

sessionKey = lightweight (deviceSecret)

Step 2. IoT Device Data Encryption:

encryptedData = AES_Encrypt(raw_data, sessionKey)

Step 3. Data Decryption:

decryptedData = AES_Decrypt(encryptedData, sessionKey)

Step 4. IoT Device Data Authentication:

signature = ECC_Sign(devicePrivateKey)

Send encryptedData and signature to Gateway

Step 5. Verify Authentication:

isValid = ECC_Verify(devicePublicKey, signature)

if isValid:

    Process decryptedData

else:

    Reject data

Step 6. Session Management:

if sessionExpires:

Repeat Step 1

Update sessionKey

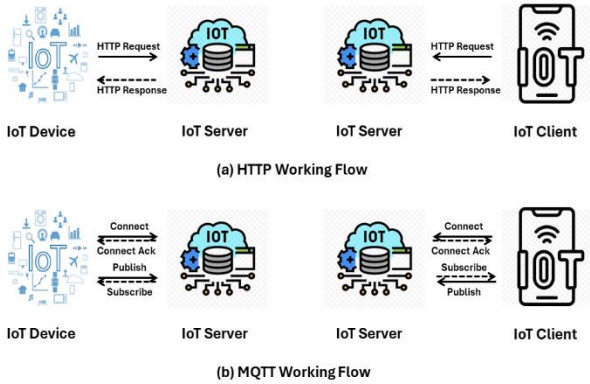

Fig. 2. HTTP and MQTT request/response workflow in the IoT model.

6. Performance Measurement

The design and operation of IoT systems are significantly influenced by the communication protocols employed. The popular protocols HTTP and MQTT are frequently used for facilitating communication between IoT devices and servers [23]. These protocols all have unique request/response workflows that are appropriate for various IoT use cases. Fig. 2 illustrates an HTTP and MQTT request/response workflow in the constrained IoT devices utilizing the suggested secure communication algorithm. Consider a smart home system that has a variety of IoT devices, such light switches, temperature sensors, and security cameras, all of which must effectively convey their status and response to control communication signals [24]. Assuming an optimal network-level latency utilization, the transmission time for an MQTT message might be in the range of 190-213 ms, accounting for both network latency and minimal processing delays. For HTTP, assuming the same network latency but adding the overheads of connection establishment and larger payloads, the transmission time could be around 247 ms or more for small payloads, and significantly higher for larger payloads such as images from a security camera.

Table 1 presents a comparison between HTTP and MQTT protocols. The filed payload indicates the different numbers of messages that could be transmitted over the very same connection. The average data amount transmitted per message is measured in milliseconds as depicted in Fig. 3. The differences in choosing the suitable protocol for the IoT device will be influenced by the communication speed, the cost of the IoT device and the cost of the service.

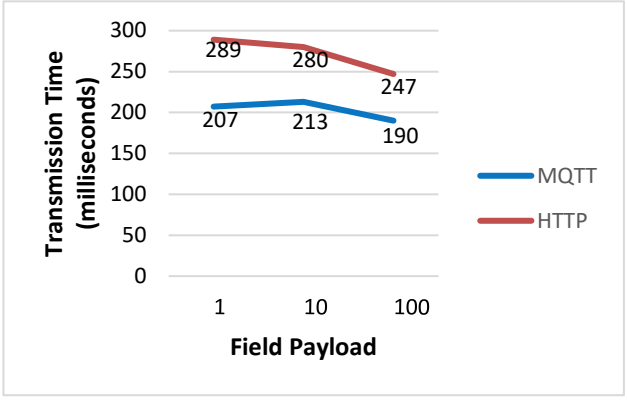

Fig. 3. Average data amounts transmitted per message.

In this scenario, MQTT shows a clear advantage in terms of efficiency and speed for transmitting small, frequent messages typical in IoT applications. HTTP, while more versatile and widely used for web applications, introduces additional overheads that can significantly increase transmission time, especially when new connections are required for each message or when dealing with large payloads. It's important to note that these figures are illustrative and can vary widely in real-world applications. To obtain precise measurements, one would need to conduct specific benchmark tests that take into account the exact conditions and configurations of the devices and networks involved.

7. Conclusions and Outlook

In order to address the challenges associated with traditional learning environments, this paper presented an integrating AES and ECC protocol for IoT security environments. By leveraging both AES for its efficient data encryption capabilities and ECC for secure key exchange and authentication, this integrated approach provides a robust security framework. It ensures that data transmitted between IoT devices and cloud services, as well as data stored within the cloud, is protected against unauthorized access and cyber threats, thereby maintaining confidentiality, integrity, and availability of the information. Achieving a balance between resource constraints and strong security mechanisms will be key to the future of IoT device security in limited circumstances. The methods for safeguarding these small devices will advance along with technology, guaranteeing their secure use in ever-more-important applications.

Table 1. Comparison between HTTP and MQTT protocols

	Average message transmission time (milliseconds)	
Field Payload	***MQTT***	***HTTP***
1	207	289
10	213	280
100	190	247

Acknowledgements

The author extend their appreciation to the deanship of scientific research at Shaqra University for funding this research work through the project number (SU-ANN-2023019).

Conflicts of interest

The authors declare that they have no conflicts of interest.

References

[1] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp.1-13, 2023.

[2] S. Bhattacharjya and H. Saiedian, "A Novel Simplified Framework to Secure IoT Communications," In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 399-406, 2021.

[3] M. Goworko and J. Wytrebowicz, "A Secure Communication System for Constrained IoT Devices—Experiences and Recommendations," *Sensors* 21, 6906, 2021.

[4] J. King and A. I. Awad, "A Distributed Security Mechanism for Resource-Constrained IoT Devices," *Informatica* 40, pp. 133-143, 2016.

[5] A-EM Taha, A. M. Rashwan, and H. S. Hassanein, "Secure Communications for Resource-Constrained IoT Devices," *Sensors* 20, no. 13: 3637, 2020.

[6] A. Nagesh and A. Gopi, "Secure Communication in Internet of Things," *International Journal of Wireless Networks and Communications*, 9(1), pp.13-20, 2017.

[7] G.E.P Kumar, M. Lydia, and Y. Levron, "Security Challenges in 5G and IoT Networks: A Review," In: S. Velliangiri, M. Gunasekaran, P. Karthikeyan (eds) *Secure Communication for 5G and IoT Networks*, Springer, Cham, pp.1-13, 2022.

[8] A. Feijoo-Añazco, D. Garcia-Carrillo, J. Sanchez-Gomez, and R. Marin-Perez, "Innovative security and compression for constrained IoT networks," *Internet of Things*, vol. 24, 2023.

[9] J. Sun, F. Khan, J. Li, M. D. Alshehri, R. Alturki and M. Wedyan, "Mutual Authentication Scheme for the Device-to-Server Communication in the Internet of Medical Things," in *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15663-15671, 2021.

[10] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 17-31, 2015.

[11] V. O. Nyangaresi, A. J. Rodrigues, and A. A. Al Rababah, "Secure Protocol for Resource-Constrained IoT Device Authentication," *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* 14, no.1, pp. 1-15, 2022.

[12] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," *International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, pp. 1-5, 2017.

[13] S. Sasirekha, S. Swamynathan, and S. Suganya, "An ECC-Based Algorithm to Handle Secure Communication Between Heterogeneous IoT Devices," In: A. Kalam, S. Das, K. Sharma (eds) *Advances in Electronics, Communication and Computing*, Lecture Notes in Electrical Engineering, vol 443, Springer, Singapore, 2018.

[14] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," In: N. Meghanathan, S. Boumerdassi, N. Chaki, D. Nagamalai, (eds) *Recent Trends Netw. Secur. Appl*., vol. 89, Springer, Berlin, Heidelberg, pp. 420-429, 2010.

[15] J. Choi *et al.*, "Secure IoT framework and 2D architecture for End-To-End security," *J. Supercomput* 74, pp. 3521–3535, 2018.

[16] J. Kim, Y. Jeon, and H. Kim, "The intelligent IoT common service platform architecture and service implementation," *J. Supercomput* 74, pp. 4242–4260, 2018.

[17] J.R. Arunkumar, S. Velmurugan, B. Chinnaiah, G. Charulatha, M.R. Prabhu, and A.P. Chakkaravarthy, "Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT," *Comput. Syst. Sci. Eng.*, vol. 45, no. 3, pp. 2635-2645, 2023.

[18] S. Li, H. Song, and M. Iqbal, "Privacy and Security for Resource-Constrained IoT Devices and Networks: Research Challenges and Opportunities," *Sensors*, 19(8):1935, 2019.

[19] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *Journal of Network and Computer Applications*, vol.169, 2020.

[20] J. Tournier, F. Lesueur, F. L. Mouël, L. Guyon, and H. Ben-Hassine, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet of Things*, vol. 16, 2021.

[21] M. Dworkin *et al.*, "Advanced Encryption Standard (AES)," Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology,

Gaithersburg, MD, 2001.

[22] H. Kadry, A. Farouk, E. A. Zanaty, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," *Alexandria Engineering Journal*, vol. 71, pp. 491-500, 2023.

[23] K.T.M. Tran *et al.*, "Analysis and Performance Comparison of IoT Message Transfer Protocols Applying in Real Photovoltaic System," *Int. J. Netw. Distrib. Comput.*, 2024.

[24] S. -M. Kim, H. -S. Choi and W. -S. Rhee, "IoT home gateway for auto-configuration and management of MQTT devices," *IEEE Conference on Wireless Sensors (ICWiSe)*, Melaka, Malaysia, 2015, pp. 12-17.