Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Secure Post-Quantum Energy Monitoring System

Y.M. Agus[1], (Student Member, IEEE), G.B. Satrya[2], (Senior Member, IEEE), F. Kurniawan [3], (Student Member, IEEE), M.A. Murti[1]

[1]School of Electronic Engineering, Telkom University, 40257, Republic of Indonesia (e-mail: marselino@ieee.org, arymurti@ieee.org)
[2]School of Applied Science, Telkom University, 40257, Republic of Indonesia (e-mail: gandevabs@ieee.org)
[3]School of Computing, Telkom University, 40257, Republic of Indonesia (e-mail: febrian@ieee.org)

Corresponding author: Gandeva B. Satrya (e-mail: gbs@telkomuniversity.ac.id).

This work was supported in part by Rispro Making Indonesia 4.0 (Invitasi 2020) and PPM Telkom University.

ABSTRACT Internet of things (IoT) has contributed greatly to the development of communication technology in our daily lives. The ease of adopting this technology is strengthened by the increasing number of electronic devices that are interconnected via the internet as shown by the results of previous research. However, the large growth in the number of uses in this system should be in line with the magnitude of concern to take security measures on IoT system communications. For example, cybercrime may be committed against an IoT system that does not use the correct topology and protocol, or data sent from an IoT sensor device is not properly protected. This study reviews the security holes that exist in typology and configuration of IoT Enery monitoring system. Furthermore, this research demonstrates the communication protocols with the NTRU 401 encryption system with encryption time 4.015 times smaller than RSA 2048 encryption systems, NTRU 401 encryption system with a decryption time of 12,200 times smaller than RSA 2048 encryption, the NTRU 539 encryption system, with a 18,519 times smaller encryption time of the RSA 7680 encryption system, the NTRU 539 encryption system with the decryption time is 308.67 times smaller than the RSA 7680 encryption system on IoT devices through real testing.

INDEX TERMS Internet of things, monitoring system, post-quantum encryption, NTRU, secure communication.

I. INTRODUCTION

Internet of Things (IoT) is the newest convergence technology of integrated sensing and transmission capabilities to the things to collect useful data. Devices with IoT capabilities can be utilized to observe and monitor important people or various parameters such as physical, electrical, environmental, etc. This information is then used to examine, recognize, and determine different problems related to daily activities e.g., smart home, smart city, smart factory, smart hospital, smart grid, etc. Managing electrical power to get economical power operation is one of the important problems to face. Intelligent and IoT-enabled power monitoring devices can help to overcome this problem by giving detailed information about electricity consumption. Supervisory control and data acquisition system (SCADA), which is now called an intelligent electrical power management system, exercises to improve cybersecurity and commercial readiness in power plants.

Smart grid can be embraced as a mechanism of various interconnected systems such as virtual power plants, transmission grids, distribution grids, etc. Each one of with its own set of devices and communication technologies, intelligent devices, automated control elements, and algorithms. The hurried deployment and poorly managed smart grid technology could place critical infrastructures vulnerable to cybercrime. On the other hand, due to limited computation power in the client's processors in an IoT system (i.e., smart grid), security provisioning changes from hardware-based to software-based in terms of effectivity and efficiency. Therefore, it is obligatory to implement a lightweight encryption algorithm providing security and authentication to sensitive information while minimizing encryption overhead regarding computation, memory, time, and power.

The status of cybersecurity in the smart grid can be assigned as dangerous when it threatens the confidentiality, integrity, or availability of information and communication technology (ICT). It encourages the organizations involves ensuring the well-function of the smart grids including the

market, customers, operation, and distribution, etc. The future of computation might bring risks to cybersecurity along with the development of quantum computers which is believed to be capable of breaking most of the commonly used encryption systems nowadays. This brought an urgency to develop and examine many candidates of the post-quantum cryptographic systems to prove its data transmission in the energy monitoring systems (EMS).

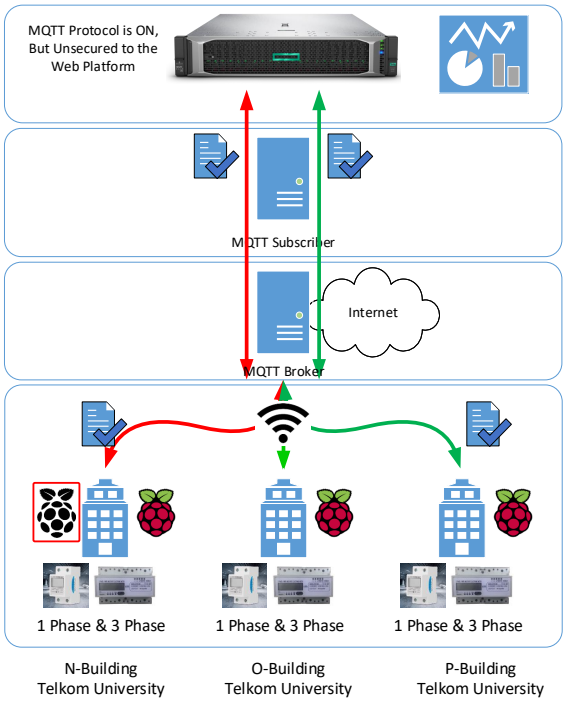

FIGURE 1. IoT Architecture for EMS

The proposed secure energy monitoring system in this research was internally implemented in buildings N, O, and P of Telkom University (as depicted in Fig. 1). The implementation was conducted by using four Raspberry Pi-4 (RPi-4), one AP, and one HPE ProLiant server with HTTPS service. Three of the RPi-4 acted as registered IoT devices while one acted as an unregistered IoT device. The perspective would be an insider attack plan i.e., an attack by an employee or contractor or external party with physical access to the system. From a particular point of view, the adversary might breach the local network when the IoT system uses the default configuration even with the MQTT protocol activated. The IoT system should ban unregistered devices. Further explanation will be discussed in the next section.

To complement models, techniques, and results from previous works, this research aims to contribute the following.

- Giving an appropriate review in IoT security outcome and countermeasures;
- Suggesting a secure post-quantum IoT by using customized MQTT public network;
- Enforcing an optimized MQTT protocol configuration based on the energy monitoring system testbed by adding lightweight cryptography from the physical layer to the application layer;
- Evaluating and benchmarking the post-quantum cryptography with the existing encryption algorithm with respect to the energy monitoring system.

The remaining sections are arranged as follows. Section II reviews IoT security issues and their countermeasures. Section III describes the proposed scheme to improve IoT network security and compares it with the conventional encryption systems. Section IV evaluates details of the unsecure and secure experiments to validate the proposed post-quantum encryption. Finally, Section V highlights the key take-away messages of this research.

II. RELATED STUDIES

A. SECURE IOT MONITORING

Consumption of electrical power is one of the parameters that need to be monitored, but a monitoring system is expensive, complicated, and has insufficient security measures. Jadhav and Rajalakshmi proposed a simple and secure power monitoring sensor with low-cost and Wi-Fi capability to overcome this problem [1]. The power monitoring sensor can be categorized into three subsystems based on its functionality. First is the power acquisition module, second is the processing and communication module, and third is the remote data logging unit. The output of the energy metering module is transferred to the processing module that calculates and calibrates the power value following the stored calibration parameters. Then, the power value is encrypted by using Advanced Encryption Standard (AES). The prototypes of the proposed power monitor sensor were deployed in Academic Block A at the Indian Institute of Technology Hyderabad (IITH).

Because of the vast scale of an IoT system and the limitation on host processor computation power, the security provisioning is changing from software-based to hardware-based security implementation. The function of infrastructure components in preserving and protecting critical components can be handed over to FPGA which can also minimize the negative impacts on these components. Liu et al. have proposed the use of Xilinx Zynq 7000 Series System-on-Chip (SoC) ZC706 prototype board in designing an IoT device [2]. As a defense against threats, the FPGA bitstream is encrypted to protect the devices from bitstream decoding; the system boot image is also encrypted to enhance system security. The FPGA was proven to works as intended via authentication to avoid spoofing and Trojan Horse attacks.

Lightweight encryption algorithms are needed due to resource limitations at the edge nodes of an IoT system. Maitra studied AES both with and without hardware accelerators [3]. The implementation of AES in low resource embedded platforms is not feasible. The memory, power, execution time, and feasibility of the algorithms are analyzed by using XTEA. The experiment results showed that the energy

efficiency and execution time of XTEA on a microcontroller without a dedicated hardware accelerator for AES were almost equivalent to that of a device with a crypto engine. The power consumption of XTEA was around 60 times more efficient than the AES on an 8-bit PIC microcontroller.

A collaboration with a third-party service provider demands trust from both the owner and user of sensor data. The fees for their services are also needed to be paid. Manzoor et al. suggested a blockchain-based proxy re-encryption scheme to address those scalability and trust issues as well as providing an automatic payment [4]. The scheme consisted of seven polynomial-time algorithms: `Setup`, `CertifiedUserKeyGen`, `Encrypt`, `ReKeyGen`, `ReEncrypt`, `Decrypt1`, and `Decrypt2`. After encryption, the IoT data are stored in a distributed cloud. The system shares the collected IoT data by setting up runtime dynamic smart contracts between the sensor and the data user without the trusted third-party involvement. The prototype containing a permission Ethereum blockchain, IoT sensors, and a cloud server for data storage is implemented to verify the proposed system's feasibility.

The newest Low-power wide-area (LPWA) technologies are one of the possible ways to overcome challenges in IoT such as lack of capital, reliability, and security, etc. Fujdiak et al. studied Sigfox as one of the most well-developed LPWA technology and provided its security assessments including the main security flaws [5]. The study compared the performance, security, and cost of three selected cryptographic encryption solutions which were AES, ChaCha, and OTP. The data exchanged between end devices and the SigFox infrastructure is secured likewise those on the internet. The message transmission consumes most of the power.

IoT remote control has to deal with challenges such as scalability, secure communication, and privacy preservation. The conventional solutions (HTTPS) also expose poor scaling problems and privacy concerns. Jin et al. used DNS with privacy preservation to design a novel lightweight and secure IoT remote monitoring mechanism [6]. The remote monitoring utilized the DNS protocol whereas the communication between IoT devices and gateways still used the conventional protocols such as CoAP and MQTT. The communication between IoT devices and the IoT gateway only occurs in the home network for data transmission. The IoT gateway encrypts the received data using asymmetric cryptography and encodes the ciphertext with base64. Then, the base64-encoded ciphertext is registered to the internal DNS server under the name of the IoT device by using the DNS TXT record [4]. It only allows the designated users to receive and decrypt the data which makes it one of the candidates in solving issues in the conventional solutions.

B. POST-QUANTUM IOT

One of the alternatives for the implementation of post-quantum public-key cryptography is the NTRU cryptosystem. Guillen et al. examined the possibility of implementing the NTRU encryption scheme (NTRUEncrypt) in low-resource devices [7]. The study examined four types of NTRUEncrypt implementations on an ARM Cortex M0-based microcontroller and compared the results. The results showed that NTRUEncrypt is applicable in battery-operated devices. C was used to write the code and then its characteristics were modified by using preprocessors directives based on the selected parameter set. The fastest parameter sets for a key generation were EES401EP1 and EES401EP2 with averages of 25.32 and 21.58 million cycles. The slowest parameter set was the EES743EP1 and EES761EP1 with 71.18 and 74.61 million cycles.

Fully homomorphic encryption (FHE) can ensure privacy protection in IoT but it still needs improvement in terms of efficiency. The only acknowledged method for obtaining a pure FHE scheme is Gentry's bootstrapping technique. Song et al. [8] enhanced the bootstrapping technique of Halevi and Shoup (EUROCRYPT 15). The study introduced a definition of "load capacity" and optimized the parameter range of the bootstrapping technique. After that, the ciphertext modulus was generalized to be closing to the more general situations than to a power of two. The tests were conducted on a four-year-old IBM System x3850 server with two 64-bit 4-core Intel Xeon E5450 processors and 35MB L2 cache and 32GB of RAM at 3.0 GHz. Taking into account the theorem, lemma, and corollary, the variant of HS has better efficiency and storage space based which gives a great possibility for applying the proposed method in a much larger environment such as IoT privacy protection.

Public-key cryptosystem holds an important role in IoT security. But, due to their complicated encryption and decryption processes, the classic public-key cryptosystems like RSA and ECC are not applicable for IoT. Shuai et al. [9] introduced a group-based NTRU-like public-key cryptosystem called as Group Theory Research Unit (GTRU). To get high performance in encryption and decryption processes of the GTRU, group G must cater to four conditions in [X]. For the NTRU, min Lf, Lj (chosen p and q) determined the key security of GTRU while Lm (encrypted message) determined the message security of GTRU. The analysis results showed that the proposed GTRU is more secure than NTRU in countering lattice-based attacks. In other words, the proposed GTRU is proven to be a safe and efficient public-key cryptosystem for IoT.

The Internet of Things (IoT) is a growing paradigm in internet network which securely connects billions of devices to the Internet. Other well-known paradigms are quantum computing and the Shor algorithm. Both were proven as threats to most cybersecurity cryptographic protocols. Agus et al. proposed an NTRU-based communication protocol to prevent unregistered IoT devices to connect to the network [10]. The research was carried out using three Raspberry Pi3 B+, one AP, and one server with HTTPS service. The proposed method was deployed in the NTRU-401 and NTRU-593. The results confirmed that NTRU encryption can efficiently be securing end-to-end communication in IoT.

Li et al. [11] proposed a lightweight homomorphic

encryption-based privacy-preserving scheme for Industrial IoT (IIoT). The study looked into the privacy issues between data owners, third-part cloud servers, and data users. The breach of information is an important matter in many critical IIoT systems, such as smart grids, industrial critical systems (ICS)/supervisory control and data acquisition (SCADA) systems, etc. The topics of privacy assurances in critical infrastructures and IoT services have been the focus of recent literature. Li et.al created an air quality monitoring system. It enables remote and non-confident cloud computing to run complex computational on encrypted data and allows data owners and users to justify the decryption accuracy.

Khalid et al. [12] observed the feasibility of deploying various classes of quantum-resistant cryptography schemes such as Lattice-based Cryptography (LBC). The study evaluated and compared the deployment of novel LBC on the low-resources devices in terms of low-power footprint, remote area, compact bandwidth requirements with high performance including low-power FPGAs and embedded microprocessors. The implementation processes were optimized by using specific techniques for Cortex-M4 in assembly. The results showed that the proposed method had the most suitable key sizes compactness and simplicity compared to other quantum-safe schemes. Nevertheless, the LBC schemes still face challenges to be implemented in the real-world system because it needs a larger public key size than the traditional Public key schemes.

III. PROPOSED SCHEME FOR IOT

A. DESIGN ARCHITECTURE

Figure 2 showed that the IoT system consisted of sensors connected to the RPi-4 which have been installed at building N, O, and P at Telkom university. The data collected by the RPi-4 was sent by using the MQTT protocol over the WiFi network from the publisher to the HPE Server. This study suggested adding a message encryption mechanism to the publisher's devices. For the encryption process, this system used the NTRU method. This method was chosen because it has high level of security and low resource consumption. By using this system, the messages sent cannot be imitated by attackers. Although the attacker can guess the message topic sent by the original publishers, but without valid data content, anything sent by the attacker will not be processed by the broker.

B. DEALING WITH PUBLIC AND PRIVATE KEY

At the stage of generating public and private keys, the main function used is the ntru_crypto_ntru_encrypt_keygen in the NTRUEncrypt SDK for C/C++ [24]. Through this function, the public and private keys can be set according to the preferred security standard. In this research, the standards used were RSA-1, RSA-2, NTRU-1, NTRU-2, Saber-1, and Saber-2. The NTRU/Saber encryption system with this standard has low computational load even though it also comes with limited character length that can be encrypted, which is only 16 bytes. The encrypted message as its output has 552 bytes

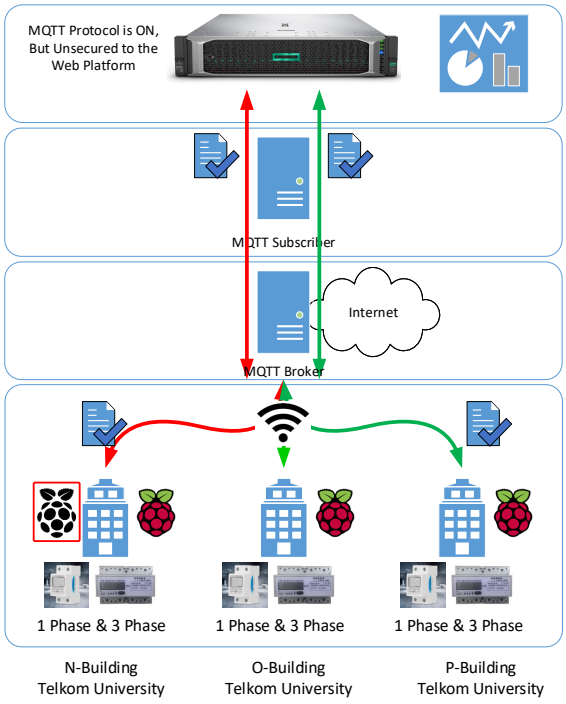

FIGURE 2. Data 1 FASA

of character length. The size of the public and private keys in this study can be seen in Table 1.

TABLE 1. Key Specification

Scheme	Type	Security	Details (Bytes)
AES	Symetric	180	sk : 16 pk : 1024 C : 1024
Fernet	Symetric	180	sk : 1024 pk : 1024 C : 1024
RSA 3072	Asymetric	180	sk : 1678 pk : 450 C : 1024
RSA 7680	Asymetric	180	sk : 5972 pk : 1404 C : 1024
NTRU 401	Asymetric	180	sk : 557 pk : 607 C : 1024
NTRU 593	Asymetric	180	sk : 821 pk : 891 C : 1024
SABER	Asymetric	180	sk : 1024 pk : 1024 C : 1024
Light SABER	Asymetric	180	sk : 1024 pk : 1024 C : 1024

C. ENCRYPTION IN PUBLISHER

In this stage, the publisher devices carried out the encryption process by using the function ntru_crypto_ntru_encrypt in

Algorithm 1 IoT Encryption for the Publisher

```
INITIALISE message;
INITIALISE publisher_ID;
INITIALISE ciphertext_array;
Function: cryptosystem (message,key)        ▷ RSA/NTRU/Saber
Function: MQTT (ciphertext_array)
while true do
    Ciphertext = base64(concatenate(ciphertext_array))
    final_data = concatenate(publisher_ID + splitter + Cipher-
text)
    CALL ← MQTT(final_data)
end while
```

the NTRUEncrypt SDK for C/C++ [24] . The encryption process was conducted by using the public key generated in the previous stage. The data was sent through the MQTT protocol using the library paho-mqtt in the Phyton 3.5 programming language. The function used from the library paho-mqtt is below.

Algorithm 2 IoT Decryption for the Subscriber

```
INITIALISE ciphertext_array = MQTT();
INITIALISE plain_array;
Function: cryptosystem_decryption(ciphertext)        ▷
RSA/NTRU/Saber
while true do
    plain_array = cryptosystem_decryption (base64 (cipher-
text_array))
    if plain_array != "ERROR": then
        Store_data(plain_array)
    else
        Record_Error(Device_ID)
    end if
end while
```

D. DECRYPTION IN SUBSCRIBER

The message received by the phyton script was then forwarded to the program in C language which will begin the decryption process by using function ntru_crypto_ntru_decrypt. If the encryption process succeeded, the received message will be sent to the device's database, otherwise it will be deemed invalid.

IV. EVALUATION AND ANALYSIS

This section discusses the testing and comparison of the encryption time consumption of RSA 2048, RSA 7680, NTRU 401, NTRU 539, Saber-1, and Saber-2 on the system explained in the previous chapter along with the reliability tests of the Saber-2 encryption system when implemented on the MQTT protocol. The tests to measure the encryption time consumption were carried out on IoT RPi-4 devices while the encryption reliability tests on the MQTT protocol were carried out on RPi-4 publisher devices, raspberry pi broker devices, and desktop subscriber devices. The test was done by calculating the encryption speed of several encryption standards on RPi-4 devices. The object to be encrypted was a file containing electrical energy monitoring for 1-phase and 2-phase voltages at building N,O, and P at Telkom University.

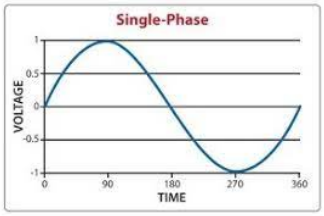

FIGURE 3. Data 1 FASA

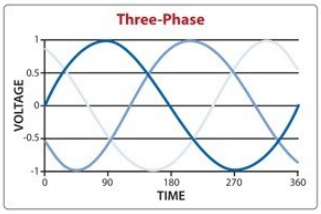

FIGURE 4. Data 3 FASA

A. 1-PHASE ENCRYTION & DECRYPTION

The testing was taken by inputting the contents of the files in Table IV-1 to each encryption system. The calculation of the encryption and decryption time was run before the encryption and decryption functions were called on the main source code.

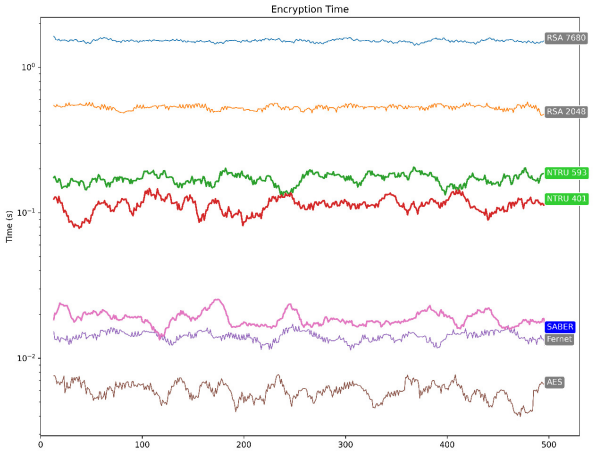

FIGURE 5. Encryption Time

B. 3-PHASE ENCRYTION & DECRYPTION

The testing was taken by inputting the contents of the files in Table IV-1 to each encryption system. The calculation of the encryption and decryption time was run before the encryption and decryption functions were called on the main source code.

C. SECURITY PERFORMANCE EVALUATION

This research tested and analyzed on the data transmission security system from the Publisher to the Subscriber. The

TABLE 2. Encryption time *(in ms)* between *publisher* and *subscriber*

Plaintext (bytes)	RSA-2048	RSA-7680	NTRU-401	NTRU-593	Saber-1	Saber-2
1	0.301	2.503	8.551	26.251	0.781	1.336
...	...	...	...	...	...	...
6	0.240	1.579	3.100	26.198	0.903	1.492
7	0.192	1.598	3.088	26.135	0.832	1.424
8	0.211	1.608	3.103	26.158	0.795	1.406
9	0.246	1.653	3.076	26.414	0.800	1.413
10	0.299	2.259	3.098	26.228	0.814	1.371
11	0.226	1.626	3.105	26.173	0.820	1.462
12	0.215	1.670	3.115	26.187	0.819	1.427
13	0.222	1.640	3.044	26.172	0.838	1.416
14	0.206	1.578	3.077	26.216	0.814	1.435
15	0.196	1.678	3.081	26.150	0.796	1.356
16	0.23	1.604	3.072	26.148	0.812	1.411

TABLE 3. Decryption time *(in ms)* between *publisher* and *subscriber*

Plaintext (bytes)	RSA-2048	RSA-7680	NTRU-401	NTRU-593	Saber-1	Saber-2
1	0.113	1.981	47.117	1348.226	3.143	4.358
...	...	...	...	...	...	...
6	0.152	1.115	38.960	1331.325	3.270	4.358
7	0.101	1.110	38.920	1360.31	3.184	4.339
8	0.098	1.312	38.883	1378.027	3.239	4.331
9	0.246	2.042	53.003	1386.334	4.249	5.138
10	0.097	1.137	39.011	1361.078	3.888	4.385
11	0.100	1.112	39.117	1361.872	3.206	4.437
12	0.098	1.172	39.628	1369.104	3.125	4.438
13	0.146	1.202	38.869	1360.975	3.222	4.380
14	0.103	1.124	39.739	1361.875	3.238	4.416
15	0.103	1.139	38.844	1374.493	3.229	4.367
16	0.149	1.404	49.914	1397.346	4.229	5.221

FIGURE 6. Decryption Time

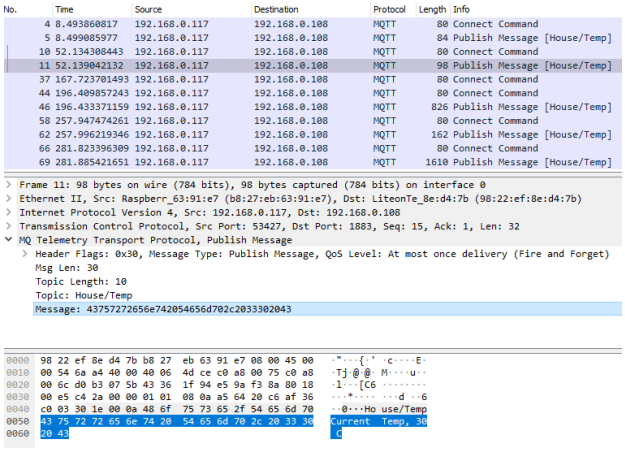

FIGURE 7. Analyzing for the conventional topology

Publisher used 1/3 Phase of data power at the N, P, and O Telkom University buildings while the Subscriber used IEMS server which was also sent via Telkom Digital Service Division DDS. Based on Shodan's data as of June 2021, there are still 134,879 brokers or IoT devices in the world that use port `1883`, as known as the default port for the MQTT protocol with South Korea being the largest user. Therefore, this research also discussed four types of attacks against IEMS systems for End-to-End communication security.

Based on Figure 2, the publishers send data to the subscriber through a broker using the MQTT protocol based on the topics that have been created by the publishers. If the broker and subscriber are streamed through the Internet, it is very possible that several attacks will occur which could be harmful to the whole system. Figure 2 also shows the possibilities of attackers act as publishers or subscribers. The attacks tested on this IEMS are data privacy, authentication, data integrity, and DDoS mitigation, as explained below.

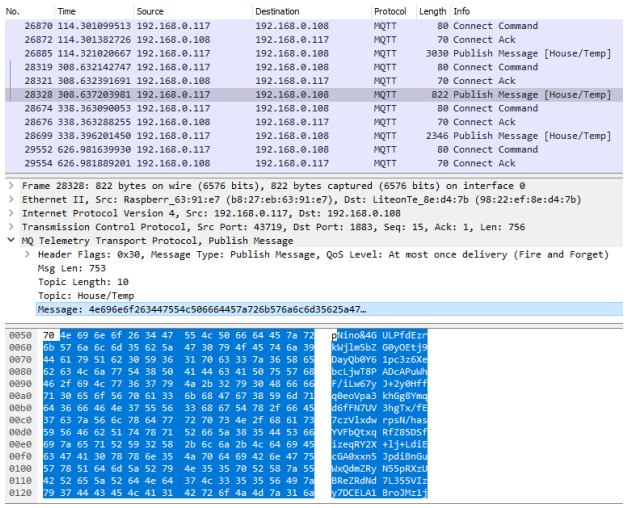

FIGURE 8. Analyzing for the secured topology

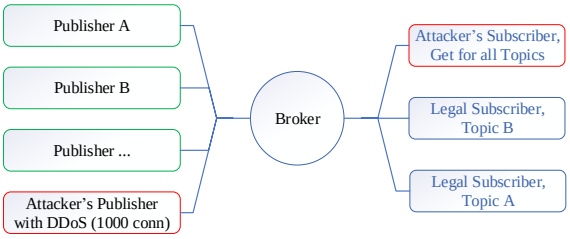

FIGURE 9. Device threats and attack scenarios

1) Attack to Data Privacy

In a scenario where the attacker knows a network with publishers and being in the same network, the attacker can do sniffing on that network. Figure 3 is the evidence that the attacker can perform sniffing on the traffic that passes through the network. As can be seen in the screenshot, the data sent by the publisher, *"This data should've been hidden"*, should not be seen by unregistered publishers.

To prevent that scenario from occurring, the payload (data content) must be secured using encryption algorithms. In the implementation, this research used several comparison algorithms such as Fernet, AES, and RSA. However, the example shown in Figure 4 shows the use of a post-quantum cryptography algorithm, namely NTRU. As seen in Figure 4, the attacker (publisher) could not see the information clearly, all communications from publishers to subscribers were encapsulated with a NTRU post-quantum cryptography header.

2) Attack to Authentication

Based on Figure 5, the subscribers will be able to decrypt if the keys exchanged between publishers and subscribers are matched. If the keys match, then communication can be carried out according to the payload (data content) sent by the publisher. Then if the keys match, the ciphertext data can be changed and read by the subscriber into plaintext again.

Based on the first authentication attack scenario, the attacker tried to impersonate an existing IoT device (publisher). Then the attacker also tried to send a tampered payload containing the original payload to be sent to the subscriber. Figure 6 shows an error: incorrect padding, which occurs when the publisher tries to enter the subscriber and sends the payload. The size of the plaintext data sent by the publisher will not have effects on the ciphertext, because it was wrapped again with the base64 encoding method.

The second authentication attack scenario is anyone who tries to subscribe to the network traffic. Legitimate subscribers will only receive an encrypted payload. Without using the correct private key, the incoming data will be considered as babbles without content. Figure 7 shows that unauthorized subscribers will receive data that is completely incomprehensible. This scenario is made to deal with attackers originated from the subscribers.

3) Attack to Data Integrity

Any changes made by the attacker to a valid encrypted payload will damage its structures. This can happen when the attacker (publisher) performs sniffing on the traffic and retransmits the modified payloads to subscribers which could be malicious. On the subscriber's side, the decryption process on the malicious payloads will fail because it was modified without the correct public key. The effect of this process will damage the payload structures and the data will be considered invalid.

4) DDOS Mitigation

Firewall rules on broker device

Whitelisted devices success transmit

Non whitelisted devices failed transmit

Broker firewall log on blocked tranmission

Whitelist as shown in figure 9 is used to overcome DDoS on the broker's devices. In other words, only devices on the whitelist are allowed to transmit with the MQTT protocol through the broker as shown in figure 10. While figure 11 shows the attacker, who was not on the list performing the DDoS and the devices got automatically rejected with the message, *"Error: Connection timed out"*. Furthermore, on the firewall side, a schedule can be made to carry out periodic monitoring to show the firewall log on the broker as shown in Figure 12.

D. DISCUSSION

The proposed design was verified by evaluating the existing benchmark encryption techniques e.g., RSA-2048, RSA-7680, NTRU-401, NTRU-593, Saber-1, and Saber-2. The detailed key specifications for those encryption algorithms are explained in Table 1. The performance evaluation for those encryption algorithms is calculated by using the encryption time *(as shown in Table 2)* and the decryption time *(as shown in Table 3)*. For the asymmetric encryption, the results

showed that NTRU-401 and NTRU-593 outperform the existing encryption (RSA-2048 and RSA-7680). Considering the post-quantum computing, this research recommends adopting the NTRU encryption for general IoT systems (ARMv8-A) even though Saber-1 still has an acceptable delay (< `100ms`) i.e., `1.321ms`.

Meanwhile, the reliability of the security system from post-quantum cryptography was determined by attacking data privacy, authentication, data integrity, and DDoS. From these 4 types of attacks, the proposed system is proven to be able to fend off SCADA system cyber-attack and cyber-warfare. Post-quantum cryptography can also help to defend against those risks, protect critical applications and data, and recover from breach or failure.

V. CONCLUDING REMARKS

The conclusion that can be drawn from the tests and analyzes results is that the IoT data delivery system via the MQTT protocol with RPi-4 devices is feasible to be implemented. The NTRU and Saber encryption systems can perform the encryption process in less than 100 ms on messages sent via the MQTT protocol. The data security system in the IoT using Saber encryption proves that the use of an encryption system with a high level of security is applicable for inexpensive IoT devices. Messages with 1-phase and 3-phase lengths can be fully encrypted by using the padding feature and sent via the MQTT protocol. Further development of the proposed system in this research, which is an IoT data delivery system through the MQTT protocol with inexpensive microcomputer devices, can be a solution to make IoT technology more affordable for the general public. As for recommendations for future research, researchers can try to apply other encryption systems on the IoT with the MQTT protocol. This encryption system should be applied to the IoT involved in the delivery of important and personal data, such as hospitals, governments, and the military.

ACKNOWLEDGMENT

This work was supported in part by Rispro Making Indonesia 4.0 (Invitasi 2020) and PPM Telkom University.

REFERENCES

[1] A. R. Jadhav and P. Rajalakshmi, "Iot enabled smart and secure power monitor," in *2017 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 2017, pp. 1–4.

[2] Y. Liu, J. Briones, R. Zhou, and N. Magotra, "Study of secure boot with a fpga-based iot device," in *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2017, pp. 1053–1056.

[3] S. Maitra, D. Richards, A. Abdelgawad, and K. Yelamarthi, "Performance evaluation of iot encryption algorithms: Memory, timing, and energy," in *2019 IEEE Sensors Applications Symposium (SAS)*. IEEE, 2019, pp. 1–6.

[4] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure iot data sharing," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 99–103.

[5] R. Fujdiak, P. Blazek, K. Mikhaylov, L. Malina, P. Mlynek, J. Misurec, and V. Blazek, "On track of sigfox confidentiality with end-to-end encryption," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ser. ARES 2018. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3230833.3232805

[6] Y. Jin, M. Tomoishi, K. Fujikawa, and V. P. Kafle, "A lightweight and secure iot remote monitoring mechanism using dns with privacy preservation," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019, pp. 1–2.

[7] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl, and J. Sepulveda, "Towards post-quantum security for iot endpoints with ntru," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*. IEEE, 2017, pp. 698–703.

[8] W.-T. Song, B. Hu, and X.-F. Zhao, "Privacy protection of iot based on fully homomorphic encryption," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–7, 2018.

[9] L. Shuai, H. Xu, L. Miao, and X. Zhou, "A group-based ntru-like public-key cryptosystem for iot," *IEEE Access*, vol. 7, pp. 75 732–75 740, 2019.

[10] Y. M. Agus, M. A. Murti, F. Kurniawan, N. Cahyani, and G. Satrya, "An efficient implementation of ntru encryption in post-quantum internet of things," in *2020 27th International Conference on Telecommunications (ICT)*, 2020, pp. 1–5.

[11] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things," *IEEE Internet of Things Journal*, pp. 1–9, 2021.

[12] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based cryptography for iot in a quantum world: Are we ready?" in *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 2019, pp. 194–199.

YOSAFAT M. AGUS (Student Member, IEEE) pursuing bachelor's degree in Informatics Engineering in Telkom University, Bandung, Indonesia. Currently active as a researcher in Telkom University affiliated with School of Computing at Telkom University focusing on post-quantum network security and artificial intelligence approach of cybersecurity. He is also a member of the Forensic and Security Laboratory of Telkom University since 2018 and algorithm designer in Vezpal as a financial organization leading in artificial intelligence-based decision making and prediction. His research includes internet of things, post-quantum cryptography, artificial intelligence based security system, and deep learning.

GANDEVA BAYU SATRYA (S'12–M'18–SM'19) received Ph.D in security communication for next-generation networks, graduated from IT Convergence Engineering, School of Electronic Engineering, Kumoh National Institute of Technology, South Korea in December 2018. He has been a lecturer and researcher at School of Applied Science in Telkom University, Bandung, Indonesia since February 2011 until now. From June 2008 to December 2010, he was a BSS Engineer at PT. ZTE Indonesia, Jakarta, Indonesia.

He is also a member of Research center of Internet of Things (RC IoT) at Telkom University since 2019 and a member of IEEE since 2012. He is currently appointed as Technical Activities Coordinator in the IEEE Communication Society (ComSoc) Indonesian Section and as Researcher in Telecom Infra Project. His research interests include routing protocol, packet scheduling, security communication in next-generation networks, and applied deep learning.

ARY MURTI (Student Member, IEEE) pursuing bachelor's degree in Informatics Engineering in Telkom University, Bandung, Indonesia. Currently active as a researcher in Telkom University affiliated with School of Computing at Telkom University focusing on post-quantum network security and artificial intelligence approach of cybersecurity. He is also a member of the Forensic and Security Laboratory of Telkom University since 2018 and algorithm designer in Vezpal as a financial organization leading in artificial intelligence-based decision making and prediction. His research includes internet of things, post-quantum cryptography, artificial intelligence based security system, and deep learning.