Review Article

Security Performance of LoRaWAN Servers using Advanced Encryption Standard

Puput Dani Prasetyo Adi[1*]

[1]National Research and Innovation Agency (BRIN) Republic of Indonesia, Jakarta, Indonesia

*Corresponding author: pupu008@brin.go.id

Abstract:

One of the essential components in LoRaWAN is managing the server with all existing components, including Device Management, Data forwarding, Network security, and real-time network monitoring. It is necessary to manage the uplink and downlink of the LoRaWAN server and maintain the quality of data transmission from the LoRa end node to the LoRaWAN server. Depending on the service provider, the LoRaWAN Server provides space for payload, uplink, and downlink data. How many times in a day, week, month, or even year? This discussion depends on the LoRaWAN server provider. Some are open sources, and some provide free uplink and downlink services. Settings on the LoRaWAN Server will determine how much data will enter the server or the network size. Security is also an essential parameter, e.g., encryption or authentication, supported by the feature requirements used on the server, which will determine the type of communication that LoRa will apply, for example, multi-communication or analysis data. Centralized management, Security, scalability, and cost-effectiveness are essential parameters if LoRaWAN is managed well.

Keywords: Device Management, Security, LoRaWAN, Network Monitoring, LoRaWAN Server

Citation: Adi, P.D.P" A Review of LoRaWAN Performance Server Advanced Security". *Iota*, **2023**, ISSN 2774-4353, Vol.03, 03. https://doi.org/10.31763/iota.v3i3.632

Academic Editor : Pranolo.A

Received : May, 25 2023

Accepted : June, 16 2023

Published : July, 06 2023

1. INTRODUCTION

The development of the IoT world continues to overgrow. More than 15.14 Billion IoT devices will be connected worldwide by 2023. Meanwhile, 730 Million LoRaWAN devices are connected worldwide. So this is an excellent market for continuing to develop Low Power Consumption devices, high scalability [33] and building effective and inexpensive tools or devices in the infrastructure. Then what is the role of Security in an extensive IoT network [34]? The excellent connectivity of IoT devices will cause many factors to hinder and yield losses, for example, Criminal Action or Hacking which hacks IoT data with low Security, making it easy to hack. From the data provided at The Things Network seminar by Cesar Cerrudo, the results of Criminal Action through hacking can reach $ 445-608 billion or 0.59% - to 0.8% of GDP. Therefore, a security system is needed for LoRaWAN [35], e.g., on NwkSKey and AppKey, such as the AES for LoRaWAN mechanism [20], a method or mechanism for making a more accurate system is used with a Machine Learning approach [1].

LoRaWAN or LoRa End-Nodes Quality of Service (QoS) conditions are determined by propagation [2,3,4,32] to the LoRa Gateway, and this defines a quality point to what extent this location is determined by SF [37], BW LoRa end-nodes, quality parameters, bit- rates, packet loss has been resolved in previous research [8,13,16,17,18,25,30]. LoRaWAN servers are essential components in the LoRaWAN architecture, including end nodes, LoRaWAN gateways [21,22], network servers, and application servers. In the LoRaWAN management system, there are three classes, i.e., Class A, B, and C; Class A talks about the function of the LoRa End Node, which communicates with the server directly. In class A, there is a significant latency because the percentage of the uplink process is not balanced with the downlink. In the uplink process, the end device directly transmits the data or payload to the LoRaWAN server. Still, it does not immediately return data or downlink to end devices from LoRaWAN Server. Class B on the LoRaWAN network [23] talks about the transmitting data process between the beacons, which is indicated by the difference in transmit data time (ms). While class C LoRaWAN is communication on the LoRaWAN Server, which shows sensor data in real-time and continuously, so it requires the most significant power consumption of the other two classes.

In this article, we discuss in detail the LoRaWAN server and in detail discuss device management, data forwarding, security [9,10,11,12,14,15], network monitoring, and details on the Advanced Encryption Standard (AES) of the LoRaWAN server. Device management is the process of The server keeping track of all devices on the network, including their unique identifiers, current state, and data usage. Data forwarding process the server forwards data between devices and applications. Security is when the server securely transmits data between devices and applications. And network monitoring is the condition of the server monitoring the network whether there are problems such as interference [39] or outages.

Several different LoRaWAN servers are available, both commercial and open source. The choice of the server will depend on the network's specific requirements. Some applications that can be used as LoRaWAN servers include TTn or The Things Network. TTn is a global application that is open and non-profit. In several studies conducted, TTn has been able to provide high performance, especially in terms of real-time data processing. The device or devices used are RF95 or RF96, with a module frequency of 920 MHz [40] or 915 MHz LoRa [36]. Besides The Things Network (TTn), is ChirpStack, and activity. Several LoRaWAN application servers that provide analysis, such as ambidata.io, tago.io, and The thingspeak [41], are more familiar to students or the developer community. The Things Network: The Things Network is a global, open, and non-profit LoRaWAN network. It offers various services, including a LoRaWAN server, a gateway, and a data storage solution. ChirpStack: ChirpStack is an open-source LoRaWAN server that is available for free. It is a popular choice for small and medium-sized networks. Actility: Actility is a commercial LoRaWAN server provider. It offers a variety of features, including support for multiple networks, Security, and data analytics. When choosing a

LoRaWAN server [43], it is essential to consider the following factors, [1]: The network size will determine the amount of data that needs to be processed by the server. [2] The security requirements: The network may have specific security requirements, such as encryption or authentication. [3] The features required: The network may require specific features, such as support for multiple networks or data analytics. The cost of a LoRaWAN server will vary depending on the features and the network size. Commercial servers are typically more expensive than open-source servers.

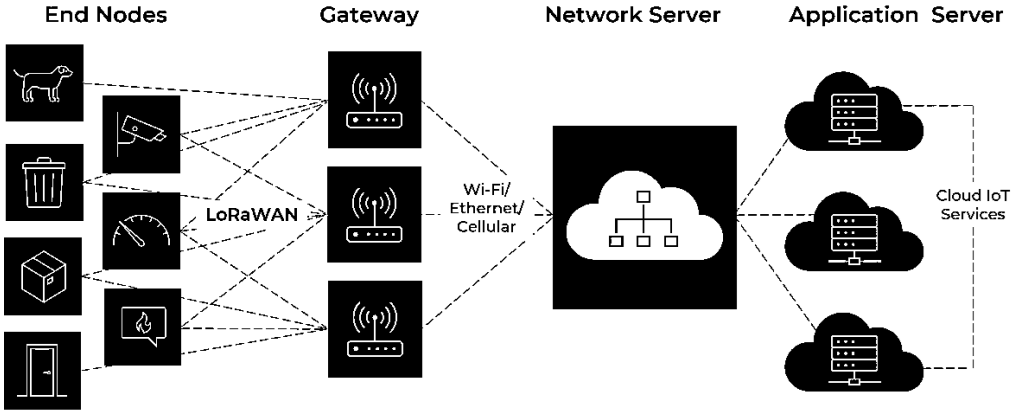

Figure 1. LoRaWAN Network Architecture (source: www.cardinalpeak.com)

2. THEORY

2.1 LoRaWAN Network Architecture

Furthermore, the essential thing is to understand the LoRaWAN Network Architecture. Figure 1 shows the LoRaWAN Network Architecture, with four main parameters: End Nodes, Gateway, Network Server, and Application Server. At End Nodes, there are sensors used for monitoring moving and static objects, for example, Pet monitoring, Garbage monitoring, speed car monitoring, smart home, etc., on the Gateway side, tasked with receiving data from end-nodes which will be forwarded to the Network Server. While the Application Server is an Application Programming Interface (API) configuration whose job is to display real-time data from sensors or End Nodes. Here are some of the benefits of using a LoRaWAN server [5]; among others are [1] Centralized management: A LoRaWAN server provides centralized network management, making it easier to configure and maintain. [2] Security: A LoRaWAN server can help to secure the network by encrypting data and authenticating devices [41]. [3] Scalability: A LoRaWAN server can be scaled to meet the needs of a growing network. And [4] Cost-effectiveness: A LoRaWAN server can be a cost-effective solution for small and medium-sized networks.

Moreover, Settings on the LoRaWAN Server [6] will determine how much data will enter the server or the size of the network, and Security is also an essential parameter, namely encryption or authentication, supported by the feature requirements used on the server, which will determine the type of

communication that LoRa will apply, for example, multi-communication or analysis data. Centralized management, Security, scalability, and cost-effectiveness are essential parameters if LoRaWAN is managed well [5,6,7].

Table 1. Difference Feature between Network Server and Application Server LoRaWAN

Feature	Network Server	Application Server
Purpose	Manages the network infrastructure	Processes data from devices and provides applications with access to that data
Tasks	Authenticates devices, manage channels, forwards data between devices and gateways and performs network-level Security.	Processes data from devices, stores data, provides APIs for applications to access data, and performs application-level Security.
Location	Typically hosted in the cloud	Typically hosted in the cloud or on-premises

Figure 2 shows an example of a Gateway that can connect to The Things Network Application Server. This is another reference, besides the one we used in building the LG01-P-based LoRaWAN using 915 MHz Dragino LoRa end nodes [8].

Figure 2. The Things Gateway (source: The Things Network)

2.2 Advanced Encryption Standard (AES) Algorithm

AES LoRaWAN Server is a type of LoRaWAN server that uses the Advanced Encryption Standard (AES) algorithm to encrypt data before it is transmitted over the LoRaWAN network [19]. AES is a robust encryption algorithm that is considered to be very secure [42]. The AES algorithm is a symmetric encryption algorithm, meaning the same key is used to encrypt and decrypt data. This makes it very efficient for LoRaWAN devices with limited processing power and memory. The AES LoRaWAN Server uses the following steps to encrypt data: The server generates a unique encryption key for each device. The server encrypts the data using the encryption key. The encrypted data is then transmitted over the LoRaWAN network. When the encrypted data reaches the receiver, the following steps are taken to decrypt it: The receiver uses the

encryption key to decrypt the data, and The decrypted data is then available to the application. The AES LoRaWAN Server provides many benefits, and The AES algorithm is a strong encryption algorithm that is considered very secure. This helps to protect data from unauthorized access. The AES algorithm ensures that the data is not tampered with during transmission. The AES algorithm is a very efficient encryption algorithm that does not significantly impact the performance of the LoRaWAN network.

The AES LoRaWAN Server is a good choice for applications requiring high data security and integrity levels. Here are some additional details about the AES LoRaWAN Server: The encryption key is a unique key used to encrypt and decrypt data. The encryption key is generated by the server and is stored on the server. The encryption key is never sent over the LoRaWAN network. The server encrypts data using the encryption key. The encryption process is performed in the background and requires no user intervention. The receiver uses the encryption key to decrypt data. The decryption process is also served in the environment and requires no user intervention. LoRaWAN security is based on three pillars: All data sent over LoRaWAN is encrypted using a symmetric encryption algorithm, such as AES. This ensures that only authorized parties can read the data. Each LoRaWAN device has a unique identifier to authenticate it to the network. This prevents unauthorized devices from connecting to the network. The LoRaWAN network is secured using various techniques like network segmentation and intrusion detection. This helps to protect the network from attacks. Data encryption, All data sent over LoRaWAN is encrypted using a symmetric encryption algorithm, such as AES. This ensures that only authorized parties can read the data.

The encryption key is shared between the LoRaWAN device and the network gateway. The key is generated randomly and is never sent over the air. This helps to prevent unauthorized parties from obtaining the key. Device authentication, Each LoRaWAN device has a unique identifier used to authenticate it to the network. This prevents unauthorized devices from connecting to the network. The device identifier is generated by the manufacturer and is burned into the device's firmware. The network gateway uses the device identifier to authenticate the device when it connects to the network. Network security, The LoRaWAN network is secured using various techniques, such as network segmentation and intrusion detection. This helps to protect the network from attacks. Network segmentation is a technique that divides the network into smaller segments. This makes it more difficult for an attacker to compromise the entire network. Intrusion detection is a technique that monitors the network for suspicious activity. This helps to detect and prevent attacks. Moreover, there are several parameters, namely Uplink and Downlink counters (16 bit), messages ACKs (optional), Integrity Control (NwKSKey), Symmetric end-to-end cipher (AppSKey), and Activation: ABP or OTAA.

AES 128-bit LoRa is a security protocol used in LoRaWAN networks [29] to encrypt and authenticate data transmissions. It uses the Advanced Encryption Standard (AES) algorithm [26], which is a symmetric key encryption algorithm [27] that is considered to be very secure. AES 128-bit LoRa uses a 128-bit key [24,28], a very long and complex key that makes it difficult to crack.

The AES 128-bit LoRa security protocol is implemented in LoRaWAN devices in two ways:

- Data encryption: AES 128-bit LoRa encrypts all data transmitted over a LoRaWAN network. This includes data such as sensor readings, device commands, and network control messages.
- Data authentication: AES 128-bit LoRa authenticates all data transmitted over a LoRaWAN network. This ensures that the data has not been tampered with or altered in transit.

Moreover, the benefits of using AES 128-bit LoRa: High Security: AES 128-bit LoRa is a very secure protocol that uses a very long and complex key, which makes it very difficult to crack. Low overhead: AES 128-bit LoRa has a very low overhead, meaning it does not consume much power or bandwidth. This is important for LoRaWAN devices, which are often battery-powered and have limited bandwidth. Easy to implement: AES 128-bit LoRa is easy to implement in LoRaWAN devices. This is because it is a standard protocol supported by many LoRaWAN development kits and platforms. Overall, AES 128-bit LoRa is a secure and efficient security protocol well-suited for use in LoRaWAN networks [31].

2.3 ABP and OTAA LoRaWAN

ABP and OTAA are two different methods for activating a LoRaWAN device on a network. ABP stands for Activation by Personalization. With ABP, the device's DevAddr, NwkSKey, and AppSKey are pre-configured on both the device and the network. This makes it easy to get started with ABP but also less secure, as the same keys are always used.

OTAA stands for Over-the-Air Activation. With OTAA, the device generates a random DevAddr and uses a join request to obtain NwkSKey and AppSKey from the network. This makes OTAA more secure but requires an extra step during activation. In general, OTAA is recommended for most applications. It is more secure and provides better flexibility, as devices can be moved to different networks without reprogramming. However, ABP may be a better choice for applications where Security is not a significant concern or where the extra step of activation is not desired.

Table 2. Difference Feature between ABP and OTAA

Feature	ABP	OTAA
Security	Less secure	More secure
Flexibility	Less flexible	More flexible
Setup	Easier to set up	More difficult to set up

3. METHOD

3.1 Architecture and Flowchart of LoRaWAN Security

In this chapter, we learned that Security on the LoRaWAN server has two core parameters: NwkSKey and AppSKey [38]. In LoRaWAN Server v.1.0.3, the architecture of the security system is shown in Figure 3. KEY from End Devices to Network Server has a key, and API access has a key to share a data graph in the application server. In LoRaWAN v.1.1 in Figure 4, developed with a join server system, namely AppKey and NwkKey deserver in NS and accessible at Gateways to End Devices. These two architectural drawings have the disadvantage that the key is shared everywhere, so the Security is very weak. The AES algorithm is also very secure. This algorithm has undergone extensive cryptanalysis, and no vulnerabilities were found. The AES algorithm can be written in the following Flowchart in Figure 5.

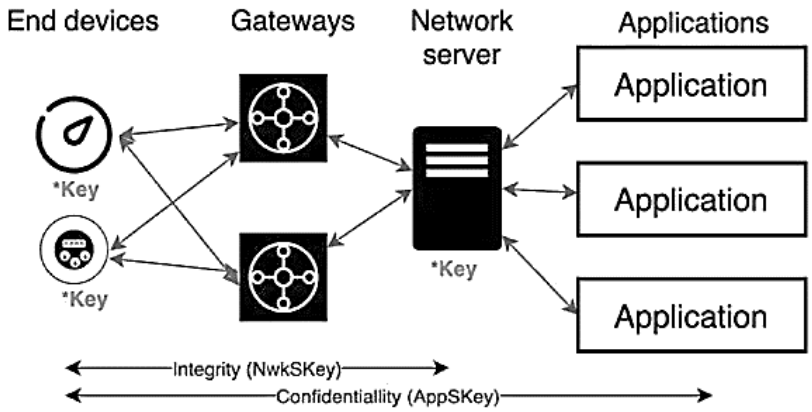

Figure 3. Session Keys and Function in LoRaWAN v.1.0.3 (source: The Things Network)

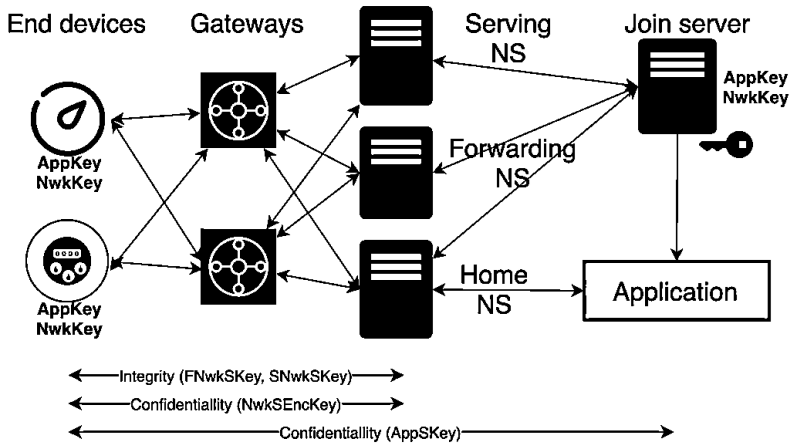

Figure 4. Session Keys and Function in LoRaWAN v.1.1 (source: The Things Network)

The three parameters of Security are Authentication, Encryption, and Integrity protection. [1] Each LoRaWAN device is authenticated with a unique identifier and key. This prevents unauthorized devices from connecting to the network. [2] Encryption is All data that is transmitted over the LoRaWAN network is encrypted. This prevents unauthorized parties from reading or modifying the data. And Integrity protection, The integrity of all data sent over the LoRaWAN network is protected. This prevents unauthorized parties from tampering with the data. The following is an example of the coding used on the LoRaWAN Server: AES (Advanced Encryption Standard). The security process in LoRaWAN depends on several parameters, including Device Manufacturer, Device Labels, Device firmware, memory, Device/Infrastructure deployment technicians, Hardcoded Open source code, Mobile Apps for configuration or deployment, Excel sheets, files, Network Servers, Join servers (Service Providers), and Support forums.

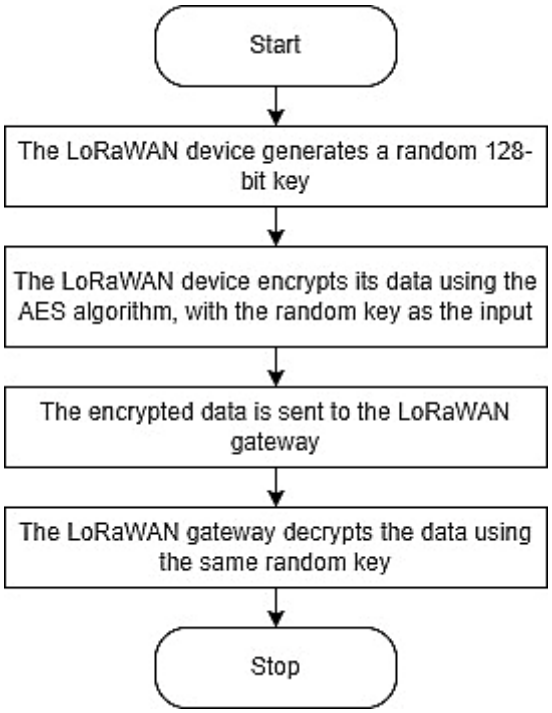

Figure 5. Flowchart of AES Algorithm LoRaWAN

3.2 OTAA Procedures

The process of transmitting data from LoRa End devices using OTA Activation or Over Air Activation can be seen in Figure 6, where LoRa end devices have an Appkey; the first step is to join Request APP EUI [Dev EUI[Dev Nonce]] to Network Server, which is also equipped with an AppKey on the Network Server, from the Network Server, End Device Authentication Session key generation (Nwk_Skey, App_SKey), SKey is Session Key. After that, the third process is Join Accept E (App Key, [App Nonce [Net ID | Dev Addr | DL Setting | Rx Delay |CF List|]); after LoRa End Devices is connected to the Network

Server, there will be a fourth process, Transfer App_Skey to Application Server, at this stage Session key generation (Nwk_Skey, App_SKey) is the final stage.

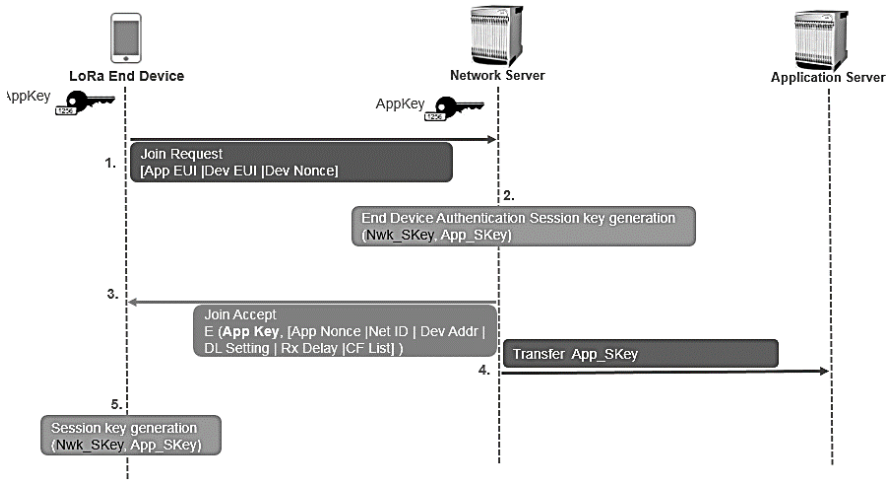

Figure 6. OTA Activation procedures

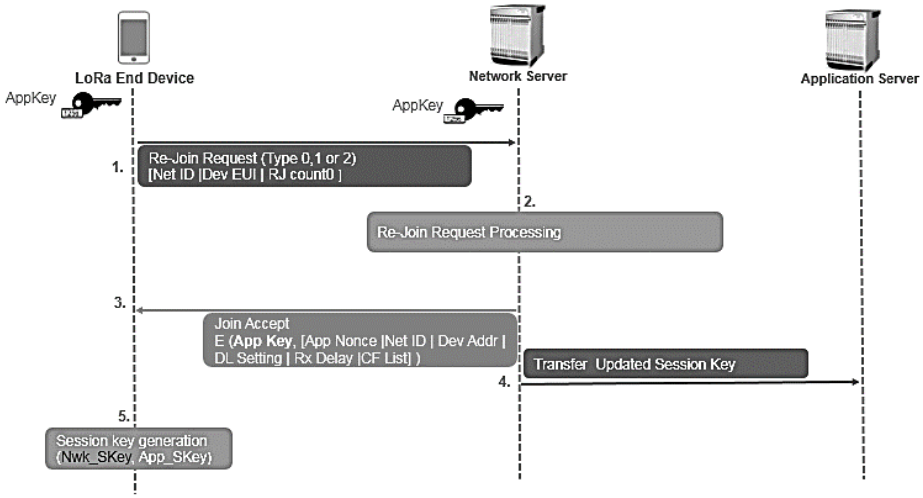

Figure 7. LoRa Re-join Procedures

In the LoRa Re-join process in Figure 6, in the LoRa communication system, there is a join the network process; after that, it is possible that transmitting data is interrupted due to a bad network or the data transmission is deliberately put to sleep by the LoRa End-nodes so that data transmission ends temporarily. In that process, there is a re-join mechanism. Re-Join Request Process {Type 0, 1 or 2} [Net ID EUI| RJ count0] as Step 1, followed by re-joining the Network Server as Step 2, followed by Step 3, Join Accept E (App Key, [App Nonce [Net ID | Dev Addr | DL Setting | Rx Delay |CF List |), step 4, is Transfer Updated Session Key, step 5—session key generation {Nwk_SKey, App_SKey}.

3.4 AES deeper

AES uses various rounds, and their size depends on the length of the encryption key. For example, AES uses ten rounds for a 128-digit key and 14 rounds for a 256-bit key. Each time, the number of rounds used may vary, calibrated by the original AES key. Moreover, AES Encryption Key Structure can be explicitly seen in Figure 8.

Table 3. Number of rounds and their size on the encryption key length

R	Key Size
10	128
12	192
14	256

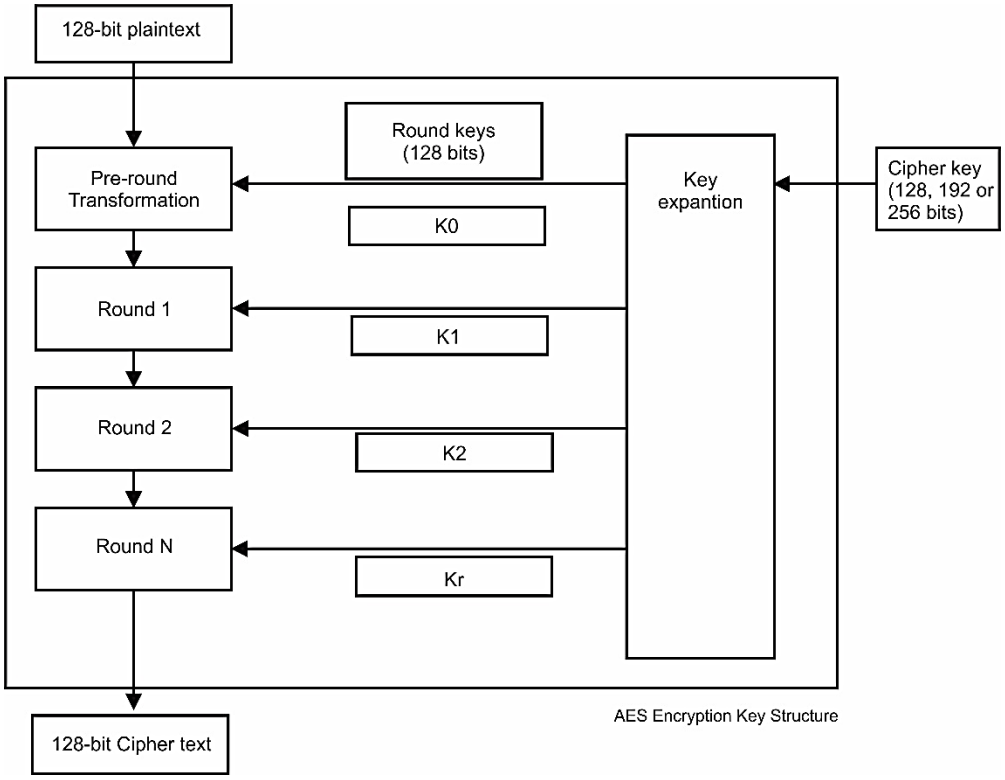

Figure 8. AES Encryption Key Structure

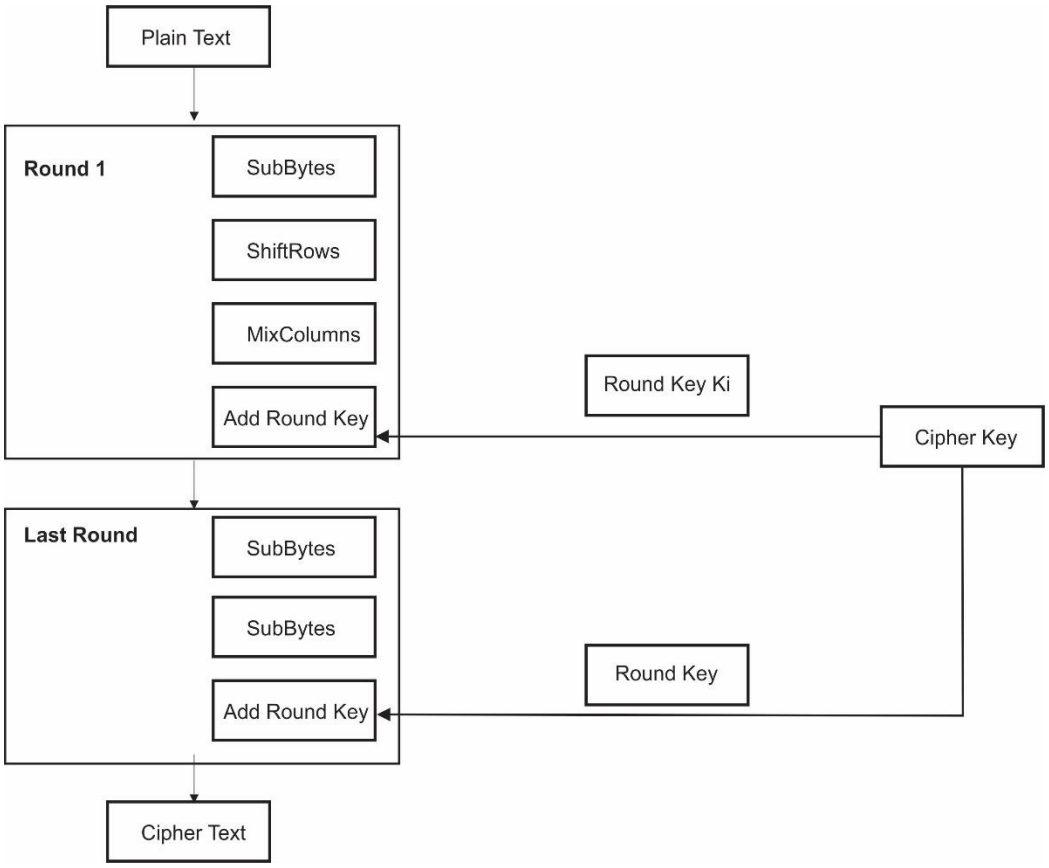

Figure 9. Encryption Process

4. RESULT AND DISCUSSION

This session will discuss how the data encryption process using LoRaWAN AES 128 bit can encrypt sensor data such as DHT11 Sensor. After the LoRa data encryption process, such as DHT11 on the server, The steps are receiving encrypted data, decrypting, validating, and interpreting data.

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
# Encryption key (16 bytes for AES-128)
key = b'0123456789abcdef'
# Sensor data
temperature = 25
humidity = 60
# Convert sensor data to byte array
data = bytearray([temperature, humidity])
# Encrypt the data using AES-128
cipher = AES.new(key, AES.MODE_ECB)
encrypted_data = cipher.encrypt(pad(data, AES.block_size))
```

```
# Transmit the encrypted data over LoRa
# Receiving end
# Receive the LoRa packet
  ----------------Encryption data Code 1 ------------
```

Table 4. Step-by-step LoRaWAN Data Encryption Process with DHT11 Sensor

Step	Description	Example Input	Example Output (Hexadecimal)
1	Read sensor data (Temperature and Humidity)	Temperature: 25°C, Humidity: 60%	Temperature: 25°C (float), Humidity: 60% (float)
2	Encrypt the data using AES encryption algorithm with a shared encryption key.	Temperature: 25°C (float)	Encrypted Temperature: 6B 10 39 A2 2D 7E 30 E1...
		Humidity: 60% (float)	Encrypted Humidity: 5F 85 2A 9F E2 60 5E C1...
3	Package the encrypted data into a data packet for transmission	Encrypted Temperature	Data Packet: [6B 10 39 A2 2D 7E 30 E1...]
		Encrypted Humidity	
4	Transmit the data packet over the LoRa network	Data Packet	-
5	Receive the data packet on the receiving end.	-	Data Packet: [6B 10 39 A2 2D 7E 30 E1...]
6	Decrypt the received data using AES decryption with the shared encryption key.	Encrypted Temperature	Decrypted Temperature: 25°C (float)
		Encrypted Humidity	Decrypted Humidity: 60% (float)

Table 5. LoRaWAN Data Encryption Process with DHT11 Sensor

Humidity (%)	Temperature (°C)	Timestamp (UNIX)	Encrypted Value
50	25	1656339309	0x7f647e7d2c56848f0xe9366954
60	26	1656339310	0x4f688285305890901e926c55
70	27	1656339311	0x1f6c868d345a9c91328e6f56
80	28	1656339312	0xef708a95385c9892468a7257
90	29	1656339313	0xbf748e9d3c5e94935a8c7558

Encryption data Code 1 is an example of using data encryption on the DHT11 sensor on LoRaWAN using 128-bit AES. The next table, 4, is step-by-step data encryption for DHT11 sensors, namely Temperature, and Temperature, starting

from the sensor reading process, encryption data, transmission data, receiving data, and decrypting data.

5. CONCLUSION

The security system in LoRaWAN is divided into two parts. The first part is integrity (FNwkSKey, SNwkSKey). This first part is a communication from End devices to the gateway. The next part is Confidentiality (AppSKey). This part is the whole communication from End-devices to the LoRaWAN Application Server. The data encryption process on LoRaWAN is known as 128-bit AES. LoRaWAN devices generate a unique 128-bit AES key (AppKey) and a globally unique identifier (EUI-64-based DevEUI) used during device authentication. The LoRaWAN network also generates a unique 128-bit AES key (called NwkSKey) for integrity protection and encryption of LoRaWAN MAC commands and application payloads. LoRaWAN devices and networks use the AppKey and NwkSKey to encrypt and decrypt data transmitted over the LoRaWAN network.

6. SUGGESTION

This paper only provides an outline of LoRaWAN Security using a data encryption process called AES-128 bit; it is necessary to provide a continuation in the practice of transmitting data using LoRa data encryption using AES-128 bit in a broadcast on the LoRaWAN server and needs to be analyzed in detail.

ACKNOWLEDGMENTS

Thanks to the National Research and Innovation Agency (BRIN), especially the Research Center for Telecommunication, Cisitu Bandung, which has allowed the author to continue to explore the LoRaWAN field. Hopefully, this Review Paper on LoRaWAN Security can be a good reference for authors and LoRaWAN developers everywhere.

AUTHOR CONTRIBUTIONS

Conceptualization; [P.D.P.Adi], Methodology; [P.D.P.Adi], validation; [P.D.P.Adi], formal analysis; [P.D.P.Adi], investigation; [P.D.P.Adi], data curation; [P.D.P.Adi], writing—original draft preparation; [P.D.P.Adi], writing—review and editing; [P.D.P.Adi], visualization; [P.D.P.Adi], supervision project administration; [P.D.P.Adi], funding acquisition; [P.D.P.Adi], have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. F. I. Maulana, P. D. P. Adi, D. Lestari, A. Purnomo and S. Y. Prihatin, "Twitter Data Sentiment Analysis of COVID-19 Vaccination using Machine Learning," *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia, 2022, pp. 582-587, doi: 10.1109/ISRITI56927.2022.10053035.
2. Y. A. Liani et al., "The Broiler Chicken Coop Temperature Monitoring Use Fuzzy Logic and LoRAWAN," *2021 3rd International Conference on Electronics Representation and Algorithm (ICERA),* Yogyakarta, Indonesia, 2021, pp. 161-166, doi: 10.1109/ICERA53111.2021.9538771.
3. M. Niswar et al., "Performance evaluation of ZigBee-based wireless sensor network for monitoring patients' pulse status," *2013 International Conference on Information Technology and Electrical Engineering (ICITEE),* Yogyakarta, Indonesia, 2013, pp. 291-294, doi: 10.1109/ICITEED.2013.6676255.
4. P. D. P. Adi et al., "ZigBee and LoRa performances on RF Propagation on the Snow Hills area," *2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE),* Bandar Lampung, Indonesia, 2021, pp. 36-41, doi: 10.1109/ICCTEIE54047.2021.9650623.
5. P. Locatelli, P. Spadaccino and F. Cuomo, "Ruling Out IoT Devices in LoRaWAN," *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2022*, pp. 1-2, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798063.
6. J. Navarro-Ortiz, N. Chinchilla-Romero, J. J. Ramos-Munoz and P. Munoz-Luengo, "Improving Hardware Security for LoRaWAN," *2019 IEEE Conference on Standards for Communications and Networking (CSCN),* Granada, Spain, 2019, pp. 1-6, doi: 10.1109/CSCN.2019.8931397.
7. N. Yakin, M. Zhitkov, A. Chernikov and P. Pepelyaev, "Security Threats and Service Degradation Detection in LoRaWAN Networks," *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* Yekaterinburg, Russia, 2021, pp. 0455-0458, doi: 10.1109/USBEREIT51232.2021.9455123.
8. P. D. P. Adi et al., "Application of IoT-LoRa Technology and Design in irrigation canals to improve the quality of agricultural products in Batu Indonesia," *2021 2nd International Conference*

On Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), Tangerang, Indonesia, 2021, pp. 88-94, doi: 10.1109/ICON-SONICS53103.2021.9617175.

9. S. N. Ilmani Binti Mohd Yusoff and Y. Binti Mohd Yussoff, "Analysis of Security Vulnerabilities in LoRaWAN Smart City," *2022 IEEE Symposium on Wireless Technology & Applications (ISWTA), Kuala Lumpur, Malaysia, 2022,* pp. 35-40, doi: 10.1109/ISWTA55313.2022.9942752.
10. S. M. Danish, H. K. Qureshi, S. Jangsher and M. Lestas, "Effects of Wireless Power Transfer on LoRaWAN Join Procedure," *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC),* Limassol, Cyprus, 2018, pp. 944-949, doi: 10.1109/IWCMC.2018.8450426.
11. Y. -C. Lee, Y. Wei, Y. Liu and K. F. Tsang, "Evaluation of the Communication Overhead of Re-join in LoRaWAN Protocol," *2022 IEEE International Conference on Industrial Technology (ICIT),* Shanghai, China, 2022, pp. 1-6, doi: 10.1109/ICIT48603.2022.10002824.
12. A. Gladisch, S. Rietschel, T. Mundt, J. Bauer, J. Goltz and S. Wiedenmann, "Securely Connecting IoT Devices with LoRaWAN," *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4),* London, UK, 2018, pp. 220-229, doi: 10.1109/WorldS4.2018.8611576.
13. P. D. P. Adi, A. Kitagawa, D. A. Prasetya and A. B. Setiawan, "A Performance of ES920LR LoRa for the Internet of Things: A Technology Review," *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT),* Surabaya, Indonesia, 2021, pp. 1-7, doi: 10.1109/EIConCIT50028.2021.9431912.
14. S. Loukil, L. C. Fourati, A. Nayyar and C. So-In, "Investigation on Security Risk of LoRaWAN: Compatibility Scenarios," *in IEEE Access*, vol. 10, pp. 101825-101843, 2022, doi: 10.1109/ACCESS.2022.3208171.
15. P. De Moraes and A. F. Da Conceição, "Protecting LoRaWan data against untrusted network servers," *2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics),* Melbourne, Australia, 2021, pp. 99-106, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00029.

16. P. D. P. Adi et al., "A Performance Evaluation of ZigBee Mesh Communication on the Internet of Things (IoT)," *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT),* Surabaya, Indonesia, 2021, pp. 7-13, doi: 10.1109/EIConCIT50028.2021.9431875.
17. P. D. P. Adi and A. Kitagawa, "Performance Evaluation of Low Power Wide Area (LPWA) LoRa 920 MHz Sensor Node to Medical Monitoring IoT Based," *2020 10th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS),* Malang, Indonesia, 2020, pp. 278-283, doi: 10.1109/EECCIS49483.2020.9263418.
18. P. D. P. Adi, A. Kitagawa and J. Akita, "Finger Robotic control use M5Stack board and MQTT Protocol based," *2020 7th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE),* Semarang, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICITACEE50144.2020.9239170.
19. Y. Jeon and Y. Kang, "Implementation of a LoRaWAN protocol processing module on an embedded device using Secure Element," *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC),* JeJu, Korea (South), 2019, pp. 1-3, doi: 10.1109/ITC-CSCC.2019.8793333.
20. N. Hayati, K. Ramli, M. Suryanegara and Y. Suryanto, "Potential Development of AES 128-bit Key Generation for LoRaWAN Security," *2019 2nd International Conference on Communication Engineering and Technology (ICCET),* Nagoya, Japan, 2019, pp. 57-61, doi: 10.1109/ICCET.2019.8726884.
21. R. Sanchez-Iborra et al., "Internet Access for LoRaWAN Devices Considering Security Issues," *2018 Global Internet of Things Summit (GIoTS),* Bilbao, Spain, 2018, pp. 1-6, doi: 10.1109/GIOTS.2018.8534530.
22. D. Naidu and N. K. Ray, "Review on Authentication Schemes for Device Security in LoRaWAN," *2021 19th OITS International Conference on Information Technology (OCIT),* Bhubaneswar, India, 2021, pp. 387-392, doi: 10.1109/OCIT53463.2021.00082.
23. C. Kamyod, "CIA Analysis for LoraWAN Communication Model," *2021 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical,*

Electronics, Computer and Telecommunication Engineering, Cha-am, Thailand, 2021, pp. 394-397, doi: 10.1109/ECTIDAMTNCON51128.2021.9425745.

24. P. Thaenkaew, B. Quoitin and A. Meddahi, "Evaluating the cost of beyond AES-128 LoRaWAN security," *2022 International Symposium on Networks, Computers and Communications (ISNCC),* Shenzhen, China, 2022, pp. 1-6, doi: 10.1109/ISNCC55209.2022.9851811.
25. P. D. P. Adi and A. Kitagawa, "A Review of the Blockly Programming on M5Stack Board and MQTT Based for Programming Education," *2019 IEEE 11th International Conference on Engineering Education (ICEED),* Kanazawa, Japan, 2019, pp. 102-107, doi: 10.1109/ICEED47294.2019.8994922.
26. A. R. Zain, P. Oktivasari, M. Agustin, A. Kurniawan, F. A. Murad and I. Nurrahman, "Evaluation of Encryption and Decryption Data Packet Delivery Performance in Smart Home Design using the LoRaWAN Protocol," *2022 5th International Conference of Computer and Informatics Engineering (IC2IE),* Jakarta, Indonesia, 2022, pp. 241-246, doi: 10.1109/IC2IE56416.2022.9970045.
27. S. Wesemeyer, I. Boureanu, Z. Smith and H. Treharne, "Extensive Security Verification of the LoRaWAN Key-Establishment: Insecurities & Patches," *2020 IEEE European Symposium on Security and Privacy (EuroS&P),* Genoa, Italy, 2020, pp. 425-444, doi: 10.1109/EuroSP48549.2020.00034.
28. P. P. Mikhailovich, C. A. Victorovich, Y. N. Nikolayevich and Z. M. Yuryevich, "Implementation of GOST 34.12-2018 Encryption for LoRaWAN End-devices," *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* Yekaterinburg, Russia, 2021, pp. 0451-0454, doi: 10.1109/USBEREIT51232.2021.9455037.
29. S. Alfayoumi and X. Vilajosana, "Attacker Identification In LoRaWAN Through Physical Channel Fingerprinting," *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022*, pp. 1-5, doi: 10.1109/VTC2022-Spring54318.2022.9860674.
30. P. D. Prasetvo Adi et al., "Development Education of Blind Adaptive Data Rate LoRaWAN Network on Mobile Node," *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI),* Yogyakarta, Indonesia, 2022, pp. 51-57, doi: 10.1109/ISRITI56927.2022.10052978.

31. J. Xu, Y. Tang, Y. Wang and X. Wang, "A Practical Side-Channel Attack of a LoRaWAN Module Using Deep Learning," *2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID),* Xiamen, China, 2019, pp. 17-21, doi: 10.1109/ICASID.2019.8925203.
32. P. D. P. Adi et al., "Performance Evaluation of LoRaWAN in Pulse Status Monitoring with Clustering of Wireless Sensor Network," *2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA),* Denpasar, Bali, Indonesia, 2022, pp. 105-110, doi: 10.1109/ICSINTESA56431.2022.10041694.
33. P. D. P. Adi et al., "Evaluation of Global Positioning System Internet of Things-LoRa based," *2022 2nd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS),* Yogyakarta, Indonesia, 2022, pp. 180-185, doi: 10.1109/ICE3IS56585.2022.10010203.
34. S. J. Philip, J. M. McQuillan and O. Adegbite, "LoRaWAN v1.1 Security: Are We in the Clear Yet?," *2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys),* Nadi, Fiji, 2020, pp. 112-118, doi: 10.1109/DependSys51298.2020.00025.
35. S. Naoui, M. E. Elhdhili and L. A. Saidane, "Trusted Third Party Based Key Management for Enhancing LoRaWAN Security," *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA),* Hammamet, Tunisia, 2017, pp. 1306-1313, doi: 10.1109/AICCSA.2017.73.
36. P. D. Prasetyo Adi et al., "Performance Evaluation of LoRa 915 MHz for Health Monitoring with Adaptive Data Rate," *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT),* Solo, Indonesia, 2022, pp. 252-257, doi: 10.1109/COMNETSAT56033.2022.9994547.
37. P. D. Prasetyo Adi, A. Mappadang, A. Wahid, S. Luhriyani, R. Jefri and N. Nurindah, "Spreading Factor of IoT-LoRa Effect for Future Smart Agriculture," *2022 International Conference on Information Technology Research and Innovation (ICITRI),* Jakarta, Indonesia, 2022, pp. 123-128, doi: 10.1109/ICITRI56423.2022.9970235.

38. B. Oniga, V. Dadarlat, E. De Poorter and A. Munteanu, "A secure LoRaWAN sensor network architecture," 2017 *IEEE SENSORS*, Glasgow, UK, 2017, pp. 1-3, doi: 10.1109/ICSENS.2017.8233990.
39. P. D. Prasetyo Adi et al., "ECG-LPWAN based for Real-time monitoring Patient's Heart Beat Status," *2022 International Seminar on Application for Technology of Information and Communication (iSemantic),* Semarang, Indonesia, 2022, pp. 7-14, doi: 10.1109/iSemantic55962.2022.9920379.
40. P. D. Prasetyo Adi, Y. Wahyu and A. Kitagawa, "Analyzes of Chirps Spread Spectrum of ES920LR LoRa 920 MHz," *2022 11th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS),* Malang, Indonesia, 2022, pp. 139-144, doi: 10.1109/EECCIS54468.2022.9902922.
41. P.D.P.Adi, et.al, "LoRaWAN Technology in Irrigation Channels in Batu Indonesia", *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI),* Vol. 7, No. 3, December 2021, pp. 522-538, ISSN: 2338-3070, DOI: 10.26555/jiteki.v7i3.22258
42. K. -L. Tsai, F. -Y. Leu, L. -L. Hung and C. -Y. Ko, "Secure Session Key Generation Method for LoRaWAN Servers," in *IEEE Access*, vol. 8, pp. 54631-54640, 2020, doi: 10.1109/ACCESS.2020.2978100.
43. Y. Chen, Y. A. Sambo, O. Onireti, S. Ansari and M. A. Imran, "LoRaWAN-5G Integrated Network with Collaborative RAN and Converged Core Network," *2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC),* Kyoto, Japan, 2022, pp. 1-5, doi: 10.1109/PIMRC54779.2022.9977480.