Implementation of Triple Des on Rat Pest Attack Detection Data Using Lora Transmission

Muhammad Nanak Zakaria[1], Rizky Ardiansyah[2], Muhammad Ibnu Atho'illah[3]

[1,2,3] Digital Telecommunication Network Study Program,
Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia.

[1]nanak_zach@polinema.ac.id , [2]riskyardiansyah@polinema.ac.id , [3]masatoqh15@gmail.com

***Abstract*— Information security is a critical requirement in Wireless Sensor Networks (WSN), where resource-constrained sensor nodes must ensure confidentiality, integrity, and availability of transmitted data. LoRa (Long Range) is widely adopted in WSN due to its long-range coverage and low power consumption, but it lacks built-in security, leaving data vulnerable to interception and attacks such as eavesdropping, selective forwarding, sinkhole, and wormhole. This research addresses these vulnerabilities by implementing the Triple Data Encryption Standard (3DES) algorithm in a LoRa-based WSN rat pest detection system. The proposed system consists of an ESP32 with a PIR sensor and buzzer as sensor nodes, a LoRa module for communication, a LoRaWAN gateway, The Things Network (TTN) as middleware, and Node-RED for data processing and visualization. Experimental results show that 3DES can be executed in real time with an average encryption delay of 1.4 milliseconds. The decryption process achieved 100% accuracy, ensuring data integrity and confidentiality, while also demonstrating resilience against ciphertext-only attacks. These findings confirm that integrating 3DES strengthens the security of LoRa-based WSN, providing a reliable cryptographic solution for smart agriculture applications, particularly in rat pest detection systems.**

Keywords*— *Triple DES, LoRa, encryption, pest detection, WSN, cryptography, LoRaWAN.

I. INTRODUCTION

In today's digital era, access and dissemination of information are so easy, making it a valuable asset for individuals, governments, and companies. Information security not only protects hardware and data but also ensures the confidentiality, availability, and integrity of all company information resources [1][2]. These efforts encompass both day-to-day information security and operational preparedness for potential threats. In the rapidly evolving digital landscape, information security has become a key foundation for the operational continuity and reputation of organizations.

Information security is defined as protecting information and information systems from unauthorized access, use, disclosure, operation, modification, or destruction to ensure confidentiality, integrity, and usability. Information security encompasses four areas: organization, people, process, and technology. Each boundary interacts not only with human factors but also with culture, management, architecture, performance, revitalization, and support [3].

In a LoRa network, all information is transmitted in its raw form, without encryption or additional protection. The LoRa module lacks appropriate data security. LoRa is a communications module, meaning it connects multiple devices, communicating end-to-end [4][5]. Without a security system, it would be extremely dangerous if the LoRa module were to receive an attack from an irresponsible party [6]. This data is also at risk of being hacked, modified, or stolen by irresponsible parties, making information security crucial when using LoRa. The increasing adoption of IoT technologies, including LoRa, demands serious attention to cybersecurity, given the potential vulnerabilities that can be exploited [7][8].

Furthermore, each LoRa transmission takes 0.9-1.2 seconds, depending on the payload length. The longer the transmission distance, the longer the data transmission takes. This delay can be exploited by attackers to carry out attacks. There are many types of attacks that can be carried out, one of which is network attacks [9]. Research [10] examined network layer attacks, including eavesdropping, selective forwarding, sinkholes, and wormholes. These various attacks can give attackers the ability to intercept and modify data in real time. One particularly dangerous attack is the wormhole. The risk of a wormhole attack opens new security vulnerabilities that must be addressed and mitigated to protect user data and privacy. Wormhole attacks on wireless networks, especially on resource-constrained IoT devices such as LoRa, are a serious threat that requires effective cryptographic security solutions [11][12][13].

The use of 3DES (Data Encryption Standard) cryptography to secure LoRa data is crucial due to its open nature and vulnerability to unauthorized access. The Triple DES (Data Encryption Standard) algorithm is a symmetric algorithm in cryptography used to secure data by encoding it. The processes involved in data encoding include encryption and decryption [14]. The Triple DES algorithm is a development of the DES algorithm. The DES algorithm only has one key. After that, the DES algorithm was further developed into the Double DES algorithm, which has two keys. After that, the accuracy of storing data was retested and it was still less accurate. Then the Double DES algorithm was further developed into the Triple DES algorithm. This algorithm has three keys that are considered more secure in storing data. The keys used in this algorithm can be the same between key 1, key 2, and key 3, or they can also be different. The Triple DES algorithm has a key

length of 168 bits, where each key consists of 56 bits in length [15][16]. As a reliable symmetric cryptographic algorithm, it offers a strong layer of security to protect data sent over the LoRa network [17][18]. 3DES is able to encrypt data before sending it, so that only recipients who have the same key can access the information. 3DES's resilience to various cryptographic attacks and its broad support across multiple platforms make it an ideal choice for securing LoRa data, particularly in the implementation of data security in a LoRa-based rat infestation detection system in rice fields using the 3DES method.

This research focuses on the implementation of 3DES cryptography to improve communication security between each node and the server using a LoRa network, with the aim of protecting sensitive data from unauthorized access, manipulation, and attacks.

II. METHOD

A. *Theoretical Study*

1) Triple DES (Triple Data Encryption Standard)

Triple Data Encryption Standard (3DES) is a symmetric algorithm in cryptography used to secure data/information by encoding it. The 3DES algorithm is a development of the Data Encryption Standard (DES) algorithm. Essentially, the algorithm used is the same, but 3DES is developed by encrypting it three times using the DES algorithm. 3DES has three 168-bit keys (three times the 56-bit key of DES) [19].

Triple DES Algorithm can be seen in Figure 1.

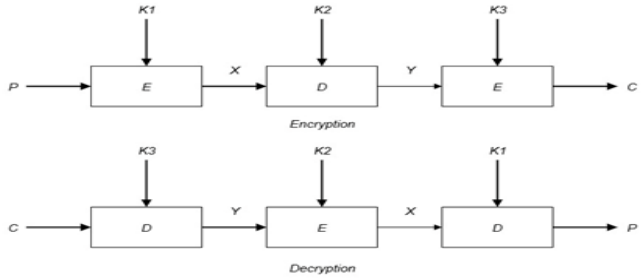

Figure 1. Triple DES Algorithm

2) LoRa

LoRa, which stands for “Long Range,” is a long-range wireless communication system promoted by the LoRa Alliance. It aims to be used in long-lasting, battery-powered devices where energy consumption is a priority. LoRa has two distinct layers: the physical layer, which uses the Chirp Spread Spectrum (CSS) modulation technique developed by Semtect, enabling long-range, low-power, and low-throughput communication [6].

3) LoRaWAN Gateway

Elegrow LR1302 LoRaWAN Gateway is an industrial-grade LoRaWAN gateway device that functions as a bridge between LoRa devices (such as sensors or trackers) and LoRaWAN server networks (such as The Things Network or personal servers), supporting long-distance communication (up to 10+ km in open areas) with low power consumption. This gateway is compatible with 868 MHz (Europe) or 915 MHz (America/Asia) frequencies, has an Ethernet interface for stable connectivity, and supports PoE (Power over Ethernet) for more flexible installation, making it suitable for large-scale IoT applications such as smart farming, smart cities, or industrial asset monitoring [20].

4) Microcontroller ESP32

The ESP32, developed by Espressif Systems, is a powerful and cost-effective platform for IoT applications, featuring built-in Wi-Fi and Bluetooth that simplify connectivity with other devices or networks. It supports Wi-Fi protocols 802.11 b/g/n and offers both Bluetooth Classic and BLE options. With numerous GPIO pins supporting interfaces such as SPI, I2C, UART, and PWM, the ESP32 enables flexible integration with external devices and sensors. Designed for power efficiency, it is well-suited for developing energy-efficient IoT solutions [21].

5) MQTT

MQTT (Message Queuing Telemetry Transport) is a lightweight, publish-subscribe based communication protocol designed specifically for IoT (Internet of Things) devices with limited connections (low bandwidth, high latency, or unstable networks) [22].

6) The Things Network

The Things Network (TTN) is a global, community-driven network that provides free LoRaWAN infrastructure to connect IoT (Internet of Things) devices such as sensors and trackers, using the energy-efficient, long-range (up to 10+ km) LoRa technology. TTN works with three main components: (1) LoRa devices (sending data), (2) gateways (receiving signals and forwarding them to the TTN cloud), and (3) user applications (processing data via MQTT/HTTP). With TTN, anyone can build IoT solutions without high infrastructure costs, for example for environmental, agricultural, or asset monitoring [23].

7) Putty

PuTTY is a lightweight open-source application that functions as an SSH, Telnet, and serial console client to access remote devices or servers through a command-line interface, commonly used by system administrators or developers to manage Linux servers, network routers, or IoT devices such as Raspberry Pi securely and efficiently. In addition to supporting text-based connections, PuTTY also comes with supporting tools such as PuTTYgen for generating SSH keys and PSFTP for file transfers, and is available for Windows (natively) and can be run on Linux/macOS via alternatives such as terminal or Wine [24].

8) Raspberry PI

The Raspberry Pi is a small, low-cost single-board computer designed for education, IoT projects, and low-power computing, using a Linux-based operating system (such as Raspberry Pi OS) or Windows IoT. With an ARM processor, GPIO ports (for interfacing with sensors/electronics), Wi-Fi/Bluetooth support, and the ability to run various programming languages (Python, JavaScript, etc.), the Raspberry Pi is often used for robotics, home servers, media centers (Kodi), or intelligent automation. Examples of popular models: the Raspberry Pi 5 (latest) and the Pi Zero 2 W (ultra-compact) [25].

B. Type of Research

Based on the stated research objectives, this research can be classified as Research and Development (R&D). Research and Development (R&D) is currently a type of research that is being widely developed. Research and Development is a type of research that is able to bridge or bridge basic research with applied research. The definition of applied research or Research and Development (R&D) is often interpreted as a process or steps in developing a new product or improving an existing product. The resulting product can be software or hardware such as books, modules, packages, learning programs or learning devices [26].

Research State Diagram can be seen in Figure 2.

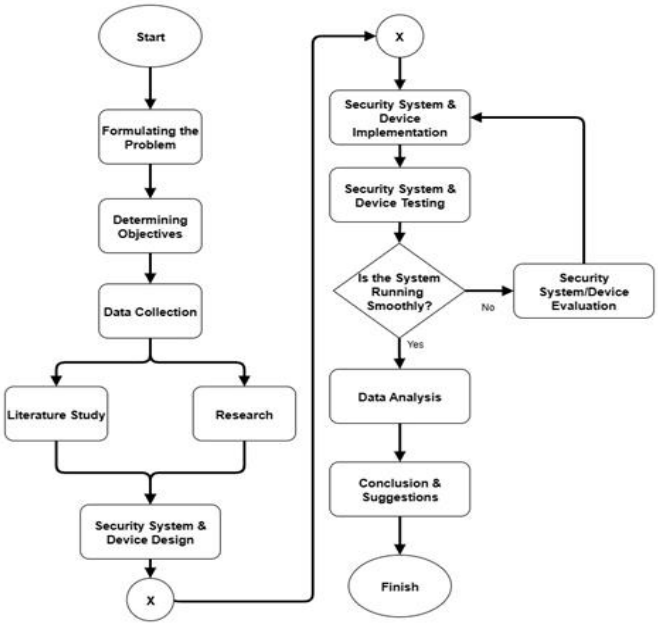

Figure 2. Research State Diagram

III. RESULTS AND DISCUSSION

A. Topology and System Under Test

System Topology can be seen in Figure 4.

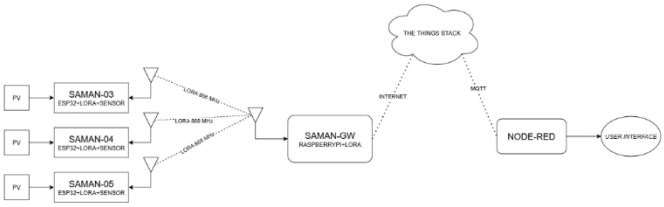

Figure 3. System Topology

Testing of the LoRa-based rodent infestation detection system with Triple DES encryption involved five ESP32 end devices equipped with PIR sensors and ultrasonic buzzers, transmitting encrypted data via LoRa to a Raspberry Pi gateway with an LR1302 module, then forwarding it to The Things Network (TTN) and accessing it through MQTT on Node-RED for decryption and display.

B. Tested Prototype

External View of Node Sensor can be seen in Figure 4.

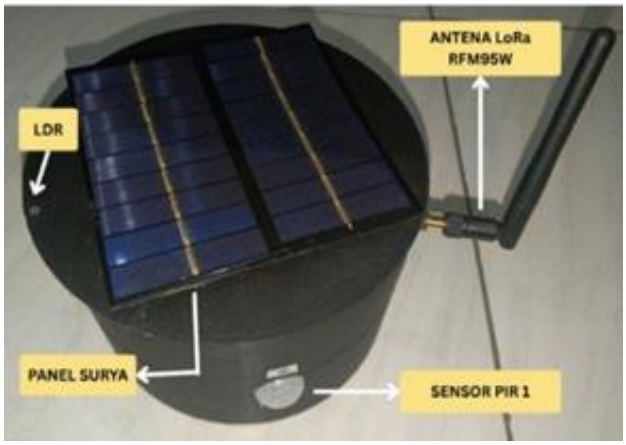

Figure 4. External View of Node Sensor

The hardware implementation for the four sensor nodes (SAMAN-01, SAMAN-02, SAMAN-04, and SAMAN-05) has an identical design and components. Internal View of Node Sensor can be seen in Figure 6.

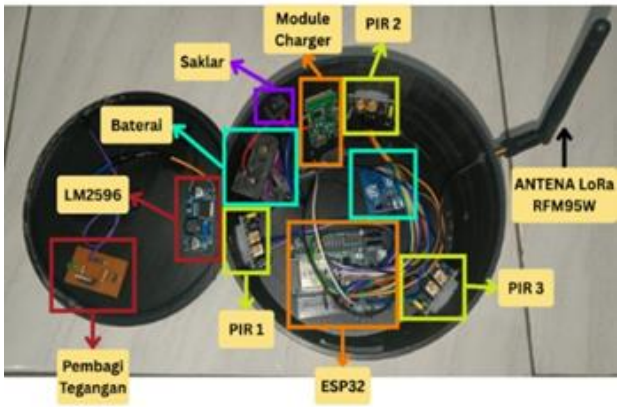

Figure 5. Internal View of Node Sensor

Each node is designed as a standalone unit equipped with a Passive Infrared Receiver (PIR) motion detection sensor, a solar panel as an energy source, and a LoRa RFM95W antenna for long-range wireless communication. Internal View of SAMAN-03 can be seen in Figure 6.

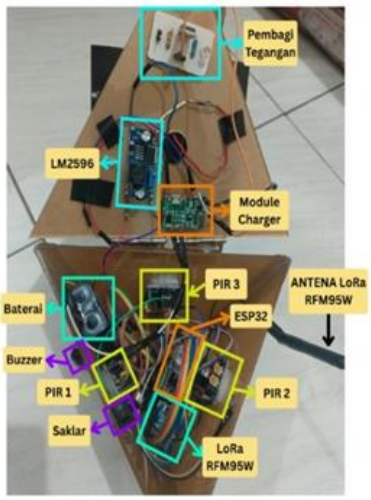

Figure 6. Internal View of SAMAN-03

The SAMAN-03 integrates a LoRa RFM95W module, an ESP32 microcontroller, and supporting power components, with its key feature being a passive buzzer that automatically activates and emits ultrasonic frequency when motion is detected by a PIR sensor. View of All Prototypes can be seen in Figure 7.

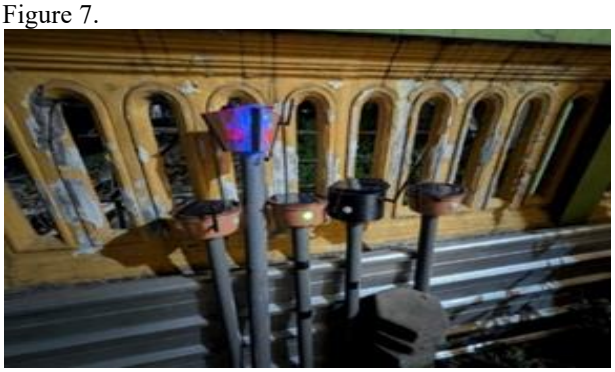

Figure 7. View of All Prototypes

Before testing the prototype, a pipe needs to be installed so that it can be inserted into the wet soil in the rice fields.

C. *Sensor Node and Gateway Placement*

Figure 8. Prototype Testing Placement in Rice Fields

Figure 8 shows the placement of the sensor nodes to be tested. The nodes furthest from the gateway are SAMAN-03 and SAMAN-05. SAMAN-04 is approximately 3 meters from the gateway, SAMAN-03 is approximately 6 meters from the gateway, and SAMAN-05 is approximately 8 meters from the gateway.

Figure 9. Gateway Position

The gateway is placed next to the rice field, there is a small terrace and it is directed towards the rice field so that all sensor nodes can reach the gateway as in Figure 9.

D. *System Testing*

1) LoRa Delay Transmission (Encryption and Decryption LoRa)

Testing was carried out 10 times sending data from node 3. The payload has a length of 8 bytes and contains the status data of three PIR sensors, three motion counts, total count, and one empty byte.

a) SAMAN-03

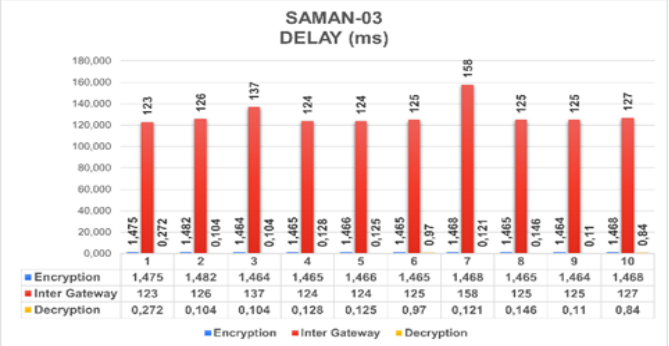

Figure 10. SAMAN-03 Delay Chart

The analysis of the graph from SAMAN-03 shows that the encryption process using TripleDES is highly efficient, with an average time ranging from 1.464 ms to 1.482 ms and very little variation across 10 tests, demonstrating stable and consistent performance. The gateway delay from the node to the gateway (LoRaWAN to TTN) ranges between 123 ms and 158 ms, with the highest delay occurring at the seventh test point, most likely due to environmental interference, while the average remains around 125 ms, reflecting reliable communication stability. Meanwhile, the decryption process in Node-RED is significantly faster, ranging only from 0.1 ms to 0.9 ms, which highlights its lightweight computation and minimal load on the server compared to encryption.

b) SAMAN-04

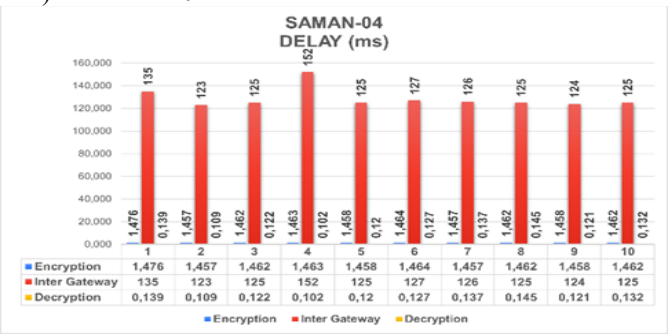

Figure 11. SAMAN-04 Delay Chart

The graph shows the processing time for 10 data transmissions, where encryption on ESP32 at node 4 remained stable between 1.457 and 1.476 ms without significant spikes, proving the consistency of Triple DES performance. Gateway delay ranged from 123 to 152 ms, with the highest delay at the fourth transmission likely due to environmental factors, while most values stayed around 125 ms, confirming reliable LoRa communication. Decryption was very fast at 0.102 to 0.145 ms, consistently efficient across all tests without issues despite varying ciphertext.

c) SAMAN-05

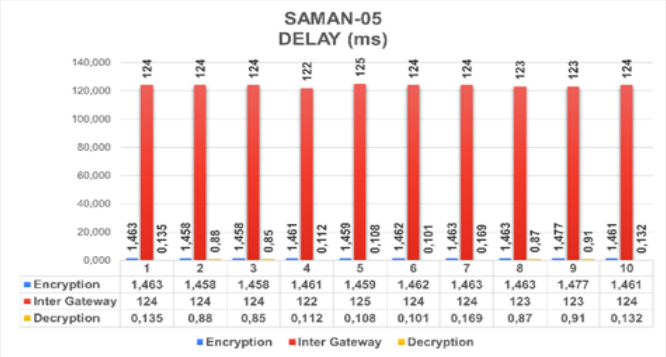

Figure 12. SAMAN-05 Delay Chart

The analysis of SAMAN-05 shows that encryption was very stable between 1.458 and 1.477 ms, confirming consistent Triple DES performance without additional load on the ESP32 processor. Gateway delay was also very close, ranging from 122 to 125 ms, suggesting ideal LoRa transmission conditions due to an unobstructed location and optimal distance from the gateway. Decryption times varied from 0.101 to 0.91 ms, with some points nearing 0.9 ms, slightly higher than other nodes, likely caused by load fluctuations on the Node-RED system during Base64 parsing and decoding, but still far below critical latency levels.

2) Security Resilience

Encryption was performed using Triple DES with the resulting ciphertext in Base64 format. Some example results:

- Plaintext: 00 01 00 02 02 06 0A 03
- Ciphertext (Hex): 5F B2 C3 8F 76 A9 3A 11
- Ciphertext (Base64): X7LDj3apOhE=
- Decryption successful: 00 01 00 02 02 06 0A 03

TABLE I
ENCRYPTION TABLE

Node	Data to-	Raw Data (Plaintext)	Encryption Data		Decryption Data (Plaintext)
			Hex	Base64	
SAMAN-03	1	00 01 00 02 02 06 0A 03	5F B2 C3 8F 76 A9 3A 11	X7LDj3 apOhE=	00 01 00 02 02 06 0A 03
	2	00 00 00 12 0B 0C 29 03	D3 64 18 6B 48 FF 49 AB	02QYa0j /Sas=	00 00 00 12 0B 0C 29 03
	3	01 00 01 20 1D 13 50 03	03 5A EF 4E 1A 88 E1 B3	A1rvThq I4bM=	01 00 01 20 1D 13 50 03
	4	00 01 00 30	38 E9 86 22	OOmGIs rjq8k=	00 01 00 30 32 1B 7D 03
	5	00 00 01 3C 43 24 A3 03	3C 47 48 A7 75 90 1B E5	PEdIp3 WQG+U =	00 00 01 3C 43 24 A3 03
	6	00 00 00 3D 4A 2B B2 03	2C 69 18 18 00 56 48 0B	LGkYG ABWSA s=	00 00 00 3D 4A 2B B2 03
	7	00 00 00 3F 54 2D C0 03	79 9B 37 9E C6 DD F9 50	eZs3nsb d+VA=	00 00 00 3F 54 2D C0 03
	8	00 00 00 47 5B 31 D3 03	67 77 AC 75 94 15 CD 27	Z3esdZ QVzSc=	00 00 00 47 5B 31 D3 03
	9	00 00 00 4D 68 38 ED 03	04 B4 AF B6 11 1E CD 16	BLSvth EezRY=	00 00 00 4D 68 38 ED 03
	10	00 01 01 50 74 40 04 03	DD 43 25 FF 15 71 BA 84	3UMl/x VxuoQ=	00 01 01 50 74 40 04 03
SAMAN-04	1	00 00 00 03 03 0C 12 04	15 05 66 C5 38 9C F4 4B	FQVmx Tic9Es=	00 00 00 03 03 0C 12 04
	2	00 00 00 05 10 13 28 04	02 7A 3F 7F EE B5 4B E2	Ano/f+6 1S+I=	00 00 00 05 10 13 28 04
	3	01 00 00 09 12 17 32 04	58 C8 DA 18 B0 38 90 1B	WMjaG LA4kBs =	01 00 00 09 12 17 32 04
	4	00 01 00 09 20 1A 43 04	C6 6E 73 66 38 EB 36 FD	xm5zZjj rNv0=	00 01 00 09 20 1A 43 04
	5	00 00 00 0D 31 23 61 04	E7 7D 4D 48 BA 2B 84 9C	531NSL orhJw=	00 00 00 0D 31 23 61 04

Node	Data to-	Raw Data (Plaintext)	Encryption Data		Decryption Data (Plaintext)
			Hex	Base64	
	6	00 01 00 0E 40 2C 7A 04	63 D0 80 D7 CA 9B 24 05	Y9CA18 qbJAU=	00 01 00 0E 40 2C 7A 04
	7	00 00 00 12 4D 35 94 04	CE B1 2C 3B 5B C2 ED 85	zrEsO1v C7YU=	00 00 00 12 4D 35 94 04
	8	00 00 00 16 5D 3D B0 04	E8 3F 9D C8 7B ED DE 66	6D+dyH vt3mY=	00 00 00 16 5D 3D B0 04
	9	00 01 00 19 6C 47 CC 04	FA 8A E3 6D 0E 07 74 0D	+orjbQ4 HdA0=	00 01 00 19 6C 47 CC 04
	10	00 00 00 22 76 4E E6 04	59 41 6C CE 24 13 10 B3	WUFszi QTELM=	00 00 00 22 76 4E E6 04
SAMAN-05	1	00 00 00 02 03 07 05	00 9C 89 7F 9D 74 04 5B	AJyJf51 0BFs=	00 00 00 02 02 03 07 05
	2	00 00 00 03 07 07 11 05	64 75 26 49 EA 31 26 79	ZHUmS eoxJnk=	00 00 00 03 07 07 11 05
	3	00 00 00 05 13 0A 22 05	AE DE 80 CE E5 1A C6 73	rt6AzuU axnM=	00 00 00 05 13 0A 22 05
	4	00 01 00 06 1C 0E 30 05	DD DE 1A 9D 3E 06 87 E7	3d4anT4 Gh+c=	00 01 00 06 1C 0E 30 05
	5	00 00 00 07 25 11 3D 05	31 2D BB B1 24 36 31 46	MS27sS Q2MUY=	00 00 00 07 25 11 3D 05
	6	00 01 00 08 31 14 4D 05	1E 5E 9D CB C2 27 17 D5	Hl6dy8I nF9U=	00 01 00 08 31 14 4D 05
	7	00 00 00 09 3F 16 5E 05	3A 4F B1 6A 1B 52 FB 1B	Ok+xaht S+xs=	00 00 00 09 3F 16 5E 05
	8	00 00 00 0A 4A 19 6D 05	A3 7F C4 D3 02 EB EE AA	o3/E0w Lr7qo=	00 00 00 0A 4A 19 6D 05
	9	00 00 00 0C 56 1B 7D 05	47 D0 FD 0B 6E 0D F6 D1	R9D9C2 4N9tE=	00 00 00 0C 56 1B 7D 05
	10	00 00 00 0D 66 1F 92 05	F3 F0 BA 4A 3D 17 E8 A8	8/C6Sj0 X6Kg=	00 00 00 0D 66 1F 92 05

This test aims to evaluate the security resilience of data encrypted using the Triple Data Encryption Standard (Triple DES) algorithm against unauthorized decryption attempts. The test was conducted using the Triple DES Online Decryption service available at https://www.devglan.com/online-tools/Triple-des-encrypt-decrypt . The ciphertexts used in this test are:

Ciphertext (Hex): 5F B2 C3 8F 76 A9 3A 11

The testing process was carried out with two scenarios of incorrect key usage, namely:

1. First Key Experiment

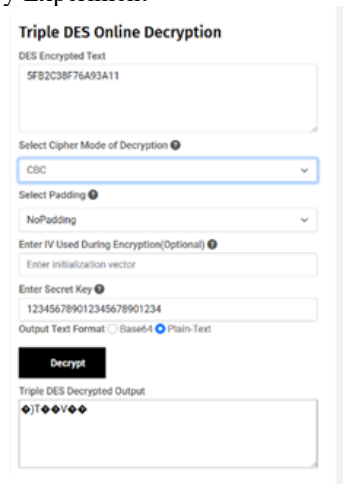

Figure 13. First Key Experiment

- Decryption mode: CBC
- Padding scheme: NoPadding
- Key: 123456789012345678901234
- Decryption result: "□T□□V□□"

2. Second Key Experiment

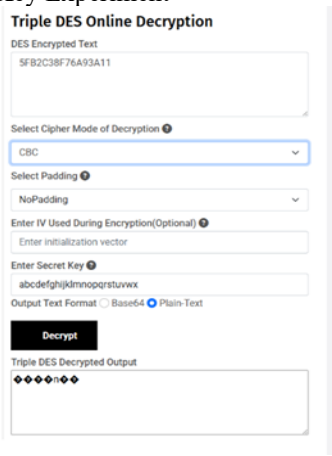

Figure 14. First Key Experiment

- Decryption mode: CBC
- Padding scheme: NoPadding
- Key: abcdefghijklmnopqrstuvwx
- Decryption result: "□□□□□□n□□"

The results show that knowing the encryption scheme and ciphertext alone cannot produce meaningful plaintext without the correct key, proving that Triple DES provides strong resistance against ciphertext-only attacks.

3) LoRa Signal Quality

1. RSSI (Received Signal Strength Indicator)

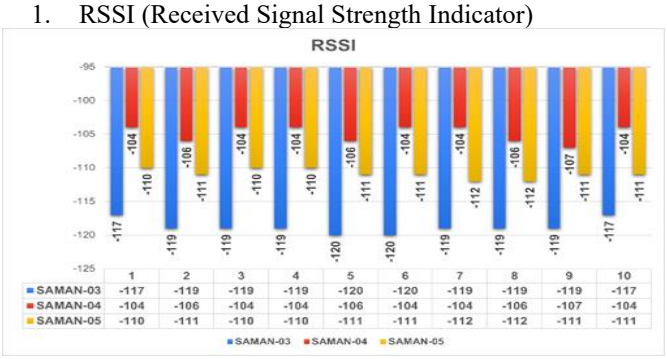

Figure 15. RSSI Chart

The RSSI indicates the signal strength received by the gateway from the LoRa node. The more negative the value (e.g., -120 dBm), the weaker the signal. LoRa generally functions well down to -120 dBm, although ideally above -110 dBm. A higher RSSI value (closer to 0 dBm) indicates a stronger and more stable connection between the node and gateway. Consistently low RSSI values may suggest issues such as excessive distance, physical obstructions, or antenna misalignment.

SAMAN-03 (Blue)

• RSSI Range: -117 dBm to -120 dBm

• Average: -119 dBm

SAMAN-03 experienced the weakest signal compared to the other nodes. This is understandable, as the node is located in the middle of a rice field. Despite the weakest signal, the system was still able to transmit data well, demonstrating LoRa's resilience in extreme conditions.

SAMAN-04 (Red)

• RSSI Range: -104 dBm to -107 dBm

• Average: -105 dBm

SAMAN-04 received the strongest and most stable signal, indicating the node's relatively open location and proximity to the gateway. This result aligns with SAMAN-04's relatively fast and stable transmission delay.

SAMAN-05 (Yellow)

• RSSI Range: -110 dBm to -112 dBm

• Average: -111 dBm

SAMAN-05 has moderate signal strength. The signal is within a safe range and shows no significant interference. This performance reflects the SAMAN-05 gateway's very stable delay throughout the test.

2. SNR (Signal to Noise Ratio)

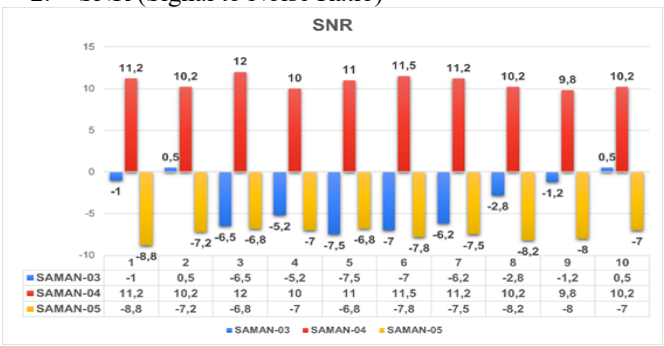

Figure 16. SNR Chart

SNR (Signal-to-Noise Ratio) is the ratio of signal strength to the ambient noise level. A positive SNR value indicates that the signal is stronger than the noise (ideal), while a negative SNR means that the noise is more dominant than the signal (not ideal). The unit is dB.

SAMAN-03 (Blue)

• SNR Range: -7.5 dB to +0.5 dB

• Average: Around -3.7 dB

Node 3 mostly produces negative SNR values, meaning the transmission is heavily interfered with by noise. This could be influenced by:

• The node's location furthest from the gateway

• The presence of obstructions such as tall rice paddies

Despite this, data is still successfully received and decrypted, demonstrating the robustness of LoRa technology even at low SNR.

SAMAN-04 (Red)

• SNR Range: 9.8 dB – 12 dB

• Average: Approximately 10.7 dB

SAMAN-04's SNR is consistently positive and high, indicating a very strong signal and very low noise. This indicates SAMAN-04 is in an ideal position with little transmission obstruction and a short distance to the gateway.

SAMAN-05 (Yellow)

• SNR Range: -8.8 dB – -6.8 dB

• Average: -7.5 dB

All values are negative, meaning noise is always dominant. This node has the worst signal quality of the three. This is due to suboptimal positioning, such as obstruction by plants, trees, and less-than-ideal node positioning.

IV. CONCLUSION

The following conclusions can be drawn from the test results of this study: The implementation of 3DES on LoRa was successful with an average encryption time of 1.4 ms, operating in real time on sensor nodes, encrypted data was transmitted through LoRa, received by the server, and correctly decrypted. Data security was ensured with 100 percent decryption success, integrity was maintained, confidentiality was guaranteed since only ciphertext was transmitted, and availability remained even under signal interference with only transmission delays. The system was resistant to ciphertext-only attacks, testing with sample ciphertext produced unreadable results, no data leakage was found, and 3DES implementation provided a high level of security against interception in LoRa networks.

REFERENCES

[1] D. K. Gupta et al., "Load Frequency Control Analysis of Cyber-Physical Power System with Denial-of-Service Attack in Deregulated Power Markets," Smart Grids Sustain. Energy, vol. 10, no. 1, p. 22, 2025, doi: 10.1007/s40866-025-00250-8.

[2] M. C. Osazuwa, O. Mitchell, and C. Osazuwa, "Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature," Int. J. Innov. Sci. Res. Technol., vol. 8, no. December 2023, 2023, doi: 10.5281/zenodo.10464076.

[3] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," J. Ekon. Manaj. Sist. Inf., vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.

[4] J. Qadir, "Cybersecurity in LoRaWAN Networks: Vulnerability Analysis and Enhancing Security Measures for IoT Connectivity," 2023.

[5] P. Maurya, A. Hazra, P. Kumari, T. B. Sørensen, and S. K. Das, "A Comprehensive Survey of Data-Driven Solutions for LoRaWAN: Challenges and Future Directions," ACM Trans. Internet Things, vol. 6, no. 1, 2025, doi: 10.1145/3711953.

[6] M. F. Iman, A. Kusyanti, and R. Primananda, "Implementasi Algoritme Clefia 128-Bit untuk Pengamanan Modul Komunikasi Lora," J. Teknol. Inf. dan Ilmu Komput., vol. 9, no. 7, pp. 1647–1654, 2022, doi: 10.25126/jtiik.2022976766.

[7] A. Budillon, F. Mazzenga, and P. Tognolatti, "Challenges and opportunities in LoRaWAN security: exploring protocol vulnerabilities, privacy threats and the role of edge computing," no. 1706250, 2024, [Online]. Available: https://iris.uniroma1.it/handle/11573/1700890

[8] F. Saghaei, H. R. Zarandi, and M. Tavakkoli, "A Comprehensive Vulnerability Analysis of LoRaWAN-based Cyber-Physical Systems in the Presence of EMI and PSD Transient Faults," 2025.

[9] M. Alfarisi and H. Nurwarsito, "Analisis Dampak Serangan Wormhole terhadap Protokol Routing Ad-Hoc On Demand Distance Vector (AODV) pada LoRa," … Teknol. Inf. dan Ilmu …, vol. 6, no. 5, pp. 2054–2063, 2022, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/10994

[10] J. R. Gómez, H. F. V. Montoya, and Á. L. Henao, "Implementing a Wormhole Attack on Wireless Sensor Networks with XBee S2C Devices," Rev. Colomb. Comput., vol. 20, no. 1, pp. 41–58, 2019, doi: 10.29375/25392115.3606.

[11] N. E. W. Industries, D. Economy, P. Of, and T. H. E. Future, "Sessions Schedule & Abstracts Програма & Резюмета".

[12] M. Jouhari, N. Saeed, M. S. Alouini, and E. M. Amhoud, "A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges," IEEE Commun. Surv. Tutorials, vol. 25, no. 3, pp. 1841–1876, 2023, doi: 10.1109/COMST.2023.3274934.

[13] A. H. Alshehri, "Wormhole attack detection and mitigation model for Internet of Things and WSN using machine learning," PeerJ Comput. Sci., vol. 10, pp. 1–22, 2024, doi: 10.7717/PEERJ-CS.2257.

[14] K. Ntshabele, B. Isong, N. Gasela, and A. M. Abu-Mahfouz, "A Comprehensive Analysis of LoRaWAN Key Security Models and Possible Attack Solutions," Mathematics, vol. 10, no. 19, pp. 1–19, 2022, doi: 10.3390/math10193421.

[15] M. H. M. Baig, H. B. Ul Haq, and W. Habib, "A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance," Manag. Sci. Adv., vol. 1, no. 1, pp. 20–30, 2024, doi: 10.31181/msa1120244.

[16] M. Siahaan and J. Manurung, "Perancangan Aplikasi Penyandian Teks Menggunakan Algoritma Triple DES," J. Ilmu Komput. dan Sist. …, vol. 3, no. 3, pp. 197–201, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/116

[17] S. Abboud and N. Abdoun, "Enhancing LoRaWAN Security: An Advanced AES-Based Cryptographic Approach," IEEE Access, vol. 12, no. December 2023, pp. 2589–2606, 2024, doi: 10.1109/ACCESS.2023.3348416.

[18] P. Thaenkaew, B. Quoitin, and A. Meddahi, "Leveraging Larger AES Keys in LoRaWAN: A Practical Evaluation of Energy and Time Costs," Sensors, vol. 23, no. 22, pp. 1–23, 2023, doi: 10.3390/s23229172.

[19] Z. Basim, "Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As- Su ' Udiyyah," Skanika, vol. 3, no. 4, pp. 54–60, 2020.

[20] V. Bonilla, B. Campoverde, and S. G. Yoo, "A Systematic Literature Review of LoRaWAN: Sensors and Applications," Sensors, vol. 23, no. 20, 2023, doi: 10.3390/s23208440.

[21] D. Hercog, T. Lerher, M. Truntič, and O. Težak, "Design and Implementation of ESP32-Based IoT Devices," Sensors, vol. 23, no. 15, 2023, doi: 10.3390/s23156739.

[22] M. Bender, E. Kirdan, M. O. Pahl, and G. Carle, "Open-source MQTT evaluation," 2021 IEEE 18th Annu.

Consum. Commun. Netw. Conf. CCNC 2021, no. January 2021, pp. 1–5, 2021, doi: 10.1109/CCNC49032.2021.9369499.

[23] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for internet-of-things networks," Futur. Internet, vol. 12, no. 3, pp. 1–14, 2020, doi: 10.3390/fi12030044.

[24] I. B. P. Widja, "Rancang Bangun Media Storage Berbasis Armbian Menggunakan Orange-Pi dan Openmediavault," Patria Artha Technol. J., vol. 5, no. 1, pp. 19–32, 2021, doi: 10.33857/patj.v5i1.396.

[25] J. W. Jolles, "Broad-scale applications of the Raspberry Pi: A review and guide for biologists," Methods Ecol. Evol., vol. 12, no. 9, pp. 1562–1579, 2021, doi: 10.1111/2041-210X.13652.

[26] H. Yamashika, W. Mustakim, and M. Giatman, "Mobile Application Design For Learning Digital Engineering Based On Figma And Android Studio," J. Comput. Sci. Inf. Technol. Telecommun. Eng., vol. 4, no. 1, pp. 370–376, 2023, doi: 10.30596/jcositte.v4i1.13184.