Implementation of Security in LoRaWAN Network Using Speck Algorithm and Message Authentication Code

Arselliana Khoirun Nisa Carolin[1], Rizky Ardiansyah[2*], Koesmarijanto Koesmarijanto[3]

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

3 Telecommunication Engineering Study Program, Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia

[1]shelyaacaroline@gmail.com , [2]rizkyardiansyah@polinema.ac.id , [3]koesmarijanto@polinema.ac.id

***Abstract*— Long Range (LoRa) is a wireless technology that provides long-range and low-power communication. However, LoRa still has weaknesses when it comes to data transmission processes, making it vulnerable to attacks. One of the common attacks during data transmission in LoRaWAN is sniffing or data theft. This research aims to create a system that can protect LoRa devices from attacks that could lead to data leakage to unauthorized parties. The research findings indicate that implementing encryption systems on LoRa using Speck and Message Authentication Code algorithms can secure LoRa devices from sniffing attacks, preventing sniffers or attacking nodes from successfully reading or altering messages sent by the sender. The implementation of encryption systems on devices affects network performance, such as packet errors, packet loss, delay, and throughput. Based on 100 experiments conducted, the encrypted system resulted in 7 packet errors and 15 packet losses, while the unencrypted devices produced 2 packet errors and 9 packet losses. The average delay for messages generated by unencrypted devices was 83 milliseconds, whereas the average delay for encrypted messages was 1.109 milliseconds or 1 second 109 milliseconds. The throughput for devices with encryption had an average value of 3224.146 KBps, while devices without encryption had an average value of 6286.252 KBps. The LoRa used in the research operates at a frequency of 433 MHz. This system employs Speck 128-bit encryption, allowing a maximum message size of 16 characters. Based on the research findings, devices with encryption affect network performance by increasing the number of packet errors and losses, resulting in longer delays and decreased throughput.**

Keywords*— *Cryptography, Encryption, LoRa, MAC, Sniffing.

I. INTRODUCTION

Long Range (LoRa) is a communication system that has the capability to transmit data over long distances with low power consumption [1]. The built-in protocol for communication systems in LoRa is called LoRaWAN.

The LoRaWAN protocol has already fulfilled the primary objective of Low Power Wide Area Network, which is a category of wireless network technology specifically designed for IoT (Internet of Things) applications and sensors requiring long-range connectivity with low power consumption [2]. However, the LoRaWAN protocol still has weaknesses because data transmitted wirelessly is vulnerable to attacks. One common attack during the data transmission process in LoRaWAN is a sniffing attack. Sniffing is the act of monitoring data packets within a network system by unauthorized parties, allowing them to eavesdrop or potentially modify the data during the process [3]. Therefore, securing data from sniffing attacks is important.

The best technology to secure data is using cryptography [4]. Cryptography is an important and widely used part of mathematics [5]. to secure privacy and data [6]. Cryptography converts text into a code so that hackers who find the information, cannot see the message directly [7]. In cryptography, it is possible to convert plain text into secret data using keys [8]. Because of this, cryptography is also referred to as a technique for providing confidential communication [9] and to achieve the confidentiality and integrity of data by using user authentication [10] through key that used in the message encryption [11], where that key is only to be known by the sender and receiver [12].

Speck is one of the lightweight block cipher cryptographic algorithms suiTable for Wireless Sensor Network (WSN) devices due to its fast processing and minimal resource requirements [13] . This algorithm is capable of providing encryption and decryption of data with reasonably good security. Furthermore, to prevent unauthorized data transmission or data modification during the transmission process, security is enhanced by employing the Message Authentication Code (MAC) method. The MAC function serves to verify that the received message originates from the authentic source and has not undergone any alterations during transmission [14].

*Corresponding autho

Previous research by Rahayu Indah Lestari and team utilized the Advanced Encryption Standard (AES) algorithm in the encryption and decryption processes of messages. Additionally, the research employed the Ed25519 algorithm for the digital signature process. The purpose of implementing a digital signature in this system is to verify that the transmitted payload data is authentic and remains unchanged during the transmission process, ensuring confidentiality. The system implementation is utilized in the LoRa module to address sniffing attacks [15].

II. METHOD

This research falls under the category of Research and Development (R&D). Research and Development is a research method that aims to produce a specific product or improve existing products while testing the effectiveness of the developed product. In this study, the research and development method is employed because the goal is to design security for LoRaWAN networks using the Speck algorithm and MAC.

A. Research Stages

The stages of system development in this research are illustrated in Figure 1.

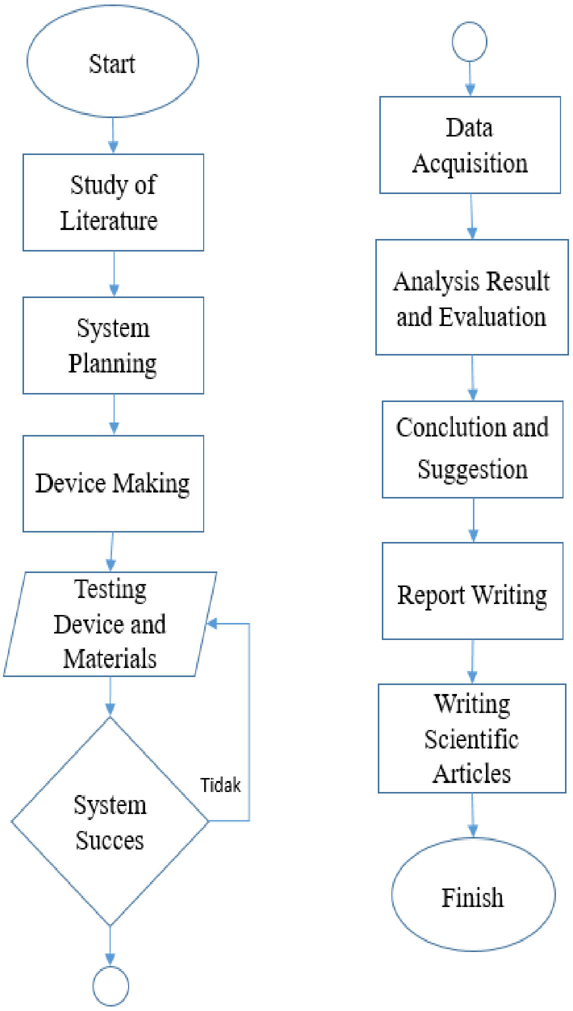
Start
Study of Literature
System Planning
Device Making
Testing Device and Materials
System Succes
Tidak
Data Acquisition
Analysis Result and Evaluation
Conclution and Suggestion
Report Writing
Writing Scientific Articles
Finish

Figure 1. Flowchart of the research stages

B. Block Diagram System

The block diagram of the research system is shown in Figure 2.

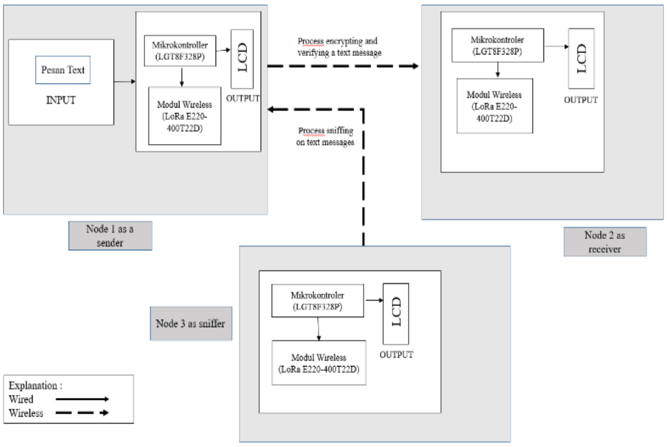
Pesan Text
INPUT
Mikrokontroller (LGT8F328P)
LCD
Modul Wireless (LoRa E220-400T22D)
OUTPUT
Node 1 as a sender
Process encrypting and verifying a text message
Process sniffing on text messages
Mikrokontroler (LGT8F328P)
LCD
Modul Wireless (LoRa E220-400T22D)
OUTPUT
Node 2 as receiver
Node 3 as sniffer
Mikrokontroler (LGT8F328P)
LCD
Modul Wireless (LoRa E220-400T22D)
OUTPUT
Explanation :
Wired
Wireless

Figure 2. Block diagram of system

Node 1 will send a data packet to Node 2. During the data transmission process between Node 1 and Node 2, Node 3, acting as a sniffer, will perform sniffing (capturing data packets) sent from Node 1 to Node 2. Therefore, the data packet sent by Node 1 will also be received by Node 3. This occurs because Node 3 operates on the same frequency as Node 1 and Node 2, which is 433 MHz, the frequency used in this research 2.

C. Flowchart Sender's Operation

The stages of the encryption system for the sender are as shown in Figures 3.

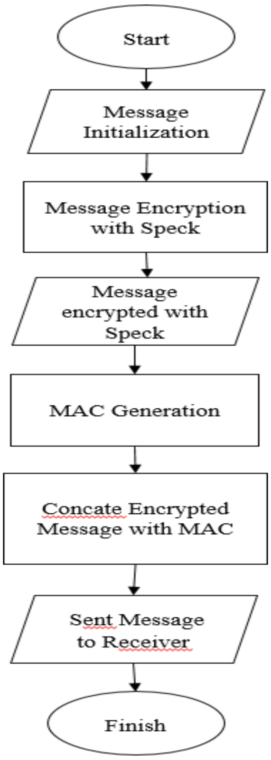
Start
Message Initialization
Message Encryption with Speck
Message encrypted with Speck
MAC Generation
Concate Encrypted Message with MAC
Sent Message to Receiver
Finish

Figure 3. Flowchart sender's operation

D. Flowchart Receiver's Operation

The stages of the encryption system for the receiver are as shown in Figures 4.

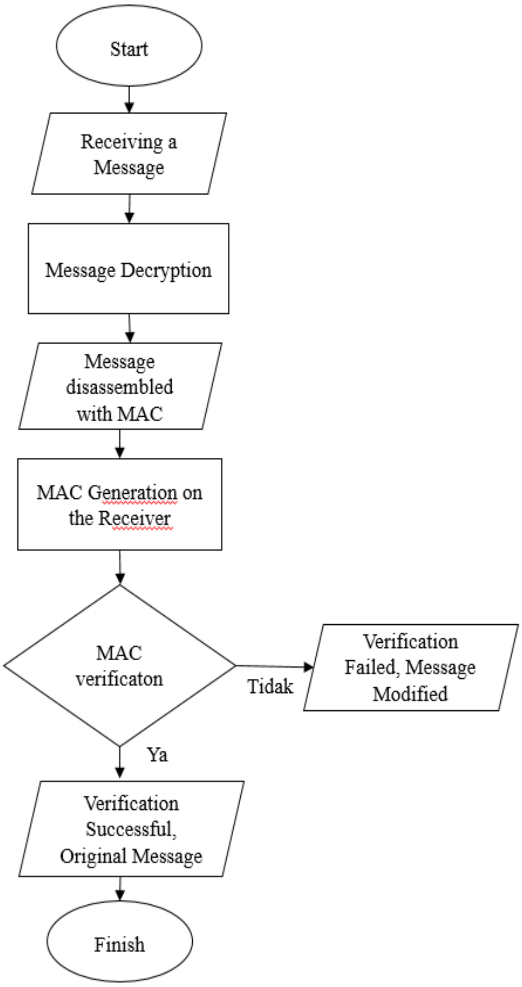
Start
Receiving a Message
Message Decryption
Message disassembled with MAC
MAC Generation on the Receiver
MAC verificaton
Tidak
Verification Failed, Message Modified
Ya
Verification Successful, Original Message
Finish

Figure 4. Flowchart of the receiver's operation

On the sender's side, the message or plaintext is first initialized. After the successful initialization of the message, it undergoes encryption using the Speck algorithm. Subsequently, the process continues with MAC generation, and the MAC value generated in the MAC generation process is combined with the encrypted message. The combined message and MAC are then sent to the receiver.

On the receiver's side, the encrypted message (consisting of the ciphertext resulting from the combination of the encrypted message and the MAC value) is first decrypted, producing the message and the still attached MAC. After successful decryption, the message is separated into the original plaintext and the MAC value. The receiver then performs the MAC value generation process on the receiver's side. Next, the receiver compares the MAC value generated from the sender's side with the MAC value generated on the receiver's side. If the MAC values on the sender's and receiver's sides match, the verification process is successful, indicating that the message sent to the receiver is the original message from the sender. However, if the MAC values on the sender's and receiver's sides are different, the verification process fails, indicating that the message sent to the receiver is not the original message from the sender.

E. Attack Model

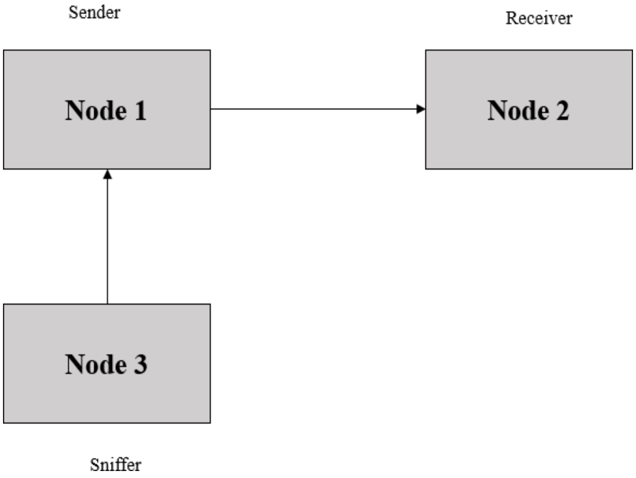

Figure 5. Attack model

Figure 5 show that node 1 is acting as the sender, then will send a message to Node 2, acting as the receiver. When the message transmission process occurs between Node 1 and Node 2, the message will also be received by Node 3, acting as a sniffer. Therefore, to prevent Node 3 from reading the message sent from Node 1 to Node 2, an encryption process is needed for the message to be transmitted.

III. RESULTS AND DISCUSSION

A. The Result of The System and Design

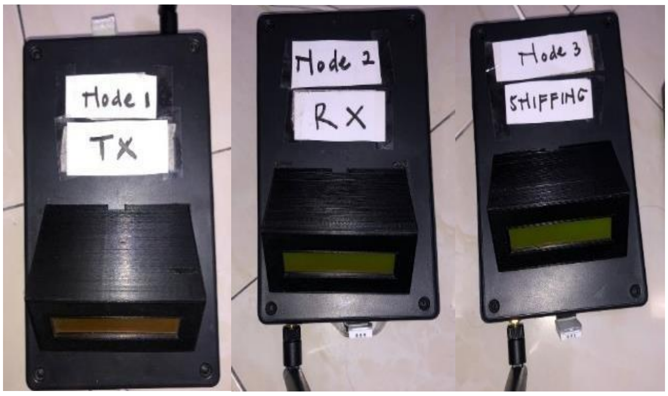

Figure 6. The result of system and design

The Figure 6 shows the results of the system design, which includes 3 nodes functioning as the sender, receiver, and the node that will perform sniffing attacks. Within each box, there are components such as the LGT8F328P, which functions as the microcontroller, LoRa E220-400T22D, serving as the transmitter, and a battery as the power source.

B. Security Data Testing

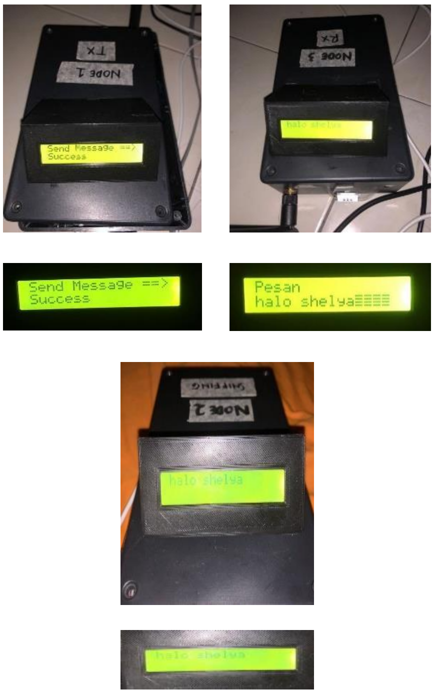

Figure 7. The Results of Passive Sniffing Attack Testing without Encryption

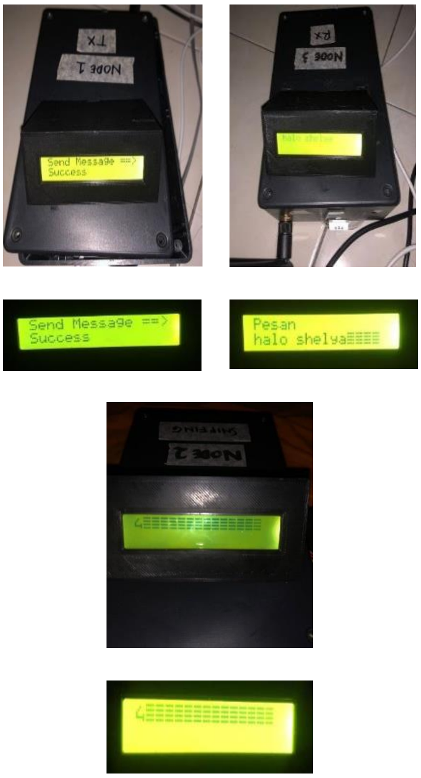

Figure 8. The Results of Passive Sniffing Attack Testing with Encryption

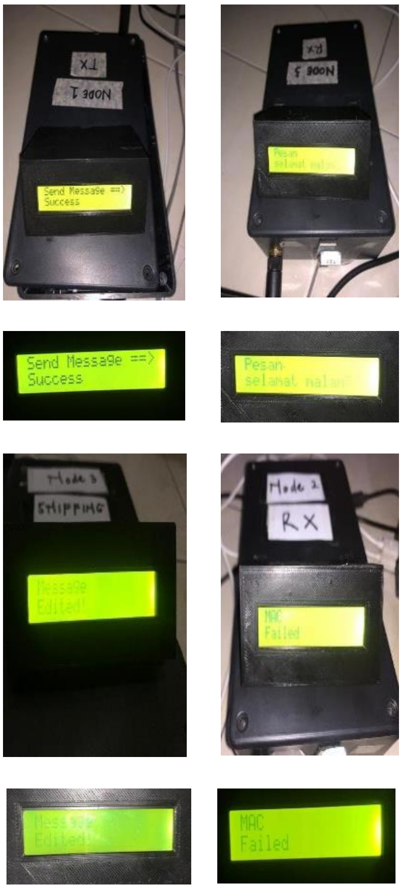

Figure 9. The Results of Passive Sniffing Attack Testing with Encryption

Figure 7, shows the results of security testing without encryption. Data transmitted from node TX to node RX without encryption can experience leaks to other parties, as demonstrated in the sniffing experiment conducted in this research. This condition indicates that the transmitted packets can be easily captured and read by unauthorized nodes. As a result, the confidentiality of the data cannot be guaranteed when encryption is not applied.

Figure 8, illustrates the results of security testing with encryption against passive sniffing attacks. Data transmitted from node TX to node RX with encryption does not experience leaks to other parties because before the data is sent to node RX, it is encrypted first and then transmitted to node RX. This encryption process ensures that intercepted data cannot be interpreted by unauthorized parties. Consequently, data confidentiality during transmission is significantly improved compared to the non-encrypted scenario.

Figure 9, shows the results of security testing with encryption against active sniffing attacks. Data transmitted from node TX to node RX can be ensured to be the authentic data from node TX without undergoing changes during the message transmission process. This is because the MAC value on the receiver's side will be compared with the MAC value from the sender's side. Therefore, if there is any alteration in the message by the sniffing node or if fake messages are sent, the MAC value on the receiver's side will verify the message with a 'failed' verification, indicating that the message has been altered or is fake and is not the original message from the sender intended for the receiver.

C. Packet Error and Packet Loss Testing

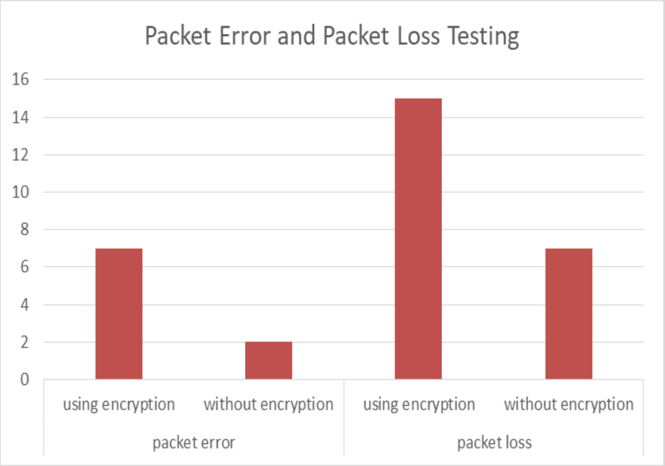

Figure 10. The Results of testing packet error and packet loss with encryption and without encryption

Figure 10, shows the testing results of packet errors and packet loss generated by devices without encryption and devices with encryption. Out of 100 transmission attempts, the results indicate that the device with encryption produces more packet errors and packet loss compared to the device without encryption.

D. Delay Testing

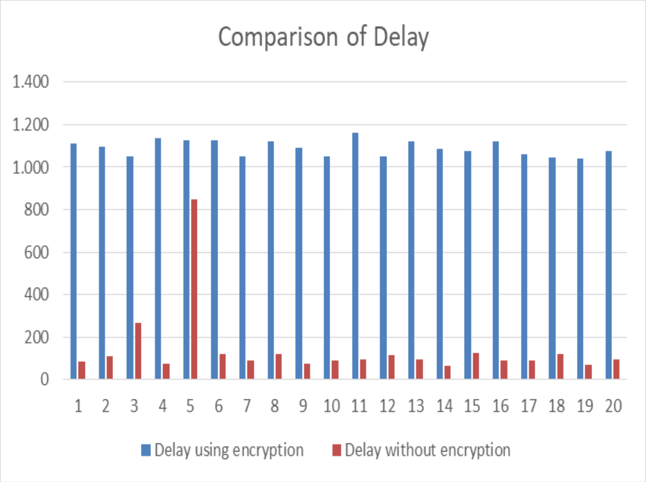

Figure 11. The results comparison of delay with encryption and without encryption

Figure 11, shows the delay testing conducted 20 times on devices without encryption and devices with encryption. The device without encryption averages a message delay of 83 milliseconds, while the average message delay with encryption is 1,109 milliseconds or 1 second and 109 milliseconds.

E. Throughput Testing

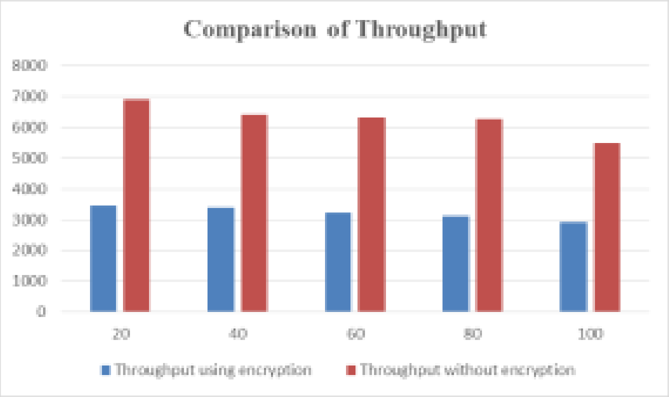

Figure 12. The results comparison of throughput with encryption and without encryption

Figure 12, shows the results of throughput testing on devices without encryption and devices with encryption. In this test, throughput was observed in every 20 data testing cycles, resulting in throughput values as shown in the Table. The average throughput on devices with encryption is 3224.146 KBps, while the average throughput on devices without encryption is 6286.252 KBps.

IV. CONCLUSION

The LoRa used in this research operates at a frequency of 433 MHz. The addition of encryption to the system introduces limitations on message transmission depending on the size of the encryption key used by the algorithm. This system uses Speck 128-bit, meaning 128 bits / 8 bits = 16 characters. In contrast, devices without encryption can transmit messages without character limitations. The use of encryption also affects the network performance in terms of packet error and packet loss, delay, and throughput. For devices without encryption, in 100 trial attempts, there were 2 packet errors and 7 packet losses. In the system using encryption, the number of packet errors increased to 7, and there were 15 packet losses. The average delay of messages generated by devices without encryption is 83 milliseconds, whereas the average delay for encrypted messages is 1,109 milliseconds or 1 second and 109 milliseconds. The throughput for devices with encryption has an average value of 3224.146 KBps, while devices without encryption have an average throughput of 6286.252 KBps.

REFERENCES

[1] A. Augustin, J. Yi, T. Clawsen dan M. W. Townsley, “A Study of LoRa: Long Range & Low Power Networks for the Internet of Things,” sensors, vol. 3, pp. 2-18, 2016.

[2] J. d. C. Silva, A. M. Albert, J. Rodrigues dan P. Šolić, “LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities,” dalam International Multidisciplinary Conference on Computer and Energy Science, Split, Croatia, 2017.

[3] A. R. Fauzi, “Monitoring jaringan wireless terhadap serangan paket sniffing,” Jurnal Manajemen Informatika, vol. 8, pp. 11-18, 2018.

[4] N. b. Anwar, M. Hasan, J. Z. Loren dan T. Hossain, “Comparative Study of Cryptography Algorithms and Its' Applications,” International Journal of Computer Networks and Communications Security, Vol. 7, no. 5.

[5] M. Benssalah, Y. Rhaskali dan K. drouiche, “An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography,” Multimedia Tools and Applications, vol. 80, pp. 2081-2107, 2021.

[6] M. Khari, A. K. Garg dan A. H. Gandomi, “Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, p. 73–80, 2020.

[7] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein dan H. F.A. Hamed, “Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques,” IEEE Access, vol. 9, p. 31805–31815, 2021.

[8] E. Hureib dan A. Gutub, “Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography,” IJCSNS International Journal of Computer Science and Network Security, vol. 20, 2020.

[9] F. Q. Alyousuf, F. Qasim, A. Al-Yousuf dan R. Din, “Review on secured data capabilities of cryptography, steganography, and watermarking domain Topic identification using filtering and rule generation algorithm for textual document View project The modeling of E- Supervised (E- SUV) for distance learning,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 17, p. 1053–1059, 2020.

[10] Z. Alqad, M. Oraiqat, A. H. Al-Saleh, . S. Hind, A. Husban dan S. Al-Rimawi, “International Journal of Computer Science and Mobile Computing A New Approach for Data Cryptography,” International Journal of Computer Science and Mobile Computing , vol. 8, 2019.

[11] Z. Qowi dan N. Hudallah, “Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm,” Journal of Physics: Conference Series, p. 1918, 2021.

[12] M. M. Abu-Faraj, K. Aldebei dan . Z. A. Alqadi, “Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography,” Traitement Du Signal, vol. 39, p. 173– 178, 2022.

[13] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks dan L. Wingers, “The SIMON and SPECK Families of Lightweight Block Ciphers,” Proceeding of the 52nd Annual Design Automation Conference on - DAC '15, pp. 48-56, 2013.

[14] M. Bellare, R. Canetti dan H. Krawczyk, “Keying Hash Functions for Message Authentication,” International Association for Cryptologic Research, 1996.

[15] R. I. Lestari, V. Suryani dan A. W. Arif, “Implementasi Pengamanan Pada Jaringan LoRaWAN Untuk Mengatasi Serangan Sniffing dengan Menggunakan Digital Signature.,” E proceeding of Engineering, vol. 7, pp. 7983-7994, 2020.