Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 13, No. 1, March 2025, pp. 110~124
ISSN: 2089-3272, DOI: 10.52549/ijeei.v13i1.6021

Developing a Prototype for Enhancing Data Security in LoRa-Based Theft Detection Systems Using ASCON-128 Encryption

Fetty Amelia[1], Bella Wulandari Hartejo[2]
[1,2]Cryptographic Hardware Engineering, National Cyber and Cryptography Polytechnic, Indonesia

Article Info

Article history:

Received Nov 6, 2024
Revised Feb 1, 2025
Accepted Mar 2, 2025

Keywords:

Theft Detector
Asset Tracking System
ASCON-128
LoRa (Long Range)

ABSTRACT

Asset protection is crucial for organizations to prevent theft. This study presents a LoRa-based theft detection prototype enhanced with ASCON-128 encryption for secure data transmission. The system consists of a transmitter attached to assets and a receiver in a monitoring room, featuring a web-based digital map for real-time tracking. ASCON-128, a NIST-standard lightweight encryption algorithm, ensures data confidentiality and integrity against Man-In-The-Middle (MITM) attacks.

The system was evaluated based on transmission speed, power consumption, and security performance. Results indicate that ASCON-128 integration reduces data transmission speed by 42.7% in Line-of-Sight (LOS) and 45.35% in Non-Line-of-Sight (NLOS) conditions. Power consumption increased by 2.7% in standby mode and 12.85% under simulated attack scenarios. Despite these trade-offs, encryption provides significant security benefits with acceptable resource overhead, making it a viable solution for LoRa-based asset tracking and theft detection.

Corresponding Author:

Fetty Amelia,
Cryptographic Hardware Engineering,
National Cyber and Cryptography Polytechnic,
Jl. Raya H. Usa, Putat Nutug, Kec. Ciseeng, Kabupaten Bogor, Jawa Barat 16120, Indonesia
Email: fetty.amelia@poltekssn.ac.id

1. INTRODUCTION

Assets are resources owned by an organization that can provide potential economic and social benefits. Assets consist of tangible and intangible assets. Intangible assets are non-financial assets that can be identified but have no physical form. Tangible assets are financial and/or non-financial assets that can be identified and have physical forms [1]. Tangible assets are mainly used by an organization to support its operational activities [2]. The assets of an organization must be securely protected to avoid threats and hazards towards the confidentiality of data [3]. In managing tangible assets of an organization, it is necessary to apply an asset security system to avoid asset theft and damage risks [4]. One of the approaches to protect and secure tangible assets is by monitoring the assets to detect and prevent illegal physical access to the assets [5].

A variety of transmission media offers low-power wireless network services that reach out an optimal distance range, such as Bluetooth, ZigBee, Wi-Fi, and Long Range (LoRa). LoRa is a wireless modulation technique that has a wide communication coverage, with low-power consumption and can transmit far distance data at an affordable cost. Therefore, LoRa is a suitable option as a transmission media in a theft detector system [6][7]. LoRa is used in many IoT (Internet of Things) applications, among others to develop smart cities, industries, and in the health sector. In Indonesia, the working frequency license for LoRa is at 433.05—434.79 MHz; 920—923 MHz; and 2400—2483.5 MHz which are categorized under the LPWAN (Low Power Wide Area Network) [8]. The ideal distance range of LoRa stretches between 10 to 15 km [9][10].

LoRa in an IoT device can be applied in a wireless warning and security system to provide a wide communication coverage [11]. As such, applying LoRa in the theft detector device can prevent and detect a theft. Research [12] in developing a theft detector device was carried out using a LoRa-based asset tracking system that detects vibration changes and traces the location as the two parameters. Data security in this

research [12] applies the AES-256 algorithm, and the result data in the receiver device are shown on the OLED display in real time, which is equipped with a buzzer and an LED light as a theft indicator. Further research [12] was developed [13] by replacing the data communication security algorithm with PRESENT, which is considered lighter, substituting the vibration indicator with an inclination indicator which better represents a theft incident. Furthermore, for efficient power usage, messages are only delivered if there are changes of the coordinate and the inclination of the asset. In another research [13], the PRESENT algorithm was set to be compatible with the vector test; however, when it was integrated into the system, the output data of the inclination sensor and the GPS could not be processed as an input to the PRESENT algorithm (the PRESENT algorithm could not be fully integrated into the system).

The security of data delivery in the theft detector system using LoRa is one of the solutions to safeguard the confidentiality of data and prevent illegal entities from tapping and modifying information. On 7 February 2023, NIST selected and standardized a light-weight cryptography algorithm known as ASCON for small-sized electronic devices that have limited power resources and for Internet of Things (IoT) devices. ASCON is one of the authenticated encryption programs using associated data (AEAD) algorithms that protect the confidentiality and authenticity of messages in the process of data transmission [14]. If applied in a theft detector device, it can prevent the tapping and modification of information or known as the attack of the Man-In-The-Middle (MITM).

Considering the above issue, this research aims to design a prototype of a theft detector system using a LoRa-based Authenticated Encryption with Associated Data (AEAD) ASCON-128 algorithm to secure data transmission. The ASCON-128 algorithm in this research is applied as the cryptography algorithm to encrypt messages transmitted and maintain the message authenticity during the transmission process and prevent any MITM attack that attempts to tap and modify information. The theft detector device consists of a transmitter device attached to the physical assets and a receiver device located in the monitoring room with the data transmission media using LoRa at the frequency of 915 MHz as determined by [8]. Moreover, this developed system is user-friendly as it shows the coordinates (GPS) of the assets through a digital map.

2. RESEARCH METHODOLOGY

This study employs an experimental approach to evaluate the impact of ASCON-128 encryption on the performance of a LoRa-based theft detection system. The research is designed to assess three key aspects: data transmission speed, power consumption, and security effectiveness. The independent variable in this experiment is the application of ASCON-128 encryption, while the dependent variables include transmission speed (measured in kilobits per second) under different environmental conditions, power consumption (measured in milliamperes and watts) in both standby and simulated attack scenarios, and the system's resistance to eavesdropping attempts. By systematically varying these factors, the study aims to provide a comprehensive analysis of how lightweight cryptographic integration affects system performance. This research follows an experimental design approach, where data is systematically collected and analyzed based on quantifiable parameters [15].

The experimental setup consists of a transmitter device, comprising an ESP32 microcontroller, an accelerometer, a GPS module, and a LoRa RFM95 transceiver, and a receiver device, built using a Raspberry Pi 4 Model B with a LoRa RFM95 module and a web-based monitoring system. Transmission speed was tested at distances of 50 meters, 100 meters, and 150 meters in both Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) conditions, with the time difference between data transmission and reception recorded for speed calculations. Power consumption measurements were conducted using a 5000 mAh power bank as the transmitter's power source, where current draw was observed under standby and attack conditions to determine energy efficiency. Additionally, a security evaluation was performed by introducing an external passive receiver to intercept transmitted data, ensuring that encrypted messages remained unreadable without the correct decryption key. The development of the system follows a structured engineering approach based on the System Development Life Cycle (SDLC) framework with a waterfall model to guide the implementation process in a systematic manner [16].

Data collected from these experiments were analyzed to quantify the impact of ASCON-128 on system performance. Percentage changes in transmission speed and power consumption were calculated to assess the trade-offs introduced by encryption. The security effectiveness of the system was verified by examining whether intercepted data could be successfully decrypted. Finally, the findings were compared with existing literature to establish the feasibility of integrating ASCON-128 into LoRa-based asset tracking and theft detection applications, particularly in environments where resource efficiency is critical.

3. THE PROPOSED SYSTEM

The proposed system is a theft detector based on LoRa with the ASCON-128 algorithm as the data transmission security. The system is developed to enable prevention of a theft, to detect a security breach in an organization, to trace and find the location of an asset from a far distance with a user-friendly monitoring system and react or respond to the theft indication which is the basic function of this theft detector [17]. In addition, applying the ASCON-128 cryptography algorithm aims to protect the data transmitted and avoid illegal entities from tapping the transmission process. The transmitter device consists of ESP32, Accelerometer Gyro GY521 MPU6050 sensor, GPS Ublox Neo 6M module, buzzer, LoRa RFM95 module, and omnidirectional antenna. Meanwhile the receiver device consists of Raspberry Pi 4 Model B, buzzer, LED, LCD monitor, LoRa RFM95 module, and omnidirectional antenna.

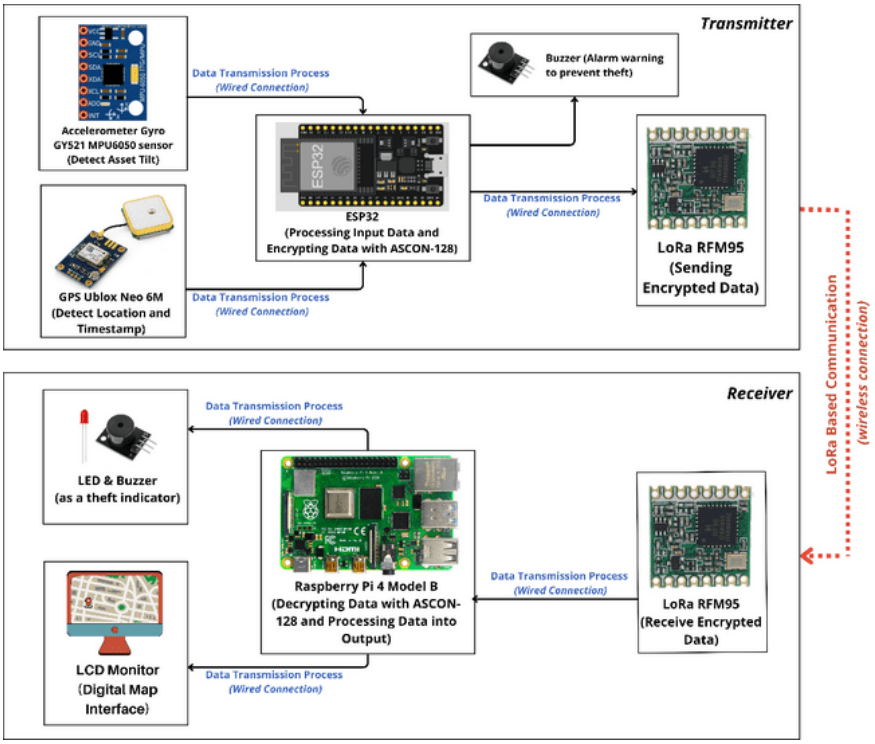

Figure 1. Proposed System Block Diagram

The workflow is presented in a system diagram block in Figure 1, starting with the accelerometer gyro GY521 MPU6050 sensor detecting changes of the inclination of the assets and the GPS Ublox Neo 6M module reading the timestamp and any change of the coordinate. The results will then be sent and processed at ESP32 (if there is an indication of a theft). The data are processed by ESP32, setting off the buzzer in the transmitter device in the event of a theft as a warning to prevent the theft. The data are processed to generate encrypted data using the ASCON-128 algorithm. The encrypted data are then forwarded to the LoRa RFM95 module (in the transmitter device) to be sent to the LoRa RFM95 module in the receiver device. In the receiver device, the LoRa RFM95 module receives the encrypted data which will be forwarded to Raspberry Pi 4 Model B to decrypt the data using the ASCON-128 algorithm and produce decrypted data. The decrypted data are stored in the database as a data log which will be further forwarded as the input for the digital map and the LCD monitor. The LCD monitor displays the digital map interface showing the coordinate change. The digital map interface operates in the web localhost of Raspberry Pi 4 Model B. If there is an indication of a theft in progress, the LED will light up, and in the monitoring room the buzzer will make a sound that indicates a theft of an asset. The theft detector in this research was further developed by applying the ASCON-128 cryptography algorithm to secure the transmission of data and use the Raspberry Pi 4 Model B as a supporting device to display a digital map interface on the LCD monitor. The transmitter device used in this research utilizes the same device as in the research of [13] by replacing the microcontroller with ESP32 that has a larger memory capacity and by adding a buzzer device in the transmitter. The model was made based on the testing results from the research of [13] which sufficiently represents a theft detector.

4. DEVELOPMENT

4.1. Transmitter Development

The function of the transmitter device is to integrate the hardware and the designed programs to run the system from the sender's side (transmitter) using the Arduino IDE software. The workflow of the transmitter device is presented in the flowchart in Figure 2.

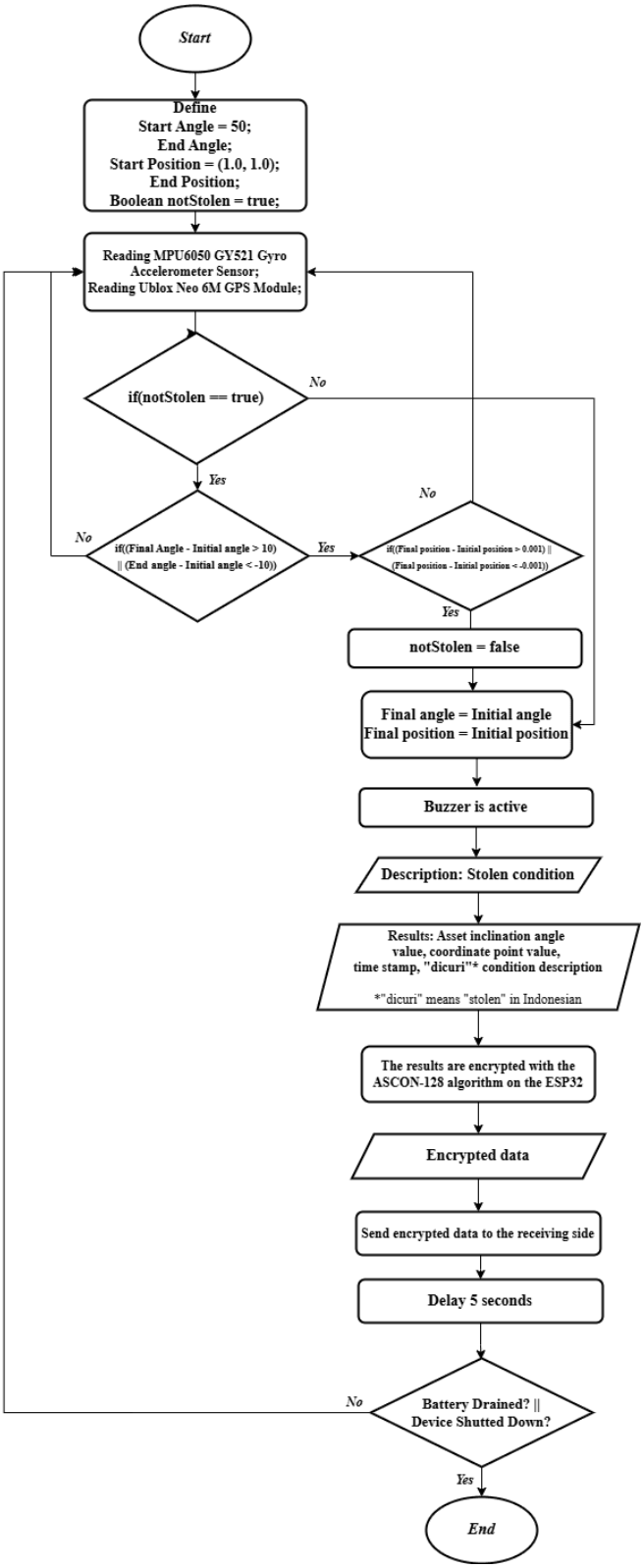

Figure 2. Transmitter Flowchart

The workflow of the transmitter device begins with the system activation and setting the variable to record the initial coordinate and angle of the asset. The Accelerometer Gyro GY521 MPU6050 sensor and the GPS Ublox Neo 6M module will detect the change of the inclination and coordinate of the assets. If the change of the angle exceeds ±10° or the coordinate shifts ±0.001, the buzzer will turn on as an alarm, indicating a theft. The data on the timestamp, the changes of the inclination and the coordinate are encrypted using the ASCON-128 algorithm and will be sent to the receiver device using the LoRa communication at the frequency of 915 MHz. The transmitter device system will keep monitoring and sending data every 5 seconds unless it is turned off or if the battery runs out.

Figure 3. Transmitter Device

Figure 3 is the transmitter device integrating all the components and the programming in the hardware of the transmitter device. The following data presents the details of the theft: the timestamp, the inclination and the coordinate of the stolen asset, and shows a ciphertext along with the tag value as seen in Figure 4.

```
17:58:29.183 -> Sending packet
17:58:29.490 -> Successs
17:58:34.495 -> Dicuri|-28.29|16/7/2024 17:54:56|-6.456428,106.666945
17:58:34.495 -> 5AB5E4D2900F5E3BDC077B7F615A87BDB5CC3D2F1A8277AD2C924D68A6F17322D7FCE0D43BD4B691C022C660BB12BD6C03B571646A
17:58:34.495 -> C6CC50ADABC4202C368FA1079020147C
17:58:34.495 -> Sending packet
17:58:34.812 -> Successs
17:58:39.810 -> Dicuri|-32.23|16/7/2024 17:54:56|-6.456428,106.666945
17:58:39.860 -> 5AB5E4D2900F5E3BDD0D7B7F6B5A87BD442423A957AB001C556AEF63DFC91A47F6AC9ED9E636062AD671C7C53971BAEDA79FF14A0E
```

Figure 4. Transmitter Device Serial Monitor

4.2. Receiver Development

The receiver device integrates all components in the hardware on the receiver side and the monitoring programming via Thonny IDE as shown in Figure 5. The workflow of the receiver device that plays a role as the asset monitoring system is presented in a flowchart in Figure 6. The workflow includes a LoRa-based communication program using the RFM95 module that decrypts the location and inclination of the asset using the ASCON-128 algorithm received from the transmitter device. As a warning of a thief, the beeping buzzer and LED light will turn on, and the data log and local database will be stored in the device, while the monitoring of the asset movement will be done through the digital map using the API platform in the web-based application operating at the local host.

Figure 5. Receiver Device

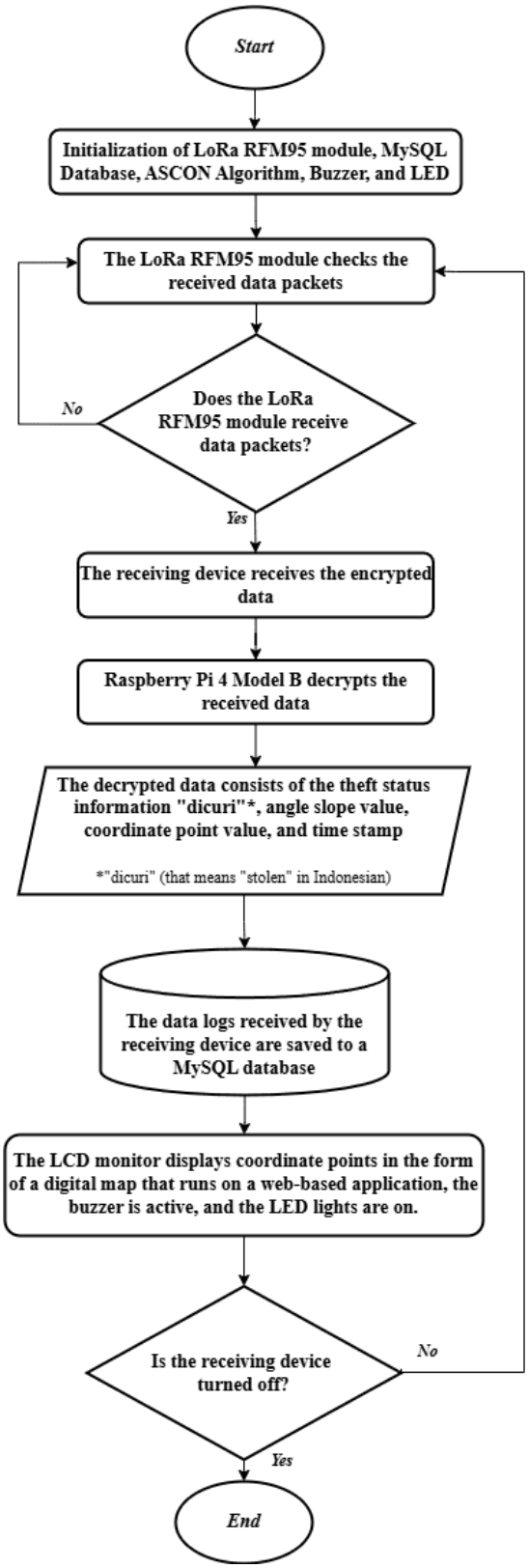

Figure 6. Receiver Flowchart

Figure 7 shows that the program runs well on the receiver side and can receive the data sent from the transmitter device without any loss of encrypted data. The data are then decrypted to generate data of the

status of theft, the inclination and the coordinate of the asset, the timestamp, and ciphertext along with the tag from ASCON-128.

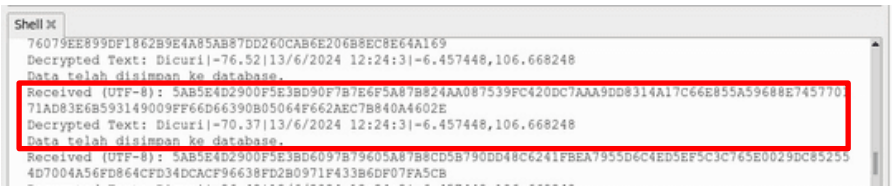

Figure 7. Receiver Device Serial Monitor

Furthermore, the data received is stored in the MySQL database. Figure 8 shows the database display used at the receiver device system.

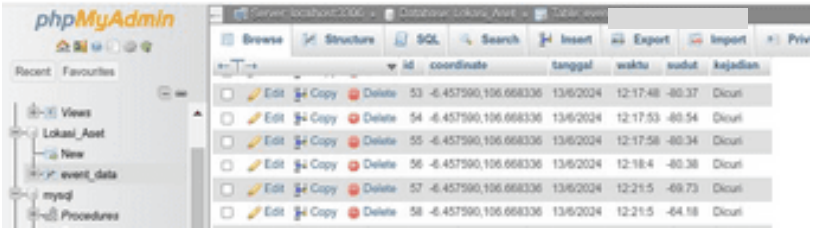

Figure 8. Receiver Device Database

The digital map interface display is shown in Figure 9 to track the asset from the monitoring room. The digital map application shows the coordinate based on the data stored in the MySQL database.

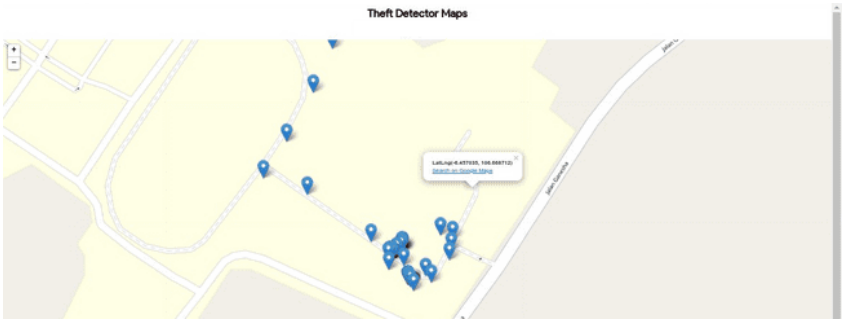

Figure 9. Web-based Digital Map Application

5. RESULT

5.1. Power Consumption

The test was conducted to compare the power consumption of the theft detector system before and after applying the ASCON-128 algorithm, under a stand-by condition and in the event of a theft (a hacked condition). The testing was only performed in the transmitter device as the transmitter has a dynamic function. In the testing scenario, the length of time required by the transmitter device to use up the power bank with a load of 5000 mAh was observed. The testing was done in four different conditions, namely:

- Condition A1, the device applies ASCON-128 in a stand-by mode.
- Condition A2, the device not applying ASCON-128 in a stand-by mode.
- Condition B1, the device applying ASCON-128 being hacked.
- Condition B2, the device not applying ASCON-128 being hacked.

The power consumption for the ESP32-based system is calculated from the average power consumed by ESP32 in one hour and expressed in Milliampere (mA). The formula used to measure the capacity in mAh is as follows [18].

$$Capacity\ (mAh) = Flow\ (mA) \times Time\ (hour) \quad (1)$$

Using this formula, the average power consumption of the device can be calculated as follows:

$$Device\ average\ power\ (mA) = \frac{Powerbank\ battery\ capacity\ (mAh)}{Device\ durability\ time\ (hour)} \quad (2)$$

Moreover, to determine the power consumption in Watt (W) units, it is necessary to identify the operational voltage of the transmitter device. The ESP32 operating in the transmitter device has a voltage of 3.3V. The power consumption (in Watt) can be measured as follows [19].

$$Power\ (W) = Current\ Flow\ (A) \times Voltage\ (V) \quad (3)$$

The increase in the percentage of power consumption before and after applying the ASCON-128 algorithm in the system, was compared to determining the percentage change using the following formula [20]. The results from the power consumption test using the above formula are presented in Table 1.

$$Percentage\ of\ Change\ (\%) = \frac{Value\ after\ (W) - Value\ before\ (W)}{Value\ Before\ (W)} \times 100\% \quad (4)$$

Table 1. Power Consumption Testing Results

Condition	Power bank Capacity (mAh)	Consumption Time of the transmitter device (hour)	Power Consumption (mA)	Power Consumption (Watt)
Condition A1	5000 mAh	12.53 hours	399 mA	1.317 W
Condition A2	5000 mAh	12.87 hours	388.5 mA	1.282 W
Condition B1	5000 mAh	11.22 hours	449.6 mA	1.484 W
Condition B2	5000 mAh	12.55 hours	398.4 mA	1.286 W

In the stand-by mode, without using the ASCON-128 algorithm, the system consumed 388.5 mA or 1.282 Watts per hour, whereas the system using the ASCON-128 algorithm consumed 399 mA or 1.317 Watts per hour. Based on these findings, the percentage of the power consumption increase is only 2.7%. However, in the hacked condition, the system without the ASCON-128 algorithm consumed 398.4 mA or 1.286 Watts per hour, while the system applying the ASCON-128 algorithm consumed on average 449.6 mA or 1.484 Watts per hour. Based on this result, the percentage of power increase is 12.85%. Under different conditions, the power consumptions in the system before and after applying the ASCON-128 algorithm shows that the device using the ASCON-128 algorithm requires processing much more data so that there is an increase in power consumption. However, the power consumption increase is considered reasonable, such as in any other product available in the market.

5.2. Data Transmission Speed

To compare the speed of the data transmission of the theft detector system with and without applying the ASCON-128 algorithm, the devices were set to have 50 meters, 100 meters, and 150 meters distance between the transmitter device and the receiver device under the conditions of Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS). The observed time starts from the time that the transmitter device sends the data to the receiver device. The difference between the time necessary to send the data and the time to receive it (the ending time) deducted by the time to send the data (the starting time) is applied as a basic calculation of the transmission duration using the following equation (5) [21].

$$Time\ duration\ (second) = ending\ time\ (second) - starting\ time\ (second) \quad (5)$$

Data transmission speed is defined as the amount of data that can be transmitted by a system in one time measured in bits per second (bps). The LoRa communication using the RFM95 module has an effective data transmission speed at the range of 0.18 Kbps to 37.5 Kbps [11]. Based on this definition, the correlation of the time duration and the data transmission speed in this research is presented in the equation of (6) below [22].

$$Data\ Transmission\ Speed\ (bps) = \frac{The\ amount\ of\ data\ transmitted\ (bit)}{Time\ duration\ (second)} \times 100\% \quad (6)$$

From the results of calculating the speed of transmitting the data, the theft detector system before and after applying the ASCON-128 algorithm was compared to determine the percentage of change by using

the the equation of (4). The test results on the speed of data transmission are presented in Table 2 based on 10 samples of data from each test.

Table 2. Data Transmission Speed Testing Results

No.	Transmission Distance (meter)	Data Transmission Time Duration (second)				Data Transmission Speed (Kbps)			
		ASCON-128		Without ASCON-128		ASCON-128		Without ASCON-128	
		LOS	NLOS	LOS	NLOS	LOS	NLOS	LOS	NLOS
1.	50 meters	0.032	0.363	0.189	0.174	30.5	2.689	5.164	5.609
		0.051	0.379	0.018	0.158	19.137	2.575	54.222	6.177
		0.018	0.335	0.204	0.187	54.222	2.913	4.784	5.219
		0.037	0.375	0.019	0.165	26.378	2.603	51.368	5.915
		0.052	0.338	0.038	0.164	18.769	2.888	25.684	5.951
		0.029	0.334	0.022	0.152	33.655	2.922	44.364	6.421
		0.021	0.340	0.043	0.178	46.476	2.871	22.698	5.483
		0.042	0.342	0.046	0.172	23.238	2.854	21.217	5.674
		0.036	0.355	0.017	0.184	27.111	2.749	57.412	5.304
		0.053	0.354	0.049	0.172	18.415	2.757	19.918	5.674
	Average (50 meters)	**0.0371**	**0.376**	**0.0645**	**0.173**	**29.790**	**2.782**	**30.683**	**5.743**
2.	100 meters	0.364	0.333	0.054	0.232	2.681	2.931	18.074	4.207
		0.368	0.355	0.054	0.203	2.652	2.749	18.074	4.808
		0.359	0.331	0.055	0.195	2.719	2.949	17.745	5.005
		0.351	0.328	0.056	0.173	2.781	2.976	17.429	5.642
		0.365	0.320	0.038	0.201	2.674	3.05	25.684	4.856
		0.359	0.315	0.056	0.206	2.719	3.098	17.429	4.738
		0.360	0.348	0.040	0.207	2.711	2.805	24.4	4.715
		0.366	0.331	0.055	0.172	2.667	2.949	17.745	5.674
		0.371	0.322	0.020	0.191	2.631	3.031	48.8	5.11
		0.380	0.323	0.035	0.166	2.568	3.022	27.886	5.88
	Average (100 meters)	**0.3663**	**0.330**	**0.0523**	**0.195**	**2.680**	**2.956**	**23.327**	**5.064**
3.	150 meters	0.342	0.365	0.229	0.237	2.854	2.674	4.262	4.118
		0.332	0.376	0.217	0.217	2.94	2.596	4.498	4.498
		0.337	0.365	0.215	0.207	2.896	2.674	4.54	4.715
		0.371	0.373	0.230	0.202	2.631	2.617	4.243	4.832
		0.265	0.381	0.229	0.236	3.683	2.562	4.262	4.136
		0.370	0.375	0.028	0.204	2.638	2.603	34.857	4.784
		0.344	0.449	0.206	0.229	2.837	2.174	4.738	4.262
		0.340	0.350	0.198	0.236	2.871	2.789	4.929	4.136
		0.276	0.347	0.117	0.223	3.536	2.813	8.342	4.377
		0.284	0.380	0.201	0.203	3.437	2.568	4.856	4.808
	Average (150 meters)	**0.326**	**0.365**	**0.209**	**0.229**	**3.032**	**2.607**	**7.953**	**4.467**
	Total average	**0.133**	**0.357**	**0.109**	**0.199**	**11.834**	**2.782**	**20.654**	**5.091**

In the LOS condition, the total average speed of the data transmission using ASCON-128 is 11.834 Kbps, while for the system not applying ASCON-128, the speed is 20.654 Kbps. The speed difference of the two systems is 8.82 Kbps. Using the equation of (4), the system applies ASCON-128 experienced a deceleration of 42.7% compared to the system not applying ASCON-128. In the NLOS condition, the total average speed of the data transmission applying ASCON-128 is 2.782 Kbps, while the speed for the system not using ASCON-128 is 5.091 Kbps. The speed difference is 2.309 Kbps. Based on the equation of (4), the system applying ASCON-128 experienced a deceleration of 45.35% compared to that of the system not using ASCON-128.

5.3. Distance Range of LoRa Communication

To test the communication range between the transmitter device and the receiver device in the system using LoRa with the farthest distance in the research of [12], which is 10.22 km in a cloudy bright weather in the LOS (Line-Of-Sight) mode, the RSSI (Receive Signal Strength Indicator) was observed to determine the signal strength value. RSSI is a receiving signal indicator in the receiver device which has a value range of 0 to -128 dBm [23]. In a distance of 10.22 km, the LoRa communication range of the designed system has a very low RSSI value, which is -121 dBm and -122 dBm causing disruption in the data receiving process. Not all data could be sent by the transmitter device and not received in full, so this indicates a failure in the decrypting process at the receiver end due to the very weak signal.

Figure 10. Data Sent from the Transmitter Device

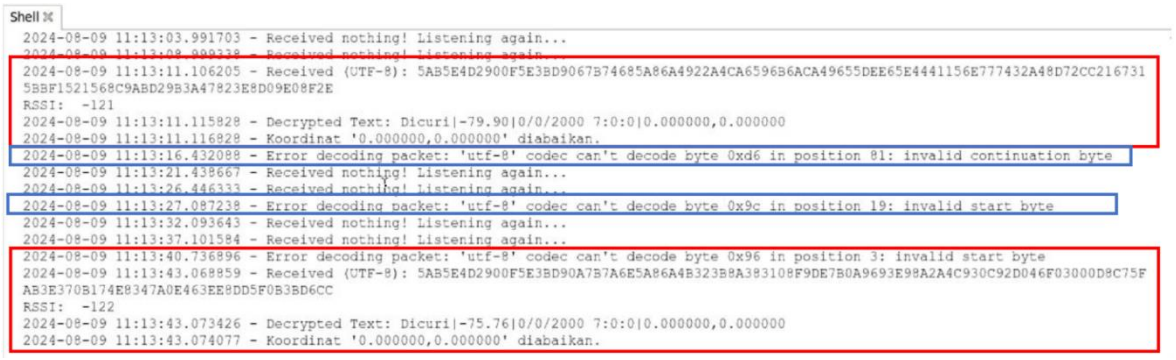

Figure 11. Data Received by the Receiver Device

Figure 10 presents the data sent from the transmitter device, and Figure 11 shows the data received by the receiver device. The red box indicates the data processed that was successfully sent and fully received by the receiver device, whereas the blue box shows the data received by the receiver device but could not be successfully decrypted. Furthermore, the volume of data also affects the quality of the data received. The larger the volume of data, the more vulnerable it is to transmission failure, particularly under a weak signal condition (low RSSI value). In the research of [12] at the same distance (10.22 km), the system was able to successfully send 512 bits of data. In the research of [13] at a farther distance (14.03 km) the system could only send 304 bits. However, in the same research, at a closer distance of 10.22 km, the system was able to send a larger volume of 976 bits. This shows that under a weak signal, the potential loss of data is higher as indicated by the results from the research of [12] and [13].

5.4. Securing the Data Transmitted

By applying the ASCON-128 algorithm in the theft detector system, an MITM attack of eavesdropping can be intercepted. This eavesdropping attack taps data using the passive receiver method [24]. The LoRa-based system which uses an open communication [24] is prone to eavesdropping that can access vital information if the data is not encrypted [25]. To try-out the security of the system, an attack of eavesdropping was applied to test whether the data sent had been encrypted using ASCON-128 and is safe from tapping. The scheme of an eavesdropping attack to test the security in this research is presented in Figure 12. The testing results are presented in Table 3.

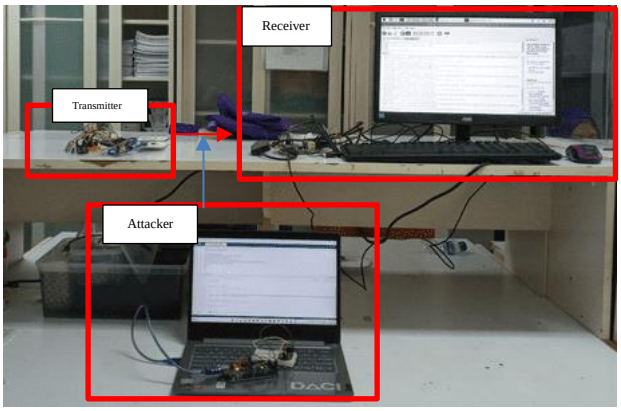

Figure 12. Eavesdropping Attack Scheme

Table 3. Security Testing Results with Eavesdropping Scheme

No.	Transmitter Device	Receiver Device	Attacker Device
1.	Plaintext: Hacked|91.40|0/0/2000 7:0:0|0.000000,0.000000 Ciphertext: 5AB5E4D2900F5E2F4AD9BCFB7819295C8A7C22E1BD63593A472CF49D785BC0143E90A48645045191ABD8B6077A Tag: 7D9662CBC96F94B038D891959B3DA710	Decrypted text: Hacked|91.40|0/0/2000 7:0:0|0.000000,0.000000	Ciphertext + Tag: 5AB5E4D2900F5E2F4AD9BCFB7819295C8A7C22E1BD63593A472CF49D785BC0143E90A48645045191ABD8B6077A7D9662CBC96F94B038D891959B3DA710
2.	Plaintext: Hacked|91.60|0/0/2000 7:0:0|0.000000,0.000000 Ciphertext: 5AB5E4D2900F5E2F4AD9BEFB7819295C71171A7696D858DB9B73D15D828E221621C25B192D73420EAC83699AF9 Tag: 5CFA123B19DD2DA8AC83AF3726C2E72A	Decrypted text: Hacked|91.60|0/0/2000 7:0:0|0.000000,0.000000	Ciphertext + Tag: 5AB5E4D2900F5E2F4AD9BEFB7819295C71171A7696D858DB9B73D15D828E221621C25B192D73420EAC83699AF95CFA123B19DD2DA8AC83AF3726C2E72A
3.	Plaintext: Hacked|91.55|0/0/2000 7:0:0|0.000000,0.000000 *Ciphertext:* 5AB5E4D2900F5E2F4AD9BDFE7819295C7422A8BED70F8C873ABCA5E59A098D2372829F59D767122DD1A7EA47A1 Tag: 400D9196B85780FA7E211AB2D497E429	Decrypted text: Hacked|91.55|0/0/2000 7:0:0|0.000000,0.000000	Ciphertext + Tag: 5AB5E4D2900F5E2F4AD9BDFE7819295C7422A8BED70F8C873ABCA5E59A098D2372829F59D767122DD1A7EA47A1400D9196B85780FA7E211AB2D497E429
4.	Plaintext: Hacked|91.49|0/0/2000 7:0:0|0.000000,0.000000 Ciphertext: 5AB5E4D2900F5E2F4AD9BCF27819295C059638E1802F895235C34502CC599E081FCAD80B1F38C5B6D1669FCFE3 Tag: 2FDF1A1A17354061D3A1C7A935C32F0E	Decrypted text: Hacked|91.49|0/0/2000 7:0:0|0.000000,0.000000	Ciphertext + Tag: 5AB5E4D2900F5E2F4AD9BCF27819295C059638E1802F8952355C34502CC599E081FCAD80B1F38C5B6D1669FCFE32FDF1A1A17354061D3A1C7A935C32F0E
5.	Plaintext: Hacked|91.35|0/0/2000 7:0:0|0.000000,0.000000 Ciphertext: 5AB5E4D2900F5E2F4AD9BBFE7819295C92398C24F85748A2A9A05775B30C1E63EB6B7C32A061FBB9FD30B47314 Tag: 839BCE9FC7CBE8CA0DC5A505DEDCCF73	Decrypted text: Hacked|91.35|0/0/2000 7:0:0|0.000000,0.000000	Ciphertext + Tag: 5AB5E4D2900F5E2F4AD9BBFE7819295C92398C24F85748A2A9A05775B30C1E63EB6B7C32A061FBB9FD30B47314839BCE9FC7CBE8CA0DC5A505DEDCCF73

The results from the security testing in Table 3 show that the theft detector system can securely transmit data using the ASCON-128 lightweight cryptography algorithm. The transmitter device managed to send the encrypted data while the attacker device only received random data. This shows that the system was able to avoid the attempt of tapping information, in this case an MITM attack of eavesdropping.

5.5. The Claim Offered by ASCON-128 in the Built System

The testing was conducted to try-out several features of ASCON-128 as claimed in the research of [26] using a developed theft detector system. In this system, the ASCON-128 algorithm was able to process authenticated encryption. In addition, the ASCON-128 algorithm can be applied in four different platforms, namely Arduino Nano, Arduino Mega, ESP32, and Raspberry Pi as depicted in Figure 13. This proves that ASCON can be applied in many platforms, as it has claimed.

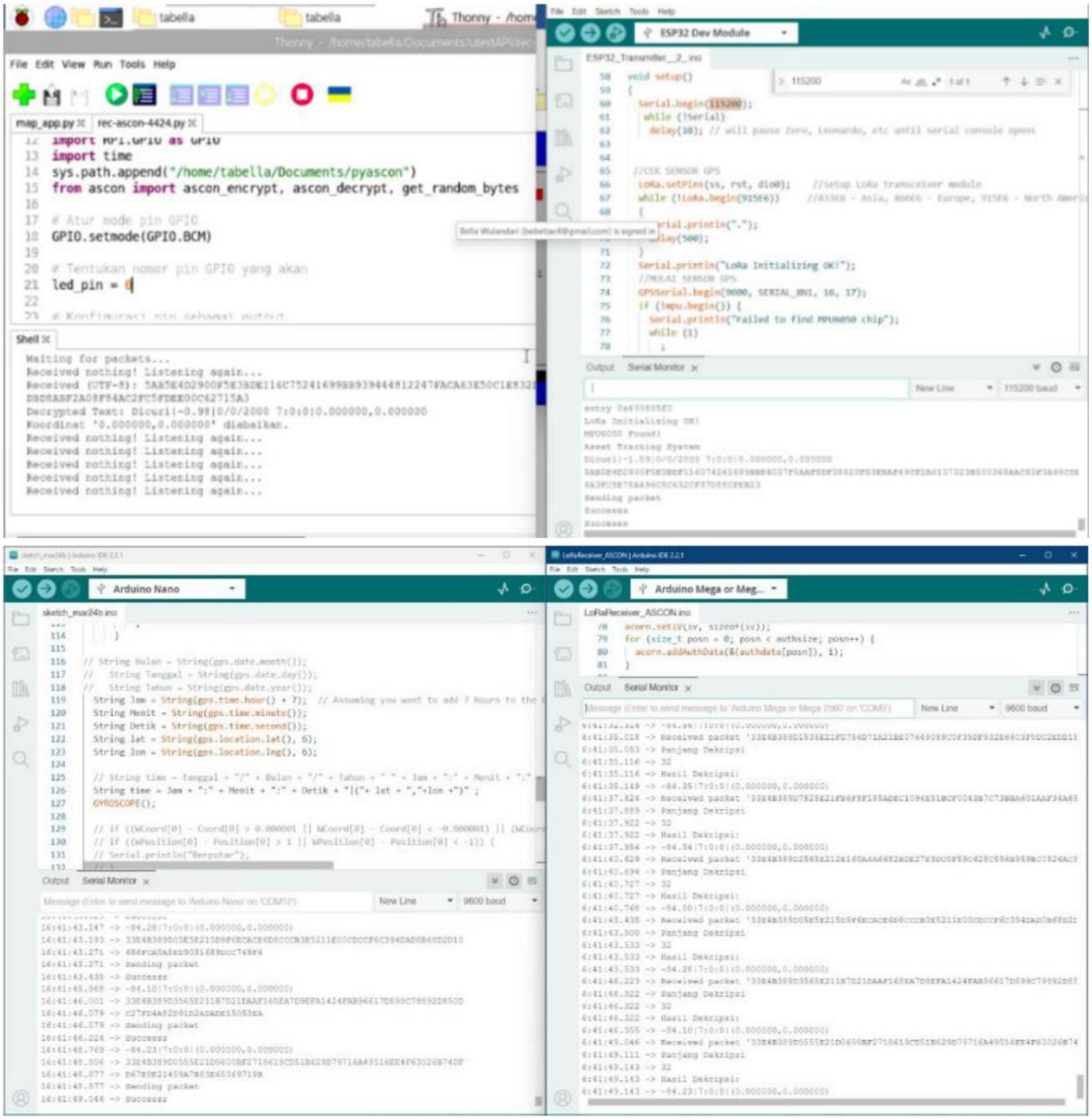

Figure 13. ASCON-128 in Raspberry Pi, ESP32, Arduino Nano, and Arduino Mega

In terms of memory consumption in ESP32, the ASCON-128 requires a ROM size of 10304 bytes or 10.304 kb. The test compared the memory usage in the theft detector system before and after applying the ASCON-128 in ESP32 and analyzed the difference of the memory usage. Figure 14 shows that the theft detector system with ASCON-128 consumes a ROM of 305069 bytes out of the total program storage capacity of 1310720 bytes. Figure 15 shows that the theft detector system without ASCON-128 consumes a ROM of 294765 bytes out of the total storage capacity. The difference of the ROM consumption between the two systems (with and without ASCON-128) is 10304 bytes. By using the formula of (4), the percentage of the ROM consumption with ASCON-128 is higher by 3.49% compared to that of the system without ASCON-128. This indicates that ASCON-128 consumes a relatively small memory so that it is suitable for small-sized hardware as claimed by the ASCON-128 algorithm.

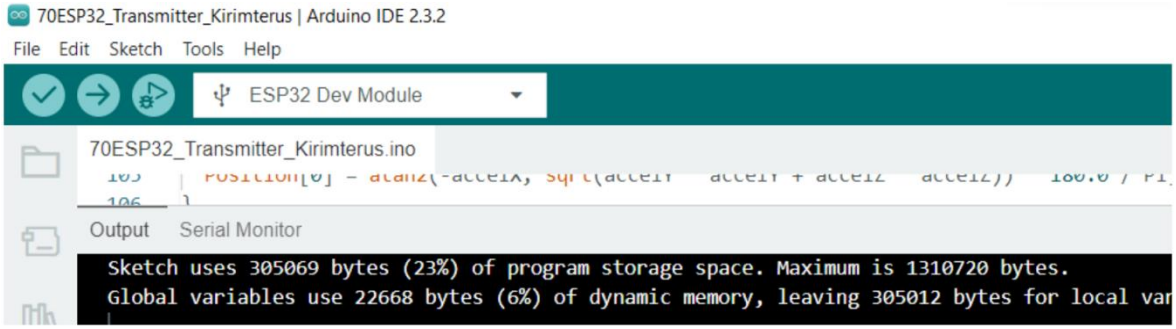

Figure 14. Memory Consumption of the Theft Detector with ASCON-128

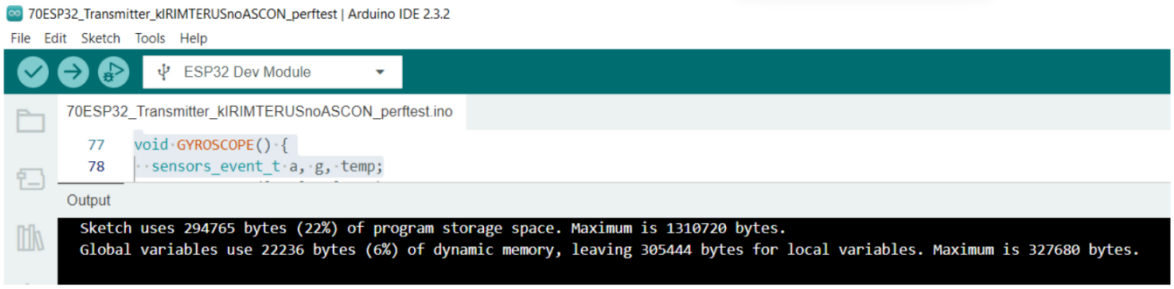

Figure 15. Memory Consumption of the Theft Detector without ASCON-128

6. DISCUSSION

The results of this study demonstrate that integrating ASCON-128 encryption into a LoRa-based theft detection system significantly impacts data transmission speed and power consumption. The observed 42.7% decrease in transmission speed under LOS conditions and 45.35% under NLOS conditions raises concerns about the trade-offs between security and system efficiency. However, in the context of LoRa communication, such reductions remain within an acceptable range when considering existing applications in low-power, long-range IoT systems. Prior research on LoRa-based asset tracking [12] reported transmission speeds between 2.7 Kbps and 20.6 Kbps, similar to the findings in this study, where speeds with ASCON-128 ranged from 2.782 Kbps to 11.834 Kbps. Although encryption introduces latency, its impact remains comparable to the performance of other secure IoT systems [13].

In terms of power consumption, ASCON-128 integration resulted in a 2.7% increase in standby mode and a 12.85% increase under attack conditions. These values align with other cryptographic implementations in IoT security systems, where lightweight encryption methods such as PRESENT [13] or AES-256 [12] also introduce additional energy costs. When compared to AES-256, which is widely used for securing data in resource-constrained environments, ASCON-128 offers a more efficient alternative in terms of power efficiency and integration flexibility, making it a viable option for theft detection applications. The trade-off between power consumption and security is particularly relevant in IoT-based asset monitoring, where extended battery life is crucial. Previous studies have shown that encryption-related power increases of up to 15% are considered tolerable for security-enhanced IoT applications [14]. Given that the power overhead in this study remains below that threshold, ASCON-128 proves to be a practical choice for securing LoRa-based systems.

The security evaluation through eavesdropping tests further confirms the effectiveness of ASCON-128 in protecting transmitted data. Unlike plaintext LoRa communication, which is inherently vulnerable to interception and manipulation [25], the encryption mechanism in this study ensures that intercepted data remains unreadable. Prior research on LoRa security [24] has highlighted the susceptibility of open transmissions to Man-In-The-Middle (MITM) attacks. In contrast, the encrypted messages in this study retained data integrity and confidentiality, demonstrating that ASCON-128 effectively mitigates such vulnerabilities. However, while this study confirms resistance to passive eavesdropping, future research should explore more sophisticated attack scenarios, such as active interference or cryptanalysis under constrained environments.

Overall, the findings of this study reinforce the viability of ASCON-128 as an encryption solution for LoRa-based theft detection. Compared to previous implementations using AES-256 [12] and PRESENT [13], ASCON-128 provides a balance between security, energy efficiency, and computational feasibility, making it well-suited for IoT-based asset tracking systems. While there are trade-offs in speed and power, these

remain within tolerable limits for long-range, low-power communication networks. Future studies should investigate further optimizations, such as adaptive encryption mechanisms, to enhance performance without compromising security.

7. CONCLUSION

This research proves that the ASCON-128 algorithm in the designed theft detector system has performed well. In this theft detector system, the ASCON-128 algorithm was able to encrypt authentic data, and this algorithm could be applied in four different platforms, namely Arduino Nano, Arduino Mega, ESP32, and Raspberry Pi. In terms of memory consumption in ESP32, the ASCON-128 requires a ROM size of 10,304 bytes or 10.304 kb. The increase of power consumption in the system using ASCON-128 is only 10.5 mA in stand-by mode and 51.2 mA in hacked conditions. Meanwhile, the system using ASCON-128 experienced a speed deceleration of 8.82 Kbps in transmitting data under the LOS condition and 2.309 Kbps under the NLOS condition when compared with the transmission speed of the system without ASCON-128. The ASCON-128 algorithm in the system was able to protect the transmitted data from the attack of eavesdropping. The speed of transmission in terms of percentage with and without applying the ASCON-128 algorithm in the theft detector system was also compared. In the LOS condition the system using ASCON-128 experienced a deceleration of 42.7% compared with the system not applying ASCON-128. In the NLOS condition, the system applying ASCON-128 experienced a deceleration of 45.35% compared to that of the system not using ASCON-128. The power consumption before and after applying the ASCON-128 algorithm in the theft detector system was compared. In the stand-by mode, the system using ASCON-128 experienced an increase of 2.7 % in power consumption. In the hacked condition, the system using ASCON-128 experienced an increase of 12.85% in power consumption. However, the increase in power consumption is considered reasonable compared to that of any other similar product available in the market. For further reseach, the prototype need to be integrated with a geolocation system that can be detect the prototype indoor dan back up power solution.

REFERENCES

[1] Presiden Republik Indonesia, Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2010 Tentang Standar Akuntansi Pemerintahan. 2010. Accessed: Jan. 17, 2024. [Online]. Available: https://peraturan.bpk.go.id/Details/5095/pp-no-71-tahun-2010

[2] Menteri Dalam Negeri Republik Indonesia, Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 1 Tahun 2019 Tentang Penyusunan Barang Milik Daerah. 2019, p. 3. Accessed: Jan. 17, 2024. [Online]. Available: https://peraturan.bpk.go.id/Details/121739/permendagri-no-1-tahun-2019

[3] ISO/IEC 2022, *ISO/IEC 27001-2022 (E) Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, vol. 3. Switzerland, 2022.

[4] NI Business Info, "Business Asset." Accessed: Jan. 17, 2024. [Online]. Available: https://www.nibusinessinfo.co.uk/content/tangible-assets

[5] ISO/IEC 2022, *ISO/IEC 27002-2022 (E) Information security, cybersecurity and privacy protection — Information security controls*, vol. 3. Switzerland, 2022.

[6] K. Lappanitchayakul, "Anti-theft device for car : Alert system using radio wave," *The 9th International Conference on Intelligent Informatics and BioMedical Sciences (ICIIBMS)*, pp. 351–355, 2019, doi: 10.1109/ICIIBMS46890.2019.8991531.

[7] F. Yao, Y. Ding, S. Hong, and S.-H. Yang, "A Survey on Evolved LoRa-Based Communication Technologies for Emerging Internet of Things Applications," *International Journal of Network Dynamics and Intelligence*, pp. 4–19, Dec. 2022, doi: 10.53941/ijndi0101002.

[8] Menteri Komunikasi dan Informatika Republik Indonesia, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 12 Tahun 2022 Tentang Tabel Alokasi Spektrum Frekuensi Radio Indonesia. 2022. Accessed: Dec. 04, 2023. [Online]. Available: https://jdih.kominfo.go.id/produk_hukum/view/id/834/t/peraturan+menteri+komunikasi+dan+informatika+nomor+12+tahun+2022

[9] Menteri Komunikasi dan Informatika Republik Indonesia, "Menteri Komunikasi dan Informatika Republik Indonesia, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 2 Tahun 2023 Tentang Penggunaan Spektrum Frekuensi Radio Berdasarkan Izin Kelas," 2023. Accessed: Dec. 04, 2023. [Online]. Available: https://jdih.kominfo.go.id/produk_hukum/view/id/862/t/peraturan+menteri+komunikasi+dan+informatika+nomor+2+tahun+2023

[10] M. Saari, A. Muzaffar Bin Baharudin, P. Sillberg, S. Hyrynsalmi, and W. Yan, "LoRa-A Survey of Recent Research Trends," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 872–877, 2018, doi: https://doi.org/10.23919/MIPRO.2018.8400161.

[11] L. HOPE MICROELECTRONICS CO., "Datasheet RFM95/96/97/98(W) - Low Power Long Range Transceiver Module" [Online]. Available: http://www.hoperf.com

[12] F. Amelia and M. F. Ramadhani, "LoRa-Based Asset Tracking System with Data Encryption Using AES-256 Algorithm," *Proceeding - 2022 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications: Emerging Science and Industrial Innovation in Electronics and Telecommunication, ICRAMET 2022*, pp. 194–199, 2022, doi: 10.1109/ICRAMET56917.2022.9991210.
[13] A. S. Tamba, "TUGAS AKHIR Implementasi Algoritma Present pada Prototipe Asset Tracking System berbasis LoRa," Politeknik Siber dan Sandi Negara, Bogor, 2023.
[14] NIST, "NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices," NIST. Accessed: Jan. 17, 2024. [Online]. Available: https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices
[15] S. B. Mishra and S. Alok, Handbook of Research Methodology. 2017. [Online]. Available: https://www.researchgate.net/publication/319207471
[16] A. Dennis, B. H. Wixom, and D. Tegarden, *SYSTEMS ANALYSIS & DESIGN : An Object-Oriented Approach with UML*, 5th ed. USA, 2015. [Online]. Available: http://store.visible.com/Wiley.aspx
[17] GOCodes, "7 Ways to Protect Fixed Assets Against Theft." Accessed: Jan. 17, 2024. [Online]. Available: https://gocodes.com/7-ways-to-protect-fixed-assets-against-theft/
[18] R. F. Rizal and H. Dwi Atmaja, "Analisis Chekup Pemeliharaan Batteray Capacity Test (BCT) 110 VDC Di PT. PLN (Persero) Gardu Induk 150 KV Jatigedong Jombang," 2022. [Online]. Available: www.elektro.itn.ac.id
[19] T. L. . Floyd, *Principles of electric circuits : conventional current version*. Pearson Education Limited, 2014.
[20] CUEMATH, "Percentage Change," https://www.cuemath.com/commercial-math/percentage-change/.
[21] Tess Loucka, "How to Calculate Elapsed Time," doodle learning by Discovery Education.
[22] W. J. Buchanan, *The Handbook of Data Communications and Networks*. Springer US, 2004. doi: 10.1007/978-1-4020-7870-5.
[23] P. Devi Dama Istianti, N. Bogi Aditya Karna, and I. Ali Nur Safa, "Perancangan dan implementasi Device Tentang Teknologi Akses LPWAN LoRa untuk Monitoring Air Sungai Citarum Device Design and Implementation about LPWAN LoRa Access Technology for Citarum River Water Monitoring," *eProceedings of Engineering*, vol. 6, no. 2, p. 4477, 2019.
[24] P. Syverson, "A Taxonomy of Replay Attacks," *Proceedings The Computer Security Foundations Workshop VII*, pp. 187–191, 1994, doi: https://doi.org/10.1109/CSFW.1994.315935.
[25] D. Basu, T. Gu, and P. Mohapatra, "Security Issues of Low Power Wide Area Networks in the Context of LoRa Networks," Jun. 2020, [Online]. Available: http://arxiv.org/abs/2006.16554
[26] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *Journal of Cryptology*, vol. 34, no. 3, Jul. 2021, doi: 10.1007/s00145-021-09398-9.

BIOGRAPHY OF AUTHORS

Fetty Amelia earned her *Magister Teknik* (M.T) (equal to Master's degree in Engineering) from Universitas Indonesia in 2019 and Bachelor of Applied Science from Sekolah Tinggi Sandi Negara in 2009. Currently she works as a lecturer at Politeknik Siber dan Sandi Negara. She has several profession certificates, which among others are Certified of Ethical Hacker (CEH) and Level 1 Security of Analyst (L1SOC). Some of her research publications include the fields of biometrics, cryptography, IoT, and communication system.

Bella Wulandari Hartejo was the last year student at Politeknik Siber dan Sandi Negara (when the research was completed), and she majored in the field of cryptography hardware engineering. She has several profession certificates, such as Junior Penetration Tester (JPT), CompTIA Security+ (Sec+), and Microsoft Security Operations Analyst. She has also published her research with the title *Implementation of AES-256 Algorithm for Secure Data Transmission in LoRa-based Forest Fire Monitoring System* at an international conference.
Contact : bella.wuladari@bssn.go.id