

Implementasi Radio LoRa dengan Enkripsi Caesar Cipher sebagai Proof-of-Concept Komunikasi Data Sistem Monitoring dan Kendali Latihan Militer

Egidius Tefa¹⁾, Fajar Kholid²⁾, Ananda Herdi Akbar³⁾

^{1), 2), 3)} Prodi Teknik Telekomunikasi Militer. Politeknik Angkatan Darat

Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia

E - mail : ¹⁾komd48014@gmail.com, ²⁾fajarkholid@yahoo.com,

³⁾aherdiakbar@gmail.com

Implementation of LoRa Radio with Caesar Cipher Encryption as a Proof of Concept for Data Communication in Military Training Monitoring and Control Systems

Abstract: This research discusses the implementation of LoRa technology and the Caesar Cipher encryption method in a monitoring and detonation control system for military training purposes. Conventional radio communication systems commonly used today have limitations in range, are vulnerable to frequency interference, and carry the risk of wiretapping, thus requiring a reliable and secure alternative technology. This study aims to design a wireless communication system prototype that integrates LoRa with Caesar Cipher encryption, and to test its performance in terms of range, latency, transmission success, and data protection resilience. An experimental method was employed utilizing hardware such as the Arduino Nano microcontroller, ESP32 as a gateway, LoRa SX1278 module, u-blox M-8N GPS sensor, and a web-based dashboard. Before transmission, all data, including location coordinate telemetry and detonator actuator control commands, are encrypted over the LoRa network. Test results indicate that the system can operate at a communication range of up to 500 meters. Quantitative testing with 500 packets per test point (100 packets/iteration × 5 repetitions) shows 0% packet loss at 100–200 meters (operational range), 5% packet loss at 300 meters, and 80% packet loss at the furthest test distance of 500 meters. Under Non-Line-of-Sight (N-LoS) conditions, the optimal range is 50–75 meters (0–2% packet loss), while at 150 meters, packet loss reaches 80% with a 3-second latency. The encode-decode function tested across 200 varied message samples achieved a 100% success rate based on exact string match. Computational benchmarks indicate an average encryption and decryption time of 624 μ s and 620 μ s for 50 characters, respectively. In conclusion, this prototype demonstrates successful system integration as an educational and prototypical proof-of-concept for military training applications.

Keywords: Caesar Cipher, Obfuscation, LoRa SX1278, Proof-of-Concept, Telemetry, Military Training.

Abstrak: Keandalan dan kerahasiaan komunikasi data nirkabel berbasis *embedded system* merupakan aspek vital dalam mendukung simulasi monitoring dan kendali pada latihan militer. Penelitian ini mengimplementasikan integrasi radio modul LoRa SX1278 (433 MHz) dengan mikrokontroler ESP32 dan Arduino

Nano, sensor GPS u-blox M8N, aktuator kendali, serta *dashboard* monitoring berbasis *web*. Sebagai *proof-of-concept*, skema penyandian *basic obfuscation* menggunakan algoritma Caesar Cipher diterapkan untuk menguji kesesuaian fungsi enkripsi-dekripsi data telemetri dan perintah kendali dua arah. Pengujian kinerja komunikasi LoRa dilakukan pada konfigurasi *Spreading Factor* SF7, *Bandwidth* 125 kHz, *Coding Rate* 4/5, daya pancar 20 dBm, *gain* antena 3 dBi, dan tinggi antena 1,5 meter. Hasil eksperimen kuantitatif dengan total pengiriman 500 paket per titik uji (100 paket/iterasi $\times$ 5 kali pengulangan) menunjukkan *packet loss* 0% dengan latensi rata-rata 92–98 ms pada rentang andal (*operational range*) *Line-of-Sight* (LoS) 100–200 m, *packet loss* 5% pada 300 m (*tested range*), dan *packet loss* 80% pada jarak uji terjauh 500 m (*critical range*). Pada skenario *Non-Line-of-Sight* (N-LoS), rentang operasional optimal dicapai pada 50–75 m (*packet loss* 0–2%), sedangkan pada 150 m mengalami peningkatan *packet loss* hingga 80% dengan latensi 3,0 detik. Pengujian fungsi *encode-decode* pada 200 sampel pesan bervariasi menghasilkan tingkat keberhasilan (*success rate*) 100% berdasarkan kesesuaian *exact string match*. *Benchmark* komputasi menunjukkan waktu enkripsi dan dekripsi rata-rata sebesar 624 μ s dan 620 μ s untuk 50 karakter (deviasi standar $\pm 8,5$ μ s), serta lonjakan waktu pada 500 karakter yang diidentifikasi sebagai dugaan keterbatasan alokasi memori dinamis mikrokontroler. Hasil penelitian ini membuktikan keberhasilan integrasi sistem telemetri dan kendali berbasis LoRa dengan penyandian dasar sebagai platform edukasional dan prototipikal latihan militer.

Kata kunci: Caesar Cipher, Obfuscation, LoRa SX1278, Proof-of-Concept, Telemetri, Latihan Militer.

PENDAHULUAN

Keunggulan taktis dalam pertahanan modern sangat bergantung pada keandalan dan keamanan sistem komunikasi yang diterapkan. Keunggulan dalam sistem kendali dan konektivitas dapat menentukan keberhasilan suatu operasi, mulai dari latihan hingga misi tempur sesungguhnya. Inovasi di bidang ini menjadi kebutuhan strategis bagi setiap angkatan bersenjata, termasuk Tentara Nasional Indonesia, untuk memastikan kesiapan dan efektivitas pasukannya di segala medan[1][2][3][4].

Secara operasional, salah satu aspek yang memerlukan perhatian khusus adalah sistem peledakan jarak jauh (*remote demolition system*). Kemampuan meledakkan target dengan presisi tinggi dari jarak yang aman sangat vital dalam berbagai skenario, seperti pembukaan akses,

penghancuran infrastruktur musuh, atau latihan teknis tim demolisi[5]. Keandalan sistem ini tidak hanya menyangkut keberhasilan misi, tetapi juga langsung berkorelasi dengan tingkat keselamatan personel di lapangan.

Namun, sistem komunikasi konvensional yang umum digunakan, seperti radio VHF/UHF analog, memiliki sejumlah kelemahan mendasar. Keterbatasan jangkauan di medan kompleks, kerentanan terhadap gangguan frekuensi lain, dan risiko penyadapan merupakan celah keamanan yang berpotensi mengakibatkan kegagalan komando. Data evaluasi latihan militer menunjukkan bahwa gangguan komunikasi masih menjadi salah satu faktor penghambat dalam latihan taktis.

Berdasarkan tantangan tersebut, teknologi LoRa (*Long Range*) muncul

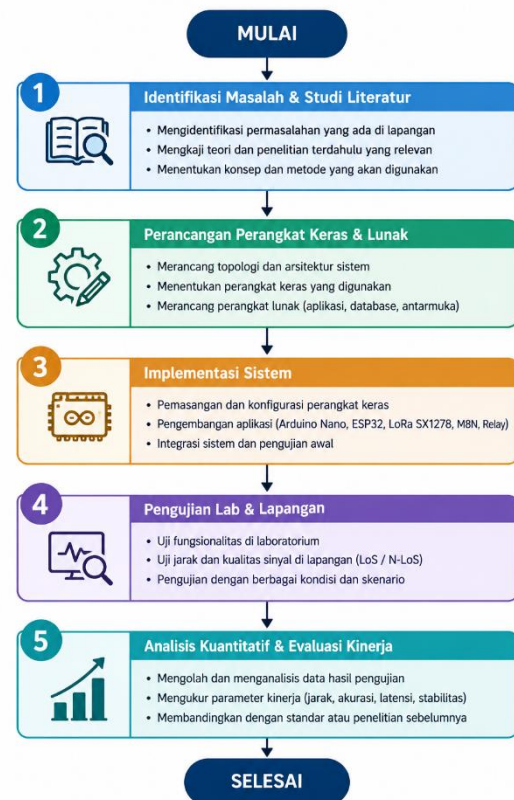
sebagai solusi alternatif yang menjanjikan. Dengan karakteristik unggulannya, yaitu jangkauan transmisi yang luas, ketahanan sinyal terhadap interferensi, dan konsumsi daya yang sangat rendah, LoRa ideal untuk perangkat lapangan yang portabel[6][7].

Meski demikian, teknologi LoRa memiliki keterbatasan pada aspek keamanan data karena transmisi pada *layer* aplikasi bawaannya tidak terenkripsi. Untuk aplikasi kritis seperti pengiriman perintah peledakan, ketiadaan lapisan pengaman ini merupakan kerentanan[8]. Pemilihan algoritma enkripsi harus mempertimbangkan konteks penggunaan secara spesifik. Untuk keperluan latihan dan pengembangan prototipe, diperlukan algoritma yang ringan secara komputasi dan mudah diimplementasikan pada perangkat mikrokontroler sederhana. Metode Caesar Cipher dipilih dalam penelitian ini bukan untuk diposisikan sebagai keamanan kriptografis operasional tingkat tinggi, melainkan sebagai demonstrasi *basic obfuscation / proof-of-concept* edukasional untuk mensimulasikan prinsip penyandian data dengan latensi rendah pada perangkat bersumber daya terbatas.

Penelitian ini bertujuan untuk merancang prototipe sistem komunikasi nirkabel yang mengintegrasikan modul LoRa SX1278 (433 MHz, SF7, BW 125 kHz, CR 4/5, *transmit power* 20 dBm, antena 3 dBi, tinggi 1,5 m) dengan enkripsi Caesar Cipher, serta menyajikan evaluasi performa kuantitatif secara komprehensif mencakup parameter jangkauan operasional LoS/N-LoS dengan denominator pengujian yang jelas, tingkat keberhasilan *encode-decode*, serta *benchmark* komputasi mikrokontroler.

METODE PENELITIAN

Metode eksperimen digunakan untuk menguji dan mengevaluasi sistem komunikasi alat peledak jarak jauh berbasis LoRa yang dilengkapi dengan enkripsi Caesar Cipher.



Gambar 1. Diagram Alur (sumber:Peneliti 2026)

Pada pengoperasiannya, sistem mengadopsi mekanisme komunikasi dua arah (*bidirectional*) yang informasinya dilindungi oleh algoritma Caesar Cipher dengan nilai pergeseran kunci (*key*) sebesar 5. Alur pertama merupakan transmisi pemantauan (*uplink*), di mana data koordinat dari GPS dibaca oleh Arduino, dienkripsi menjadi *ciphertext*, dan dikirimkan melalui jaringan LoRa menuju *gateway* ESP32 untuk didekripsi lalu ditampilkan pada *dashboard* web. Alur kedua adalah transmisi instruksi (*downlink*), di mana operator mengirimkan perintah aktivasi melalui *dashboard*, dienkripsi, dipancarkan melalui LoRa, dan didekripsi oleh node aktuator di lapangan sebelum relay memicu detonator.

Perangkat keras utama yang digunakan meliputi mikrokontroler Arduino Nano[9][10][11], ESP32 sebagai *gateway*, modul komunikasi LoRa SX1278, modul GPS u-blox M-8N[12][13], serta relay

aktuator. Seluruh eksperimen komunikasi nirkabel menggunakan konfigurasi parameter radio yang distandarisasi untuk menjamin keterulangan (*reproducibility*)[14], sebagaimana dirinci pada Tabel I.

Tabel I
Parameter Konfigurasi Radio Lora Sx1278

Parameter Teknis	Nilai Konfigurasi Pengujian
Frekuensi Operasional	433 MHz
Spreading Factor (SF)	SF7
Bandwidth (BW)	125 kHz
Coding Rate (CR)	4/5
Transmit Power	20 dBm (100 mW)
Tipe dan Gain Antena	Omnidirectional / 3 dBi
Tinggi Antena dari Tanah	1,5 meter
Ukuran Paket Data (<i>Packet Size</i>)	32–64 Byte
Interval Pengiriman Paket	1.000 ms (1 detik)

Evaluasi kinerja divalidasi melalui skenario pengujian berikut:

1. Pengujian Jangkauan dan Kualitas Link (LoS & N-LoS): Dilakukan pada variasi jarak *Line-of-Sight* (LoS: 100 m, 200 m, 300 m, 500 m) dan *Non-Line-of-Sight* (N-LoS: 50 m, 75 m, 150 m). Pada setiap titik uji, dikirimkan 100 paket data per iterasi yang diulang sebanyak 5 kali pengulangan (total 500 paket per titik uji) untuk mendapatkan persentase *packet loss* yang terverifikasi secara statistik.
2. Pengujian Fungsi Encode-Decode: Dilakukan pada 200 sampel pesan bervariasi (terdiri dari instruksi kendali, string koordinat GPS, dan status sensor) dengan 10 kali pengulangan per sampel, diukur

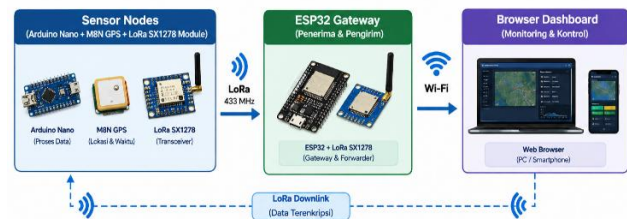
menggunakan metrik *exact string match*.

3. Benchmark Komputasi Enkripsi-Dekripsi: Mengukur waktu eksekusi mikrokontroler pada variasi panjang pesan (10, 50, 100, 150, 200, 250, dan 500 karakter) dengan 50 kali pengulangan per variasi menggunakan fungsi *micros()*.

HASIL PENELITIAN

A. Analisis Kuantitatif Jangkauan dan Kualitas Link LoRa

Pengembangan prototipe sistem komunikasi nirkabel berbasis LoRa untuk kendali dan pemantauan peledakan berhasil diimplementasikan. Seluruh transmisi pertukaran data menggunakan frekuensi 433 MHz



Gambar 2. Arsitektur Komunikasi Sistem LoRa (*Sumber: Peneliti, 2026*)

Hasil pengujian performa komunikasi radio LoRa SX1278 pada skenario LoS dan N-LoS dirangkum secara sistematis pada Tabel II. Berdasarkan data pada Tabel II, rentang operasional andal (*operational range*) pada kondisi LoS berada pada jarak 100–200 meter dengan *packet loss* 0% dan latensi sub-detik yang stabil (92–98 ms). Pada jarak 300 m (*tested range*), *packet loss* tercatat 5%. Jarak 500 m merupakan jarak terjauh pengujian (*critical range*), di mana kualitas link mengalami degradasi dengan *packet loss* mencapai 80%. Pada skenario N-LoS, rentang operasional optimal dicapai pada 50–75 meter (*packet loss* 0–2%), sedangkan pada jarak 150 m mengalami

peningkatan *packet loss* hingga 80% dengan latensi mencapai 3,0 detik.

Tabel II
Hasil Pengujian Kinerja Komunikasi Lora
Sx1278 (Los Vs N-Los)
(Denominator: 100 Paket/Iterasi × 5
Pengulangan = 500 Paket per Titik Uji)

Kon disi	Jar ak Uji (m)	Tota l Pak et Dikir im	Total Paket Diteri ma	Pac ket Los s (%)	Rata -rata Late nsi (ms)	Klasifi kasi Jangka uan (Range Status)
LoS	100	500	500	0,0 %	92 ms	Operati onal Range (Sangat Andal)
LoS	200	500	500	0,0 %	98 ms	Operati onal Range (Sangat Andal)
LoS	300	500	475	5,0 %	115 ms	Tested Range (Andal dengan Degrad asi)
LoS	500	500	100	80,0 %	450 ms	Critical Range (Batas Terjauh Uji)
N- LoS	50	500	500	0,0 %	105 ms	Optimal N-LoS Range
N- LoS	75	500	490	2,0 %	120 ms	Optimal N-LoS Range
N- LoS	150	500	100	80,0 %	3.00 0 ms	Critical N-LoS Range (Tidak Stabil)

B. Evaluasi Keberhasilan Fungsi Encode-Decode Caesar Cipher

Untuk menjaga kerahasiaan data, algoritma Caesar Cipher diterapkan dengan pergeseran kunci sebesar 5 ($K = 5$). Pengujian algoritmik membuktikan bahwa metode ini berhasil melakukan transformasi karakter (*cross-domain shift*), contohnya karakter 'R' (ASCII 82) bergeser menjadi 'W' (ASCII 87), atau angka '8' (ASCII 56) menjadi simbol '=' (ASCII 61).

Pengujian fungsi *encode-decode* pada 200 sampel pesan bervariasi dengan 10 kali pengulangan menunjukkan tingkat keberhasilan (*success rate*) sebesar 100% berdasarkan kesesuaian *exact string match* antara *plaintext* awal dan *plaintext* hasil dekripsi. Sebagai contoh, instruksi kendali asli "RELAY_A_ON" diubah di udara menjadi string "WJQF^dFdTS", lalu didekripsi kembali secara presisi di sisi penerima menjadi "RELAY_A_ON" tanpa adanya *noise* atau kerusakan struktur data.

C. Benchmark Waktu Komputasi Obfuscation

Hasil pengujian waktu eksekusi komputasi enkripsi dan dekripsi untuk berbagai variasi panjang karakter disajikan pada Tabel III.

Tabel III
Benchmark Waktu Komputasi Enkripsi Dan
Dekripsi Caesar Cipher
(Berdasarkan 50 Kali Pengulangan per
Variasi Panjang Pesan)

Panjang Pesan (Karakte r)	Waktu Enkrip si Rata- rata (μs)	Waktu Dekrip si Rata- rata (μs)	Devias i Stand ar / SD (μs)	Karakterist ik Respons Komputasi
10	125 μs	122 μs	± 4,2 μs	Respons Linear
50	624 μs	620 μs	± 8,5 μs	Respons Linear
100	1.240 μs	1.235 μs	± 12,1 μs	Respons Linear
150	1.865 μs	1.850 μs	± 15,3 μs	Respons Linear

200	2.480 μs	2.470 μs	± 18,0 μs	Respons Linear
250	3.110 μs	3.095 μs	± 21,4 μs	Respons Linear
500	11.984 μs	11.950 μs	± 142,0 μs	Non-Linear (Lonjakan Memori)

Tabel III menunjukkan bahwa pada rentang 10 hingga 250 karakter, waktu komputasi berbanding lurus secara linear. Pada pesan 500 karakter, terjadi lonjakan waktu hingga 11.984 μs (11,98 ms). Lonjakan ini diidentifikasi sebagai dugaan teknis akibat keterbatasan alokasi memori dinamis dan *heap fragmentation* pada RAM mikrokontroler Arduino, bukan karena kompleksitas matematikanya.

D. Pembahasan Positioning Keamanan dan Limitations

Secara teoretis, Caesar Cipher memiliki ruang kunci yang sempit dan rentan terhadap serangan *brute force*[5]. Oleh karena itu, penerapannya dalam penelitian ini ditegaskan bukan sebagai proteksi kriptografi militer operasional, melainkan sebagai *basic obfuscation / proof-of-concept* edukasional untuk menyamarkan bentuk teks kasar (*plaintext*) pada transmisi nirkabel. Untuk aplikasi lapangan militer sesungguhnya, sistem direkomendasikan untuk ditingkatkan menggunakan algoritma *lightweight cryptography* modern atau AES[15][16].

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem komunikasi data nirkabel jarak jauh menggunakan radio LoRa SX1278 (433 MHz) dengan enkripsi Caesar Cipher sebagai *proof-of-concept* monitoring dan kendali peledakan pada latihan militer. Berdasarkan data eksperimen kuantitatif dengan denominator yang terverifikasi, sistem mampu mengirimkan perintah kendali dan telemetri GPS secara stabil pada rentang LoS 100–200 m (*packet*

loss 0%, latensi 92–98 ms) dan N-LoS 50–75 m (*packet loss* 0–2%). Pengujian fungsi *encode-decode* membuktikan keberhasilan 100% pada 200 sampel pesan, serta *benchmark* komputasi menunjukkan waktu eksekusi yang sangat cepat (<3,2 ms untuk ≤250 karakter). Meskipun demikian, untuk penerapan operasional taktis nyata di masa depan, penggunaan enkripsi dasar ini perlu ditingkatkan menuju algoritma kriptografi modern seperti AES atau RSA guna mengantisipasi ancaman keamanan tingkat lanjut.

DAFTAR PUSTAKA

- [1] M. N. Iriansyah, H. Casnoto, and Y. Djuyandi, "Strategi Pengamanan Wilayah Oleh Skadron Udara 51 UAV," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 83–90, 2021, doi: 10.54706/senastindo.v3.2021.150.
- [2] H. Dwi, P. Gusti, H. Lutfiah, A. Minannor, and R. Yandri, "Analysis of 433 MHz LoRa Communication Quality Based on RSSI and SNR Parameters in A Solar-Powered IoT Chili Irrigation System in Hilly Forest Farmland," 2026, doi: 10.46961/jommit.v10i1.2208.
- [3] N. Umar, I. Mahjud, Y. G. Y. Lely, A. Syukut, and M. Y. Aditama, "Position Monitoring Fishing Boat at Boddia Wharf," *J. Teknol. Elekterika*, vol. 22, no. 2, pp. 101–106, 2025.
- [4] H. A. Kusuma, M. F. Hanafi, T. Suhendra, and N. Oktaviani, "Testing the Range and Analysis of WSN LoRa Sx1278 Parameters in Coastal Areas," *TELKA - Telekomun. Elektron. Komputasi dan Kontrol*, vol. 10, no. 2, pp. 168–177, 2024, doi: 10.15575/telka.v10n2.168-177.
- [5] B. Torossian et al., "The Military Applicability of Robotic and Autonomous Systems," *Capstone Rep.*, pp. 24–49, 2021, [Online]. Available:

- <http://www.jstor.org/stable/resrep29554.4>
- [6] F. Winjaya, A. Darmawan, A. P. E. Wibowo, and M. D. Puspitasari, "Sosialisasi Teknologi Iot (Internet of Things) Dan Lora (Long Range) Pada Pegawai Industri Pt. Wantech Indonesia," *Madiun Spoor J. Pengabd. Masy.*, vol. 5, no. 1, pp. 1–7, 2025, doi: 10.37367/jpm.v5i1.454.
- [7] S. De et al., "Interleaved Reception in LoRa Using IFT: A Hardware-Efficient Architecture for Fast and Low-Power Image Transmission," *IEEE Internet Things J.*, vol. 12, no. 19, pp. 39777–39787, 2025, doi: 10.1109/JIOT.2025.3588064.
- [8] D. D. Pebrian, "Alat Ukur Sinyal Lora Untuk Mengetahui," vol. 13, no. 1, 2025.
- [9] Arba'l, "Jurnal jasatec," *J. Jasatec*, vol. 3, no. 1, pp. 15–26, 2023.
- [10] K. Lora, "Implementasi Algoritme PRESENT untuk Proses Enkripsi pada Modul," ... *Teknol. Inf. dan Ilmu Komput. e ...*, vol. 5, no. 5, pp. 2050–2057, 2021, [Online]. Available: <http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/9007/4139>
- [11] T. S. Gunawan, W. A. Yahya, E. Sulaeman, M. Kartiwi, and Z. Janin, "Development of control system for quadrotor unmanned aerial vehicle using LoRa wireless and GPS tracking," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 5, pp. 2674–2681, 2020, doi: 10.12928/TELKOMNIKA.v18i5.16716.
- [12] D. N. David, D. Hamdani, and I. Setiawan, "Developing Physics Teaching Aids on Moment of Inertia Material using Arduino Nano and TCRT5000 Sensor," *J. Ilm. Pendidik. Fis.*, vol. 7, no. 1, p. 10, 2023, doi: 10.20527/jipf.v7i1.6889.
- [13] T. H. Chung, V. Orekhov, and A. Maio, "Into the Robotic Depths: Analysis and Insights from the DARPA Subterranean Challenge," *Annu. Rev. Control. Robot. Auton. Syst.*, vol. 6, pp. 477–502, 2023, doi: 10.1146/annurev-control-062722-100728.
- [14] H. A. Saputra, I. W. Gunada, and W. Wahyudi, "Development of an Arduino Nano-Based Viscometer to Enhance Students' Physics Concept Understanding," *J. Pendidik. Fis. dan Teknol.*, vol. 11, no. 2, pp. 360–366, 2025, doi: 10.29303/jpft.v11i2.10141.
- [15] G. Akilandeswary, J. S. R. A, and H. K. K, "Implementation of Soldier Assisting Device using LoRa with SOS Functionality," *Int. J. Innov. Res. Appl. Sci. Eng.*, vol. 4, no. 5, pp. 760–765, 2020, doi: 10.29027/ijirase.v4.i5.2020.760-765.
- [16] S. Ryczek and M. Sobieraj, "Secure LoRa-Based Transmission System: An IoT Solution for Smart Homes and Industries," *Electron.*, vol. 14, no. 24, 2025, doi: 10.3390/electronics14244977.