ANALISIS MITIGASI SERANGAN *MAN-IN-THE-MIDDLE* PADA KOMUNIKASI LORA PEER-TO-PEER BERBASIS *DYNAMIC KEY MANAGEMENT* DI JARINGAN NON-INTERNET

SKRIPSI

MOHAMMAD RIZKI FADILLAH (2207421016)

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

ANALISIS MITIGASI SERANGAN *MAN-IN-THE-MIDDLE* PADA KOMUNIKASI LORA PEER-TO-PEER BERBASIS *DYNAMIC KEY MANAGEMENT* DI JARINGAN NON-INTERNET

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

MOHAMMAD RIZKI FADILLAH

2207421016

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	:	Mohammad Rizki Fadillah
NIM	:	2207421016
Jurusan / Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Mitigasi Serangan *Man In The Middle* Pada Komunikasi LoRa Peer-to-Peer Berbasis *Dynamic Key Management* Di Jaringan Non-Internet

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat orang lain dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 5 Juni 2026

Yang membuat pernyatan

(Mohammad Rizki Fadillah)

NIM. 2207421016

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama	:	Mohammad Rizki Fadillah
NIM	:	2207421016
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Mitigasi Serangan *Man In The Middle* Pada Komunikasi LoRa *Peer-to-Peer* Berbasis *Dynamic Key Management* Di Jaringan Non-Internet

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Jumat, Tanggal 19, Bulan Juni, Tahun 2026 dan dinyatakan **LULUS**

Disahkan Oleh

Pembimbing I	: Defiana Arnaldy, S.T.P., M.Si.	( )
Penguji I	: Ayu Rosyida Zain, S.ST. M.T.	( )
Penguji II	: Fachroni Arbi Murrad, S.Kom., M.Kom.	( )
Penguji III	: Iik Muhamad Malik Matin, S.Kom., M.T.	( )

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M. Kom.

NIP. 197908032003122003

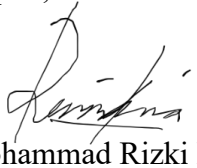
KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan skripsi berjudul "Analisis Mitigasi Serangan *Man-In-The-Middle* Pada Komunikasi LoRa *Peer-to-Peer* Berbasis *Dynamic Key Management* Di Jaringan Non-Internet" sebagai salah satu syarat memperoleh gelar Sarjana Terapan Komputer di Politeknik Negeri Jakarta. Penulis menyadari bahwa kelancaran penyusunan skripsi ini tidak terlepas dari bantuan serta bimbingan berbagai pihak, sehingga pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Allah SWT atas kemudahan, kekuatan, petunjuk, dan karunia-Nya sehingga penulis bisa menyelesaikan skripsi ini tepat waktu.
2. Bapak Defiana Arnaldy, S.T.P., M.Si., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini;
3. Seluruh staf, pengajar, dan karyawan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta yang telah memberikan ilmu dan bantuan administrasi selama masa perkuliahan;
4. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan material dan moral;
5. Rekan-rekan mahasiswa TMJ 8A 2022 yang telah banyak membantu penulis dalam memberikan ide serta dukungan dalam menyelesaikan ini.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan.

Depok, 6 Juni 2026



Mohammad Rizki Fadillah

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI
SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

Nama : Mohammad Rizki Fadillah
NIM : 2207421016
Jurusan / Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Eksklusif atas karya ilmiah saya yang berjudul:

Analisis Mitigasi Serangan *Man In The Middle* Pada Komunikasi LoRa Peer-to-Peer Berbasis *Dynamic Key Management* Di Jaringan Non-Internet

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 5 Juni 2026
Yang menyatakan,

METERAI TEMPEL
1FAIX673121544

(Mohammad Rizki Fadillah)
NIM. 2207421016

Analisis Mitigasi Serangan Man-In-The-Middle Pada Komunikasi LoRa Peer-to-Peer Berbasis Dynamic Key Management Di Jaringan Non-Internet

ABSTRAK

Pemanfaatan Internet of Things (IoT) di area blank spot sering mengandalkan komunikasi Point-to-Point (P2P) karena efisiensi daya dan jangkauannya. Namun, berbeda dengan LoRaWAN, LoRa P2P tidak memiliki standar keamanan bawaan sehingga rentan terhadap penyadapan, manipulasi pesan (Man-In-The-Middle/MITM), dan Replay Attack. Risiko ini memburuk dengan penggunaan kunci statis, di mana pencurian perangkat fisik dapat mengkompromikan seluruh jaringan. Penelitian ini bertujuan merancang sistem keamanan LoRa P2P menggunakan mikrokontroler ESP32 dengan menerapkan kriptografi hibrida dan manajemen kunci dinamis. Metode yang digunakan mencakup algoritma AES-128 untuk kerahasiaan data dan HMAC-SHA256 untuk verifikasi integritas pesan. Untuk mengatasi kelemahan kunci statis dan Replay Attack, dikembangkan mekanisme Dynamic Key Management yang memperbarui kunci enkripsi secara otomatis berdasarkan counter internal, serta Counter-based Nonce untuk memastikan kesegaran pesan. Hasil pengujian menunjukkan bahwa sistem yang diusulkan mampu memitigasi serangan MITM dengan mendeteksi perubahan tanda tangan HMAC dan menolak paket replay yang tidak valid. Kesimpulannya, sistem ini berhasil menjaga kerahasiaan dan integritas data secara dinamis, dengan tetap mempertahankan efisiensi komputasi pada perangkat berdaya rendah.

Kata Kunci: AES-128, *Dynamic Key Management*, ESP32, HMAC-SHA256, LoRa P2P, *Man-In-The-Middle.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan *Internet of Things* (IoT) telah mendorong adopsi teknologi *Low Power Wide Area Network* (LPWAN), khususnya LoRa, untuk berbagai aplikasi monitoring jarak jauh. Meskipun protokol LoRaWAN umum digunakan, keandalan jaringannya sangat bergantung pada infrastruktur gateway dan network server yang harus selalu terhubung ke internet, (Rosyida Zain et al., 2022). Selain itu, tingginya harga infrastruktur perangkat LoRaWAN Gateway komersial seringkali menjadi kendala besar bagi industri menengah dan kecil. Sebagai alternatif pengganti LoRaWAN, pengembangan gateway mandiri (*custom gateway*) berbiaya rendah menggunakan mode komunikasi *Point-to-Point* (P2P) menjadi solusi yang efisien dan mandiri, terutama di wilayah yang tidak terjangkau jaringan seluler (blank spot) (C. Sun et al., 2020).

Namun, kemandirian infrastruktur *custom gateway* ini membawa tantangan keamanan yang signifikan karena modulasi LoRa pada lapisan fisik tidak memiliki mekanisme keamanan bawaan. Berbeda dengan protokol LoRaWAN yang memiliki lapisan keamanan standar yang diatur di sisi server, komunikasi LoRa P2P mengirimkan data secara terbuka (*plaintext*), sehingga sangat rentan terhadap penyadapan. Hal ini diperkuat oleh penelitian yang membuktikan bahwa payload LoRa P2P dapat dengan mudah disadap di udara menggunakan perangkat *Software Defined Radio* (SDR) jika tidak dibekali mekanisme enkripsi yang memadai, (McWeeney et al., 2024).

Selain ancaman penyadapan, integritas data pada jaringan nirkabel jarak jauh juga menjadi perhatian kritis. Penyerang dapat melakukan manipulasi data di tengah jalur transmisi tanpa terdeteksi oleh penerima sah melalui teknik packet injection. Pernyataan ini didukung oleh riset yang berhasil mendemonstrasikan serangan *Man-In-The-Middle* (MITM) pada perangkat IoT berbasis LoRa, (Olazabal et al., 2022). Kerentanan ini sangat berbahaya jika diimplementasikan pada sektor kritis seperti smart metering atau infrastruktur publik, karena dapat menyebabkan data konsumsi energi atau status sensor dimanipulasi untuk keuntungan pihak tertentu, (Zaraket et al., 2020).

Upaya pengamanan menggunakan algoritma kriptografi lightweight seperti AES-128 dan HMAC-SHA256 telah terbukti optimal untuk perangkat dengan sumber daya terbatas seperti ESP32, (Windya et al., 2021). Meskipun AES-128 mampu menjaga kerahasiaan payload, penggunaan kunci statis (*static key*) tetap menjadi titik lemah utama. Sebagaimana dijelaskan pada tinjauan keamanan jaringan berskala besar, manajemen kunci merupakan tantangan terbesar dalam IoT jangka panjang; kunci yang statis dan tidak pernah berubah sangat rentan terhadap eksploitasi melalui serangan replay dan pembongkaran kunci secara paksa, (Li & Cao, 2022). Hal ini diperkuat oleh penelitian lain yang menegaskan pentingnya mekanisme anti-replay (seperti sequence number atau timestamp) serta pembaruan kunci secara berkala untuk menjaga kepercayaan pada transmisi data rutin, (Hayati, 2024).

Oleh karena itu, diperlukan sebuah sistem mitigasi pada *custom gateway* LoRa P2P yang tidak hanya mengenkripsi data, tetapi juga mampu mengelola kunci secara dinamis tanpa harus bergantung pada koneksi internet atau server eksternal. Penelitian ini mengusulkan implementasi *dynamic key management* berbasis *Key Derivation Function* (KDF). Dengan mekanisme ini, kunci enkripsi akan diperbarui secara otomatis berdasarkan parameter dinamis, sehingga setiap sesi paket dilindungi oleh kunci sesi (*session key*) yang berbeda-beda, (Hakeem et al., 2021). Pendekatan ini diharapkan dapat memberikan perlindungan berlapis yang resilien terhadap serangan MITM, *sniffing*, dan *replay attack* pada jaringan LoRa P2P di area offline.

1.2 Perumusan Masalah

Berdasarkan identifikasi masalah yang telah dipaparkan pada latar belakang, terutama mengenai kerentanan komunikasi LoRa terhadap serangan MITM dan penggunaan kunci statis, maka perumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang dan mengimplementasikan mekanisme *dynamic key management* menggunakan metode *Key Derivation Function* (KDF) pada arsitektur jaringan LoRa P2P berbasis ESP32?
2. Sejauh mana tingkat efektivitas skema keamanan yang diusulkan dalam mendeteksi dan menolak gangguan yang berasal dari serangan *sniffing*, *packet injection* (MITM), dan *replay attack*?

3. Bagaimana dampak implementasi pengamanan (KDF, AES-128, dan HMAC-SHA256) terhadap performa mikrokontroler ESP32, khususnya pada indikator waktu pemrosesan komputasi (latensi) dan pemakaian memori (RAM usage)?

1.3 Batasan Masalah

Untuk mengantisipasi meluasnya pembahasan dan agar penelitian ini tetap terfokus pada solusi yang direncanakan, maka ditetapkan batasan masalah sebagai berikut:

1. Perangkat keras difokuskan pada penggunaan mikrokontroler ESP32 dan modul transceiver LoRa Ra-02 (SX1278) yang beroperasi pada frekuensi 433 MHz.
2. Implementasi sistem keamanan pada *custom gateway* LoRa P2P ini difokuskan pada studi kasus lingkungan Industrial *Internet of Things* (IIoT) atau *Smart Agriculture* yang berada di area blank spot tanpa infrastruktur LoRaWAN komersial.
3. Sistem pengamanan menggunakan algoritma kriptografi *lightweight* AES-128 untuk confidentiality, HMAC-SHA256 untuk *data integrity*, serta fungsi hash KDF untuk pembaharuan *session key*.
4. Parameter pengujian performa mikrokontroler (ESP32) dibatasi pada evaluasi waktu pemrosesan komputasi (*computational latency*), penggunaan memori (RAM) akibat penambahan beban komputasi dari algoritma kriptografi.

1.4 Tujuan dan Manfaat

Tujuan penelitian mengungkapkan sasaran yang ingin dicapai, sedangkan manfaat berisikan uraian hasil positif dari dilaksanakannya penelitian ini. Tujuan Penelitian Adapun tujuan yang ingin dicapai melalui pelaksanaan penelitian ini adalah:

1. Mengimplementasikan protokol pembaruan kunci secara dinamis (*dynamic key management*) guna menghindari penggunaan kunci statis yang berisiko tinggi pada jaringan LoRa P2P.
2. Menguji dan membuktikan ketahanan sistem *gateway* secara eksperimental dalam memblokir paket data tidak sah yang dikirimkan oleh pihak penyerang dalam skenario MITM.

3. Menganalisis parameter performa secara kuantitatif untuk membuktikan kelayakan implementasi berlapis keamanan ini pada perangkat IoT dengan sumber daya yang sangat terbatas.
4. Menganalisis performa sistem keamanan yang diusulkan berdasarkan parameter keberhasilan penangkalan serangan, waktu komputasi (*computation overhead*), penggunaan memori pada perangkat dengan sumber daya terbatas (*constrained device*).

Melalui pencapaian tujuan tersebut, penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Menyediakan solusi infrastruktur Gateway LoRa yang efisien biaya (*low-cost*) dan aman, sehingga dapat dijangkau dan diterapkan oleh industri kecil atau sektor pertanian di area tanpa sinyal internet (*blank spot*).
2. Menghasilkan sistem keamanan yang terbukti mampu melindungi data sensor dari ancaman nyata seperti penyadapan (*sniffing*), manipulasi data (*Man-In-The-Middle*), dan pengiriman ulang paket (*replay attack*).
3. Memberikan referensi teknis mengenai penerapan algoritma kriptografi hibrida (AES-128 dan HMAC-SHA256) serta manajemen kunci dinamis yang optimal pada perangkat mikrokontroler dengan sumber daya terbatas.

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran menyeluruh mengenai alur pembahasan penelitian. Adapun sistematika penulisannya adalah sebagai berikut:

1. BAB I Pendahuluan

   Bab ini menguraikan mengenai latar belakang pemilihan topik penelitian, identifikasi masalah terkait keamanan komunikasi LoRa P2P, perumusan masalah, batasan masalah, tujuan yang ingin dicapai, serta manfaat penelitian bagi pengembang sistem IoT dan instansi terkait.
2. BAB II Tinjauan Pustaka

   Bab ini memaparkan teori-teori dasar yang menjadi landasan penelitian, meliputi teknologi LoRa P2P, algoritma kriptografi AES-128 dan HMAC-SHA256, mekanisme *Counter-based Nonce*, serta konsep *Key Derivation*

Function (KDF). Selain itu, bab ini juga menyajikan tinjauan terhadap penelitian-penelitian relevan terdahulu.

3. BAB III Metodologi Penelitian

   Bab ini menjelaskan mengenai kerangka pemikiran dan prosedur penelitian yang meliputi tahapan identifikasi masalah, studi literatur, perancangan sistem keamanan, teknik pengumpulan data melalui simulasi serangan MITM, serta teknik analisis data untuk menguji performa dan keamanan protokol yang dikembangkan.

4. BAB IV Hasil dan Pembahasan

   Bab ini berisi tentang hasil dari implementasi protokol pada perangkat ESP32, hasil pengujian mitigasi serangan, serta analisis terhadap parameter waktu proses dan penggunaan memori pada perangkat.

5. BAB V Penutup

   Bab ini berisi kesimpulan dari seluruh rangkaian penelitian yang telah dilakukan serta saran-saran bagi pengembangan penelitian selanjutnya di masa yang akan datang.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan perancangan, implementasi, dan hasil pengujian komparatif terhadap mitigasi serangan *Man-In-The-Middle* (MITM) pada komunikasi LoRa *Point-to-Point* (P2P) berbasis ESP32, dapat ditarik simpulan sebagai berikut:

1. Implementasi *dynamic key management* menggunakan metode *Key Derivation Function* (KDF) berbasis algoritma HMAC-SHA256 berhasil menggantikan kerentanan sistem kunci statis (*static key*). Sistem secara mandiri dan otomatis mampu melakukan pembaruan kunci sesi (*session key*) setiap kelipatan 10 paket transmisi menggunakan parameter nilai *Sequence Counter*, sehingga memastikan setiap sesi komunikasi memiliki kunci yang unik tanpa perlu melakukan pertukaran kunci secara terbuka di udara.
2. Skema keamanan *Full Security* yang diusulkan terbukti memiliki efektivitas yang absolut dalam memitigasi tiga model serangan siber. Algoritma AES-128 mode CTR sukses menyembunyikan *plaintext* dari serangan penyadapan (*sniffing*). Integrasi HMAC-SHA256 berhasil mencapai *drop rate* 100% terhadap serangan manipulasi data (*tampering* / MITM) karena sistem mampu mendeteksi ketidaksesuaian nilai hash di udara. Selain itu, penggunaan *Counter-based Nonce* juga sukses mencapai drop rate 100% dalam memblokir dan menolak serangan pengiriman ulang paket usang (*replay attack*).
3. Penerapan algoritma keamanan kriptografi secara logis memberikan beban komputasi tambahan terhadap performa mikrokontroler ESP32, yang ditandai dengan peningkatan waktu pemrosesan dari 32,50 ms pada sistem *baseline* menjadi 140,05 ms. Walaupun terjadi peningkatan, latensi ini dinilai masih sangat responsif untuk aplikasi IoT. Dari segi penggunaan memori, pustaka kriptografi mbedTLS terbukti sangat ringan (*lightweight*) dengan sisa kapasitas RAM yang bertahan konstan di angka 350.204 *Bytes* selama pengujian transmisi ratusan paket data berdurasi panjang, sehingga mengonfirmasi bahwa sistem mampu mengelola memori secara efisien dan terbebas dari kebocoran memori (*memory leak*).

5.2 Saran

Meskipun sistem yang dikembangkan telah mencapai tujuan penelitian, terdapat beberapa aspek yang dapat disempurnakan. Oleh karena itu, saran yang dapat diberikan untuk penelitian dan pengembangan selanjutnya perlu melakukan analisis konsumsi daya (*power profiling*) secara langsung untuk mengukur dampak konsumsi baterai (dalam satuan *miliampere* atau *Joule*) pada perangkat *end-node* akibat beban penambahan siklus komputasi kriptografi, sehingga masa pakai (*lifetime*) baterai untuk implementasi *Internet of Things* (IoT) jangka panjang dapat dipastikan secara optimal.

DAFTAR PUSTAKA

Artha Lesmana, D. D., Arsa Suyadnya, I. M., & Shandyasa, I. W. (2023). Rancang Bangun Perangkat Keras Sistem Smart Lampu Penerangan Jalan Umum Berbasis Internet of Things Guna Mendukung Implementasi Smart City. *Jurnal SPEKTRUM*, *10*(3), 21. https://doi.org/10.24843/spektrum.2023.v10.i03.p3

Components101. (2018). *DHT22 – Temperature and Humidity Sensor*. https://components101.com/sensors/dht22-pinout-specs-datasheet

Designer, C. (n.d.). *How to Use LoRa Ra-02 SX1278: Examples, Pinouts, and Specs*. Retrieved June 7, 2026, from https://docs.cirkitdesigner.com/component/ea67bc39-2543-48d1-915c-5686eed5bac4/lora-ra-02-sx1278

Guimarães, A. (2024). *Gateway IoT usando Raspberry Pi*.

Hakeem, S. A. A., El-Kader, S. M. A., & Kim, H. W. (2021). A Key Management Protocol Based on the Hash Chain Key Generation for Securing LoRaWAN Networks. *Sensors (Basel, Switzerland)*, *21*(17), 1–35. https://doi.org/10.3390/s21175838

Hayati, N. (2024). The Design of Security Framework for LoRaWAN FUOTA. *Journal of Electrical Technology UMY*, *7*(2), 82–88. https://doi.org/10.18196/jet.v7i2.22360

Instiperjogja, R. (2021). *Mikrokontroler ESP32 (IoT Device)*. https://robotics.instiperjogja.ac.id/post/ESP32

Kreaweb. (2023). *LARAGON, an easy and yet powerful Local Web Development Server*. https://www.kreaweb.be/laragon/

Lestari, R. I., Suryani, V., & Wardana, A. A. (2020). Implementasi Pengamanan Pada Jaringan LoRaWAN Untuk Mengatasi Serangan Sniffing Dengan Menggunakan Metode Digital Signature. *EProceedings …*, *7*(2), 7983–7994. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/13079

Li, C., & Cao, Z. (2022). LoRa Networking Techniques for Large-scale and Long-term IoT: A Down-to-top Survey. *ACM Computing Surveys*, *55*(3). https://doi.org/10.1145/3494673

Lv, Z. (2021). Security of Internet of Things edge devices. *Software - Practice and Experience*, *51*(12), 2446–2456. https://doi.org/10.1002/spe.2806

McWeeney, B., Mudritskiy, I., & Verbruggen, R. (2024). Analysis of Payload Confidentiality for the IoT/ LPWAN Technology 'Lora.' *International Conference on Information Systems Security and Privacy*, *1*(Icissp), 91–102. https://doi.org/10.5220/0012271400003648

Ningsih, K. S., Aruan, N. J., & Siahaan, A. T. A. A. (2022). Aplikasi Buku Tamu Menggunakan Fitur Kamera Dan Ajax Berbasis Website Pada Kantor Dispora Kota Medan. *SITek: Jurnal Sains, Informatika, Dan Tekonologi*, *1*, 94–99.

Olazabal, A. A., Kaur, J., & Yeboah-Ofori, A. (2022). Deploying Man-In-the-Middle Attack on IoT Devices Connected to Long Range Wide Area Networks (LoRaWAN). *ISC2 2022 - 8th IEEE International Smart Cities Conference*. https://doi.org/10.1109/ISC255366.2022.9922377

Palcomtech. (2024). *Laragon Sebuah Platform Pengembangan Lokal Terkini untuk Pengembang Web*. https://palcomtech.ac.id/laragon-sebuah-platform-pengembangan-lokal-terkini-untuk-pengembang-web/

PlatformIO. (n.d.). *PlatformIO*. Retrieved June 2, 2026, from https://platformio.org/

Puspasari, F., Satya, T. P., Oktiawati, U. Y., Fahrurrozi, I., & Prisyanti, H. (2020). Analisis Akurasi Sistem sensor DHT22 berbasis Arduino terhadap Thermohygrometer Standar. *Jurnal Fisika Dan Aplikasinya*, *16*(1), 40. https://doi.org/10.12962/j24604682.v16i1.5776

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors*, *24*(12). https://doi.org/10.3390/s24124008

Ramadhani, E. H., Wulandari, A., & Hikmaturokhman, A. (2025). Perancangan Sistem Keamanan Komunikasi Data pada Jaringan LoRA Menggunakan Algoritme PRESENT. *Jurnal Telematika*, *19*(2), 72–81. https://journal.ithb.ac.id/index.php/telematika/article/view/674

Rosyida Zain, A., Hudi, S. A. R., & Neforawati, I. (2022). Analisis Pengiriman Data dari LoRa Gateway ke Network Server. *Multinetics*, *7*(1), 21–29. https://doi.org/10.32722/multinetics.v7i1.3971

Semtech. (n.d.). *Marks and Logos*. Retrieved June 7, 2026, from https://www.semtech.com/company/brand-resources

Setiowati, S., Riandini, R., Sari, V. A., Purwanti, I. L., & Andriansyah, N. (2023). LoRa Communication in the Service Level Monitoring Satu Duit Bogor Bridge. *JITCE (Journal of Information Technology and Computer Engineering)*, *7*(01), 19–28. https://doi.org/10.25077/jitce.7.01.19-28.2023

Shkoropad, Y., & Beshley, H. (2025). Development of Embedded Software for Esp32-Based Lora Modules With Adaptive Configuration and Link Quality Monitoring. *Information and Communication Technologies, Electronic Engineering*, *5*(2), 25–37. https://doi.org/10.23939/ictee2025.02.025

Simões, T., Cruz, T., Sousa, B., & Simões, P. (2025). A Security-Conscious Primer on LoRa and LoRaWAN Technologies. *European Conference on Information Warfare and Security, ECCWS*, 638–646. https://doi.org/10.34190/eccws.24.1.3575

Sun, C., Zheng, F., Zhou, G., & Guo, K. (2020). Design and Implementation of Cloud-based Single-channel LoRa IIoT Gateway Using Raspberry Pi. *Chinese Control Conference, CCC*, *2020-July*, 5259–5263. https://doi.org/10.23919/CCC50068.2020.9189480

Sun, Z., Yang, H., Liu, K., Yin, Z., Li, Z., & Xu, W. (2022). Recent Advances in LoRa: A Comprehensive Survey. *ACM Transactions on Sensor Networks*, *18*(4). https://doi.org/10.1145/3543856

Tech, F. (2025). *AMS1117 Voltage Regulator IC: Pinout, Features & Applications*. https://www.flywing-tech.com/blog/ams1117-voltage-regulator-ic-pinout-features-applications/

Wikipedia. (n.d.-a). *MySQL*. Retrieved June 1, 2026, from https://id.wikipedia.org/wiki/MySQL

Wikipedia. (n.d.-b). *VS Code*. Retrieved June 3, 2026, from https://en.wikipedia.org/wiki/Visual_Studio_Code

Windya, P. A., Suryani, V., & Wardana, A. A. (2021). Penerapan keamanan komunikasi pada jaringan LoRa(long range) menggunakan algoritma advanced encryption standard(AES) dan message authentication code(MAC). *E-Proceeding of Engineering*, *8*(2), 3406.

Zaraket, C., Papageorgas, P., Aillerie, M., Agavanakis, K., & Salame, C. (2020). Cyber security vulnerabilities of smart metering based on LPWAN wireless communication technologies. *AIP Conference Proceedings*, *2307*. https://doi.org/10.1063/5.0032709

Zhang, J. C., Khieng, D. H. T., & Huang, N. F. (2022). A Long Range Reliable Precise Irrigation System Based on LoRaP2P Protocol. *International Conference on Information Networking*, *2022-Janua*, 107–112. https://doi.org/10.1109/ICOIN53446.2022.9687187

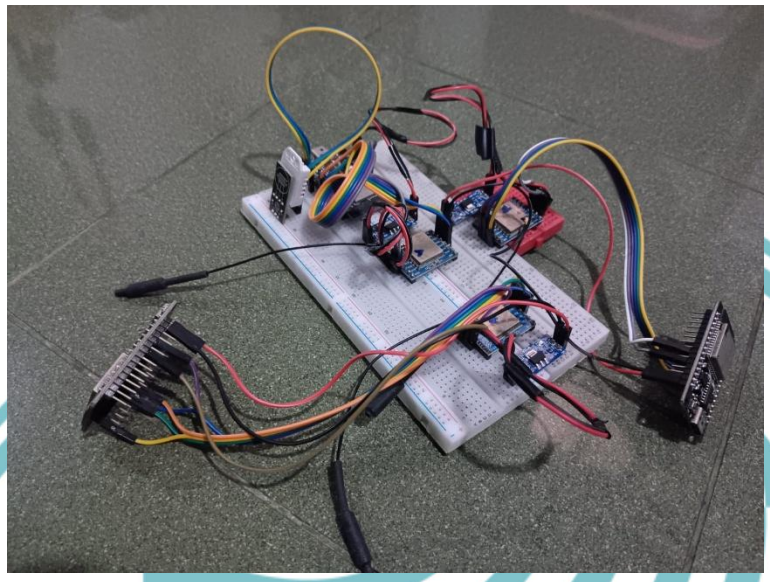
DAFTAR RIWAYAT HIDUP PENULIS

Mohammad Rizki Fadillah

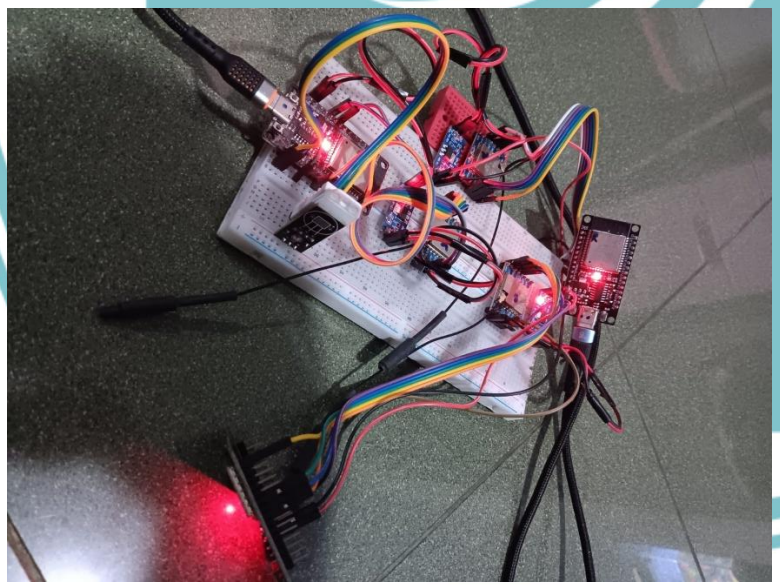
Lahir pada 2 Oktober 2004, saat ini berdomisili di Jakarta Selatan. Putra pertama dari dua bersaudara. Lulus dari Sekolah Dasar (SD) tahun 2016, lulus dari Sekolah Menengah Pertama (SMP) tahun 2019, dan dari Sekolah Menengah Kejuruan (SMK) dengan kompetensi keahlian Teknik Komputer dan Jaringan pada tahun 2022. Berkesempatan untuk melanjutkan pendidikan Diploma IV di Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta dari tahun 2022 hingga tahun 2026. Selama masa perkuliahan, Penulis memiliki ketertarikan yang mendalam dan sangat berminat untuk mendalami bidang Network Engineering, khususnya pada implementasi infrastruktur jaringan, konfigurasi perangkat multi-vendor, penyusunan arsitektur routing, serta analisis sistem keamanan jaringan nirkabel.

LAMPIRAN

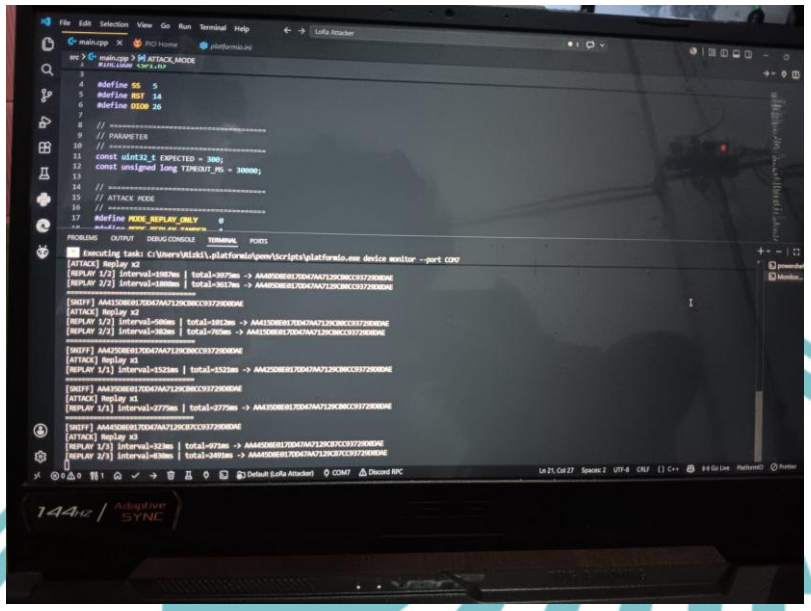
Lampiran 1. Dokumentasi Perangkat Keras



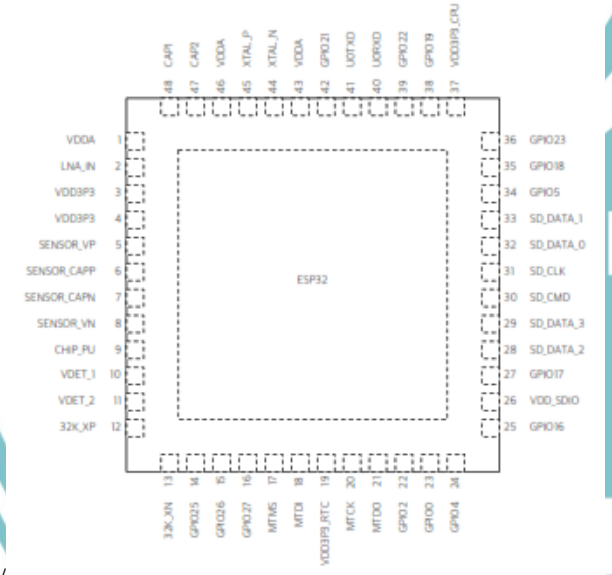
Lampiran 2. Dokumentasi Implementasi Sistem



Lampiran 3. Dokumentasi Pengujian Sistem



Lampiran 4. Spesifikasi Teknis Mikrokontroler ESP32



/

4.5 Cryptographic Hardware Accelerators

ESP32 is equipped with hardware accelerators of general algorithms, such as AES (FIPS PUB 197), SHA (FIPS PUB 180-4), and RSA. The chip also supports independent arithmetic, such as large-number modular multiplication and large-number multiplication. The maximum operation length for RSA, large-number modular multiplication, and large-number multiplication is 4096 bits.

The hardware accelerators greatly improve operation speed and reduce software complexity. They also support code encryption and dynamic decryption, which ensures that code in the flash will not be hacked.

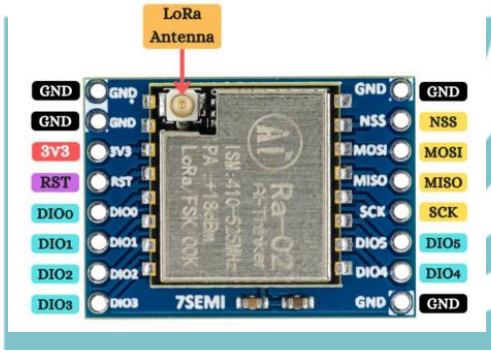
Lampiran 5. Spesifikasi Teknis LoRa Ra-02

2.Technical Specification

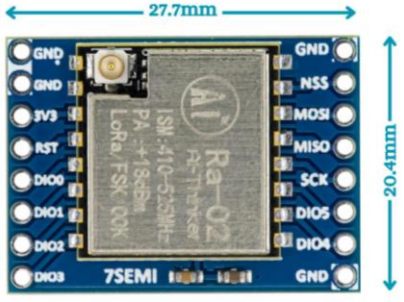
The **Technical Specification** table provides detailed information about **7Semi SX1278 LoRa Ra-02**, including its operating voltage, current consumption, and electrical characteristics. This data helps users understand the power requirements, communication parameters, and performance capabilities of the sensor. It ensures compatibility with different microcontrollers and embedded systems while providing guidelines for efficient integration into various applications.

SX1278 Specifications

- Chipset: Semtech SX1278
- Frequency Range: 410 MHz – 525 MHz (Typically 433 MHz)
- Transmission Distance: Up to 10 km (in open areas with ideal conditions)
- Operating Voltage: 1.8V – 3.3V (Typically 3.3V)
- Operating Temperature: -40°C to +85°C
- Antenna Interface: IPEX (U.FL) Connector
- Sensitivity: Up to -148 dBm
- Module Breakout Size: 27.7mm x 20.4mm.
- Weight:

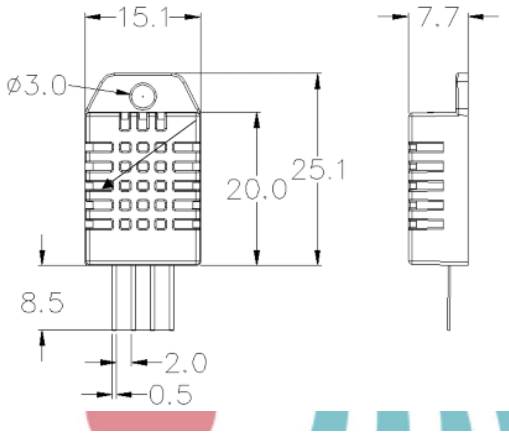


Pin	Name	Description
1	GND	Ground connection
2	3V3	Power supply input (3.3V)
3	RST	Module Reset
4	DIO0	Digital I/O for interrupts
5	DIO1	Digital I/O for interrupts
6	DIO2	Digital I/O for interrupts
7	DIO3	Digital I/O for interrupts
8	DIO4	Digital I/O for interrupts
9	DIO5	Digital I/O for interrupts
10	SCK	SPI Clock
11	MISO	SPI Data Output
12	MOSI	SPI Data Input
13	NSS	SPI Chip Select



Lampiran 6. Spesifikasi Teknis DHT22

Aosong Electronics Co.,Ltd



Pin sequence number: 1 2 3 4 (from left to right direction).

Pin	Function
1	VDD----power supply
2	DATA--signal
3	NULL
4	GND

Lampiran 7. Tautan Repositori Kode Program (*Source Code*)

Seluruh kode program implementasi algoritma AES-128 Mode CTR, HMAC-SHA256, serta mekanisme *Dynamic Key Management* (KDF) menggunakan pustaka mbedTLS pada perangkat ESP32 diunggah pada platform GitHub. Kode program untuk Node Pengirim dan Node Penerima tersebut dapat diakses secara publik melalui tautan berikut: https://github.com/rizkifrtma11/TA-LoRa-P2P-Security/tree/main

Lampiran 8. Tautan Akses Dataset Pengujian

Data hasil pengujian disimpan pada layanan *cloud storage* Google Drive. Folder ini memuat data mentah (*raw data log*) hasil pengukuran performa komputasi (*processing time*), nilai RSSI, SNR, serta pencatatan eror (*packet drop* atau HMAC *invalid*) selama pengujian mitigasi serangan *replay* dan *tampering*. Seluruh dataset dapat diakses melalui tautan berikut: https://s.pnj.ac.id/DatasetHasilPengujian.