

IMPLEMENTASI KEAMANAN GATEWAY PADA LORA MENGGUNAKAN AES (ADVANCED ENCRYPTION STANDARD) UNTUK SISTEM PENGAMATAN LINGKUNGAN

DIVO WIBOWO ADI



**TEKNOLOGI REKAYASA KOMPUTER
SEKOLAH VOKASI
INSTITUT PERTANIAN BOGOR
BOGOR
2025**



PERNYATAAN MENGENAI LAPORAN AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa laporan akhir dengan judul “Implementasi Keamanan *Gateway* pada LoRa Menggunakan AES (*Advanced Encryption Standard*) untuk Sistem Pengamatan Lingkungan” adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir laporan akhir ini.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Juli 2025

Divo Wibowo Adi
J0304211126

ABSTRAK

DIVO WIBOWO ADI. Implementasi Keamanan *Gateway* pada LoRa Menggunakan AES (*Advanced Encryption Standard*) untuk Sistem Pengamatan Lingkungan. Dibimbing oleh SHELVIE NIDYA NEYMAN.

Peningkatan penggunaan *Internet of Things* (IoT) dalam sistem pengamatan lingkungan menuntut solusi komunikasi jarak jauh yang hemat daya dan aman. LoRa (*Long Range*) merupakan teknologi komunikasi nirkabel yang mampu menjangkau area luas dengan konsumsi daya rendah, namun memiliki kelemahan dalam aspek keamanan data. Penelitian ini bertujuan untuk mengimplementasikan mekanisme keamanan pada gateway LoRa menggunakan algoritma *Advanced Encryption Standard* (AES) guna menjaga kerahasiaan dan integritas data yang ditransmisikan. Sistem dirancang menggunakan mikrokontroler ESP32 yang terintegrasi dengan modul GSM SIM800L untuk konektivitas jaringan, serta menggunakan protokol MQTT untuk komunikasi data. Enkripsi dilakukan pada sisi *transmitter* menggunakan AES-256, sedangkan dekripsi dan validasi dilakukan di sisi *gateway* sebelum data diteruskan ke server. Hasil pengujian menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan benar serta menjaga integritas data selama transmisi. Implementasi ini juga menunjukkan kinerja yang baik dengan waktu pemrosesan yang singkat. Oleh karena itu, sistem yang dikembangkan dapat meningkatkan keamanan komunikasi LoRa dalam sistem pengamatan lingkungan.

Kata kunci: AES, enkripsi, keamanan IoT, LoRa, pengamatan lingkungan

ABSTRACT

DIVO WIBOWO ADI. Gateway Security Implementation on LoRa Using AES (*Advanced Encryption Standard*) Algorithm for Environmental Monitoring System. Supervised by SHELVIE NIDYA NEYMAN.

The increasing use of the *Internet of Things* (IoT) in environmental monitoring systems demands long-range communication solutions that are both energy-efficient and secure. LoRa (*Long Range*) is a wireless communication technology capable of covering wide areas with low power consumption; however, it has weaknesses in data security. This study aims to implement gateway-level security for LoRa using the *Advanced Encryption Standard* (AES) to ensure the confidentiality and integrity of transmitted data. The system is designed using an ESP32 microcontroller integrated with a SIM800L GSM module for network connectivity and utilizes the MQTT protocol for data communication. Encryption is performed at the transmitter side using AES-256, while decryption and validation are carried out at the gateway before forwarding the data to the server. Test results show that the system is capable of correctly encrypting and decrypting data while preserving data integrity during transmission. This implementation also demonstrates good performance with a short processing time. Therefore, the developed system can enhance the security of LoRa-based communication in environmental monitoring applications.

Keywords: AES, encryption, environmental monitoring, IoT security, LoRa



Judul Proyek Akhir : Implementasi Keamanan Gateway pada LoRa Menggunakan AES (*Advanced Encryption Standard*) untuk Sistem Pengamatan Lingkungan

Nama
NIM

: Divo Wibowo Adi
: J0304211126

@Hak cipta milik IPB University

Disetujui oleh

Pembimbing:

Dr. Shelve Nidya Neyman, S.Kom., M.Si.

Diketahui oleh

Ketua Program Studi:

Dr. Inna Novianty, S.Si., M.Si.
NPI 201811198611192014

Dekan Sekolah Vokasi:

Dr. Ir. Aceng Hidayat, M.T.
NIP 196607171992031003

Tanggal Ujian:
05 Agustus 2025

Tanggal Lulus:

PRAKATA

Puji dan syukur penulis panjatkan kepada Allah subhanaahu wa ta'ala atas segala karunia-Nya sehingga karya ilmiah ini berhasil diselesaikan. Lokasi penelitian dilaksanakan di Badan Riset dan Inovasi Nasional (BRIN) Puspiptek Serpong dan tema yang dipilih dalam penelitian yang dilaksanakan sejak bulan Januari 2025 sampai bulan Mei 2025 ini ialah *Automation System* berbasis IoT, dengan judul “Implementasi Keamanan Gateway pada LoRa Menggunakan AES (*Advanced Encryption Standard*) untuk Sistem Pengamatan Lingkungan”.

Terima kasih penulis ucapkan kepada pembimbing, yang telah membimbing dan banyak memberi saran. Ucapan terima kasih juga disampaikan kepada pembimbing akademik (untuk program D-4 dan S-1), penguji luar komisi pembimbing yang telah membantu selama pengumpulan data. Ungkapan terima kasih juga disampaikan kepada ayah, ibu, serta seluruh keluarga yang telah memberikan dukungan, doa, kasih sayangnya dan seterusnya.

Terima kasih penulis ucapkan kepada:

1. Ibu Dr. Shelvie Nidya Neyman, S.Kom, M.Si. selaku Dosen Pembimbing Sekolah Vokasi Institut Pertanian Bogor (IPB);
2. Ibu Dr. Inna Novianty, S.Si, M.Si. selaku Ketua Program Studi Teknologi Rekayasa Komputer Sekolah Vokasi Institut Pertanian Bogor (IPB).
3. Para dosen serta seluruh staf pengajar IPB University yang telah memberikan ilmu selama perkuliahan.
4. Bapak Dr. Yudi Adityawarman, BSEE, MSc. selaku pembimbing lapangan yang telah membimbing dan memberi masukan dalam pengerjaan topik kajian.
5. Orang tua serta seluruh keluarga yang selalu memberi dukungan, do'a dan kasih sayangnya.
6. Teman – teman yang telah membantu penulis serta memberi masukan selama menjalani perkuliahan.

Semoga karya ilmiah ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Juli 2025

Divo Wibowo Adi



Hak Cipta Dilindungi Undang-undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

DAFTAR ISI

DAFTAR TABEL	viii
DAFTAR GAMBAR	viii
I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Manfaat	3
1.5 Ruang Lingkup	3
II TINJAUAN PUSTAKA	4
2.1 <i>Internet of Things</i> (IoT)	4
2.2 <i>LoRa (Long Range)</i>	4
2.3 Protokol Keamanan Data	5
2.4 Enkripsi dan Dekripsi Data	6
2.5 <i>Advanced Encryption Standard</i> (AES)	6
2.6 <i>Message Queuing Telemetry Transport</i> (MQTT)	7
III METODE	8
3.1 Lokasi dan Waktu Proyek Akhir	8
3.2 Alat dan Bahan	8
3.3 Teknik Pengumpulan Data dan Analisis Data	9
3.4 Prosedur Kerja	10
IV HASIL DAN PEMBAHASAN	11
4.1 Klasifikasi Keamanan Protokol Data	11
4.2 Hasil Implementasi Sistem	13
4.3 Arsitektur Sistem	19
4.4 Pengujian Sistem	21
4.5 Evaluasi Sistem	23
V SIMPULAN DAN SARAN	27
5.1 Simpulan	27
5.2 Saran	27
DAFTAR PUSTAKA	28
LAMPIRAN	30
RIWAYAT HIDUP	33



DAFTAR TABEL

1	Daftar <i>software</i>	8
2	Daftar <i>hardware</i>	8
3	Perbandingan protokol keamanan	13
4	Perbedaan tanpa menggunakan AES dan menggunakan AES	23

DAFTAR GAMBAR

1	<i>Internet of things</i>	4
2	LoRa (<i>Long Range</i>)	4
3	Proses enkripsi dan dekripsi data	6
4	AES (<i>Advanced Encryption Standard</i>)	6
5	<i>Message Queuing Telemetry Transport</i> (MQTT)	7
6	Prosedur kerja	10
7	<i>Schematic</i> rangkaian	14
8	Fisik alat	15
9	Konfigurasi MQTT	17
10	<i>Output</i> integrasi modul GSM	18
11	Diagram alir sistem	19
12	Arsitektur alat	20
13	Data yang sudah dilakukan enkripsi	21
14	Dekripsi data yang diterima dari <i>transmitter</i>	22
15	Dekripsi data yang ditolak	22
16	Waktu proses enkripsi	23
17	Waktu proses dekripsi	24
18	<i>Total transmission time</i>	24
19	<i>Encryption-decryption time</i>	25
20	<i>Temperature</i> (suhu)	25
21	<i>Humidity</i> (kelembaban)	26