IMPLEMENTASI ALGORITMA AES-GCM (ADVANCED ENCRYPTION STANDARD - GALOIS/COUNTER MODE) PADA NODEMCU ESP32 UNTUK KEAMANAN DATA PADA SISTEM PEMANTAUAN GAS METANA DI LAHAN GAMBUT BERBASIS IOT

MUHAMMAD IQBAL NUR
H1051211116

SKRIPSI

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

IMPLEMENTASI ALGORITMA AES-GCM (ADVANCED ENCRYPTION STANDARD - GALOIS/COUNTER MODE) PADA NODEMCU ESP32 UNTUK KEAMANAN DATA PADA SISTEM PEMANTAUAN GAS METANA DI LAHAN GAMBUT BERBASIS IOT

MUHAMMAD IQBAL NUR
H1051211116

Skripsi
Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer pada Program Studi Rekayasa Sistem Komputer

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Implementasi Algoritma AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) Pada Nodemcu Esp32 untuk keamanan data pada sistem pemantauan gas metana di lahan gambut berbasis iot
Nama Mahasiswa	: Muhammad Iqbal Nur
NIM	: H1051211116
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 21 Juli 2026
SK Pembimbing	: 626/DST/UN22.8/DT.00.09/2026 - 20 Februari 2026
SK Penguji	: 4255/DST/UN22.8/DT.00.09/2026 - 17 Juli 2026

Dosen Pembimbing

Pembimbing I	Pembimbing II
Kasliono, S.Mat., M.Cs.	Dwi Marisa Midyanti, S.T., M.Cs.
NIP. 199306202022031005	NIP. 198003192015042001

Dosen Penguji

Ketua Penguji	Anggota Penguji
Hirzen Hasfani , S.Kom., M.Cs.	Hafiz Muhardi, S.T, M.Kom.
NIP. 199305032022031003	NIP. 199007232023211017

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Kasliono, S.Mat., M.Cs.	Dwi Marisa Midyanti, S.T., M.Cs.
NIP. 199306202022031005	NIP. 198003192015042001

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusrizal, S.Si, M.Si
NIP 197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Iqbal Nur
NIM	: H1051211116
Program Studi/ Jurusan	: Rekayasa Sistem Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

dengan ini menyatakan bahwa dokumen ilmiah Tugas Akhir yang disajikan ini tidak mengandung unsur pelanggaran integritas akademik sesuai Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 39 Tahun 2021. Apabila di kemudian hari dokumen ilmiah Tugas Akhir ini mengandung unsur pelanggaran integritas akademik sesuai ketentuan perundangan tersebut, maka saya bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Demikian pernyatan ini untuk digunakan sebagaimana mestinya.

Pontianak, 22 Juli 2026



Muhammad Iqbal Nur
H1051211116

Implementasi Algoritma AES-GCM (Advanced Encryption Standard Galois/Counter Mode) Pada Nodemcu Esp32 Untuk Keamanan Data Pada Sistem Pemantauan Gas Metana Di Lahan Gambut Berbasis IoT

Abstrak

Pemantauan gas metana di lahan gambut berbasis *Internet of Things* (IoT) rentan terhadap ancaman *sniffing* dan manipulasi data. Penelitian ini mengimplementasikan algoritma *Advanced Encryption Standard–Galois/Counter Mode* (AES-GCM) pada mikrokontroler NodeMCU ESP32 untuk mengamankan pengiriman data dari sensor MQ-5 menuju *web server*. Hasil pengujian menunjukkan bahwa AES-GCM efektif menjaga kerahasiaan data melalui pembentukan *ciphertext* sepanjang 98 karakter heksadesimal, serta berhasil menolak seluruh paket data ilegal pada simulasi serangan *ARP Poisoning* dan *MITM Proxy*. Dari aspek performa, penerapan algoritma ini hanya memberikan tambahan beban komputasi yang relatif kecil. Rata-rata waktu respons sistem meningkat sebesar 20,65 ms, yaitu dari 295,61 ms menjadi 316,26 ms, sedangkan rata-rata *delay* bertambah sebesar 19,98 ms, yaitu dari 295,51 ms menjadi 315,49 ms. Hasil tersebut menunjukkan bahwa implementasi AES-GCM mampu meningkatkan keamanan komunikasi data tanpa memberikan penurunan kinerja yang signifikan, sehingga tetap layak diterapkan pada sistem pemantauan gas metana berbasis IoT secara *real-time*.

Kata kunci: Internet of Things, gas metana, AES-GCM, keamanan data, ESP32.

Implementation of the AES-GCM (Advanced Encryption Standard – Galois/Counter Mode) Algorithm on NodeMCU ESP32 For Data Security in an IoT-Based Methane Gas Monitoring System in Peatland Areas

Abstract

IoT-based methane gas monitoring in peatland areas is vulnerable to data interception and manipulation attacks, such as sniffing, Man-in-the-Middle (MITM), and ARP poisoning. This study implements the 128-bit Advanced Encryption Standard–Galois/Counter Mode (AES-GCM) algorithm on a NodeMCU ESP32 microcontroller to secure data transmission from an MQ-5 sensor to a web server. The experimental results demonstrate that AES-GCM effectively preserves data confidentiality by generating a 98-character hexadecimal ciphertext and successfully rejects all unauthorized data packets during ARP Poisoning and MITM Proxy attack simulations. In terms of performance, the proposed algorithm introduces only a small computational overhead. The average system response time increased by 20.65 ms, from 295.61 ms to 316.26 ms, while the average transmission delay increased by 19.98 ms, from 295.51 ms to 315.49 ms. These results indicate that AES-GCM enhances data confidentiality, integrity, and authenticity without significantly degrading system performance. Therefore, AES-GCM is proven to be a reliable security solution for real-time IoT-based methane gas monitoring systems.

Keywords: Internet of Things, methane gas, AES-GCM, data security, ESP32.

PRAKATA

Puji syukur ke hadirat Allah SWT atas segala limpahan rahmat dan karunia-Nya, sehingga penyusunan skripsi berjudul "Implementasi Algoritma AES-GCM (Advanced Encryption Standard Galois/Counter Mode) Pada Nodemcu Esp32 Untuk Keamanan Data Pada Sistem Pemantauan Gas Metana Di Lahan Gambut Berbasis IoT " dapat diselesaikan dengan baik dan tepat waktu. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program pendidikan pada jenjang sarjana dan mendapatkan gelar Sarjana Komputer (S.Kom) di Universitas Tanjungpura.

Selama proses penyusunan skripsi, penulis banyak menerima bantuan dan dukungan. Serta bimbingan yang diberikan oleh berbagai pihak. Atas segala kontribusi tersebut, ucapan terima kasih yang sebesar-besarnya disampaikan kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Bapak Kasliono, S.Mat., M.Cs., sebagai dosen PA sekaligus dosen pembimbing pertama yang telah memberikan arahan dan saran yang membangun dalam penyusunan skripsi ini.
3. Ibu Dwi Marisa Midyanti, S.T.,M.Cs., sebagai dosen pembimbing kedua yang telah memberikan bimbingan, masukan, dan motivasi selama proses penyusunan skripsi ini.
4. Bapak Hirzen Hasfani , S.Kom., M.Cs., sebagai dosen penguji pertama yang telah memberikan saran dan arahan dalam penulisan skripsi ini.
5. Bapak Hafiz Muhardi, S.T, M.Kom., sebagai dosen penguji kedua yang telah memberikan saran dan masukan dalam penulisan skripsi ini.
6. Kepada orangtua yang selalu memberikan dukungan, bantuan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan proses dalam perkulihan serta dalam setiap langkah kehidupan penulis.

7. Saudara M.Fatturahman yang memberi semangat, melakukan penelitian bersama dan membantu belajar dalam hal pengujian serangan manipulasi data sehingga dapat menyelesaikan penulisan skripsi ini.
8. Saudara Devin yang sudah memberi Semangat, melakukan penelitian bersama, dan membantu dalam mengerjakan skripsi sehingga dapat menyelesaikan penulisan skripsi ini.
9. Saudari Maulidia yang sudah memberi Semangat, melakukan penelitian bersama, dan membantu dalam mengerjakan skripsi sehingga dapat menyelesaikan penulisan skripsi ini.
10. Para rekan-rekan seperjuangan mahasiswa khususnya Sistem Komputer angkatan 2021 yang telah memberikan semangat dan dukungan dalam menjalani proses perkuliahan.

Disadari bahwa dalam proses penyusunan skripsi ini masih banyak hal yang dapat disempurnakan. Oleh karena itu, segala bentuk kritik dan saran yang membangun sangat diharapkan untuk menjadi bahan evaluasi di masa mendatang. Semoga karya ini dapat memberikan manfaat bagi pihak-pihak yang membutuhkan maupun yang tertarik pada bidang terkait.

Pontianak, 22 Juli 2026

Muhammad Iqbal Nur

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
Abstrak iv
Abstract v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
DAFTAR KODE PROGRAM xiv
DAFTAR LAMPIRAN xv
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 5
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan 5
BAB 2 LANDASAN TEORI 8
2.1 Penelitian Terdahulu 8
2.2 AES 9
2.3 AES-GCM 14
2.4 Sensor MQ-5 18
2.5 Lampu LED 19
2.6 Buzzer 19
2.7 Power Bank 19
2.8 Basis Data 20
2.9 Arduiono IDE 20
2.10 Balsamiq Mockup 21

2.11Quality of Service 21
2.12Sniffing 22
2.13ARP Poisoning 22
2.14MITM Proxy 23
2.15Parts per Milion 23
2.16Kali Linux 24
2.17Wireshark 25
2.18Ettercap 25
BAB 3 METODE PENELITIAN 27
3.1 Studi Literatur 27
3.2 Analisis Kebutuhan 28
3.3 Perancangan Sistem 29
3.4 Implementasi Sistem 29
3.5 Pengujian Sistem 30
3.6 Kesimpulan dan Saran 30
BAB 4 PERANCANGAN 32
4.1 Deskripsi Sistem 32
4.2 Perancangan Arsitektur 33
4.3 Perancangan Perangkat Keras 34
4.4 Perancangan Perangkat Lunak 37
4.5 Algoritma AES-GCM 40
4.6 Perancangan Basis Data 44
4.7 Perancangan *Pseudocode* 46
4.8 Perancangan Antarmuka Website 53
4.9 Perancangan Pengujian sistem 56
BAB 5 IMPLEMENTASI, PENGUJIAN, DAN PEMBAHASAN 59
5.1 Implementasi Sistem 59
5.2 Implementasi Perangkat Keras 59
5.3 Implementasi Perangkat Lunak 61
5.4 Implementasi Algoritma AES-GCM 77
5.5 Pengujian Sistem 91

5.6 Pembahasan 108
BAB 6 PENUTUP 111
6.1 Kesimpulan 111
6.2 Saran 112
DAFTAR PUSTAKA 113
LAMPIRAN 117

DAFTAR GAMBAR

Gambar 2. 1 Proses enkripsi dan dekripsi AES 10
Gambar 2. 2 Ilustrasi fungsi AddRoundKey 11
Gambar 2. 3 Ilustrasi fungsi SubBytes. 11
Gambar 2. 4 Ilustrasi fungsi ShiftRows. 12
Gambar 2. 5 Ilustrasi fungsi MixColumns 12
Gambar 2. 6 Rounds (putaran) pada AES-128. 13
Gambar 2. 7 Skema Enkripsi dan Dekripsi AES-GCM 14
Gambar 2. 8 NodeMCU ESP32 18
Gambar 2. 9 Sensor MQ-5 18
Gambar 2. 10 Lampu LED 19
Gambar 2. 11 Buzzer 19
Gambar 2. 12 Power Bank 20
Gambar 2. 13 Arduino IDE 20
Gambar 3. 1 Diagram Alir Penelitian 27
Gambar 4. 1 Diagram Blok Perancangan Sistem 32
Gambar 4. 2 Rancangan Arsitektur Sistem 34
Gambar 4. 3 Perancangan Perangkat Keras 36
Gambar 4. 4 Diagram Alir Perangkat Lunak 39
Gambar 4. 5 Flowchart enkripsi AES-GCM 42
Gambar 4. 6 Flowchart dekripsi AES-GCM 43
Gambar 4. 7 Diagram ERD 44
Gambar 4. 8 Halaman Login 53
Gambar 4. 9 Halaman Dashboard 54
Gambar 4. 10 Halaman Monitor Data 54
Gambar 4. 11 Halaman Riwayat Data 55
Gambar 4. 12 Halaman Grafik Analisis 55
Gambar 4. 13 Log Serangan 56
Gambar 4. 14 Diagram Skema Penyerangan 58
Gambar 5. 1 Implementasi Perangkat Keras 61
Gambar 5. 2 Halaman *Log* 62

Gambar 5. 3 Halaman *Dashboard*..... 62
Gambar 5. 4 Halaman Monitor Data..... 63
Gambar 5. 5 Riwayat Data..... 63
Gambar 5. 6 Tampilan Grafik Kadar Gas Metana 64
Gambar 5. 7 Tampilan Grafik Response time 64
Gambar 5. 8 Halaman Delay..... 65
Gambar 5. 9 Halaman Log Serangan 65

DAFTAR TABEL

Tabel 2. 1 Perbandingan penelitian terdahulu 8
Tabel 2. 2 Kategori *Delay*..... 22
Tabel 4. 1 Koneksi Pin pada NodeMCU ESP32……..……36
Tabel 4. 2 Sensor data 45
Tabel 4. 3 Admin 45
Tabel 4. 4 Log Serangan..... 46
Tabel 5. 1 plaintext dalam bentuk ASCII hexadecimal 77
Tabel 5. 2 kunci AES-128 78
Tabel 5. 3 Initialization Vector (IV)AES-GCM 79
Tabel 5. 4 Proses XOR..... 83
Tabel 5. 5 Perhitungan XOR (Dekripsi)..... 88
Tabel 5. 6 Pengujian Waktu Respon Sistem Tanpa AES-GCM..... 92
Tabel 5. 7 Pengujian Waktu Respon Sistem Dengan AES-GCM 93
Tabel 5. 8 Pengujian Delay Sistem Tanpa AES-GCM 95
Tabel 5. 9 Pengujian Delay Sistem Dengan AES-GCM..... 96
Tabel 5. 10 Pengujian Sniffing pada Sistem tanpa AES-GCM 98
Tabel 5. 11 Pengujian Sniffing pada Sistem dengan AES-GCM 99
Tabel 5. 12 Pengujian manipulasi data pada sistem tanpa AES-GCM 104
Tabel 5. 13 Pengujian manipulasi data pada sistem dengan AES-GCM 106

DAFTAR KODE PROGRAM

Kode Program 5. 1 Pembacaan Sensor MQ-5 66
Kode Program 5. 2 Enkripsi AES-GCM 68
Kode Program 5. 3 Dekripsi AES-GCM 71
Kode Program 5. 4 Pengambilan data dan perintah server 74
Kode Program 5. 5 Aktivasi led dan buzzer 76

DAFTAR LAMPIRAN

Lampiran 1 Hasil sniffing pada sistem tanpa AES-GCM 117
Lampiran 2 Hasil sniffing pada sistem dengan AES-GCM 117
Lampiran 3 Hasil ARP Poisoning 118
Lampiran 4 Proses Manipulasi data pada sistem tanpa AES-GCM 118
Lampiran 5 proses Manipulasi data pada sistem dengan AES-GCM 118
Lampiran 6 Manipulasi data pada sistem tanpa AES-GCM 119
Lampiran 7 Manipulasi data pada sistem dengan AES-GCM 119
Lampiran 8 Tampilan data pada website setelah dilakukan Manipulasi data pada 119
Lampiran 9 Tampilan data pada website setelah dilakukan Manipulasi data pada 119
Lampiran 10 Hasil log serangan di database pada sistem dengan AES-GCM.. 120
Lampiran 11 Hasil log serangan pada website 120

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan teknologi yang menghubungkan objek fisik ke jaringan internet sehingga memungkinkan pertukaran data dan komunikasi secara otomatis (Zikria et al., 2021). Dunia IoT(internet of things) semakin berkembang pesat dan banyak diminati dalam aplikasi sistem kendali khususnya mikrokontroler dan sensor gas. Dengan memanfaatkan teknologi Internet of Things (IoT), sistem ini dirancang untuk memberikan pemantauan realtime dan akurat terhadap kadar gas metana (Ningrum et al., 2024). Sistem pemantauan konsentrasi gas metana yang bersifat responsif sangat penting untuk mendukung deteksi dini serta memberikan peringatan terhadap kemungkinan peningkatan kadar gas metana. Teknologi Internet of Things (IoT) menjadi solusi yang banyak diterapkan dalam sistem pemantauan lingkungan karena mampu melakukan akuisisi data secara real-time serta mentransmisikan informasi tersebut ke platform berbasis web (Yulianto et al., 2024).

Informasi konsentrasi gas metana pada lahan gambut merupakan data yang sangat krusial karena gas metana termasuk gas mudah terbakar dan berpotensi menyebabkan kebakaran lahan serta ledakan apabila mencapai ambang batas tertentu (Mulyono, 2019). Selain itu, Gas metana dapat menyerap panas lebih besar daripada karbon dioksida (CO_2) dan merupakan salah satu bagian dari gas rumah kaca yang berbahaya (Osa Novantri & Yusmaniar Oktiawati, 2022). Dalam proses transmisi data kadar metana dari sensor menuju sistem pemantauan berbasis IoT, terdapat potensi ancaman keamanan seperti serangan Manipulasi Data dimana penyerang bisa mengubah data yang dikirim menjadi 0 ppm. Apabila data kadar gas metana dimanipulasi oleh penyerang, misalnya data asli menunjukkan konsentrasi berbahaya sebesar 1000 ppm tetapi diubah menjadi 0 ppm yang dianggap aman, sistem tidak akan mengaktifkan buzzer dan led sebagai tanda bahaya. Kondisi ini dapat menyebabkan keterlambatan deteksi kebakaran, peningkatan risiko ledakan, kerusakan lingkungan yang luas, serta kerugian ekonomi yang signifikan. Oleh

sebab itu, keamanan data gas metana perlu dijaga dengan mekanisme enkripsi agar integritas, kerahasiaan, dan keaslian data tetap terjamin selama proses pengiriman.

Meskipun teknologi IoT memberikan banyak manfaat dalam pemantauan kadar gas metana, muncul tantangan signifikan terkait keamanan data. Data yang dikirimkan melalui jaringan IoT rentan terhadap berbagai ancaman, seperti serangan ARP poisoning dan Sniffing. Investasi keamanan merupakan sebuah kunci dalam mengupayakan kenyamanan dalam menggunakan IoT. Peningkatan keamanan pada sistem IoT memberikan keuntungan strategis berupa pencegahan terhadap potensi serangan siber berskala besar serta meminimalkan risiko kerugian finansial akibat biaya pemulihan yang signifikan.

Pada tahun 2000 National institute of standards and technology (NIST) menetapkan sebuah acuan kriptografi yang baru yaitu Algoritma AES dan ditetapkan sebagai Advanced Encryption Standard (AES) . AES secara umum dapat berfungsi diblok 128-bit atau 16 karakter (Hulu et al., 2020). Beberapa tahun kemudian, pada tahun 2007, NIST merilis NIST Special Publication 800-38D yang merekomendasikan Galois/Counter Mode (GCM) sebagai mode operasi resmi untuk block cipher seperti AES. Kombinasi AES dengan mode GCM (AES-GCM) inilah yang kemudian menjadi standar industri untuk enkripsi terautentikasi (authenticated encryption). AES-GCM (Advanced Encryption Standard – Galois/Counter Mode) merupakan mode operasi dari algoritma AES yang dirancang untuk melakukan proses enkripsi sekaligus autentikasi data dalam satu langkah komputasi. Dengan menggunakan counter mode untuk melaksanakan proses enkripsi dan algoritma Galois (GHASH) sebagai mekanisme autentikasi (Jamaluddin et al., 2020). Dipilihnya algoritma AES-GCM karena mampu menjamin kerahasiaan serta integritas data dari ancaman manipulasi. Selain itu, mode ini memiliki keunggulan tinggi dalam efisiensi karena memungkinkan proses enkripsi dan autentikasi dilakukan secara paralel dalam satu tahapan (Susanti et al., 2024).

Pada penelitian sebelumnya yang berjudul “Implementasi Internet Of Things Untuk Monitoring Kadar Gas Metana Pada Bioga” (Avilsyah et al., 2024). Penelitian ini dilakukan menggunakan mikrokontroler NodeMCU ESP32 yang

terintegrasi dengan sensor MQ-4, DS18B20, BMP280, dan SEN0161. Sensor MQ-4 dikalibrasi terlebih dahulu untuk memperoleh nilai ppm yang akurat. Hasil kalibrasi menunjukkan bahwa sensor MQ-4 mampu mendeteksi konsentrasi gas metana dalam rentang 200 hingga 10.000 ppm secara presisi. Namun, terdapat celah penelitian yang signifikan pada studi tersebut, di mana parameter evaluasi performa hanya bertumpu pada aspek fungsionalitas akurasi sensor dan analisis kualitas jaringan (*Quality of Service*). Keamanan data selama proses transmisi sepenuhnya diabaikan, sehingga data parameter lingkungan mengalir secara terbuka tanpa proteksi.

Pada penelitian selanjutnya yang berjudul "Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File pada Aplikasi Berbasis Web" (Bibiola et al., 2023). Penelitian ini berhasil menerapkan implementasi AES untuk melindungi file dokumen dengan berbagai format seperti .pdf, .doc, dan .docx. Uji coba juga dilakukan dengan Wireshark (sniffing test) menunjukkan bahwa data terenkripsi tidak dapat dibaca atau diretas saat dikirim melalui jaringan. Hal ini membuktikan sistem efektif dalam mencegah kebocoran data selama transmisi. Meskipun demikian, penelitian tersebut hanya berfokus pada pengamanan file statis pada aplikasi web dan belum mengimplementasikan AES pada perangkat IoT yang memiliki keterbatasan sumber daya komputasi serta kebutuhan komunikasi data secara real-time.

Pada penelitian selanjutnya yang berjudul "Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya"(R.M. Hilmy Hernandi & Joko Christian Chandra, 2024). Penelitian ini berhasil mengimplementasikan algoritme kriptografi AES-256 dan AES-GCM pada sistem berbasis web untuk mengamankan dokumen rekam medis pasien di Klinik Mulya. Penerapan algoritme AES-256 dan AES-GCM menghasilkan peningkatan signifikan pada aspek keamanan data, yang ditunjukkan oleh perubahan ukuran dan struktur file hasil enkripsi yang menjadi lebih besar dan tidak terbaca dalam format aslinya. Kondisi ini menunjukkan keberhasilan sistem dalam menjaga kerahasiaan dan integritas data medis sesuai dengan standar keamanan informasi. Selain itu, proses dekripsi berhasil mengembalikan file ke

bentuk semula tanpa kehilangan informasi. Akan tetapi, penerapan yang dilakukan masih terbatas pada pengamanan dokumen di lingkungan aplikasi web dan belum mengkaji implementasi AES-GCM pada sistem IoT yang mengirimkan data sensor secara berkelanjutan melalui jaringan yang rentan terhadap serangan siber.

Berdasarkan penelitian-penelitian terdahulu, diangkat judul "Implementasi Algoritma AES-GCM pada NodeMCU ESP32 untuk Keamanan Data Sistem Pemantauan Gas Metana di Lahan Gambut Berbasis IoT". Melalui penelitian ini, telah berhasil dirancang dan diimplementasikan sistem pemantauan gas metana berbasis Internet of Things (IoT) dengan penerapan algoritma AES-GCM untuk meningkatkan keamanan data. Sistem yang dikembangkan mampu menyajikan informasi kadar gas metana secara real-time serta melindungi data dari potensi penyadapan dan manipulasi selama proses transmisi. Hasil penelitian menunjukkan bahwa penerapan AES-GCM mampu menjaga kerahasiaan, integritas, dan keaslian data yang dikirimkan antara NodeMCU ESP32 dan server. Selain itu, implementasi AES-GCM tidak memberikan pengaruh yang signifikan terhadap performa sistem sehingga tetap layak digunakan pada sistem pemantauan gas metana berbasis IoT..

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dari penelitian ini yaitu:

1. Bagaimana waktu respon sistem dan delay setelah di terapkan algoritma AES-GCM ?
2. Bagaimana pengaruh penerapan algoritma AES-GCM terhadap keamanan data dari serangan sniffing dan manipulasi data pada sistem pemantauan gas metana berbasis IoT?

1.3 Batasan Masalah

Berikut merupakan batasan masalah dalam penelitian ini, antara lain:

1. Sistem yang dibangun difokuskan pada pemantauan dan pengiriman data konsentrasi gas metana menggunakan sensor MQ-5 yang terintegrasi dengan mikrokontroler NodeMCU ESP32.
2. Algoritma kriptografi yang digunakan AES-GCM.

3. Sistem hanya dibangun berbasis web, tidak mencakup aplikasi mobile atau platform lain.
4. Pengujian sistem dilakukan menggunakan data hasil pembacaan sensor MQ-5 pada lingkungan pengujian atau simulasi.
5. Serangan yang diuji pada sistem adalah Sniffing dan ARP Poisoning.
6. Serangan diuji pada jaringan local.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain sebagai berikut:

1. Mengukur waktu respon sistem dan delay setelah diterapkannya algoritma enkripsi AES-GCM pada sistem pemantauan berbasis IoT.
2. Menganalisis efektivitas algoritma AES-GCM dalam menjaga kerahasiaan dan integritas data dari upaya *sniffing* dan manipulasi data.

1.5 Manfaat Penelitian

Penelitian ini memberikan peningkatan keamanan pada sistem pemantauan gas metana melalui pengamanan jalur komunikasi data antara NodeMCU ESP32 dan server. Selain itu, penelitian ini turut mendorong penerapan aspek keamanan siber dalam pengembangan sistem berbasis Internet of Things (IoT). Dengan demikian, sistem monitoring yang dibangun tidak hanya berfokus pada aspek fungsionalitas, tetapi juga memperhatikan perlindungan dan keamanan data yang dikirimkan.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini disusun untuk memberikan gambaran yang jelas mengenai isi, urutan pembahasan, serta keterkaitan antar bab dalam penelitian yang dilakukan. Adapun sistematika penulisan laporan tugas akhir ini terdiri dari enam bab, yaitu sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang penelitian, rumusan masalah, batasan, tujuan, dan manfaat dari penelitian. Disampaikan pula sistematika penulisan sebagai panduan pembaca dalam memahami susunan laporan. Bab ini menjadi dasar untuk memahami ruang lingkup dan arah penelitian.

BAB 2 LANDASAN TEORI

Bab ini berisi landasan teori dan kajian pustaka yang mendukung pelaksanaan penelitian. Pembahasan meliputi karakteristik lahan gambut dan gas metana, prinsip kerja sensor gas MQ-5, mikrokontroler NodeMCU ESP32, buzzer dan lampu LED sebagai sistem peringatan dini, konsep Internet of Things (IoT), serta website sebagai media pemantauan berbasis web. Selain itu, bab ini juga mengulas algoritma kriptografi Advanced Encryption Standard (AES) dan mode Galois/Counter Mode (AES-GCM), serta penelitian-penelitian terdahulu yang relevan sebagai dasar pengembangan sistem.

BAB 3 METODE PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan dalam pengembangan sistem, meliputi tahapan studi literatur, analisis kebutuhan sistem, perancangan, implementasi, dan pengujian. Pada bab ini juga dijelaskan kebutuhan perangkat keras dan perangkat lunak yang digunakan, serta metode evaluasi untuk menilai kinerja dan keamanan sistem pemantauan gas metana berbasis IoT yang diimplementasikan.

BAB 4 PERANCANGAN

Bab ini membahas secara rinci proses perancangan sistem pemantauan kadar gas metana berbasis Internet of Things (IoT). Pembahasan mencakup deskripsi umum sistem, arsitektur sistem, serta perancangan perangkat keras dan perangkat lunak. Perancangan sistem meliputi penggunaan mikrokontroler NodeMCU ESP32, sensor MQ-5, serta buzzer dan LED sebagai sistem peringatan dini, termasuk perancangan mekanisme pengamanan data menggunakan algoritma AES-GCM dan skenario pengujian serangan pada sistem.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi sistem yang telah dirancang serta pengujian yang dilakukan. Pengujian meliputi pengujian fungsional sistem dalam mendeteksi kadar gas metana, proses enkripsi dan autentikasi data menggunakan algoritma AES-GCM, pengiriman data ke server berbasis web, serta aktivasi buzzer dan LED ketika kadar gas metana melebihi ambang batas yang ditentukan serta

misal terjadi manipulasi data maka led kuning akan menyala sebagai tanda peringatan. Hasil pengujian selanjutnya dianalisis dan dibahas untuk menilai kinerja, keamanan sistem.

BAB 6 PENUTUP

Bab ini berisi kesimpulan yang diperoleh berdasarkan hasil implementasi dan pengujian sistem yang telah dilakukan, sesuai dengan tujuan penelitian. Selain itu, disampaikan pula saran-saran yang dapat digunakan sebagai bahan pertimbangan untuk pengembangan dan penyempurnaan sistem pemantauan gas metana berbasis IoT pada penelitian selanjutnya. Bab ini merupakan penutup dari seluruh rangkaian pembahasan dalam laporan skripsi.