IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK ENKRIPSI DATA SENSOR PADA SISTEM MONITORING KUALITAS UDARA

RENDY PAMUNGKAS
H1051201014

SKRIPSI

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2025

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK ENKRIPSI DATA SENSOR PADA SISTEM MONITORING KUALITAS UDARA

RENDY PAMUNGKAS
H1051201014

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
2025

LEMBAR PENGESAHAN

Judul Tugas Akhir	:	Implementasi Algoritma *Advanced Encryption Standard* (AES) Untuk Enkripsi Data Sensor Pada Sistem Monitoring Kualitas Udara
Nama Mahasiswa	:	Rendy Pamungkas
NIM	:	H1051201014
Jurusan/Program Studi	:	Rekayasa Sistem Komputer
Tanggal Lulus	:	24 Juli 2025
SK Pembimbing	:	No.1911/UN22.8/TD.06/2024/Tanggal 09 Juli 2024
SK Penguji	:	No.2259/UN22.8/TD.06/2025/Tanggal 17 Juli 2025

Dosen Pembimbing

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

Dosen Penguji

Ketua Penguji	Anggota Penguji
Syamsul Bahri, S.Kom., M.Cs.	Kartika Sari, S.Kom., M.Cs.
NIP.198802272015041001	NIP.199206162022032014

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

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	: Rendy Pamungkas
NIM	: H1051201014
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, 24 Juli 2025



Rendy Pamungkas

H1051201014

Implementasi Algoritma *Advanced Encryption Standard* (Aes) Untuk Enkripsi Data Sensor Pada Sistem Monitoring Kualitas Udara

Abstrak

Seiring dengan berkembangnya teknologi, data telah menjadi salah satu aset paling berharga dalam berbagai sektor. Namun, semakin meningkatnya ketergantungan terhadap data, semakin tinggi pula risiko manipulasi yang dapat merusak integritas informasi. Data yang tidak terlindungi dapat dengan mudah dimanipulasi oleh pihak yang tidak bertanggung jawab, yang pada akhirnya dapat menyebabkan kesalahan dalam pengambilan keputusan dan berdampak negatif pada orang yang melihat informasi yang salah tersebut. Oleh karena itu, kriptografi diperlukan untuk menjaga keamanan dan integritas data yang dihasilkan. Dalam penelitian ini, algoritma *Advanced Encryption Standard* (AES*)* diimplementasikan untuk mengenkripsi data sensor yang dihasilkan oleh sistem monitoring kualitas udara. Hasil pengujian menunjukkan bahwa algoritma AES-128 memiliki rata-rata waktu enkripsi sebesar 0,877 ms dan waktu dekripsi rata-rata 1,756 ms. Implementasi algoritma AES dalam sistem ini memberikan pengaruh terhadap peningkatan *delay* pada proses transmisi data. Sebelum penerapan algoritma, waktu transmisi tercatat sebesar 110,9 ms dan dikategorikan sebagai sangat baik berdasarkan standar *TIPHON*. Setelah penerapan algoritma AES, *delay* meningkat menjadi 162,6 ms, yang masih berada dalam kategori baik menurut klasifikasi yang sama. Selain itu, Pengujian menunjukkan AES-128 berhasil mengenkripsi dan mendekripsi seluruh data dengan tingkat keberhasilan 100%, di mana setiap ciphertext dapat dipulihkan sepenuhnya menjadi plaintext tanpa perubahan atau kesalahan.

Kata kunci: *Advanced Encryption Standard (AES),* kriptografi, sistem monitoring kualitas udara, *NodeMCU ESP32*.

Implementation Of Advanced Encryption Standard (Aes) Algorithm For Sensor Data Encryption In Air Quality Monitoring System

Abstract

With the advancement of technology, data has become one of the most valuable assets across various sectors. However, as reliance on data increases, so does the risk of manipulation that can compromise the integrity of information. Unprotected data can be easily altered by unauthorized parties, potentially leading to errors in decision-making and negatively impacting individuals who rely on inaccurate information. Therefore, cryptography is essential to safeguard the security and integrity of generated data. In this study, the Advanced Encryption Standard (AES) algorithm was implemented to encrypt sensor data produced by an air quality monitoring system. The test results show that the AES-128 algorithm achieved an average encryption time of 0.877 ms and an average decryption time of 1.756 ms. Implementing the AES algorithm in this system had an impact on increasing the delay in data transmission. Before applying the algorithm, the transmission time was recorded at 110.9 ms and categorized as very good based on the TIPHON standard. After applying the AES algorithm, the delay increased to 162.6 ms, which is still within the good category according to the same classification. Furthermore, testing showed that AES-128 successfully encrypted and decrypted all data with a 100% success rate, where each ciphertext could be fully restored to its original plaintext without any changes or errors

Keywords: *Advanced Encryption Standard (AES), cryptography, air quality monitoring system, NodeMCU ESP32.*

HALAMAN PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT dan atas dukungan dan doa dari orang tercinta, akhirnya skripsi ini dapat diselesaikan. Oleh karena itu, dengan rasa bangga dan bahagia penulis ucapkan rasa syukur dan terima kasih kepada :

1. Allah SWT, karena hanya atas izin dan karunianya lah maka skripsi ini dapat dibuat dan selesai pada waktunya.
2. Ibu tercinta, Rusmina, yang dengan penuh kesabaran dan kasih sayang tidak pernah lelah memberikan dukungan moral, doa-doa yang tulus, serta motivasi yang tak pernah surut sepanjang perjalanan penulisan tugas akhir ini. Setiap dukungan dan perhatian Ibu telah memberikan kekuatan yang luar biasa bagi penulis. Semoga tugas akhir ini menjadi sebuah penghargaan dan tanda terima kasih yang mendalam dari lubuk hati penulis yang tak terhingga.
3. Ayah tercinta, Muhammad Jauji (Alm), yang selama 21 tahun dengan penuh kasih sayang telah membimbing, menginspirasi, dan tidak pernah henti-hentinya memberikan dukungan serta pelajaran hidup yang berharga kepada penulis. Setiap langkah dan nasihat Ayah telah membentuk penulis menjadi pribadi yang lebih baik. Semoga tugas akhir ini menjadi bukti penghargaan dan rasa terima kasih yang mendalam dari hati penulis, yang tak akan pernah terbalaskan.
4. Adik tercinta, Widya dan Raisya, yang selalu ada di setiap langkah penulis. Dukungan, kebersamaan, dan semangat yang diberikan telah menjadi sumber motivasi dan kekuatan yang luar biasa selama penulisan tugas akhir ini.
5. Saudari Linda yang telah memberikan dukungan, semangat, dan kasih yang tiada henti, serta menjadi teman setia dalam setiap langkah penulis, baik dalam suka maupun duka, sehingga penulis dapat menyelesaikan skripsi ini dengan baik.

PRAKATA

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat-Nya yang telah memberikan kekuatan, kesehatan, dan kemampuan untuk menyelesaikan tugas akhir berjudul "Implementasi *Algoritma Advanced Encryption Standard (AES)* Untuk Enkripsi Data Sensor pada Sistem Monitoring Kualitas Udara". Tugas akhir ini disusun sebagai syarat untuk meraih gelar Sarjana Komputer (S.Kom) di Jurusan Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura.

Penulis menyadari bahwa penyelesaian tugas akhir ini tidak terlepas dari dukungan berbagai pihak, baik material, ilmu, maupun doa. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Bapak Tedy Rismawan, S.Kom., M.Cs. selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak.
3. Ibu Dwi Marisa Midyanti, S.T., M.Cs., sebagai dosen pembimbing utama yang dengan penuh perhatian memberikan masukan berharga, serta meluangkan waktu dan pikiran untuk mendukung penulisan skripsi ini.
4. Bapak Kasliono, S.Mat., M.Cs., sebagai dosen pembimbing pendamping yang telah memberikan arahan, bimbingan, dan wawasan yang sangat berarti selama penulisan skripsi ini.
5. Bapak Syamsul Bahri, S.Kom., M.Cs., sebagai dosen penguji pertama yang telah meluangkan waktu untuk memberikan masukan dan kritik konstruktif yang sangat berarti dalam ujian skripsi ini.
6. Ibu Kartika Sari, S.Kom., M.Cs., sebagai dosen penguji kedua yang telah memberikan masukan yang sangat berharga dan kritikan yang membangun selama ujian skripsi ini.
7. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., sebagai dosen Pembimbing Akademik (PA) yang telah dengan sabar memberikan masukan, bimbingan, dan motivasi yang membangun sepanjang masa perkuliahan.
8. Dosen dan Staf Prodi Rekayasa Sistem Komputer atas pengetahuan dan bantuan yang telah diberikan kepada penulis.

9. Comdev & Outreaching Universitas Tanjungpura yang telah mendanai seluruh kebutuhan kuliah serta menyediakan berbagai pelatihan dan kegiatan yang bermanfaat.
10. Rekan-rekan seperjuangan Angkatan Sistem Komputer 2020 (Sycomas), yang telah memberikan dukungan, semangat, dan kerja sama yang luar biasa selama perkuliahan dan pengerjaan tugas akhir ini.
11. Semua pihak yang memberikan kontribusi, baik secara langsung maupun tidak langsung, dalam penulisan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran konstruktif sangat diharapkan untuk perbaikan di masa depan. Semoga skripsi ini bermanfaat, baik bagi penulis maupun pembaca.

Pontianak, 24 Juli 2025

Rendy Pamungkas

DAFTAR ISI

LEMBAR PENGESAHAN ..... **Error! Bookmark not defined.**
PERNYATAAN INTEGRITAS AKADEMIK ..... **Error! Bookmark not defined.**
Abstrak iv
Abstract v
PRAKATA vi
DAFTAR ISI viii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR KODE PROGRAM xiii

BAB 1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan 5

BAB 2 LANDASAN TEORI 8
2.1 Perbandingan dengan Penelitian Terdahulu 8
2.2 Kriptografi 10
2.3 *Advanced Encryption Standard* (AES) 10
2.4 Medan Galois (*Galois Field*) 12
2.5 *American Standard Code for International Interchange* (ASCII) 13
2.6 NodeMCU ESP32 14
2.7 Sensor MQ-7 14
2.8 Sensor GP2Y1010AU0F 15
2.9 Sensor DHT-22 15
2.10 Indeks Standar Pencemaran Udara (ISPU) 16
2.11 Internet Of Things 16
2.12 Arduino IDE 17
2.13 *Hypertext Transfer Protocol* 17
2.14 HTTP Kode Respon 17

2.15 MySQL 18
2.16 Server 18
2.17 *Quality of Service* (QoS) 18

BAB 3 METODE PENELITIAN 20
3.1 Studi Literatur 21
3.2 Analisis Kebutuhan 21
3.2.1 Kebutuhan Perangkat Keras 21
3.2.2 Kebutuhan Perangkat Lunak 21
3.3 Perancangan Sistem 22
3.3.1 Rancangan Perangkat Keras 22
3.3.2 Rancangan Perangkat Lunak. 22
3.4 Implementasi 23
3.5 Pengujian 23
3.6 Kesimpulan dan Saran 23

BAB 4 PERANCANGAN 24
4.1 Deskripsi Sistem 24
4.2 Perancangan Arsitektur Sistem 25
4.3 Perancangan Perangkat Keras 26
4.3.1 Perancangan Sistem Pemantauan Kualitas Udara. 26
4.4 Perancangan Perangkat Lunak 28
4.4.1 *Flowchart* Proses Keseluruhan Sistem 28
4.4.2 Perancangan Perluasan Kunci (*Key Expansion*) 30
4.4.3 Perancangan Implementasi Algoritma AES pada Enkripsi Data Sensor. 30
4.4.4 Perancangan Implementasi Algoritma AES pada Dekripsi Data Sensor 32
4.5 Perancangan Basis Data 33
4.6 Perancangan Antarmuka 34
4.7 Perancangan Pengujian 35
4.7.1 Pengujian Waktu Enkripsi Data Sensor 35
4.7.2 Pengujian Waktu Dekripsi Data Sensor 36
4.7.3 Pengujian Pengaruh Algoritma AES Terhadap Waktu Transmisi Data Sensor 36
4.7.4 Pengujian Tingkat Keberhasilan Algoritma AES. 36

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 37
5.1 Implementasi Sistem 37
5.1.1 Implementasi Perangkat Keras 37
5.1.2 Implementasi Antarmuka 38
5.2 Implementasi Kode Program 38
5.2.1 Implementasi *Library* Arduino IDE 39
5.2.2 Konfigurasi Pin Sensor dan Pin NodeMCU ESP32 39
5.2.3 Implementasi Kode Program Konstanta Untuk Enkripsi 40
5.2.4 Implementasi Kode Program Inisiasi Sistem 41
5.2.5 Implementasi Kode Program Fungsi *Key Expansion* 42
5.2.6 Implementasi Kode Program Fungsi *AddRoundkey* 43
5.2.7 Implementasi Kode Program Fungsi *SubByte* 44
5.2.8 Implementasi Kode Program Fungsi *ShiftRows* 44
5.2.9 Implementasi Kode Program Fungsi *MixColumns* 45
5.2.10 Implementasi Kode Program Fungsi *InvShiftRows* 46
5.2.11 Implementasi Kode Program Fungsi *InvSubBytes* 47
5.2.12 Implementasi Kode Program Fungsi *InvMixColumns* 47
5.3 Perhitungan dengan Metode *Advanced Encryption Standard* (AES) 48
5.3.1 Proses Perluasan Kunci (*Key Expansion*) 48
5.3.2 Proses Enkripsi Data Sensor 52
5.3.3 Proses Dekripsi Data Sensor 55
5.4 Pengujian Sistem 60
5.4.1 Pengujian Waktu Enkripsi AES-128 pada Sistem Monitoring Kualitas Udara 60
5.4.2 Pengujian Waktu Dekripsi AES-128 Pada Dalam Sistem Monitoring Kualitas Udara 67
5.4.3 Pengujian Akurasi Enkripsi Dan Dekripsi AES-128 73
5.4.4 Pengujian Waktu Transmisi Data 75
5.5 Analisis dan Pembahasan 77

BAB 6 PENUTUP 79
6.1 Kesimpulan 79
6.2 Saran 79

DAFTAR PUSTAKA 80
LAMPIRAN 83

DAFTAR TABEL

Tabel 2.1 Perbandingan Dengan Penelitian Terdahulu 9
Tabel 2.2 Konversi Nilai Konsentrasi Parameter ISPU 16
Tabel 2.3 Kategori *Delay* 19
Tabel 4.1 Konfigurasi Pin MQ7 27
Tabel 4.2 Konfigurasi Pin DHT22 27
Tabel 4.3 Konfigurasi Pin GP2Y1010AU0F 27
Tabel 4.4 Rancangan Basis Data 33
Tabel 5.1 Waktu Eksekusi Enkripsi Data Suhu 60
Tabel 5.2 Waktu Eksekusi Enkripsi Kelembapan 62
Tabel 5.3 Waktu Eksekusi Enkripsi CO 64
Tabel 5.4 Waktu Eksekusi Enkripsi PM10 65
Tabel 5.5 Waktu Dekripsi Data Suhu 67
Tabel 5.6 Waktu Dekripsi Data Kelembapan 69
Tabel 5.7 Waktu Dekripsi Data CO 70
Tabel 5.8 Waktu Dekripsi Data PM10 72
Tabel 5.9 Pengujian Akurasi Algoritma 74
Tabel 5.10 Pengujian Waktu Transmisi Data 76

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Enkripsi Aes-128 11
Gambar 2.2 Ilustrasi Dekripsi Aes-128 12
Gambar 2.3 NodeMCU ESP32 14
Gambar 2.4 MQ-7 14
Gambar 2.5 Sensor GP2Y1010AU0F 15
Gambar 2.6 Sensor DHT22 15
Gambar 3.1 Diagram Alir Penelitian 20
Gambar 4.1 Sistem Secara Umum 24
Gambar 4.2 Perancangan Arsitektur Sistem 25
Gambar 4.3 Rancangan Perangkat Keras 26
Gambar 4.4 *Flowchart* Proses Keseluruhan Sistem 29
Gambar 4.5 *Flowcharts* Rancangan *Key Expansion* 30
Gambar 4.6 *Flowchart* Perancangan Proses Enkripsi 31
Gambar 4.7 *Flowchart* Perancangan Proses Dekripsi 32
Gambar 4.8 Rancangan Antarmuka *Website* 34
Gambar 4.9 Halaman Kedua Perancangan Antarmuka *Website* 35
Gambar 5.1 Implementasi Perangkat Keras 37
Gambar 5.2 Antarmuka *Website* 38
Gambar 5.3 Ilustrasi Pemecahan *Word* 49
Gambar 5.4 Ilustrasi *Expandedkeys* 49
Gambar 5.5 Ilustrasi Operasi *RotWord* 50
Gambar 5.6 Tabel S-Box 50
Gambar 5.7 Ilustrasi Operasi *SubWord* 50
Gambar 5.8 Nilai *Rcon* 51
Gambar 5.9 Perhitungan XOR 51
Gambar 5.10 Hasil Proses *Key Expansion* 52
Gambar 5.11 *State* Awal 53
Gambar 5.12 Proses *Initial Round* 53
Gambar 5.13 Hasil *SubBytes* 53
Gambar 5.14 Operasi *ShiftRows* 54
Gambar 5.15 Hasil Operasi *Mixcollumns* 55
Gambar 5.16 Proses *AddRoundKey* 55
Gambar 5.17 Ilustrasi Pemisahan *Ciphertext* dan Kunci 56
Gambar 5.18 Grafik Waktu Eksekusi Enkripsi Suhu 62
Gambar 5.19 Grafik Waktu Enkripsi Kelembapan 63
Gambar 5.20 Grafik Waktu Enkripsi CO 65
Gambar 5.21 Grafik Waktu Enkripsi PM10 66
Gambar 5.22 Grafik Waktu Enkripsi Keseluruhan 67
Gambar 5.23 Grafik waktu dekripsi data suhu 68
Gambar 5.24 Grafik Waktu Dekripsi Data Kelembapan 70
Gambar 5.25 Grafik Waktu Dekripsi Data CO 71
Gambar 5.26 Grafik Waktu Dekripsi Data PM10 73
Gambar 5.27 Grafik Total Waktu Dekripsi Data 73
Gambar 5.28 Grafik Perbandingan waktu transmisi data 77

DAFTAR KODE PROGRAM

Kode Program 5.1 Implementasi *Library* Arduino IDE 39
Kode Program 5.2 Konfigurasi Pin Sensor 40
Kode Program 5.3 Konstanta Enkripsi 40
Kode Program 5.4 Inisialisasi Sistem dan Menghubungkan ke Jaringan 41
Kode Program 5.5 Inisialisasi Sensor 42
Kode Program 5.6 Fungsi *Key Expansion* 43
Kode Program 5.7 Fungsi *AddRoundKey* 44
Kode Program 5.8 Fungsi *SubByte* 44
Kode Program 5.9 Fungsi *ShiftRows* 45
Kode Program 5.10 Fungsi Perkalian *Byte* dalam GF(2^8) 45
Kode Program 5.11 Fungsi *MixColumns* 46
Kode Program 5.12 Fungsi *InvShiftRows* 46
Kode Program 5.13 Fungsi *InvSubBytes* 47
Kode Program 5.14 Fungsi *InvMixColumns* 48

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Sebagai sumber daya alam yang sangat mempengaruhi kehidupan makhluk hidup di bumi, udara merupakan sesuatu yang penting untuk dijaga dan dipelihara. Salah satu faktor penting dalam hal kesehatan manusia dan lingkungan adalah kualitas udara. Kualitas udara memiliki peran penting, baik dalam kesehatan manusia maupun keberlanjutan lingkungan. Menurut *World Health Organization* (WHO, 2018), udara yang tercemar berpotensi menyebabkan berbagai gangguan kesehatan, seperti penyakit pernapasan, kanker, dan penyakit kardiovaskular. Oleh karena itu, pengembangan sistem monitoring kualitas udara mempunyai peran penting dalam dalam upaya memantau dan mengelola kualitas udara (Saini et al., 2020).

Untuk menentukan kualitas udara, sistem monitoring kualitas udara menggunakan sensor untuk mengumpulkan data dari lingkungan sekitar. Sensor-sensor tersebut mengukur berbagai parameter seperti PM10, karbon monoksida, suhu, kelembapan udara dan lain - lain (Prayoga et al., 2020). Data yang dikumpulkan oleh sensor kemudian dikirim ke server menggunakan NodeMCU yang terhubung ke jaringan *Wi-Fi* dan internet.

Dalam hal pengamanan data, sistem sensor kualitas udara menghadapi berbagai tantangan salah satu tantangan utama adalah manipulasi data. Data sensor yang tidak dilindungi dengan baik rentan terhadap manipulasi oleh pihak yang tidak bertanggung jawab. Perubahan data ini dapat mengakibatkan laporan yang tidak akurat tentang kondisi kualitas udara, yang berpotensi membahayakan kesehatan. Sebagai contoh, apabila data mengindikasikan kualitas udara yang lebih baik dari kenyataannya, individu dengan masalah pernapasan berpotensi tidak melakukan tindakan pencegahan yang diperlukan, seperti menghindari daerah yang tercemar atau menggunakan masker. Sebaliknya, apabila data menunjukkan kualitas udara yang lebih buruk, individu dapat mengalami kecemasan yang tidak perlu, yang berpotensi mengganggu aktivitas sehari-hari mereka. Untuk mencegah hal ini terjadi, penting untuk memastikan bahwa data yang dikumpulkan oleh sensor

terlindungi dengan baik. Salah satu metode yang telah banyak diterapkan dalam pengamanan data adalah algoritma kriptografi. Dalam penelitian ini, akan digunakan salah satu algoritma kriptografi yaitu *Advanced Encryption Standard* (AES) yang bisa digunakan untuk mengenkripsi data.

Implementasi algoritma AES ini perlu dianalisis secara menyeluruh, terutama dari segi waktu komputasi, pengaruhnya terhadap delay transmisi data, serta tingkat akurasi data yang diterima setelah proses enkripsi dan dekripsi dilakukan. Analisis ini perlu dilakukan karena sistem monitoring kualitas udara merupakan sistem berbasis teknologi real-time yang menuntut pengiriman data secara cepat dan akurat. Ketepatan waktu dan keandalan transmisi menjadi sangat krusial, terutama dalam kondisi di mana sistem digunakan pada wilayah yang luas dengan tingkat polusi udara yang tinggi, sehingga keterlambatan atau kesalahan dalam pengiriman data dapat berdampak pada efektivitas pengambilan keputusan atau tindakan yang diperlukan. Oleh karena itu, pemilihan dan evaluasi algoritma kriptografi seperti AES harus mempertimbangkan tidak hanya aspek keamanannya, tetapi juga performa teknisnya dalam konteks aplikasi real-time ini.

Berbagai penelitian sebelumnya telah mengkaji penerapan algoritma *Advanced Encryption Standard (AES)* pada berbagai sistem berbasis *Internet of Things (IoT)* dan *aplikasi web*, masing-masing dengan fokus dan hasil yang berbeda. Penelitian oleh (Rachmayanti & Wirawan, 2022) menerapkan algoritma AES-128 untuk menangani masalah *sniffing* pada perangkat IoT dalam bidang *smart healthcare*. AES dipilih karena efisiensi daya dan keamanannya, dengan hasil menunjukkan sistem tetap berfungsi baik meskipun waktu proses enkripsi dan dekripsi sedikit lebih lambat dibanding tanpa enkripsi. Di sisi lain, penelitian oleh (Wahyuni et al., 2023) menerapkan algorita AES dengan lebih menekankan pada keamanan jalur komunikasi antara perangkat IoT menggunakan protokol MQTT, dengan hasil menunjukkan tidak ada error dalam proses enkripsi maupun dekripsi, meskipun terdapat perbedaan waktu pengiriman data akibat perbedaan sumber daya perangkat. Sementara itu, (Linda et al., 2023) menerapkan AES-128 pada sistem keamanan database aplikasi kepelangganan berbasis web untuk menjaga kerahasiaan data pelanggan, dan hasilnya menunjukkan bahwa sistem berhasil mengamankan data dengan tingkat keberhasilan enkripsi sebesar 70,3%.

Ketiga penelitian ini menunjukkan bahwa algoritma AES dapat diimplementasikan pada berbagai jenis sistem untuk meningkatkan keamanan data. Namun hingga saat ini, belum ada penelitian yang secara spesifik menerapkan algoritma AES pada sistem monitoring kualitas udara berbasis *Internet of Things* (IoT), meskipun sistem ini sangat rentan terhadap potensi serangan manipulasi data. Hal ini disebabkan oleh kenyataan bahwa data sensor dikirimkan melalui saluran nirkabel tanpa lapisan keamanan yang memadai, sehingga membuka peluang bagi pihak yang tidak bertanggung jawab untuk melakukan manipulasi terhadap data yang dikumpulkan. Oleh karena itu, penelitian ini dilakukan untuk mengisi celah tersebut dengan mengimplementasikan algoritma AES guna melindungi data sensor dari manipulasi yang dapat memengaruhi akurasi pengambilan keputusan sistem.

Berdasarkan latar belakang dan penelitian terkait yang dibahas sebelumnya, maka akan dilakukan penelitian dengan judul "Implementasi Algoritma *Advanced Encryption Standard (AES)* Untuk Enkripsi Data Sensor pada Sistem Monitoring Kualitas Udara." Pada penelitian ini, algoritma *AES* akan diimplementasikan untuk mengamankan data sensor yang akan dikirimkan ke *server*. Data sensor tersebut diamankan dengan tujuan agar tidak mudah dimanipulasi sehingga tidak menyebabkan kesalahan sistem dalam mengambil keputusan. Sistem monitoring kualitas udara yang berbasis *Internet of Things (IoT)* cenderung rentan terhadap serangan, seperti penyadapan dan manipulasi data, mengingat data dikirimkan melalui jaringan nirkabel tanpa pengamanan yang memadai.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah yang didapat dalam penelitian ini adalah sebagai berikut.

1. Berapa waktu yang diperlukan algoritma AES dalam mengenkripsi dan mendekripsi data sensor pada sistem monitoring kualitas udara ?
2. Bagaimana pengaruh implementasi algoritma AES terhadap delay waktu transmisi data pada sistem monitoring kualitas udara menurut standar *TIPHON* ?
3. Bagaimana tingkat keberhasilan enkripsi dan dekripsi data pada pengujian algoritma AES-128?

1.3 Batasan Masalah

Batasan masalah dibuat agar maksud dan tujuan dari penelitian dapat terfokus sesuai dengan tujuan. Adapun Batasan masalah dalam penelitian ini antara lain sebagai berikut.

1. Penelitian ini berfokus pada penggunaan algoritma *Advanced Encryption Standard* dalam mengamankan data sensor pada sistem monitoring kualitas udara.
2. Penelitian ini terbatas pada pengukuran waktu yang diperlukan untuk proses enkripsi dan dekripsi data sensor menggunakan algoritma *Advanced Encryption Standard* pada sistem monitoring kualitas udara.
3. Penelitian akan membatasi evaluasi terhadap dampak implementasi algoritma *Advanced Encryption Standard* terhadap kecepatan transmisi data dari sensor ke server pada konteks sistem monitoring kualitas udara.
4. Penelitian tidak akan membahas aspek implementasi fisik dari sistem monitoring kualitas udara, fokusnya hanya pada penggunaan algoritma *Advanced Encryption Standard* dalam mengamankan data sensor.

1.4 Tujuan Penelitian

Berdasarkan permasalahan yang didapat, tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengatasi masalah-masalah yang terkait dengan keamanan dan integritas data dalam sistem monitoring kualitas udara. Tujuan ini mencakup beberapa aspek penting, yaitu:

1. Mengetahui waktu yang diperlukan oleh algoritma *Advanced Encryption Standard* untuk mengenkripsi dan mendekripsi data sensor pada sistem monitoring kualitas udara.
2. Mengetahui berapa delay waktu yang dihasilkan dari proses transmisi data dari sensor ke server setelah data tersebut diimplementasikan algoritma *Advanced Encryption Standard* dan sebelumnya pada sistem monitoring kualitas udara.
3. Mengetahui akurasi algoritma *Advanced Encryption Standard* untuk enkripsi data sensor pada sistem monitoring kualitas udara.

1.5 Manfaat Penelitian

Penelitian ini dapat meningkatkan keamanan data sensor pada sistem monitoring kualitas udara dengan mengimplementasikan algoritma AES, sehingga dapat mencegah manipulasi data. Selain itu, penelitian ini akan menilai efisiensi sistem dengan menganalisis waktu yang dibutuhkan untuk enkripsi dan dekripsi data, serta mengukur pengaruh penerapan algoritma AES terhadap kecepatan transmisi data dari sistem ke server. Hasil dari penelitian ini dapat menjadi panduan bagi pengembang dalam menyeimbangkan keamanan dan kinerja sistem monitoring kualitas udara berbasis IoT, serta menambah wawasan ilmiah di bidang keamanan data IoT. Secara keseluruhan, penelitian ini bertujuan untuk meningkatkan kepercayaan pengguna terhadap sistem monitoring kualitas udara dan mendorong adopsi teknologi yang lebih aman.

1.6 Sistematika Penulisan

Dalam penelitian ini, penulisan dibagi menjadi enam bab sehingga permasalahan yang dibahas dapat disesuaikan secara urut dan sistematis. Adapaun pembagian bab dalam penelitian ini adalah sebagai berikut.

BAB 1 PENDAHULUAN

Bab bagian pendahuluan adalah bab yang memberikan dasar dan juga gambaran awal mengenai penelitian yang akan dilakukan. Di dalam bab ini, akan dijelaskan berbagai hal yang menjadi landasan bagi penelitian, antara lain latar belakang yang menjelaskan tentang konteks serta alasan akan pentingnya penelitian ini. Terdapat juga perumusan masalah yang memerinci isu utama yang akan diteliti itu, di samping tujuan penelitian yang menjelaskan capaian yang ingin diraih melalui penelitian ini pula. Ruang lingkup penelitian dijelaskan secara spesifik dalam batasan masalah di bab ini juga agar tidak meluas ke topik yang tidak relevan. Manfaat dari penelitian ini akan diuraikan lebih lanjut dalam bab ini yang menunjukkan kontribusi yang diharapkan dari hasil penelitian ini bagi pihak terkait lainnya, praktisi, atau ilmu pengetahuan. Sistematika penulisan tersebut disajikan guna memberikan gambaran tentang struktur dari bab-bab yang akan dibahas dalam penelitian ini.

BAB 2 LANDASAN TEORI

Bab Landasan Teori ini membahas berbagai teori yang mendukung penelitian yang dilakukan. Teori yang dibahas adalah kriptografi, algoritma AES, *American Standard Code for Information Interchange* (ASCII), *NodeMCU ESP32*, Sensor MQ-7, Sensor GP2Y1010AU0F, Sensor DHT-22, IoT, Arduino IDE, *Hypertext Transfer Protocol* (HTTP), HTTP *Code Response*, MySQL, server, dan QoS.

BAB 3 METODOLOGI PENELITIAN

Bab metodologi penelitian ini berisi uraian mengenai rencana penelitian yang mencakup berbagai langkah yang akan diambil dalam proses penelitian. Langkah pertama adalah studi literatur, yang bertujuan untuk menggali informasi dan referensi yang relevan guna mendasari penelitian ini. Selanjutnya, bab ini akan menjelaskan metode penelitian yang digunakan untuk memperoleh data yang valid dan relevan. Analisis kebutuhan menjadi bagian penting berikutnya, yang mencakup penentuan kebutuhan perangkat keras dan perangkat lunak yang diperlukan untuk mendukung sistem yang akan dikembangkan. Setelah itu, dilakukan perancangan sistem untuk menggambarkan secara rinci bagaimana sistem yang akan dibangun akan bekerja. Terakhir, bab ini menguraikan proses implementasi sistem, yaitu tahap pelaksanaan dari perancangan yang telah dibuat, sehingga sistem dapat berfungsi sesuai dengan tujuan penelitian. Semua langkah ini diharapkan dapat memberikan gambaran yang jelas tentang bagaimana penelitian ini dilaksanakan secara sistematis dan terstruktur.

BAB 4 PERANCANGAN SISTEM

Bab perancangan sistem merupakan bagian penting dari penelitian yang menjelaskan secara rinci tentang rancangan sistem yang akan dibangun, mencakup aspek perangkat keras dan perangkat lunak. Bagian pertama yang dibahas adalah deskripsi sistem, yang memberikan gambaran umum mengenai sistem yang akan dikembangkan, termasuk tujuan dan fungsinya. Selanjutnya, perancangan arsitektur sistem menjelaskan struktur dan hubungan antar komponen dalam sistem, memastikan setiap bagian dapat berfungsi dengan baik dalam kerangka kerja yang telah ditentukan. Perancangan perangkat keras menjelaskan tentang perangkat fisik yang digunakan dalam sistem, seperti sensor dan mikrokontroler, sedangkan

perancangan perangkat lunak berfokus pada pengembangan aplikasi atau program yang mendukung sistem. Selain itu, bagian ini juga mencakup perancangan antarmuka website, yang meliputi desain tampilan dan interaksi pengguna dengan sistem melalui website. Terakhir, perancangan pengujian menjelaskan metode dan prosedur yang akan digunakan untuk menguji sistem yang telah dirancang, untuk memastikan bahwa sistem berfungsi sesuai dengan harapan dan dapat memenuhi kebutuhan yang telah ditetapkan.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian, dan pembahasan mencakup langkah-langkah yang diambil untuk mengimplementasikan, menguji, dan menganalisis sistem yang telah dirancang. Proses pertama adalah implementasi sistem, di mana sistem yang telah dirancang diterapkan ke dalam bentuk nyata, baik perangkat keras maupun perangkat lunaknya. Selanjutnya, penulisan kode program dilakukan untuk mengembangkan aplikasi atau sistem yang dapat menjalankan fungsi yang telah ditentukan dalam perancangan. Setelah sistem selesai diimplementasikan, dilakukan pengujian sistem untuk mengevaluasi apakah sistem berjalan sesuai dengan tujuan dan spesifikasi yang diharapkan. Pengujian ini dapat meliputi uji coba fungsionalitas, kecepatan, keamanan, dan lain-lain. Setelah pengujian selesai, hasil dari pengujian sistem akan dianalisis dan dibahas untuk mengevaluasi kinerja sistem secara keseluruhan. Bagian pembahasan ini juga akan mengidentifikasi kelebihan, kekurangan, serta potensi perbaikan dari sistem yang telah dibangun, memberikan pemahaman yang lebih mendalam mengenai efektivitas dan efisiensi sistem dalam memenuhi tujuan penelitian.

BAB 6 PENUTUP

Bab penutup memuat ringkasan hasil dari penelitian yang telah dilaksanakan, memberikan kesimpulan menyeluruh mengenai temuan dan pencapaian dari penelitian. Selain itu, bab ini juga menyajikan saran dan rekomendasi terhadap permasalahan yang masih belum terselesaikan. Saran ini bertujuan untuk memberikan panduan bagi penelitian selanjutnya agar dapat memperbaiki dan mengembangkan aspek-aspek yang masih memerlukan perhatian lebih. Dengan demikian, diharapkan penelitian di masa mendatang dapat melanjutkan upaya yang telah dilakukan dan mencapai hasil yang lebih optimal.