



**PENERAPAN *ADVANCED ENCRYPTION STANDARD* UNTUK
PENGIRIMAN DATA SUHU DAN KELEMBAPAN PADA FREKUENSI 2.4
GHz DALAM *MULTI-TRANSMITTER* SKENARIO**

Skripsi

**Untuk Memenuhi Persyaratan
Dalam Menyelesaikan Sarjana Strata-1 Ilmu Komputer**

**Oleh
MUHAMMAD IKHSAN AKBARI
NIM. 1611016210022**

**PROGRAM STUDI S1 ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU
JUNI 2023**



**PENERAPAN *ADVANCED ENCRYPTION STANDARD* UNTUK
PENGIRIMAN DATA SUHU DAN KELEMBAPAN PADA FREKUENSI 2.4
GHz DALAM *MULTI-TRANSMITTER* SKENARIO**

Skripsi

**Untuk Memenuhi Persyaratan
Dalam Menyelesaikan Sarjana Strata-1 Ilmu Komputer**

**Oleh
MUHAMMAD IKHSAN AKBARI
NIM. 1611016210022**

**PROGRAM STUDI S1 ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU
JUNI 2023**

SKRIPSI

PENERAPAN ADVANCED ENCRYPTION STANDARD UNTUK PENGIRIMAN DATA SUHU DAN KELEMBAPAN PADA FREKUENSI 2.4 GHZ DALAM MULTI-TRANSMITTER SKENARIO

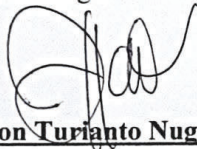
Oleh :

MUHAMMAD IKHSAN AKBARI

1611016210022

Telah dipertahankan di depan Dosen Penguji pada tanggal 23 Juni 2023,
Susunan Dosen Penguji :

Pembimbing I



**Dodon Turianto Nugrahadi, S.Kom.,
M.Eng**
NIP. 198001122009121002

Dosen Penguji I



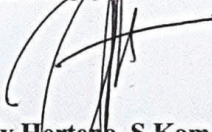
**Muhammad Itqan Mazdadi, S.Kom.,
M.Kom**
NIP. 199006122019031013

Pembimbing II



Friska Abadi, S.Kom, M.Kom
NIP. 19880913201612110001

Dosen Penguji II



Rudy Hertono, S.Kom., M.Kom
NIP. 198809252022031003



Banjarbaru, 23 Juni 2023

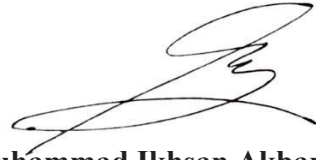
Koordinator Program Studi Ilmu Komputer

Irwan Budiman, S.T., M.Kom
NIP. 197703252008121001

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Banjarbaru, 23 Juni 2023



Muhammad Ikhsan Akbari

NIM. 1611016310007

ABSTRAK

PENERAPAN ADVANCED ENCRYPTION STANDARD UNTUK PENGIRIMAN DATA SUHU DAN KELEMBAPAN PADA FREKUENSI 2.4 GHz DALAM MULTI-TRANSMITER SKENARIO (Oleh : Muhammad Ikhsan Akbari; Pembimbing: Dodon Turianto Nugrahadi, S.Kom., M.Eng.dan Friska Abadi, S.Kom., M.Kom.; 2023; 64 halaman)

Dalam era digital yang semakin maju ini, keamanan data menjadi salah satu aspek yang sangat penting. Data yang dikirimkan pada jaringan WSN biasanya data dari sensor – sensor yang biasanya tidak diamankan dan dikirim secara langsung. Pada penelitian ini akan melakukan penerapan algoritma AES 128, 192 dan 256 bit untuk mengirimkan data suhu dan kelembapan menggunakan sensor DHT11 yang akan dikirimkan melalui jaringan nirkabel menggunakan modul nRF24L01 dengan membandingkan *multi-transmitter* dan *single-transmitter*. Perubahan waktu pengiriman pada topologi *single transmitter* pada transmitter 1 mengalami perubahan di algoritma AES 128 bit sebesar 189%, AES 192 bit sebesar 26% dan AES 256 bit sebesar 7%. Perubahan pada topologi *mutli transmitter* pada transmitter 1 mengalami perubahan di algoritma AES 128 bit sebesar 182%, AES 192 bit sebesar 24% dan AES 256 bit sebesar 5%, pada transmitter 2 mengalami perubahan di algoritma AES 128 bit sebesar 179%, AES 192 bit sebesar 23% dan AES 256 bit sebesar 6%. Sehingga semakin tinggi bit algoritma enkripsi AES, maka perubahan *delay* juga mengalami penurunan menjadi rendah. semakin rendah bit AES maka makin banyak perubahan *delay*-nya. Penggunaan algoritma AES 256 bit pada jaringan 2,4Ghz pada modul NRF24L01 pada Arduino Uno memiliki waktu *delay* yang lebih baik dari pada AES 128 bit dan 192 bit.

Kata kunci: Arduino UNO, *AES Encryption*, 2.4 GHz , *Multi-Transmitter*

ABSTRACT

APPLICATION OF ADVANCED ENCRYPTION STANDARD FOR TRANSMISSION OF TEMPERATURE AND HUMIDITY DATA AT 2.4 UGH_z IN MULTI-TRANSMITTER SCENARIOS (by : Muhammad Ikhsan Akbari; Pembimbing: Dodon Turianto Nugrahadi, S.Kom., M.Eng. and Friska Abadi, S.Kom., M.Kom.; 2023; 64 page)

In this increasingly advanced digital era, data security is one of the most important aspects. Data sent on WSN networks is usually data from sensors that are usually not secured and sent directly. In this study, we will apply the AES 128, 192 and 256 bit algorithms to transmit temperature and humidity data using the DHT11 sensor which will be sent via a wireless network using the nRF24L01 module by comparing multi-transmitter and single-transmitter. The change in transmission time in the single transmitter topology at transmitter 1 has changed in the 128 bit AES algorithm by 189%, 192 bit AES by 26% and 256 bit AES by 7%. Changes in the mutli transmitter topology at transmitter 1 experienced changes in the AES 128 bit algorithm by 182%, AES 192 bits by 24% and AES 256 bits by 5%, at transmitter 2 experienced changes in the AES 128 bit algorithm by 179%, AES 192 bits by 23% and AES 256 bits by 6%. So that the higher the bit of the AES encryption algorithm, the change in delay also decreases to low. the lower the AES bit, the more delay changes. The use of the 256 bit AES algorithm on a 2.4Ghz network on the NRF24L01 module on Arduino Uno has a better delay time than AES 128 bit and 192 bit.

Translated with www.DeepL.com/Translator (free version)

Keywords: Arduino UNO, AES Encryption, 2.4GHz, Multi-Transmitter

PRAKATA

Syukur kepada ALLAH SWT atas rahmat dan karunia-Nya sehingga penulis bisa menyelesaikan skripsi yang berjudul “Penerapan *Advanced Encryption Standard* Untuk Pengiriman Data Suhu Dan Kelembapan Pada Frekuensi 2.4 Ghz Dalam *Multi-Transmitter* Skenario”, guna memenuhi syarat untuk menyelesaikan Pendidikan Program Strata-1 di jurusan Ilmu Komputer pada Universitas Lambung Mangkurat. Tidak lupa penulis mengucapkan terima kasih kepada pihak-pihak terkait yang sudah membantu dalam penyelesaian skripsi ini, diantaranya:

1. Keluarga yang telah mendukung selama ini dan khususnya penulis menyampaikan terima kasih sebanyak-banyaknya kepada orang tua yang selalu memberikan doa, bantuan, semangat, dukungan baik rohani maupun materi dan selalu memotivasi untuk berjuang dalam proses penyelesaian skripsi ini.
2. Bapak Dodon Turianto Nugrahadhi S.Kom., M.Eng., selaku dosen pembimbing utama dan Bapak Friska Abadi S.Kom., M.Kom yang telah memberikan waktu dan bimbingannya kepada penulis dalam pengerjaan skripsi.
3. Bapak Muhammad Itqan Mazdadi S.Kom., M.Kom., dan Bapak Rudy Herteno S.Kom., M.Kom., selaku dosen penguji yang telah memberikan masukan-masukkan untuk penyajian skripsi ini
4. Bapak Irwan Budiman, S.T., M.Kom., selaku ketua program studi Ilmu Komputer beserta seluruh dosen dan karyawan/staff pegawai Fakultas MIPA Universitas Lambung Mangkurat atas bantuan yang diberikan selama penulis mengikuti studi.
5. Seluruh sahabat dan teman-teman penulis yang telah banyak memberikan bantuan, dorongan serta motivasi sehingga skripsi ini dapat terselesaikan.
6. Semua pihak yang tidak dapat disebutkan satu persatu yang telah turut membantu dalam penyelesaian skripsi ini.
7. Hairunnisa Fahnetta sebagai partner special saya, you are the best support system yang selalu mendengarkan keluh kesah saya, meluangkan waktunya, tenaga, mendukung ataupun menghibur dalam kesedihan, memberikan semangat dan doa.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, maka saran dan kritik dari semua pihak sangat diharapkan demi penyempurnaan selanjutnya. Akhirnya hanya kepada Tuhan yang maha esa kita kembalikan semua urusan dan oleh karena itu diharapkan skripsi ini dapat bermanfaat bagi semua pihak dan dapat menambah pengetahuan kita semua.

Banjarbaru, Juni 2023

A handwritten signature in black ink, featuring a large, stylized initial 'M' followed by a series of loops and a long horizontal stroke extending to the right.

Muhammad Ikhsan Akbari

DAFTAR ISI

HALAMAN JUDUL.....	i
PERNYATAAN.....	iii
ABSTRAK.....	iv
<i>ABSTRACT</i>	v
PRAKATA.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian.....	4
1.4 Manfaat Penelitian.....	4
1.5 Batasan Masalah.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Kajian Terdahulu.....	5
2.2 Keaslian Penelitian.....	6
2.3 Arduino Uno R3.....	10
2.4 Modul nRF24L01.....	12
2.5 Kriptografi.....	13
2.6 Enkripsi Dekripsi.....	15
2.7 Algoritma Enkripsi <i>Advanced Encryption Standard</i> (AES).....	16
2.8 AES Mode CBC.....	18
2.9 Komunikasi SPI.....	20
2.10 <i>Packet Loss</i>	21
2.11 <i>Non Line Of Sight</i>	23
BAB III METODE PENELITIAN.....	24
3.1 Alat Penelitian.....	24
3.2 Komponen Elektronik.....	24

3.3	Prosedur Kerja	25
BAB IV HASIL DAN PEMBAHASAN		28
4.1	Perancangan Alat dan Desain alat dan Sistem.....	28
4.1.1	Perancangan Perangkat keras	28
4.1.2	Skema Rangkaian Instrumen	30
4.1.3	Perancangan Alur Diagram program	31
4.1.4	Alur diagram instrumen sensor/sender	32
4.1.4	Alur diagram instrumen receiver	33
4.1.5	Alur diagram perekaman data.....	34
4.1.6	Skenario pengujian	34
4.1.6	Instrument sensor/sender	36
4.1.7	Instrumen penerima/ <i>receiver</i>	39
4.1.8	Program perekam data	42
4.2	Implementasi.....	43
4.3	Pengujian	44
4.3.1	Pengujian Algoritma AES 128 Bit	44
a.	AES 128 Bit jarak 10 meter.....	44
b.	AES 128 Bit jarak 20 meter.....	45
c.	AES 128 Bit jarak 30 meter.....	46
d.	AES 128 Bit jarak 40 meter.....	47
e.	AES 128 Bit jarak 50 meter.....	48
4.3.2	Pengujian Algoritma AES 192 Bit	49
a.	AES 192 Bit jarak 10 meter.....	49
b.	AES 192 Bit jarak 20 meter.....	50
c.	AES 192 Bit jarak 30 meter.....	51
d.	AES 192 Bit jarak 40 meter.....	52
e.	AES 192 Bit jarak 50 meter.....	53
4.3.3	Pengujian Algoritma AES 256 Bit	54
a.	AES 256 Bit jarak 10 meter.....	54
b.	AES 256 Bit jarak 20 meter.....	55
c.	AES 256 Bit jarak 30 meter.....	56

d. AES 256 Bit jarak 40 meter.....	57
e. AES 256 Bit jarak 50 meter.....	58
4.4 Pembahasan	59
4.4.1 Perbandingan Hasil	59
4.4.2 Analisa Perbedaan Hasil	62
BAB V PENUTUP.....	64
5.1 Kesimpulan.....	64
5.2 Saran	64
DAFTAR PUSTAKA	65
LAMPIRAN.....	67

DAFTAR TABEL

Tabel 1. Keaslian Penelitian	7
Tabel 2. Spesifikasi Arduino Uno R3	10
Tabel 3. Spesifikasi nRF24L01	13
Tabel 4. Standar persentase <i>Packet Loss</i>	22
Tabel 5. Komponen alat penelitian.....	24
Tabel 6. Skenario Pengujian.....	35
Tabel 7. Tabel Perbandingan Hasil Pengujian Jarak 10 Meter 128 Bit.....	44
Tabel 8. Tabel Perbandingan Hasil Pengujian Jarak 20 Meter 128 Bit.....	45
Tabel 9. Tabel Perbandingan Hasil Pengujian Jarak 30 Meter 128 Bit.....	46
Tabel 10. Tabel Perbandingan Hasil Pengujian Jarak 40 Meter 128 Bit.....	47
Tabel 11. Tabel Perbandingan Hasil Pengujian Jarak 50 Meter 128 Bit.....	48
Tabel 12. Tabel Perbandingan Hasil Pengujian Jarak 10 Meter 192 Bit.....	49
Tabel 13. Tabel Perbandingan Hasil Pengujian Jarak 20 Meter 192 Bit.....	50
Tabel 14. Tabel Perbandingan Hasil Pengujian Jarak 30 Meter 192 Bit.....	51
Tabel 15. Tabel Perbandingan Hasil Pengujian Jarak 40 Meter 192 Bit.....	52
Tabel 16. Tabel Perbandingan Hasil Pengujian Jarak 50 Meter 192 Bit.....	53
Tabel 17. Tabel Perbandingan Hasil Pengujian Jarak 10 Meter 256 Bit.....	54
Tabel 18. Tabel Perbandingan Hasil Pengujian Jarak 10 Meter 256 Bit.....	55
Tabel 19. Tabel Perbandingan Hasil Pengujian Jarak 30 Meter 256 Bit.....	56
Tabel 20. Tabel Perbandingan Hasil Pengujian Jarak 40 Meter 256 Bit.....	57
Tabel 21. Tabel Perbandingan Hasil Pengujian Jarak 50 Meter 256 Bit.....	58
Tabel 22. Perbandingan Hasil Peningkatan Jumlah Waktu Perjarak 128 Bit	59
Tabel 23. Perbandingan Hasil Peningkatan Jumlah Waktu Perjarak 192 Bit	60
Tabel 24. Perbandingan Hasil Peningkatan Jumlah Waktu Perjarak 256 Bit	61

DAFTAR GAMBAR

Gambar 1. Model Arduino Uno R3	12
Gambar 2. Skema Enkripsi dan Dekripsi Figure	14
Gambar 3. Skema Kriptografi Simetri.....	14
Gambar 4. Skema Kriptografi Assimetri	15
Gambar 5. Proses Enkripsi dan Dekripsi.....	15
Gambar 6. AES Enkripsi dan Dekripsi.....	18
Gambar 7. Alur Algoritma AES	18
Gambar 8. Enkripsi AES mode CBC	19
Gambar 9. Setup Hardware SPI.....	21
Gambar 10. Diagram Alur Penelitian	25
Gambar 11. Rancangan rangkaian pada Transmitter.....	29
Gambar 12. Rancangan rangkaian pada Receiver	30
Gambar 13. Rangkaian pada transmission/pengirim.....	30
Gambar 14. Rancangan pada receiver/penerima	31
Gambar 15. Alur diagram instrument transmitter/sender.....	32
Gambar 16. Alur diagram receiver/penerima	33
Gambar 17. Alur diagram perekaman data.....	34
Gambar 18. Rancangan skema jaringan multitransmitter	35
Gambar 19. Instrument transmitter.....	37
Gambar 20. Instrument penerima/ receiver.	40
Gambar 21. Perekaman data menggunakan Coolterm	43
Gambar 22. Hasil Grafik Pengujian Jarak 10 Meter 128 Bit.....	44
Gambar 23. Hasil Grafik Pengujian Jarak 20 Meter 128 Bit.....	45
Gambar 24. Hasil Grafik Pengujian Jarak 30 Meter 128 Bit.....	46
Gambar 25. Hasil Grafik Pengujian Jarak 40 Meter 128 Bit.....	47
Gambar 26. Hasil Grafik Pengujian Jarak 50 Meter 128 Bit.....	48
Gambar 27. Hasil Grafik Pengujian Jarak 10 Meter 192 Bit.....	49
Gambar 28. Hasil Grafik Pengujian Jarak 20 Meter 192 Bit.....	50
Gambar 29. Hasil Grafik Pengujian Jarak 30 Meter 192 Bit.....	51
Gambar 30. Hasil Grafik Pengujian Jarak 40 Meter 192 Bit.....	52

Gambar 31. Hasil Grafik Pengujian Jarak 50 Meter 192 Bit.....	53
Gambar 32. Hasil Grafik Pengujian Jarak 10 Meter 256 Bit.....	54
Gambar 33. Hasil Grafik Pengujian Jarak 20 Meter 256 Bit.....	55
Gambar 34. Hasil grafik Pengujian Jarak 30 Meter 256 Bit.	56
Gambar 35. Hasil Grafik Pengujian Jarak 40 Meter 256 Bit.....	57
Gambar 36. Hasil Grafik Pengujian Jarak 50 Meter 256 Bit.....	58
Gambar 37. Grafik Hasil Rata-Rata <i>Delay</i> Jarak dan Skenario 128 Bit.....	59
Gambar 38. Grafik Hasil Rata-Rata <i>Delay</i> Jarak dan Skenario 192 Bit.....	60
Gambar 39. Grafik Hasil Rata-Rata <i>Delay</i> Jarak dan Skenario 256 Bit.....	61