



**IMPLEMENTASI ALGORITMA ENKRIPSI AES-128 BIT PADA SISTEM
KUNCI RFID PINTU OTOMATIS DENGAN MONITORING JARAK
JAUH BERBASIS MQTT**

Skripsi

Untuk Memenuhi Persyaratan

Dalam Menyelesaikan Strata-1 Ilmu Komputer

Oleh

M. Apriannur

NIM 1711016310010

**PROGRAM STUDI S-1 ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU**

JUNI 2023

SKRIPSI

IMPLEMENTASI ALGORITMA ENKRIPSI AES-128 BIT PADA SISTEM KUNCI RFID PINTU OTOMATIS DENGAN MONITORING JARAK JAUH BERBASIS MQTT

Oleh :

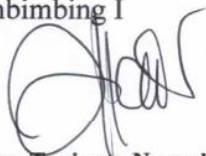
M. APRIANNUR

1711016310010

Telah dipertahankan di depan Dosen Penguji pada tanggal 27 Juni 2023

Susunan Dosen Penguji :

Pembimbing I



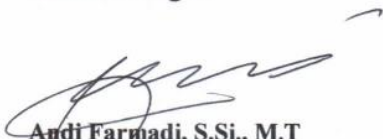
Dodon Turianto Nugrahadi, S.Kom., M.Eng
NIP. 198704212012122003

Dosen Penguji I



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

Pembimbing II



Andi Farmadi, S.Si., M.T
NIP. 197307252008011006

Dosen Penguji II



Fatma Indriani, S.T, M.I.T., Ph.D.
NIP. 198404202008122004



Banjarbaru, Juni 2023

Ketua Program Studi Ilmu Komputer

Iwan 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, Juni 2023

Yang Menyatakan,



M. Apriannur

NIM. 1711016310010

ABSTRAK

IMPLEMENTASI ALGORITMA ENKRIPSI AES-128 BIT PADA SISTEM KUNCI RFID PINTU OTOMATIS DENGAN MONITORING JARAK JAUH BERBASIS MQTT

(Oleh : M. Apriannur; Dodon Turianto Nugrahadi, S.Kom, M.Eng; Andi Farmadi, S.Si, M.T; 2023; 61 halaman)

Telah dilakukan penelitian implementasi algoritma enkripsi AES-128 bit pada sistem kunci RFID pintu otomatis dengan monitoring jarak jauh berbasis mqtt. Dalam penelitian ini pembacaan sensor rfid dilakukan menggunakan skenario dengan enkripsi dan tanpa enkripsi. Hardware yang digunakan pada penelitian yaitu mikrokontroler NodeMCU ESP8266, adaptor 5V, dan sensor MFRC522. Tujuan pada penelitian ini adalah untuk mengetahui pengaruh proses enkripsi AES 128-bit pada proses pembacaan data dari kartu RFID terhadap penggunaan RAM pada mikrokontroler NodeMCU, serta transfer data kartu RFID melalui protokol MQTT menggunakan jaringan wireless 802.11 terhadap delay dan throughput pada mikrokontroler NodeMCU. Berdasarkan hasil pengujian dan analisis yang telah dilakukan mendapatkan kesimpulan bahwa proses enkripsi dalam transfer data sensor RFID menggunakan protokol MQTT mempengaruhi penggunaan RAM pada mikrokontroler. Pada tipe router 802.11n, skenario dengan enkripsi diperoleh hasil sisa RAM rata – rata sebesar 58,84%. Sedangkan skenario tanpa enkripsi sebesar 72,58%. Pada tipe router 802.11ac, skenario dengan enkripsi diperoleh hasil sisa RAM rata – rata sebesar 58,84%. Sedangkan skenario tanpa enkripsi sebesar 72,77%. Penggunaan enkripsi tidak menunjukkan adanya pengaruh enkripsi terhadap delay. Pada tipe router 802.11n, Transfer data menggunakan enkripsi memiliki delay rata – rata sebesar 137,8 ms. Sedangkan transfer data tanpa enkripsi sebesar 128,1 ms. Pada tipe router 802.11ac, Transfer data menggunakan enkripsi memiliki delay rata – rata sebesar 145,7 ms. Sedangkan transfer data tanpa enkripsi sebesar 126,4 ms. Penggunaan enkripsi mempengaruhi throughput secara signifikan karena proses enkripsi menyebabkan ukuran data yang dikirim lebih besar tetapi delay tetap sehingga nilai throughputnya juga lebih besar.

Kata kunci : Aes-128 bit, NodeMCU ESP8266, RFID, mikrokontroler

ABSTRACT

IMPLEMENTATION OF AES-128 BIT ENCRYPTION ALGORITHM ON RFID DOOR LOCK SYSTEM WITH MQTT BASED REMOTE MONITORING

(By : M. Apriannur; Dodon Turianto Nugrahadi, S.Kom, M.Eng; Andi Farmadi, S.Si, M.T; 2023; 60 pages)

Research on the implementation of the AES-128 bit encryption algorithm on an automatic door RFID lock system with mqtt-based remote monitoring has been carried out. In this study, the reading of the RFID sensor was carried out using scenarios with encryption and without encryption. The hardware used in this research is the NodeMCU ESP8266 microcontroller, 5V adapter, and MFRC522 sensor. The purpose of this study was to determine the effect of the 128-bit AES encryption process on the process of reading data from the RFID card on RAM usage on the NodeMCU microcontroller, as well as transferring RFID card data via the MQTT protocol using the 802.11 wireless network on delay and throughput on the NodeMCU microcontroller. Based on the results of testing and analysis that has been done, it can be concluded that the encryption process in transferring RFID sensor data using the MQTT protocol affects the use of RAM on the microcontroller. In the 802.11n router type, the scenario with encryption results in an average RAM remaining of 58.84%. While the scenario without encryption is 72.58%. On the 802.11ac router type, the scenario with encryption results in an average RAM remaining of 58.84%. While the scenario without encryption is 72.77%. The use of encryption does not show the effect of encryption on delay. On the 802.11n router type, data transfer using encryption has an average delay of 137.8 ms. Meanwhile, data transfer without encryption is 128.1 ms. On the 802.11ac router type, data transfer using encryption has an average delay of 145.7 ms. Meanwhile, data transfer without encryption is 126.4 ms. The use of encryption significantly affects throughput because the encryption process causes a larger data size to be sent but the delay remains so that the throughput value is also greater.

Keyword : Aes-128 bit, NodeMCU ESP8266, RFID, mikrokontroler

PRAKATA

Puji syukur kepada Tuhan Yang Maha Esa sehingga penulis bisa menyelesaikan skripsi yang berjudul **IMPLEMENTASI ALGORITMA ENKRIPSI AES-128 BIT PADA SISTEM KUNCI RFID PINTU OTOMATIS DENGAN MONITORING JARAK JAUH BERBASIS MQTT**, guna memenuhi syarat untuk menyelesaikan Pendidikan Program Strata-1 Ilmu Komputer di Universitas Lambung Mangkurat.

Penulis mengucapkan syukur kepada Tuhan Yang Maha Esa, karena atas izin dan berkat-Nya penulis dapat menyelesaikan skripsi ini. Penulis juga menyampaikan terimakasih kepada berbagai pihak yang telah memberikan dukungan dan telah membantu dalam menyelesaikan penelitian ini, diantaranya:

1. Orang tua dan seluruh anggota keluarga yang selalu memberikan doa dan dukungan, baik moril dan material kepada penulis dalam menyelesaikan skripsi ini.
2. Bapak Dodon Turianto Nugrahadi, S.Kom, M.Eng selaku dosen pembimbing utama dan Bapak Andi Farmadi, S.Si, M.T selaku pembimbing pendamping yang telah banyak memberikan masukan dan bimbingannya kepada penulis.
3. Bapak Muhammad Itqan Mazdadi, S.Kom, M.Kom dan Ibu Fatma Indriani, S.T, M.I.T selaku dosen penguji yang telah memberikan saran serta kritikan membangun bagi penulis dalam membuat skripsi ini menjadi lebih baik.
4. Bapak Irwan Budiman, S.T, M.Kom selaku ketua program studi ilmu komputer beserta seluruh dosen dan staff Fakultas MIPA Universitas Lambung Mangkurat atas bantuan yang diberikan selama penulis mengikuti studi.
5. Seluruh teman-teman Angkatan 2017 Ilmu Komputer serta rekan-rekan mahasiswa Jaringan yang telah banyak memberikan dukungan serta

semangat kepada penulis yang telah banyak mendorong penulis dalam pengerjaan skripsi ini.

6. Kepada pacar saya Yensi Hariyanto Tue, S.Si yang telah banyak membantu dan memberikan support dalam menyelesaikan skripsi ini.

Penulis menyadari bahwa skripsi ini tidak dapat dikatakan sempurna. Oleh sebab itu, penulis mengharapkan kritik dan saran dari seluruh pihak untuk menjadikan penelitian ini menjadi lebih baik lagi ke depannya. Akhirnya, penulis hanya dapat berharap bahwa skripsi ini dapat memberikan manfaat kepada berbagai pihak dan diharapkan penelitian ini dapat memberikan dampak positif bagi kemajuan ilmu pengetahuan dan teknologi.

Banjarbaru, Juni 2023



M. Apriannur

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
ABSTRAK	iv
ABSTRACT	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.....	4
1.4. Batasan Masalah.....	4
1.5. Manfaat Penelitian.....	4
BAB II LANDASAN TEORI	5
2.1. Tinjauan Pustaka	5
2.2. Dasar Teori.....	12
2.2.1. Enkripsi <i>Advance Encryption Standard</i>	12
2.2.2. Protokol MQTT	14
2.2.3. Mosquitto	14
2.2.4. Mikrokontroler.....	15
2.2.5. Modul Wifi ESP8266.....	17
2.2.6. Sensor RFID MFRC-552	17
2.2.7. Fritzing.....	18

2.2.8.	SPSS.....	19
2.2.9.	Uji Hipotesis	19
BAB III METODE PENELITIAN		27
3.1.	Alur Penelitian.....	27
3.2.	Skenario Pengujian.....	29
3.3.	Alat dan Bahan Penelitian	30
BAB IV IMPLEMENTASI		31
4.1.	Perancangan Hardware.....	31
4.2.	Perancangan Software	32
4.3.	Alur Enkripsi dan Dekripsi	33
4.4.	Hasil dan Pembahasan Data Penggunaan RAM Dengan Router 802.11n ...	35
4.4.1.	Data Hasil Pengujian.....	35
4.4.2.	Uji Hipotesis	37
4.4.3.	Pembahasan.....	38
4.5.	Hasil dan Pembahasan Data Penggunaan RAM Dengan Router 802.11ac..	39
4.5.1.	Data Hasil Pengujian.....	39
4.5.2.	Uji Hipotesis	41
4.5.3.	Pembahasan.....	42
4.6.	Hasil dan Pembahasan Data Delay dengan Router 802.11n	43
4.6.1.	Data Hasil Pengujian.....	43
4.6.2.	Uji Hipotesis	45
4.6.3.	Pembahasan.....	46
4.7.	Hasil dan Pembahasan Data Delay dengan Router 802.11ac.....	47
4.7.1.	Data Hasil Pengujian.....	47
4.7.2.	Uji Hipotesis	49

4.7.3.	Pembahasan.....	50
4.8.	Hasil dan Pembahasan Data Throughput dengan Router 802.11n.....	51
4.8.1.	Data Hasil Pengujian.....	51
4.8.2.	Uji Hipotesis	53
4.8.3.	Pembahasan.....	54
4.9.	Hasil dan Pembahasan Data Throughput dengan Router 802.11ac	55
4.9.1.	Data Hasil Pengujian.....	55
4.9.2.	Uji Hipotesis	57
4.9.3.	Pembahasan.....	59
BAB V	PENUTUP	60
5.1.	Kesimpulan.....	60
5.2.	Saran.....	60
DAFTAR PUSTAKA		62
LAMPIRAN.....		66
RIWAYAT PENULIS		79

DAFTAR TABEL

Tabel 1. Keaslian Penelitian.....	7
Tabel 2. Penelitian Penulis.....	12
Tabel 3. Distribusi T	20
Tabel 4. Data Penggunaan RAM Dengan Router 802.11n.....	37
Tabel 5. Hasil Uji Hipotesis RAM 802.11n.....	37
Tabel 6. Data Penggunaan RAM Dengan Router 802.11ac	41
Tabel 7. Hasil Uji Hipotesis RAM 802.11ac	41
Tabel 8. Data Delay Dengan Router 802.11n.....	45
Tabel 9. Hasil Uji Hipotesis Delay 802.11n	45
Tabel 10. Data Delay Dengan Router 802.11ac.....	49
Tabel 11. Hasil Uji Hipotesis Delay 802.11ac.....	49
Tabel 12. Data Throughput Dengan Router 802.11n.....	53
Tabel 13. Hasil Uji Hipotesis Throughput 802.11n.....	53
Tabel 14. Data Throughput Dengan Router 802.11ac	57
Tabel 15. Hasil Uji Hipotesis Throughput 802.11ac	57

DAFTAR GAMBAR

Gambar 1. Skema Proses Enkripsi AES-128 Bit	13
Gambar 2. Alur Proses Mikrokontroler	16
Gambar 3. Modul Wifi ESP8266.....	17
Gambar 4. Alur Penelitian	27
Gambar 5. Rancangan Skenario Pengujian Router 802.11n.....	29
Gambar 6. Rancangan Skenario Pengujian Router 802.11ac	30
Gambar 7. Skematik Rancangan Sistem Sensor	31
Gambar 8. Diagram Alir Untuk Pengirim.....	32
Gambar 9. Diagram Alir Untuk Penerima	33
Gambar 10. Alur Enkripsi.....	34
Gambar 11. Alur Dekripsi.....	34
Gambar 12. Grafik Pengaruh Enkripsi Terhadap Penggunaan RAM Dengan Router 802.11n.....	38
Gambar 13. Grafik Pengaruh Enkripsi Terhadap Penggunaan RAM Dengan Router 802.11ac	42
Gambar 14. Grafik Pengaruh Enkripsi Terhadap Delay Dengan Router 802.11n.....	46
Gambar 15. Grafik Pengaruh Enkripsi Terhadap Delay Dengan Router 802.11ac	50
Gambar 16. Grafik Pengaruh Enkripsi Terhadap Throughput Dengan Router 802.11n	54
Gambar 17. Grafik Pengaruh Enkripsi Terhadap Throughput Dengan Router 802.11ac	59