IMPLEMENTASI PROTOKOL OTENTIKASI ECDSA P-256 DAN SHA-256 PADA ESP32-C3 UNTUK MENINGKATKAN KEAMANAN SMART DOOR LOCK BERBASIS NFC

ARYA RIDHO YUDISTIRA
H1051221054

SKRIPSI

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

IMPLEMENTASI PROTOKOL OTENTIKASI ECDSA P-256 DAN SHA-256 PADA ESP32-C3 UNTUK MENINGKATKAN KEAMANAN SMART DOOR LOCK BERBASIS NFC

ARYA RIDHO YUDISTIRA
H1051221054

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

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

LEMBAR PENGESAHAN

Judul Tugas Akhir	:	Implementasi Protokol Otentikasi ECDSA P-256 dan SHA-256 pada ESP32-C3 untuk Meningkatkan Keamanan *Smart Door Lock* Berbasis NFC
Nama Mahasiswa	:	Arya Ridho Yudistira
NIM	:	H1051221054
Jurusan/Program Studi	:	Rekayasa Sistem Komputer
Tanggal Lulus	:	20 Juli 2026
SK Pembimbing	:	No. 1016/DST/UN22.8/DT.00.09/2026 /10 Maret 2026
SK Penguji	:	No. 4254/DST/UN22.8/DT.00.09/2026 /15 Juli 2026

Dosen Pembimbing

Pembimbing I	Pembimbing II
Kasliono, S.Mat., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199306202022031005	NIP. 199007232023211017

Dosen Penguji

Ketua Penguji	Anggota Penguji
Ikhwan Ruslianto, S.Kom., M.Cs.	Dwi Marisa Midyanti, S.T., M.Cs.
NIP. 198607012014041001	NIP. 198003192015042001

Pemimpin Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Kasliono, S.Mat., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199306202022031005	NIP. 199007232023211017

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 : Arya Ridho Yudistira

NIM : H1051221054

Program Studi : 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 pernyataan dapat dipergunakan sebagaimana mestinya.

Pontianak, 13 Agustus 2026



Arya Ridho Yudistira

NIM. H1051221054

Implementasi Protokol Otentikasi ECDSA P-256 dan SHA-256 pada ESP32-C3 untuk Meningkatkan Keamanan Smart Door Lock Berbasis NFC

ABSTRAK

Sistem *smart door lock* berbasis *Near Field Communication* (NFC) yang hanya mengandalkan UUID sebagai identitas akses masih rentan terhadap *replay attack* dan *data tampering*. Penelitian ini bertujuan menganalisis pengaruh penerapan nonce, SHA-256, dan ECDSA P-256 terhadap waktu respons sistem serta kemampuannya menolak kedua serangan tersebut. Pada sistem utama, UUID disamarkan, digabungkan dengan nonce dari server, diproses menggunakan SHA-256, kemudian ditandatangani dengan ECDSA P-256. Pengujian waktu respons dilakukan pada empat kondisi dengan total 480 pengambilan data, yaitu sistem pembanding dan sistem utama pada akses diterima dan ditolak. Rata-rata waktu respons masing-masing sebesar 391,67 ms, 476,22 ms, 703,95 ms, dan 523,18 ms. Penerapan mekanisme keamanan meningkatkan rata-rata waktu respons sebesar 312,28 ms atau 79,73% pada akses diterima dan 46,96 ms atau 9,86% pada akses ditolak. Pengujian keamanan dilakukan sebanyak 30 percobaan untuk setiap kondisi serangan. Sistem pembanding menerima seluruh *replay attack* dan *data tampering*, sedangkan sistem utama menolak seluruh percobaan pada kedua skenario tersebut. Tingkat penolakan meningkat dari 0% menjadi 100%. Hasil penelitian menunjukkan bahwa mekanisme yang diterapkan meningkatkan kemampuan sistem dalam menolak serangan yang diuji dengan konsekuensi penambahan waktu respons pada jaringan lokal.

Kata Kunci: ECDSA P-256, SHA-256, nonce, waktu respons, otentikasi NFC.

Implementasi Protokol Otentikasi ECDSA P-256 dan SHA-256 pada ESP32-C3 untuk Meningkatkan Keamanan Smart Door Lock Berbasis NFC

ABSTRACT

Near Field Communication (NFC)-based smart door lock systems that rely solely on UUIDs as access identities remain vulnerable to replay attacks and data tampering. This study analyzes the effect of nonce*, SHA-256, and ECDSA P-256 on system response time and its ability to reject both attacks. In the proposed system, the UUID is pseudonymized, combined with a server-generated* nonce*, processed using SHA-256, and signed with ECDSA P-256. Response-time testing was conducted under four conditions with 480 data collections in total: baseline and proposed systems with accepted and rejected access. The average response times were 391.67 ms, 476.22 ms, 703.95 ms, and 523.18 ms, respectively. The security mechanisms increased the average response time by 312.28 ms or 79.73% for accepted access and 46.96 ms or 9.86% for rejected access. Security testing consisted of 30 trials for each attack condition. The baseline system accepted all replay attacks and data-tampering attempts, whereas the proposed system rejected all attempts in both scenarios. The rejection rate increased from 0% to 100%. These results show that the implemented mechanisms improve the system's ability to reject the tested attacks at the cost of additional response time under local network conditions.*

Keywords: *ECDSA P-256, SHA-256,* nonce*, response time*, *NFC authentication.*

PRAKATA

Alhamdulillah, segala puji syukur penulis ucapkan kehadirat Allah Subhanahu Wa Ta'ala serta nabi besar Muhammad Shallallahu'alaihi Wa Sallam karena atas rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi ini dengan judul "**Implementasi Protokol Otentikasi ECDSA P-256 dan SHA-256 pada ESP32-C3 untuk Meningkatkan Keamanan Smart Door Lock Berbasis NFC**".

Penyusunan skripsi ini bertujuan untuk memenuhi salah satu syarat untuk memperoleh gelar sarjana komputer pada Program Studi Rekayasa Sistem Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.

Penulis menyadari bahwa dalam penulisan laporan ini banyak mengalami kendala. Namun, dalam penyelesaian penulisan ini tidak terlepas dari bimbingan, pengarahan, saran, dan bantuan moril maupun material dari berbagai pihak. Untuk itu penulis mengucapkan terima kasih yang tak terhingga kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Ibu Rahmi Hidayati, S.Kom., M.Cs., selaku Ketua Jurusan/Program Studi Rekayasa Sistem Komputer sekaligus Dosen Pembimbing Akademik yang telah memberikan arahan dan bimbingan tentang perkuliahan.
3. Bapak Kasliono, S.Mat., M.Cs., selaku Dosen Pembimbing Utama yang telah memberikan petunjuk, bimbingan, dan pengarahan dalam penyusunan skripsi ini.
4. Bapak Hafiz Muhardi, S.T., M.Kom., selaku Dosen Pembimbing Pendamping yang telah memberikan petunjuk, bimbingan, dan pengarahan dalam penyusunan skripsi ini.
5. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., selaku Dosen Penguji Pertama yang telah memberikan saran dan masukan dalam penulisan skripsi ini.
6. Ibu Dwi Marisa Midyanti, S.T., M.Cs., selaku Dosen Penguji Kedua yang telah memberikan saran dan masukan dalam penulisan skripsi ini.

7. Bapak dan Ibu Dosen serta Staf Administrasi Jurusan/Program Studi Rekayasa Sistem Komputer.
8. Kedua orang tua tercinta, keempat adikku, kakek dan nenek, serta seluruh keluarga yang tak bisa saya sebutkan satu per satu yang senantiasa telah mendoakan saya, serta dukungan moril maupun materil yang tak terhingga selama masa perkuliahan hingga penyelesaian skripsi ini.
9. Kepada sahabat saya, Zaidan (Slicky/Salone), atas segala bantuan, semangat, dan kebersamaannya selama ini.
10. Kepada teman-teman Balqies dan Firda yang selalu menemani bermain game dan juga telah memberikan dorongan untuk menyelesaikan skripsi ini.
11. Kepada teman-teman terbaik Mabar The Ghost (Abang Husnal Ismail, Ahnaf Fikriyansyah, Alvin Nataniel dan Fajar Muttaqien Aska) yang tidak pernah lelah menemani dan memberi dukungan serta membantu dalam pengambilan data maupun memberi masukan terkait penyusunan skripsi ini.
12. Teman-teman seperjuangan mahasiswa Jurusan/Program Studi Rekayasa Sistem Komputer angkatan 2022 (Cytigon) yang tidak bisa disebut satu per satu.
13. Pihak-pihak yang tidak dapat disebutkan satu per satu yang turut membantu dalam penyusunan skripsi ini.

Penulis menyadari bahwa penyusunan skripsi ini masih memiliki kekurangan dan jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang bersifat membangun akan penulis terima dengan senang hati. Semoga skripsi ini bermanfaat bagi penulis maupun pembaca.

Pontianak, 20 Juli 2026



Arya Ridho Yudistira
H1051221054

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
ABSTRAK iv
ABSTRACT v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR KODE PROGRAM xiii
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 6
1.5 Manfaat Penelitian 6
1.6 Sistematika Penulisan 7
BAB 2 LANDASAN TEORI 9
2.1 Perbandingan dengan Penelitian Terdahulu 9
2.2 *Near Field Communication* (NFC) 10
2.3 Algoritma SHA-256 11
2.4 *Elliptic Curve Digital Signature Algorithm* (ECDSA) 15
2.5 Mekanisme *Challenge-Response* dan *Replay attack* 18
2.6 *Response Time* 19
2.7 *Data Tampering* dan Validasi Integritas Data 19
2.7.1 Persentase Penolakan Request Serangan 20
2.8 ESP32-C3 21
2.9 Modul NFC Reader MFRC522 22
2.10 Arduino IDE 23
2.11 Pustaka Pendukung Sistem 23
2.12 Solenoid Door Lock 24

2.13 Relay 25
2.14 MySQL 25
2.15 *Flowchart* 25
BAB 3 METODE PENELITIAN 27
3.1 Studi Literatur 27
3.2 Analisis Kebutuhan 28
3.2.1 Kebutuhan Perangkat Keras 28
3.2.2 Kebutuhan Perangkat Lunak 29
3.3 Perancangan Sistem 29
3.3.1 Perancangan Perangkat Keras 29
3.3.2 Rancangan Perangkat Lunak 30
3.4 Implementasi 30
3.5 Pengujian 31
3.6 Data Hasil Pengujian 32
3.7 Kesimpulan dan Saran 33
BAB 4 PERANCANGAN 34
4.1 Deskripsi Sistem 34
4.2 Perancangan Arsitektur Sistem 35
4.3 Perancangan Perangkat Keras 37
4.3.1 Perancangan Perangkat Klien *Smart Door Lock* 37
4.3.2 Perancangan Rangkaian Kendali Aktuator 39
4.4 Perancangan Perangkat Lunak 41
4.4.1 Perancangan Program Klien ESP32-C3 42
4.4.2 Perancangan Proses *Hashing* dan *Digital Signature* ECDSA P-25643
4.4.3 Perancangan Pencatatan Log dan *Response Time* 46
4.5 Perancangan Komunikasi Klien-Server 47
4.5.1 Perancangan Protokol Otentikasi dan Verifikasi Server Berbasis SHA-256 dan ECDSA P-256 49
4.6 Perancangan Sistem Pembanding Tanpa Mekanisme Keamanan Kriptografi 51
4.7 Perancangan Basis Data 52
4.8 Perancangan Antarmuka 54
4.9 Perancangan Pengujian Keseluruhan Sistem 55

4.9.1 Perancangan Pengujian Response Time 56
4.9.2 Perancangan Pengujian *Replay Attack* dan *Data Tampering* 60
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN.....66
5.1 Implementasi Perangkat Keras 66
5.1.1 Implementasi Perangkat Klien *Smart Door Lock* 66
5.1.2 Implementasi Rangkaian Kendali Aktuator.....67
5.2 Implementasi Perangkat Lunak.....69
5.2.1 Implementasi SHA-256 pada ESP32-C3 69
5.2.2 Implementasi Program Klien ESP32-C3 76
5.2.3 Implementasi dan Proses *Digital Signature* ECDSA P-256.....77
5.2.4 Implementasi Protokol Otentikasi dan Verifikasi Server Berbasis SHA-256 dan ECDSA P-256 83
5.2.5 Implementasi Komunikasi Klien-Server 88
5.2.6 Implementasi Pencatatan Log dan *Response Time* 90
5.3 Perhitungan Fungsi SHA-256 92
5.4 Implementasi Antarmuka.....101
5.5 Pengujian Keseluruhan Sistem 102
5.5.1 Pengujian *Response Time* 103
5.5.2 Pengujian *Replay Attack* 105
5.5.3 Pengujian *Data Tampering* 108
5.6 Pembahasan.....112
BAB 6 PENUTUP.....116
6.1 Kesimpulan 116
6.2 Saran 117
DAFTAR PUSTAKA 118
LAMPIRAN 123

DAFTAR GAMBAR

Gambar 2.1 *Key Chain* NFC/RFID 13.56 MHz.....11
Gambar 2.2 ESP32-C3.....22
Gambar 2.3 MFRC-522 RFID Module.....22
Gambar 2.4 Arduino IDE 1.8.19.....23
Gambar 2.5 *Solenoid Door Lock*.....24
Gambar 3.1 Diagram *Flowchart* Penelitian.....27
Gambar 4.1 Arsitektur dan Alur Sistem *Smart Door Lock* Berbasis NFC.....36
Gambar 4.2 Rangkaian ESP32-C3 dengan Modul MFRC522 dan *Buzzer*.....38
Gambar 4.3 Rangkaian Kendali Aktuator Relay dan *Solenoid Door Lock*.....40
Gambar 4.4 *Flowchart* Program Klien ESP32-C3.....42
Gambar 4.5 *Flowchart* Proses *Hashing* dan *Digital Signature* Menggunakan ECDSA P-256.....43
Gambar 4.6 Komunikasi Klien-Server *Smart Door Lock* Berbasis NFC.....48
Gambar 4.7 *Flowchart* Protokol Otentikasi dan Verifikasi Server.....49
Gambar 4.8 Rancangan Antarmuka *Web Admin*.....54
Gambar 4.9 *Flowchart* Pengujian *Replay Attack* pada Sistem Utama.....62
Gambar 4.10 *Flowchart* Pengujian *Data Tampering* pada Sistem Utama.....63
Gambar 5.1 Perangkat Klien *Smart Door Lock*.....67
Gambar 5.2 Perangkat Rangkaian Kendali Aktuator.....68
Gambar 5.3 Tampilan Hasil Ekspor Data Log dan *Response Time*.....92
Gambar 5.4 Proses *Padding*.....94
Gambar 5.5 Tampilan *Dashboard Web Admin Smart Door Lock*.....101

DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu.....9
Tabel 2.2 Simbol *Flowchart* 26
Tabel 4.1 Penggunaan Pin ESP32-C3 pada Modul MFRC522.....38
Tabel 4.2 Penggunaan Pin ESP32-C3 dengan Buzzer.....39
Tabel 4.3 Penggunaan Pin ESP32-C3 pada Rangkaian Aktuator.....41
Tabel 4.4 Struktur Tabel users 53
Tabel 4.5 Struktur Tabel access_logs.....53
Tabel 4.6 Skenario Pengujian Keseluruhan Sistem 56
Tabel 4.7 Skenario Perbandingan Sistem Pembanding dan Sistem Utama 57
Tabel 4.8 Parameter Pengujian *Response Time* 58
Tabel 4.9 Skenario Pengujian Response Time pada Sistem Utama.....59
Tabel 4.10 Skenario Pengujian *Replay Attack* dan *Data Tampering*.....64
Tabel 5.1 Data Identitas Kartu Berdasarkan Log Sistem.....102
Tabel 5.2 Ringkasan Hasil Pengujian Keseluruhan Sistem 102
Tabel 5.3 Statistik Total *Response Time* Sistem.....103
Tabel 5.4 Ringkasan Parameter Pendukung *Response Time* 104
Tabel 5.5 Ringkasan Hasil Pengujian *Replay Attack*.....105
Tabel 5.6 Data Log Pengujian *Replay Attack* pada Sistem Utama 106
Tabel 5.7 Ringkasan Hasil Pengujian *Data Tampering*.....109
Tabel 5.8 Data Log Pengujian *Data Tampering* pada Sistem Utama.....109

DAFTAR KODE PROGRAM

Kode Program 5.1 Membaca UUID Melalui Modul MFRC522 70
Kode Program 5.2 Memanggil Fungsi SHA-256.....70
Kode Program 5.3 Fungsi sha256Hash() 70
Kode Program 5.4 Proses *Padding* SHA-256.....71
Kode Program 5.5 Pembentukan $W0$ sampai $W15$.....71
Kode Program 5.6 Ekspansi 16 kata menjadi 64 kata.....72
Kode Program 5.7 Fungsi $\sigma 0$.....72
Kode Program 5.8 Fungsi $\sigma 1$.....72
Kode Program 5.9 Potongan Kode Nilai Variabel.....73
Kode Program 5.10 Konstanta SHA-256.....73
Kode Program 5.11 Fungsi Kompresi.....74
Kode Program 5.12 Fungsi choose().....74
Kode Program 5.13 Fungsi majority() 75
Kode Program 5.14 Fungsi $\sum 0$ 75
Kode Program 5.15 Fungsi $\sum 1$ 75
Kode Program 5.16 Pembentukan *Output* Akhir SHA-256.....75
Kode Program 5.17 Potongan Kode Konversi Menjadi String Heksadesimal 76
Kode Program 5.18 Proses Utama Klien ESP32-C3 77
Kode Program 5.19 Payload String.....78
Kode Program 5.20 Fungsi Pembentukan *Message Digest Payload*.....78
Kode Program 5.21 Fungsi Pembangkit Kunci Privat dan Kunci Publik.....79
Kode Program 5.22 Inisialisasi ECDSA P-256.....80
Kode Program 5.23 Input Parameter mbedTLS ECDSA.....80
Kode Program 5.24 Fungsi Ubah Format ke Heksadesimal 81
Kode Program 5.25 Verifikasi Tanda Tangan pada Server (Python) 82
Kode Program 5.26 Implementasi Protokol Otentikasi dan Verifikasi Server 84
Kode Program 5.27 Proses Pencocokan Data Pengguna 86
Kode Program 5.28 Pembentukan Respons Server.....86
Kode Program 5.29 Konfigurasi *Endpoint*.....88
Kode Program 5.30 Pengiriman Data Otentikasi dari ESP32-C3 ke Server.....88

Kode Program 5.31 *Endpoint* /get_nonce 89
Kode Program 5.32 Fungsi Pencatatan Log.....90
Kode Program 5.33 *Endpoint* /update_total.....91

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi *Internet of Things* (IoT) telah mengubah sistem keamanan dan kontrol akses, termasuk pada sistem *smart door lock*. Sistem kunci mekanis tradisional mulai digantikan oleh sistem berbasis mikrokontroler, sensor, jaringan nirkabel dan server untuk melakukan proses verifikasi akses. Di antara berbagai platform perangkat IoT, ESP8266 dan ESP32 telah mendapatkan popularitas yang signifikan karena menawarkan harga terjangkau, konektivitas yang kuat, dan ekosistem yang komprehensif untuk mendukung inovasi teknologi (Williams dkk., 2022). Meskipun memberikan kemudahan dalam proses kontrol akses, sistem *smart door lock* berbasis jaringan masih memiliki tantangan keamanan khususnya pada aspek otentikasi dan integritas data (Sabonchi & Obaid, 2023).

Permasalahan utama pada sistem akses berbasis NFC/RFID terletak pada penggunaan *Universally Unique Identifier* (UUID) sebagai identitas akses. Apabila UUID dikirimkan atau digunakan secara langsung tanpa mekanisme pengamanan tambahan, maka data tersebut berisiko disalahgunakan saat melalui jalur komunikasi. Penyerang dapat mencoba melakukan penyadapan, penggunaan ulang data akses yang pernah valid (*replay attack*), maupun manipulasi data pada saat proses komunikasi berlangsung (Alrawais, 2020). Kerentanan ini menunjukkan bahwa sistem *smart door lock* tidak cukup hanya mengandalkan pencocokan identitas kartu, tetapi juga membutuhkan mekanisme otentikasi yang mampu memastikan bahwa data akses benar-benar berasal dari perangkat yang sah dan tidak mengalami perubahan selama proses transmisi (Khan dkk., 2023). Oleh karena itu, salah satu metode yang dapat digunakan adalah *Elliptic Curve Digital Signature Algorithm* (ECDSA), yang mampu memberikan tingkat keamanan setara RSA dengan ukuran kunci yang jauh lebih kecil sehingga mendukung komputasi yang lebih efisien untuk aplikasi *real-time* (Parmar dkk., 2023).

Untuk memperkuat keamanan, SHA-256 digunakan sebagai fungsi *hash* satu arah untuk membentuk identitas tersamar dari UUID kartu NFC menjadi id_samaran serta menghasilkan *message digest* dari *payload* otentikasi. SHA-256 menghasilkan nilai *hash* sepanjang 256 bit dan bersifat sensitif terhadap perubahan *input*, sehingga dapat digunakan untuk membantu mendeteksi perubahan data pada proses komunikasi (Krisna Priastawan dkk., 2025). Namun, penerapan mekanisme kriptografi pada perangkat IoT tetap perlu memperhatikan aspek waktu komputasi dan responsivitas sistem karena proses keamanan tambahan dapat memengaruhi waktu respons proses otentikasi. Oleh karena itu, pengujian *response time* digunakan untuk mengukur performa proses pembentukan *id_samaran*, pembuatan *message digest*, *digital signature*, dan verifikasi akses pada sistem *smart door lock* (Jin, 2022).

Penelitian sebelumnya yang berjudul "*A Systematic Literature Review on Authentication and Threat Challenges on RFID Based NFC Applications*" (El Gaabouri dkk., 2023). Penelitian tersebut menjelaskan bahwa aplikasi NFC/RFID masih menghadapi berbagai ancaman keamanan, seperti penyadapan, pelacakan *tag*, pemalsuan identitas, *cloning tag*, perubahan data, dan gangguan komunikasi. Selain itu, penelitian tersebut juga menunjukkan bahwa pendekatan berbasis kriptografi, seperti *Elliptic Curve Cryptography* (ECC) dan mekanisme *challenge-response*, dapat digunakan sebagai alternatif pengamanan pada sistem NFC/RFID yang memiliki keterbatasan sumber daya. Hal ini menunjukkan bahwa sistem akses berbasis NFC/RFID membutuhkan mekanisme otentikasi yang lebih kuat, khususnya apabila digunakan pada sistem kontrol akses fisik seperti *smart door lock*. Dalam penelitian pada kontrol fisik dengan kasus serupa yang berjudul "Perancangan Sistem Absensi Otomatis Mahasiswa Berbasis RFID Terintegrasi Google Spreadsheet dan *Smart Door Lock*" (Pardani & Yulianti, 2026). Penelitian ini merancang sistem absensi otomatis berbasis RFID yang terintegrasi dengan Google Spreadsheet dan *smart door lock* menggunakan mikrokontroler ESP32. Sistem tersebut menerapkan proses verifikasi akses berbasis *whitelist* melalui Google *Spreadsheet* serta melakukan pengujian terhadap *success rate*, *False Accept Rate* (FAR), *False Rejection Rate* (FRR), dan *Response Time*. Hasil penelitian menunjukkan bahwa sistem berhasil melakukan pembacaan UUID dan pencatatan

data dengan tingkat keberhasilan 100% serta FAR sebesar 0%. Namun, *Response Time* sistem dilaporkan berada pada rentang 7–10 detik akibat latensi komunikasi *cloud*. Hal ini menunjukkan bahwa sistem *smart door lock* tidak hanya membutuhkan mekanisme keamanan akses, tetapi juga perlu mempertimbangkan waktu respons agar proses otentikasi tetap sesuai untuk kebutuhan akses pintu secara *real-time*.

Dari sisi metode keamanan, penelitian yang berjudul "*Enhancing Security Using ECDSA-Based Hardware Security Module with DS28E38 Secure Data Authentication IC*" (Istiyanto dkk., 2025). Penelitian ini menerapkan ECDSA dan SHA-256 pada sistem berbasis *hardware security module* DS28E38 untuk mendukung otentikasi perangkat dan validasi integritas data. Penelitian tersebut menunjukkan bahwa ECDSA dapat digunakan untuk menghasilkan *digital signature*, sedangkan SHA-256 digunakan untuk membentuk *message digest* dari data yang akan divalidasi. Konsep keamanan tersebut berkaitan dengan kebutuhan sistem *smart door lock* karena *digital signature* dapat digunakan untuk membuktikan keaslian pengirim data, sedangkan SHA-256 digunakan untuk membentuk *message digest* dari data yang akan diverifikasi. Dengan demikian, perubahan data selama proses komunikasi dapat dideteksi melalui proses verifikasi *digital signature* terhadap *message digest* tersebut.

Penelitian lain yang berjudul "Keamanan Transmisi Data Pada Sistem Iot Melalui Metode *Checksum* SHA-256, AES-128 Untuk Pencegahan *Data Tampering*" (Krisna Priastawan dkk., 2025). Penelitian tersebut menerapkan *checksum* SHA-256, *salt*, dan AES-128 untuk mendeteksi serta mencegah manipulasi data pada sisi *subscriber*. Proses validasi dilakukan dengan membandingkan nilai *checksum* SHA-256 yang diterima dengan nilai *checksum* hasil perhitungan ulang di sisi *subscriber*. Apabila nilai *checksum* berbeda, data dianggap telah mengalami manipulasi dan proses dekripsi dihentikan. Penelitian tersebut menunjukkan bahwa mekanisme *hash* dapat digunakan untuk mendeteksi perubahan data selama transmisi. Namun, penerapan metode keamanan seperti SHA-256 dan AES-128 pada perangkat IoT juga dapat menambah beban komputasi pada mikrokontroler dengan sumber daya terbatas. Oleh karena itu, implementasi

keamanan pada sistem IoT perlu mempertimbangkan aspek integritas data dan efisiensi waktu komputasi agar sistem tetap responsif.

Berdasarkan permasalahan dan penelitian terdahulu tersebut, penelitian ini melakukan implementasi protokol otentikasi pada *smart door lock* berbasis NFC dengan menggabungkan mekanisme *challenge-response* menggunakan nonce, fungsi *hash* SHA-256 dan *digital signature* ECDSA P-256 pada ESP32-C3. Penelitian ini difokuskan pada pengujian performa *response time* sistem serta pengujian kemampuan protokol dalam menolak *replay attack* dan *data tampering* pada jalur komunikasi lokal antara ESP32-C3 dan server berdasarkan skenario pengujian yang dilakukan. Oleh karena itu, penulis tertarik untuk melakukan penelitian dengan judul "IMPLEMENTASI PROTOKOL OTENTIKASI ECDSA P-256 DAN SHA-256 PADA ESP32-C3 UNTUK MENINGKATKAN KEAMANAN SMART DOOR LOCK BERBASIS NFC".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka didapatlah rumusan permasalahan sebagai berikut:

1. Bagaimana performa *total response time* sistem *smart door lock* berbasis ESP32-C3 pada proses otentikasi, mulai dari pembentukan id_samaran menggunakan SHA-256, permintaan nonce, pembuatan *digital signature* ECDSA P-256, hingga keputusan akses diterima atau ditolak?
2. Bagaimana kemampuan protokol otentikasi berbasis nonce, SHA-256, dan ECDSA P-256 dalam menolak *replay attack* dan *data tampering* pada komunikasi antara ESP32-C3 dan server berdasarkan skenario pengujian yang dilakukan?

1.3 Batasan Masalah

Dalam penelitian ini diterapkan ruang lingkup batasan-batasan sebagai berikut:

1. Perangkat keras utama yang digunakan meliputi mikrokontroler ESP32-C3, modul NFC MFRC522, dan *Solenoid Door Lock* sebagai simulasi aktuator kunci pintu.

2. Algoritma kriptografi dibatasi pada penggunaan SHA-256 untuk pembentukan id_samaran dan *message digest payload*, serta ECDSA P-256 untuk proses *digital signature* dan verifikasi. Pada sisi ESP32-C3, fungsi SHA-256 diimplementasikan secara manual di dalam *firmware* untuk membentuk id_samaran dan *message digest payload*, sedangkan proses *digital signature* ECDSA P-256 dijalankan menggunakan *library* mbedTLS. Pada sisi server Flask proses SHA-256 dijalankan menggunakan hashlib Python, sedangkan proses verifikasi *digital signature* dan penandatanganan untuk respons dijalankan menggunakan *library* ECDSA pada Python.
3. Protokol keamanan komunikasi menggunakan mekanisme *challenge-response* berbasis nonce untuk mendukung sesi otentikasi, serta SHA-256 dan ECDSA P-256 untuk membentuk dan memverifikasi *digital signature*. Pengujian keamanan dibatasi pada kemampuan sistem dalam menolak *replay attack* dan *data tampering* berdasarkan skenario pengujian yang dilakukan.
4. Komunikasi sistem dilakukan secara khusus melalui jaringan Wi-Fi lokal antara mikrokontroler ESP32-C3 dan server Flask yang terhubung dengan basis data MySQL.
5. Sistem menggunakan adaptor 5V untuk menyuplai ESP32-C3, sedangkan *solenoid door lock* menggunakan adaptor DC 12V yang dikendalikan melalui modul *relay*.
6. Penelitian ini berfokus pada keamanan komunikasi dan integritas data pada jalur komunikasi antara ESP32-C3 dan server. Penelitian ini tidak membahas perlindungan kunci privat terhadap ekstraksi fisik dari *firmware*, *Secure Boot*, *Flash Encryption*, eFuse, maupun *secure element*.
7. Antarmuka *web admin* dan *endpoint* pencatatan metrik *response time* digunakan sebagai alat bantu pengujian pada jaringan lokal. Pengujian keamanan pada penelitian ini difokuskan pada protokol otentikasi akses, khususnya *replay attack* berupa penggunaan ulang data otentikasi lama dengan nonce yang sama atau kedaluwarsa, serta *data tampering* berupa manipulasi nilai id_samaran pada *request* /verify saat terjadi komunikasi

antara ESP32-C3 dan server. Keamanan *dashboard* admin tidak menjadi objek pengujian utama.

8. Peningkatan keamanan yang dimaksud dibatasi pada skenario *replay attack* dan *data tampering* pada komunikasi ESP32-C3 dan server di jaringan lokal.
9. Mekanisme nonce pada prototipe dirancang dan diuji untuk satu proses otentikasi aktif pada satu waktu. Penelitian ini belum menguji beberapa permintaan otentikasi yang berlangsung secara bersamaan.

1.4 Tujuan Penelitian

Berdasarkan rumusan permasalahan, penelitian ini memiliki tujuan sebagai berikut:

1. Mengetahui performa *total response time* sistem *smart door lock* berbasis ESP32-C3 pada proses otentikasi, mulai dari pembentukan id_samaran menggunakan SHA-256, permintaan nonce, pembuatan *digital signature* ECDSA P-256, hingga keputusan akses diterima atau ditolak.
2. Menguji kemampuan protokol otentikasi berbasis nonce, SHA-256, dan ECDSA P-256 dalam menolak *replay attack* dan *data tampering pada* komunikasi antara ESP32-C3 dan server berdasarkan skenario pengujian yang dilakukan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan gambaran mengenai implementasi protokol otentikasi berbasis nonce, SHA-256, dan ECDSA P-256 pada sistem *smart door lock* berbasis NFC menggunakan ESP32-C3. Selain itu, penelitian ini juga memberikan gambaran mengenai pengaruh penerapan mekanisme keamanan kriptografi terhadap *total response time* sistem pada kondisi akses diterima dan akses ditolak. Hasil implementasi dan pengujian diharapkan dapat menjadi referensi dalam pengembangan sistem kontrol akses berbasis NFC yang membutuhkan mekanisme otentikasi tambahan untuk mengurangi risiko penggunaan ulang data akses dan manipulasi data pada komunikasi antara perangkat dan *server*. Penelitian ini juga dapat menjadi acuan bagi penelitian

selanjutnya yang berkaitan dengan penerapan SHA-256, ECDSA P-256, mekanisme *challenge-response* berbasis nonce, serta pengujian *response time* pada sistem berbasis ESP32.

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi enam bab agar pembahasan penelitian dapat disajikan secara sistematis dan terarah. Setiap bab memiliki keterkaitan mulai dari dasar permasalahan, landasan teori, metode penelitian, perancangan, implementasi, pengujian, hingga penarikan kesimpulan. Adapun sistematika penulisan tugas akhir ini terdiri atas bagian-bagian berikut.

BAB 1 PENDAHULUAN

Bab pendahuluan membahas latar belakang mengenai permasalahan keamanan pada sistem akses berbasis NFC, khususnya penggunaan UUID sebagai identitas akses. Bab ini juga memuat rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan. Permasalahan penelitian difokuskan pada performa *response time* serta kemampuan protokol dalam menolak *replay attack* dan *data tampering* berdasarkan skenario pengujian yang dilakukan.

BAB 2 LANDASAN TEORI

Bab landasan teori membahas teori-teori yang digunakan sebagai dasar penelitian, meliputi NFC, SHA-256, ECDSA P-256, mekanisme *challenge-response* berbasis nonce, *replay attack*, *response time*, dan *data tampering*. Selain itu, bab ini juga membahas perangkat dan teknologi pendukung seperti ESP32-C3, MFRC522, Arduino IDE, MySQL, solenoid *door lock*, *relay*, dan *flowchart*. Landasan teori tersebut digunakan sebagai dasar dalam proses perancangan, implementasi, pengujian, dan pembahasan sistem.

BAB 3 METODE PENELITIAN

Bab metode penelitian menjelaskan tahapan yang dilakukan secara sistematis untuk mencapai tujuan penelitian dan menjawab rumusan masalah. Tahapan tersebut meliputi diagram alir penelitian, studi literatur, analisis kebutuhan, perancangan sistem, implementasi, pengujian, serta pengumpulan data hasil pengujian. Bab ini juga menjelaskan proses penyusunan kesimpulan dan saran berdasarkan hasil penelitian.

BAB 4 PERANCANGAN

Bab perancangan menjelaskan rancangan sistem *smart door lock* berbasis NFC yang dikembangkan dalam penelitian ini. Perancangan meliputi arsitektur sistem, perangkat keras, perangkat lunak, proses *hashing* dan *digital signature*, protokol otentikasi, komunikasi klien-server, basis data, antarmuka, serta pencatatan *response time*. Bab ini juga menjelaskan rancangan skenario pengujian keseluruhan sistem, *response time*, *replay attack*, dan *data tampering*.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian, dan pembahasan menjelaskan penerapan sistem berdasarkan rancangan yang telah dibuat pada tahap sebelumnya. Bab ini mencakup implementasi perangkat keras dan perangkat lunak, proses SHA-256 dan ECDSA P-256, pengujian keseluruhan sistem, pengujian *response time*, *replay attack*, dan *data tampering*, serta pembahasan terhadap hasil yang diperoleh. Pembahasan tersebut digunakan untuk menghubungkan hasil implementasi dan pengujian dengan rumusan masalah serta tujuan penelitian.

BAB 6 PENUTUP

Bab penutup memuat kesimpulan yang disusun berdasarkan hasil implementasi, pengujian, dan pembahasan penelitian. Kesimpulan digunakan untuk menjawab rumusan masalah mengenai performa *response time* dan kemampuan protokol dalam menolak *replay attack* serta *data tampering*. Bab ini juga memuat saran untuk pengembangan sistem dan penelitian berikutnya berdasarkan keterbatasan yang ditemukan selama penelitian.