

RANCANG BANGUN SISTEM KEYLESS ANTI-RAMPAS UNTUK KENDARAAN BERMOTOR BERBASIS ESP32 MENGGUNAKAN BLUETOOTH DAN FINGERPRINT SEBAGAI IDENTITAS PEMILIK

Dinal Mustofa¹, Ganjar Febriyani Pratiwi, S.T., M.T.^{2*}

^{1,2} Program Studi Teknik Elektro, Fakultas Teknik dan Informatika, Universitas Dian Nusantara, Jakarta, Indonesia

e-mail: ¹531221020@mahasiswa.undira.ac.id; *ganjar.febriyani.pratiwi@undira.ac.id

ABSTRAK

Pencurian dan perampasan kendaraan bermotor memerlukan sistem keamanan yang tidak hanya membatasi akses awal, tetapi juga mampu merespons ketika kendaraan telah dikuasai pihak yang tidak berwenang. Penelitian ini merancang dan mengimplementasikan sistem keyless anti-rampas berbasis ESP32 dengan sensor fingerprint sebagai autentikasi pemilik dan Bluetooth Low Energy (BLE) Tag sebagai penanda keberadaan pengguna. Metode Research and Development digunakan melalui tahapan analisis kebutuhan, perancangan perangkat keras dan perangkat lunak, pembuatan prototipe, implementasi pada kendaraan, serta pengujian fungsional. Sistem terdiri atas ESP32, sensor fingerprint AS608, BLE Tag, relay, buzzer, modul step-down, sekring, dan aki 12 V. Hasil pengujian menunjukkan bahwa tegangan 12,13 V berhasil diturunkan menjadi 5,02 V. Sepuluh percobaan sidik jari terdaftar menghasilkan keberhasilan 100% dengan rata-rata waktu respons 0,8 detik. BLE Tag terdeteksi secara konsisten pada jarak 5–10 m. Ketika tag tidak terdeteksi atau berada lebih dari 10 m, sistem mengaktifkan buzzer dan memutus arus kendaraan melalui relay. Pengujian terintegrasi memperlihatkan seluruh komponen bekerja sesuai logika yang dirancang. Sistem ini dapat menjadi alternatif pengamanan kendaraan yang bekerja secara lokal tanpa ketergantungan pada internet, meskipun pengujian lanjutan masih diperlukan untuk menilai akurasi biometrik dan keselamatan pemutusan mesin pada kondisi dinamis.

Kata Kunci: ESP32, fingerprint, Bluetooth Low Energy, keyless, anti-rampas, keamanan kendaraan.

ABSTRACT

Motorcycle theft and robbery require a security system that not only restricts initial access but also responds after the vehicle has been taken by an unauthorized person. This study designs and implements an ESP32-based keyless anti-robbery system using a fingerprint sensor for owner authentication and a Bluetooth Low Energy (BLE) Tag for user-presence monitoring. A Research and Development approach was applied through requirement analysis, hardware and software design, prototype development, vehicle implementation, and functional testing. The system consists of an ESP32, AS608 fingerprint sensor, BLE Tag, relay, buzzer, step-down converter, fuse, and a 12 V vehicle battery. Test results show that the 12.13 V input was reduced to 5.02 V. Ten trials using registered fingerprints achieved a 100% success rate with an average response time of 0.8 s. The BLE Tag was consistently detected at 5–10 m. When the tag was not detected or moved beyond 10 m, the system activated the buzzer and disconnected the vehicle electrical circuit through the relay. Integrated testing confirmed that all components operated according to the programmed logic. The proposed system provides a locally operated vehicle-security alternative without internet dependency; however, further testing is required to evaluate biometric error rates and the safety of engine cutoff under dynamic driving conditions.

Keywords: ESP32, fingerprint, Bluetooth Low Energy, keyless system, anti-robbery, vehicle security.

I. PENDAHULUAN

Pencurian kendaraan bermotor masih menjadi persoalan keamanan, terutama pada kendaraan yang hanya mengandalkan kunci mekanis dan kunci stang. Mekanisme tersebut relatif mudah dimanipulasi dan tidak memberikan respons otomatis ketika kendaraan telah berpindah penguasaan[1], [2]. Kebutuhan sistem keamanan karena itu bergeser dari penguncian pasif menuju autentikasi elektronik dan pengendalian aktuator secara otomatis.

Sistem berbasis Internet of Things (IoT), GSM, dan GPS telah digunakan untuk pemantauan, pelacakan, dan pemutusan arus dari jarak jauh[3]. Pendekatan tersebut memperluas jangkauan kendali, tetapi kinerjanya bergantung pada ketersediaan jaringan dan memerlukan proteksi komunikasi yang memadai[4]. Pada lingkungan dengan koneksi tidak stabil, komunikasi lokal menjadi alternatif karena proses autentikasi dan pengambilan keputusan dapat dilakukan langsung oleh perangkat kendaraan.

Bluetooth Low Energy (BLE) sesuai untuk komunikasi jarak dekat berdaya rendah dan dapat diintegrasikan langsung pada ESP32 [5], [6]. Pada sisi identitas, autentikasi biometrik memberikan penghalang akses yang lebih kuat karena sidik jari melekat pada pengguna[7]. Penelitian terdahulu umumnya menerapkan RFID-GSM-GPS, Bluetooth-GPS, atau fingerprint sebagai mekanisme terpisah[8]. Keterbatasan yang masih terlihat adalah ketergantungan jaringan, autentikasi tunggal, dan belum terintegrasinya pemantauan keberadaan pemilik dengan respons anti-rampas otomatis.

Penelitian ini mengembangkan sistem keyless anti-rampas berbasis ESP32 yang bekerja secara offline. Sidik jari digunakan untuk mengaktifkan kendaraan, sedangkan BLE Tag dipantau selama kendaraan beroperasi. Ketika tag tidak terdeteksi, ESP32 memutus arus melalui relay dan mengaktifkan buzzer. Kontribusi utama penelitian adalah integrasi autentikasi awal dan pemantauan keberadaan pemilik dalam satu pengendali lokal. Tujuan penelitian adalah mengevaluasi fungsi catu daya, autentikasi fingerprint, jangkauan deteksi BLE, keluaran relay-buzzer, dan kinerja sistem secara terintegrasi. Sistem yang dikembangkan memiliki batasan operasional berupa penggunaan autentikasi fingerprint sebagai akses awal kendaraan dan Bluetooth Low Energy (BLE) Tag sebagai indikator keberadaan pengguna selama kendaraan beroperasi. Sistem bekerja secara lokal menggunakan ESP32 tanpa ketergantungan jaringan internet. Jarak deteksi BLE dibatasi pada rentang 5 hingga 10 meter dalam kondisi lingkungan uji. Sistem tidak mencakup integrasi dengan sistem pelacakan berbasis GPS maupun komunikasi jarak jauh.

1.1 Studi Terkait dan Posisi Penelitian

Kajian terhadap penelitian terdahulu digunakan untuk menentukan posisi sistem yang dikembangkan. Sistem berbasis RFID, GSM, dan GPS memberikan fungsi pelacakan serta pemutusan mesin jarak jauh, tetapi masih bergantung pada kualitas jaringan seluler[9]. Sistem berbasis fingerprint meningkatkan kekuatan autentikasi, namun pada umumnya hanya mengamankan tahap akses awal. Sistem berbasis Bluetooth memberikan komunikasi lokal yang sederhana dan hemat daya, tetapi tanpa verifikasi biometrik berpotensi bergantung pada kepemilikan perangkat saja[10].

Tabel 1. Perbandingan penelitian terdahulu dan penelitian yang diusulkan

Pendekatan	Fitur utama	Keterbatasan	Posisi penelitian ini
RFID, GSM, dan GPS [5]	Autentikasi kartu, pelacakan, pemutusan jarak jauh	Jangkauan RFID terbatas dan bergantung sinyal GSM	Menghilangkan ketergantungan jaringan melalui keputusan lokal

Pendekatan	Fitur utama	Keterbatasan	Posisi penelitian ini
ESP32, fingerprint, dan Telegram [2]	Biometrik dan pemantauan internet	Memerlukan internet dan layanan aplikasi	Menggunakan BLE lokal sebagai pemantauan keberadaan
Arduino dan fingerprint [10]	Autentikasi sidik jari	Belum memantau keberadaan pemilik setelah kendaraan aktif	Menambahkan verifikasi keberadaan berkelanjutan melalui BLE
ESP32, Bluetooth, dan GPS [7]	Kontrol lokal dan pelacakan	Tidak menggunakan autentikasi biometrik	Menggabungkan biometrik dan komunikasi lokal
ESP32 dan Bluetooth [6]	Kontrol akses berbiaya rendah	Autentikasi tunggal dan tanpa respons anti-rampas	Mengaktifkan relay-buzzer ketika tag hilang

(Sumber: diolah dari penelitian terdahulu)

Perbandingan pada Tabel 1 menunjukkan bahwa kebaruan penelitian terletak pada integrasi dua tahap pengamanan dalam satu sistem embedded. Tahap pertama memverifikasi identitas melalui sidik jari, sedangkan tahap kedua memantau keberadaan BLE Tag ketika kendaraan telah aktif. Arsitektur ini diarahkan untuk menjaga kemandirian sistem, mengurangi latensi akibat jaringan eksternal, dan menyediakan respons anti-rampas otomatis pada tingkat perangkat.

II. METODE PENELITIAN

2.1 Metode dan Tahapan Penelitian

Penelitian menggunakan metode Research and Development (R&D) yang meliputi identifikasi masalah, studi literatur, perancangan sistem, pembuatan prototipe, implementasi pada kendaraan, pengujian, dan analisis hasil [11]. Perangkat lunak dikembangkan menggunakan Arduino IDE dengan bahasa C/C++. Pengujian dilaksanakan pada prototipe yang dipasang pada kendaraan bermotor dalam lingkungan terkendali di Jakarta.

Tahap perancangan mencakup arsitektur perangkat keras, jalur catu daya, komunikasi serial sensor fingerprint, pemindaian BLE, serta logika pengendalian relay dan buzzer. Setelah perakitan, setiap komponen diuji secara parsial sebelum dilakukan pengujian integrasi. Perancangan sistem diperbarui untuk menyesuaikan struktur terbaru yang terdiri atas dua lapis pengamanan. Lapisan pertama menggunakan fingerprint sebagai autentikasi awal, sedangkan lapisan kedua menggunakan BLE Tag sebagai mekanisme pemantauan keberadaan pengguna saat kendaraan aktif. Seluruh keputusan sistem diproses oleh ESP32 melalui logika state machine yang mengatur kondisi standby, autentikasi, operasi normal, dan anti-rampas.

2.2 Kebutuhan Sistem

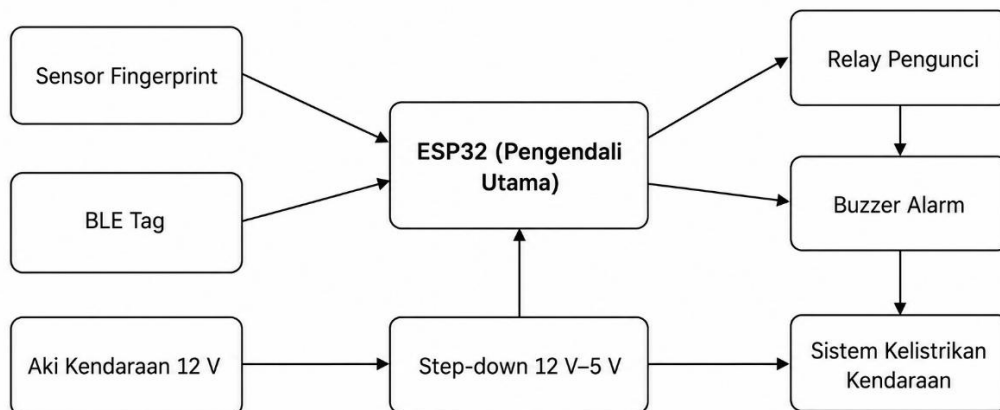
Kebutuhan sistem dirumuskan berdasarkan fungsi keamanan, keandalan operasi, dan kemudahan integrasi pada kendaraan. Kebutuhan fungsional menjelaskan layanan yang harus dijalankan, sedangkan kebutuhan nonfungsional menjadi batas desain agar perangkat dapat digunakan secara stabil pada sumber daya kendaraan.

Tabel 2. Kebutuhan fungsional dan nonfungsional sistem

Kategori	Kebutuhan	Kriteria verifikasi
Fungsional	Menerima dan mencocokkan sidik jari terdaftar	Relay hanya aktif setelah autentikasi valid
Fungsional	Menolak sidik jari tidak terdaftar atau pembacaan tidak sempurna	Relay tetap OFF dan akses ditolak
Fungsional	Mendeteksi BLE Tag selama kendaraan aktif	Operasi normal pada jarak pengujian 5-10 m
Fungsional	Mengaktifkan mode anti-rampas ketika tag hilang	Relay OFF dan buzzer ON
Fungsional	Mengembalikan sistem ke kondisi aman	Autentikasi ulang sebelum kendaraan aktif
Nonfungsional	Bekerja tanpa internet dan aplikasi eksternal	Keputusan diproses secara lokal oleh ESP32
Nonfungsional	Menggunakan catu daya kendaraan	Tegangan 12 V diturunkan menjadi sekitar 5 V
Nonfungsional	Menyediakan pengaman rangkaian	Sekering dan pemisahan jalur daya diterapkan

(Sumber: hasil analisis kebutuhan penelitian)

2.3 Arsitektur Perangkat Keras



Gambar 1. Arsitektur sistem keyless anti-rampas berbasis ESP32

(Sumber: dokumentasi dan hasil perancangan penelitian)

Gambar 1 menunjukkan ESP32 sebagai pengendali utama. Sensor fingerprint mengirimkan hasil pembacaan melalui komunikasi serial, sedangkan BLE Tag dipantau menggunakan radio

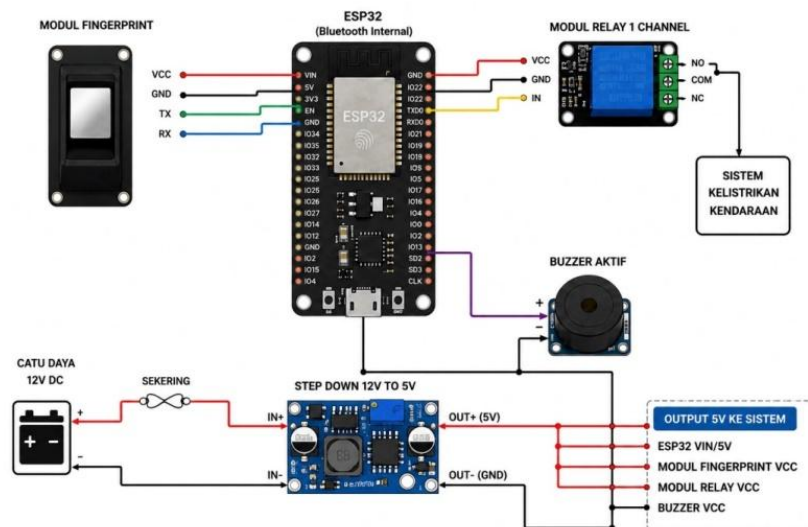
BLE internal ESP32. Relay menjadi antarmuka penghubung dan pemutus sistem kelistrikan kendaraan, sedangkan buzzer memberikan indikasi kondisi tidak aman. Sumber daya berasal dari aki 12 V dan diturunkan menjadi 5 V menggunakan step-down converter. Sekering ditempatkan pada jalur daya untuk membatasi risiko arus berlebih. Prinsip penurunan tegangan dan pengendalian beban melalui relay mengacu pada praktik catu daya switching dan aktuasi elektronik [12]. Block diagram terbaru menunjukkan alur kontrol terpusat pada ESP32 yang mengelola input dari sensor fingerprint dan modul BLE, kemudian menghasilkan output berupa relay dan buzzer sebagai aktuator utama. Perubahan struktur sistem menegaskan bahwa BLE tidak lagi berperan sebagai perangkat kontrol langsung, tetapi sebagai indikator keberadaan pengguna yang dipantau secara periodik oleh sistem.

Tabel 3. Komponen utama sistem

No.	Komponen	Fungsi
1	ESP32	Pemrosesan autentikasi, pemindaian BLE, dan pengendalian keluaran
2	Sensor fingerprint AS608	Autentikasi sidik jari pengguna
3	BLE Tag	Penanda keberadaan pemilik kendaraan
4	Relay	Menghubungkan atau memutus arus kendaraan
5	Buzzer	Alarm kegagalan akses dan kondisi anti-rampas
6	Step-down converter	Menurunkan tegangan aki 12 V menjadi sekitar 5 V
7	Aki 12 V dan sekering	Sumber daya dan pengaman rangkaian

(Sumber: hasil perancangan penelitian)

2.4 Rangkaian dan Alur Kerja Sistem



Gambar 2. Wiring sistem keyless anti-rampas

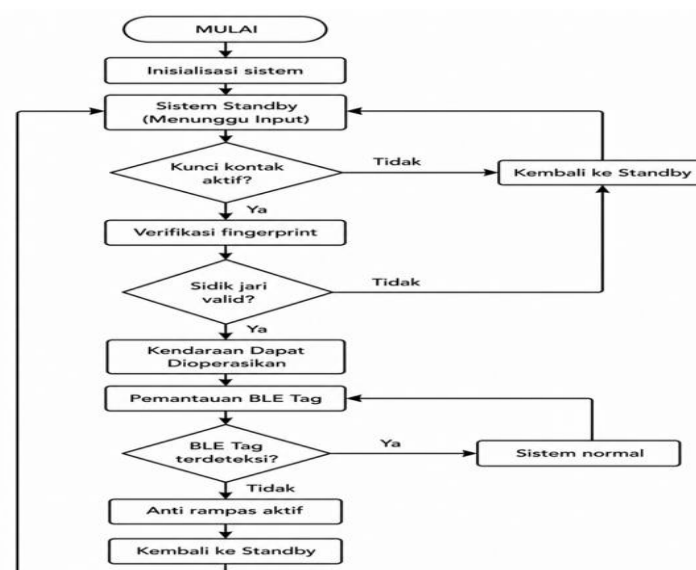
(Sumber: dokumentasi dan hasil perancangan penelitian)

Flowchart sistem yang diperbarui menunjukkan urutan proses dimulai dari inisialisasi perangkat, dilanjutkan dengan autentikasi fingerprint sebagai syarat aktivasi kendaraan. Setelah sistem aktif, ESP32 melakukan pemantauan BLE Tag secara kontinu. Jika BLE Tag tidak terdeteksi dalam rentang waktu tertentu, sistem langsung memasuki mode anti-rampas dengan menonaktifkan relay dan mengaktifkan buzzer. Proses ini memastikan kendaraan hanya dapat beroperasi ketika identitas dan keberadaan pengguna terverifikasi secara bersamaan. Sensor fingerprint terhubung ke ESP32 melalui jalur TX dan RX. Relay 5 V menerima sinyal digital dari ESP32 dan mengendalikan jalur kelistrikan kendaraan. BLE Tag tidak terhubung secara fisik karena mengirimkan identitas secara nirkabel. Sistem mengizinkan kendaraan aktif hanya setelah template sidik jari cocok. Setelah relay aktif, ESP32 memindai BLE Tag secara berulang. Mekanisme alarm suara digunakan sebagai pemberitahuan ketika terjadi akses ilegal atau kehilangan tag[3].

Tabel 4. Hubungan antarmuka dan jalur sinyal

Perangkat	Antarmuka/jalur	Arah data atau fungsi
Sensor fingerprint AS608	UART TX-RX dan catu 5 V	Pengiriman ID hasil pencocokan ke ESP32
BLE Tag	Komunikasi nirkabel BLE 2,4 GHz	Penyiaran identitas perangkat secara periodik
Relay 5 V	GPIO digital ESP32	Perintah ON/OFF jalur kelistrikan kendaraan
Buzzer	GPIO digital ESP32	Indikasi suara pada akses gagal dan mode anti-rampas
Step-down converter	Input 12 V; output 5 V	Penyedia tegangan logika untuk modul kontrol
Sekering	Seri pada jalur sumber	Proteksi terhadap arus berlebih dan hubungan singkat

(Sumber: hasil perancangan perangkat keras)



Gambar 3. Alur kerja perangkat lunak sistem

(Sumber: dokumentasi dan hasil perancangan penelitian)

Flowchart dimulai dari inisialisasi sistem untuk menyiapkan seluruh komponen agar siap digunakan. Sistem kemudian berada pada kondisi standby dan menunggu aktivasi kunci kontak. Setelah aktif, sistem menjalankan verifikasi fingerprint sebagai autentikasi pengguna. Jika sidik jari tidak valid, sistem kembali ke mode standby. Jika valid, kendaraan dapat dioperasikan.

Saat kendaraan aktif, sistem melakukan pemantauan BLE Tag secara terus-menerus untuk memastikan keberadaan pemilik. Jika BLE Tag terdeteksi, sistem tetap berjalan normal. Jika BLE Tag tidak terdeteksi, sistem mengaktifkan mode anti-rampas untuk memutus arus dan memberikan peringatan. Setelah itu, sistem kembali ke kondisi standby untuk proses autentikasi ulang. Sistem menerapkan dua lapis keamanan, yaitu fingerprint sebagai akses awal dan BLE Tag sebagai pengawasan keberadaan pemilik.

2.5 Perancangan Perangkat Lunak dan Status Operasi

Perangkat lunak menerapkan mesin keadaan sederhana yang terdiri atas standby, autentikasi, operasi normal, dan anti-rampas. Pemisahan status digunakan agar pengendalian relay tidak hanya bergantung pada satu pembacaan sensor [13]. Pembaruan logika state machine menegaskan bahwa transisi antar status tidak hanya bergantung pada validasi fingerprint, tetapi juga pada kondisi keberadaan BLE Tag. Sistem akan tetap berada pada status operasi normal selama BLE terdeteksi dalam rentang yang ditentukan. Perubahan status ke mode anti-rampas dilakukan apabila terjadi kehilangan sinyal BLE yang bersifat berkelanjutan, sehingga mengurangi potensi false trigger akibat fluktuasi sinyal sesaat. Pada kondisi awal, relay OFF dan sistem menunggu sidik jari. Setelah sidik jari valid, relay ON dan pemindaian BLE dimulai. Kehilangan tag memindahkan sistem ke status anti-rampas, yaitu relay OFF dan buzzer ON. Sistem kembali ke standby untuk mencegah aktivasi otomatis tanpa autentikasi ulang.

Tabel 5. Status operasi dan transisi sistem

Status awal	Kondisi pemicu	Aksi keluaran	Status berikutnya
Standby	Sidik jari valid	Relay ON; buzzer OFF	Operasi normal
Standby	Sidik jari tidak valid	Relay OFF; buzzer peringatan	Standby
Operasi normal	BLE Tag terdeteksi	Relay ON; buzzer OFF	Operasi normal
Operasi normal	BLE Tag tidak terdeteksi	Relay OFF; buzzer ON	Anti-rampas
Anti-rampas	Tag kembali terdeteksi	Relay tetap OFF	Standby/autentikasi ulang

(Sumber: hasil perancangan algoritma)

2.6 Skenario dan Parameter Pengujian

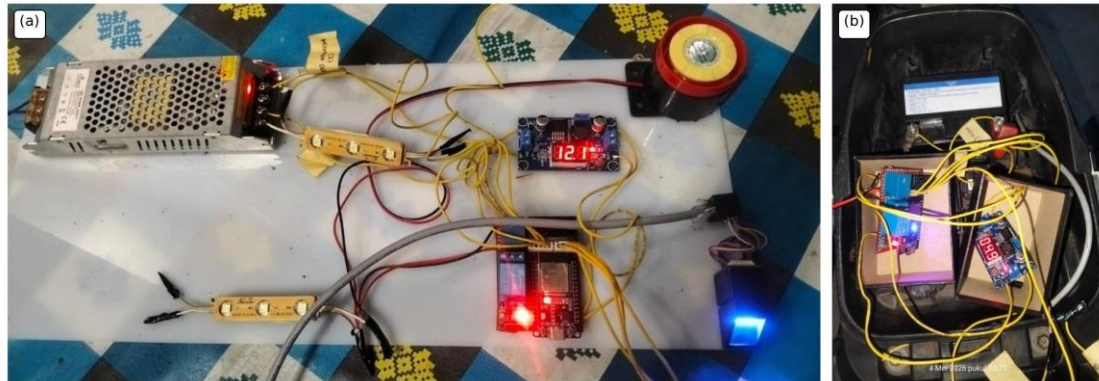
Pengujian dilakukan terhadap: (1) tegangan pada input-output step-down, ESP32, fingerprint, dan relay; (2) respons fingerprint untuk sidik jari terdaftar, tidak terdaftar, pembacaan tidak sempurna, dan kondisi tanpa input; (3) sepuluh percobaan sidik jari terdaftar untuk memperoleh persentase keberhasilan dan rata-rata waktu respons; (4) deteksi BLE pada jarak 5 m, 10 m, dan lebih dari 10 m dengan tiga pengulangan; serta (5) fungsi relay, buzzer, anti-rampas, dan integrasi keseluruhan. Pengujian deteksi BLE juga mempertimbangkan kondisi stabilitas sinyal untuk menghindari perubahan status sistem akibat variasi pembacaan sementara. Sistem hanya merespons kondisi kehilangan BLE apabila kondisi tersebut bertahan melewati ambang waktu yang ditentukan pada program kontrol ESP32.

$$\text{Keberhasilan} = (\text{jumlah percobaan berhasil} / \text{jumlah seluruh percobaan}) \times 100\%$$

$$\text{Rata-rata waktu respons} = \Sigma t_i / n$$

III. HASIL DAN PEMBAHASAN

3.1 Realisasi Sistem dan Catu Daya



Gambar 4. Realisasi sistem: (a) perakitan perangkat keras dan (b) pemasangan pada kendaraan
(Sumber: dokumentasi dan hasil perancangan penelitian)

Seluruh komponen berhasil dirakit dan diintegrasikan pada kendaraan. Jalur daya 12 V dipisahkan dari jalur logika 5 V melalui step-down converter. Pemasangan sensor fingerprint ditempatkan pada area yang dapat dijangkau pengguna, sedangkan ESP32, relay, dan modul daya ditempatkan pada kompartemen kendaraan.

Tabel 6. Hasil pengukuran tegangan sistem

Titik pengukuran	Tegangan spesifikasi	Tegangan terukur
Input step-down	12 V	12,13 V
Output step-down	5 V	5,02 V
VCC ESP32	5 V	5,01 V
VCC fingerprint	5 V	4,44 V
Input relay	5 V	5,01 V

(Sumber: hasil pengujian penelitian)

Modul step-down menurunkan tegangan 12,13 V menjadi 5,02 V, dengan deviasi sekitar 0,4% terhadap nilai nominal 5 V. ESP32 dan relay menerima 5,01 V. Tegangan sensor fingerprint sebesar 4,44 V lebih rendah dari nominal, tetapi sensor tetap berfungsi pada seluruh pengujian. Meskipun hasil fungsional memadai, penurunan tegangan tersebut perlu diperhatikan pada pengembangan berikutnya karena rugi kabel, konektor, dan arus sesaat dapat memengaruhi stabilitas sensor.

3.2 Kinerja Autentikasi Fingerprint

Tabel 7. Hasil pengujian autentikasi fingerprint

Kondisi	Respons sistem	Hasil
Sidik jari terdaftar	Sistem aktif	Berhasil
Sidik jari tidak terdaftar	Akses ditolak	Berhasil
Sidik jari tidak terbaca sempurna	Akses ditolak	Berhasil
Sensor tidak digunakan	Sistem tetap tidak aktif	Berhasil
10 percobaan sidik jari terdaftar	10/10 berhasil; rata-rata 0,8 s	100%

(Sumber: hasil pengujian penelitian)

Tabel 8. Rincian waktu respons autentikasi sidik jari terdaftar

Percobaan	Kondisi	Hasil	Waktu respons (s)
1	Terdaftar	Berhasil	0,8
2	Terdaftar	Berhasil	0,7
3	Terdaftar	Berhasil	0,9
4	Terdaftar	Berhasil	0,8
5	Terdaftar	Berhasil	0,8
6	Terdaftar	Berhasil	0,7
7	Terdaftar	Berhasil	0,9
8	Terdaftar	Berhasil	0,8
9	Terdaftar	Berhasil	0,8
10	Terdaftar	Berhasil	0,8

(Sumber: hasil pengujian penelitian)

Sepuluh percobaan sidik jari terdaftar menghasilkan waktu respons 0,7–0,9 s dengan rata-rata 0,8 s dan seluruh percobaan berhasil. Sistem juga menolak sidik jari tidak terdaftar dan pembacaan yang tidak sempurna. Hasil ini menunjukkan fungsi autentikasi berjalan konsisten pada pengujian prototipe dan mendukung temuan bahwa fingerprint dapat digunakan sebagai kontrol akses kendaraan[14].

Sebaran waktu respons hanya berada pada rentang 0,2 s, yang menunjukkan variasi kecil selama kondisi pengujian. Waktu tercepat 0,7 s terjadi pada percobaan ke-2 dan ke-6, sedangkan waktu terlama 0,9 s terjadi pada percobaan ke-3 dan ke-7. Dengan simpangan rentang yang rendah, proses pencocokan dapat dinilai responsif untuk penggunaan prototipe, tetapi belum mencerminkan pengaruh kondisi jari basah, kotor, terluka, atau perubahan posisi penempelan.

Persentase 100% pada penelitian ini tidak dapat diperlakukan sebagai ukuran akurasi biometrik umum karena jumlah pengguna dan percobaan terbatas. Pengujian belum menghitung

false acceptance rate, false rejection rate, variasi kondisi jari, maupun pengaruh debu dan kelembapan. Evaluasi tersebut diperlukan sebelum sistem digunakan pada skala operasional.

3.3 Deteksi BLE dan Fitur Anti-Rampas

Tabel 9. Hasil pengujian BLE dan respons anti-rampas

Kondisi pengujian	Respons sistem	Keberhasilan
BLE Tag pada jarak 5 m	Terdeteksi; kendaraan aktif	3/3
BLE Tag pada jarak 10 m	Terdeteksi; kendaraan aktif	3/3
BLE Tag pada jarak >10 m	Tidak terdeteksi; relay OFF dan buzzer ON	3/3
BLE Tag dimatikan saat kendaraan aktif	Mode anti-rampas aktif	Berhasil
BLE Tag terdeteksi kembali	Sistem kembali normal setelah autentikasi	Berhasil

(Sumber: hasil pengujian penelitian)

BLE Tag terdeteksi konsisten pada 5 m dan 10 m. Pada jarak lebih dari 10 m atau ketika tag dimatikan, ESP32 memutus relay dan mengaktifkan buzzer. Mekanisme ini menambahkan verifikasi keberadaan pengguna setelah autentikasi awal, sehingga berbeda dari sistem fingerprint-only yang berhenti pada tahap pengaktifan kendaraan[14]. Sistem juga tidak memerlukan koneksi internet, sehingga mengurangi ketergantungan jaringan yang terdapat pada sistem IoT atau GSM[15].

Batas lebih dari 10 m merupakan hasil empiris pada lokasi pengujian dan bukan jarak baku BLE. Nilai tersebut dapat berubah akibat orientasi antena, penghalang, interferensi 2,4 GHz, daya pancar tag, dan parameter pemindaian. Pengembangan lebih lanjut perlu menyimpan received signal strength indicator (RSSI), menerapkan hysteresis, dan menggunakan beberapa siklus kehilangan paket sebelum mengaktifkan relay agar sistem tidak bereaksi terhadap gangguan sesaat.

Tabel 10. Pengujian keluaran relay

Kondisi pengujian	Respons relay	Status
Autentikasi berhasil	Relay ON	Berhasil
Autentikasi gagal	Relay tetap OFF	Berhasil
Mode anti-rampas aktif	Relay OFF; arus terputus	Berhasil
Sistem belum diakses	Relay OFF	Berhasil

(Sumber: hasil pengujian penelitian)

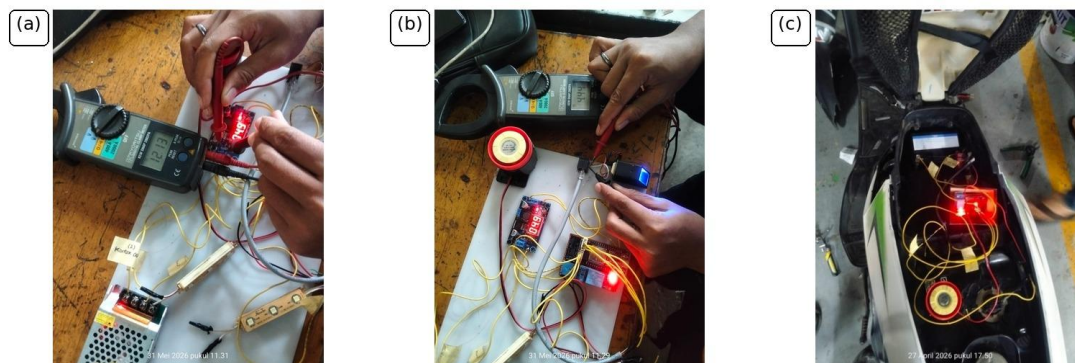
Tabel 11. Pengujian keluaran buzzer

Kondisi pengujian	Respons buzzer	Status
Sistem anti-rampas aktif	Buzzer ON	Berhasil
Sistem normal	Buzzer OFF	Berhasil
BLE Tag tidak terdeteksi	Buzzer ON	Berhasil
Sidik jari tidak dikenali	Buzzer memberikan peringatan	Berhasil

(Sumber: hasil pengujian penelitian)

Relay dan buzzer menunjukkan respons yang konsisten terhadap seluruh kondisi uji. Relay mempertahankan kondisi aman secara default, yaitu OFF sebelum pengguna memperoleh otorisasi. Buzzer berfungsi sebagai kanal informasi langsung bagi pengguna dan lingkungan sekitar. Kombinasi keduanya membentuk respons ganda: penghentian akses pada jalur kelistrikan dan pemberian alarm suara.

3.4 Pengujian Keluaran dan Integrasi Sistem



Gambar 5. Pengujian sistem: (a) pengukuran tegangan, (b) relay dan buzzer, dan (c) integrasi pada kendaraan

(Sumber: dokumentasi dan hasil perancangan penelitian)

Tabel 12. Hasil pengujian keseluruhan sistem

Kondisi	Hasil sistem	Status
Fingerprint valid dan BLE Tag terdeteksi	Kendaraan dapat dioperasikan	Berhasil
Fingerprint tidak sesuai	Akses ditolak; relay tetap OFF	Berhasil
BLE Tag hilang saat kendaraan aktif	Relay OFF dan buzzer ON	Berhasil

Kondisi	Hasil sistem	Status
Mode anti-rampas aktif	Kendaraan tidak dapat dioperasikan	Berhasil

(Sumber: hasil pengujian penelitian)

Pengujian keseluruhan menunjukkan bahwa fingerprint, BLE, relay, buzzer, dan catu daya dapat bekerja secara berurutan sesuai logika program. Relay tidak aktif sebelum autentikasi, aktif setelah sidik jari valid, dan kembali OFF ketika BLE Tag hilang. Buzzer memberikan indikasi pada kegagalan akses dan kondisi anti-rampas. Integrasi dua mekanisme autentikasi meningkatkan lapisan pengamanan dibandingkan penggunaan kunci mekanis atau satu faktor identitas.

Pengujian dilakukan pada prototipe dan lingkungan terkendali. Pemutusan sistem kelistrikan secara langsung belum dievaluasi pada kendaraan yang bergerak, sehingga implementasi lapangan harus memasukkan aspek keselamatan fungsional. Interlock berbasis kecepatan, penundaan bertahap, peringatan awal, dan fail-safe perlu dipertimbangkan agar fungsi anti-rampas tidak menimbulkan risiko kehilangan kendali kendaraan.

3.5 Analisis Komparatif dan Keterbatasan Sistem

Tabel 13. Analisis komparatif karakteristik sistem

Karakteristik	Sistem jaringan/IoT	Sistem satu faktor	Sistem yang diusulkan
Ketergantungan jaringan	Tinggi	Rendah	Tidak bergantung internet
Autentikasi awal	Bervariasi	Satu metode	Fingerprint
Pemantauan setelah aktif	Dapat melalui server	Umumnya tidak ada	BLE Tag lokal
Respons ketika identitas hilang	Perintah jarak jauh	Tidak tersedia	Relay OFF dan buzzer ON
Risiko utama	Gangguan jaringan dan keamanan data	Kompromi satu faktor	Gangguan BLE dan keselamatan pemutusan

(Sumber: analisis hasil penelitian dan studi literatur)

Sistem yang diusulkan memiliki keunggulan pada kemandirian operasi dan integrasi autentikasi berlapis. Keputusan keamanan tidak dikirim ke server sehingga waktu respons tidak dipengaruhi latensi internet. Namun, pendekatan lokal juga membatasi kemampuan pelacakan dan pemberitahuan jarak jauh. Kehilangan BLE Tag, baterai tag yang habis, atau gangguan frekuensi dapat dibaca sebagai kondisi ancaman apabila algoritma tidak dilengkapi validasi temporal.

Keterbatasan lain berada pada desain pengujian. Sampel autentikasi hanya terdiri atas sepuluh percobaan sidik jari terdaftar, sedangkan pengujian jarak BLE dilakukan pada tiga kategori jarak dengan tiga pengulangan. Penelitian belum mengevaluasi konsumsi arus, durasi operasi aki, pengaruh suhu dan getaran kendaraan, ketahanan sambungan, keamanan penyimpanan template sidik jari, maupun serangan spoofing terhadap BLE. Data yang diperoleh

karena itu harus dipahami sebagai verifikasi fungsi prototipe, bukan sertifikasi keandalan untuk penggunaan komersial.

3.6 Implikasi Keselamatan dan Rekomendasi Pengembangan

Fitur pemutusan arus harus ditempatkan pada jalur yang tidak menimbulkan kehilangan kendali mendadak. Implementasi yang lebih aman dapat menggunakan tahapan peringatan, verifikasi kehilangan tag selama beberapa siklus, pembatasan aktivasi ketika kecepatan kendaraan telah rendah, serta jalur fail-safe untuk mempertahankan fungsi lampu dan pengereman elektronik. Pada sisi perangkat lunak, parameter RSSI dan time-out perlu dicatat agar keputusan tidak hanya didasarkan pada satu paket BLE yang hilang.

Pengembangan berikutnya juga dapat menambahkan pencatatan kejadian pada memori lokal, indikator kondisi baterai BLE Tag, enkripsi identitas perangkat, dan mode administrasi untuk pendaftaran atau penghapusan sidik jari. Penambahan komunikasi seluler atau GPS dapat dipertimbangkan sebagai lapisan opsional, bukan sebagai syarat utama operasi, sehingga sistem tetap bekerja lokal ketika jaringan tidak tersedia.

3.7 Rencana Validasi Lanjutan

Validasi lanjutan perlu dirancang untuk menilai keandalan sistem pada kondisi yang lebih mendekati penggunaan nyata. Pengujian biometrik harus melibatkan beberapa pengguna, sidik jari terdaftar dan tidak terdaftar, serta variasi kondisi permukaan jari. Parameter yang dicatat tidak hanya keberhasilan pencocokan, tetapi juga false acceptance rate, false rejection rate, waktu respons, dan jumlah percobaan ulang. Pada komunikasi BLE, pengujian perlu dilakukan pada ruang terbuka, area dengan penghalang, lingkungan padat perangkat 2,4 GHz, serta berbagai orientasi tag terhadap antena ESP32.

Tabel 14. Rencana pengujian lanjutan

Aspek	Variabel uji	Parameter evaluasi	Tujuan
Fingerprint	Pengguna, kondisi jari, sudut penempelan	FAR, FRR, waktu respons	Menilai akurasi dan konsistensi biometrik
BLE	Jarak, penghalang, interferensi, orientasi tag	RSSI, kehilangan paket, waktu deteksi	Menentukan ambang dan hysteresis yang stabil
Catu daya	Tegangan aki, arus beban, kondisi start mesin	Drop tegangan, ripple, konsumsi arus	Memastikan kestabilan selama operasi kendaraan
Mekanik	Getaran, suhu, kelembapan, sambungan kabel	Kegagalan koneksi dan perubahan fungsi	Menilai ketahanan instalasi
Keselamatan	Kecepatan kendaraan dan skenario kehilangan tag	Waktu peringatan dan urutan pemutusan	Mencegah penghentian yang membahayakan
Keamanan data	Pendaftaran sidik jari dan identitas BLE	Akses tidak sah dan spoofing	Menguji proteksi identitas pengguna

(Sumber: rancangan pengembangan penelitian)

Pengujian catu daya juga harus mencakup kondisi ketika motor starter bekerja karena penurunan tegangan aki dapat menyebabkan reset ESP32 atau kegagalan pembacaan sensor. Konsumsi arus sistem pada standby dan operasi normal perlu diukur untuk memperkirakan pengaruhnya terhadap aki kendaraan. Uji getaran dan temperatur diperlukan karena modul elektronik ditempatkan pada kompartemen kendaraan yang mengalami perubahan lingkungan lebih besar dibandingkan meja laboratorium.

Tahap akhir validasi sebaiknya menggunakan prototipe dengan pengaman berlapis dan prosedur uji keselamatan. Aktivasi anti-rampas perlu didahului alarm, periode konfirmasi kehilangan tag, dan pemeriksaan kondisi kendaraan sebelum relay memutus jalur yang ditentukan. Pendekatan tersebut menghasilkan data yang lebih representatif sekaligus mengurangi risiko ketika sistem diuji pada kendaraan bergerak.

IV. KESIMPULAN

Sistem keyless anti-rampas berbasis ESP32 berhasil dirancang dan diimplementasikan dengan mengintegrasikan fingerprint, BLE Tag, relay, buzzer, dan catu daya kendaraan. Step-down menghasilkan keluaran 5,02 V dari masukan 12,13 V. Pada sepuluh percobaan sidik jari terdaftar, autentikasi berhasil 100% dengan rata-rata waktu respons 0,8 s. BLE Tag terdeteksi pada jarak 5–10 m; kehilangan tag atau jarak lebih dari 10 m mengaktifkan buzzer dan memutus arus melalui relay. Seluruh komponen bekerja terintegrasi sesuai rancangan dan sistem dapat beroperasi tanpa internet. Hasil tersebut masih bersifat pengujian fungsional prototipe. Penelitian berikutnya perlu mengevaluasi FAR/FRR fingerprint, karakteristik RSSI BLE, ketahanan lingkungan, konsumsi daya, keamanan perangkat lunak, dan mekanisme pemutusan mesin yang aman saat kendaraan bergerak.

DAFTAR PUSTAKA

- [1] M. Yugas De Silva, M. Bagus Anggara, and R. Ardi Indrianto, “Sistem Keamanan Kendaraan Berbasis Fingerprint,” *Pros. Semin. Nas. Teknol. Inf. dan Bisnis*, pp. 1286–1295, 2025, doi: 10.47701/cve7bq24.
- [2] H. Azwar and F. Gary, “Implementasi Transport Layer Security dengan Algoritma AES Pada Jaringan IoT Menggunakan Protokol MQTT,” *J. Elektro dan Mesin Terap.*, vol. 11, no. 1, pp. 60–66, May 2025, doi: 10.35143/elementer.v11i1.6478.
- [3] C. Kusuma Johan, D. Abdullah, A. Wijaya, and M. Imanullah, “Implementasi Smart Padlock Guna Meningkatkan Sistem Keamanan Pada Kendaraan Roda Dua Berbasis Sidik Jari Dan Mikrokontroler Esp32,” *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 9, no. 6, pp. 9758–9763, 2025, doi: 10.36040/jati.v9i6.15668.
- [4] Zumhur Alamin and Muhammad Amirul Mu'min, “Analisis Keamanan Jaringan pada Sistem Kendali Jarak Jauh untuk Infrastruktur Kritis,” *J. Pengemb. Sains dan Teknol.*, vol. 1, no. 1, pp. 25–41, 2025, doi: 10.63866/jpst.v1i1.39.
- [5] D. F. Hakim and A. S. Budi, “Lokalisasi Sistem Deteksi Lokasi Kendaraan Pada Lahan Parkir Menggunakan Metode Multilaterasi Berbasis Protokol Bluetooth Low Energy,” *J. Pengemb. Teknol. Inf. dan ...*, vol. 9, no. 8, pp. 1–8, 2025, [Online]. Available: <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/15206%0Ahttps://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/15206/6750>
- [6] A. Sasongko, S. Prastya, E. J. Brillianshah, M. Taruna, and A. Hakim, “Design and Implementation of Bluetooth Low Energy Based Access Control System,” *Komputika J. Sist. Komput.*, vol. 13, no. 1, pp. 73–82, Apr. 2024, doi: 10.34010/komputika.v13i1.11227.
- [7] N. Anugraha, M. Riswanto, L. Lindawati, and A. Asrul, “Sistem E-Voting berbasis Blockchain dengan Autentikasi Biometrik Sidik Jari dan Protokol Zero-Knowledge Proof

- Untuk Pengaman Privasi,” *J. Minfo Polgan*, vol. 14, no. 2, pp. 2756–2767, 2025, doi: 10.33395/jmp.v14i2.15536.
- [8] S. Nur, “Advancing Localization Accuracy- Fusion of Multiple Positioning Technologies for Robust and Adaptive Solutions,” *Int. J. Innov. Res. Comput. Sci. Technol.*, vol. 12, no. 3, pp. 162–167, May 2024, doi: 10.55524/ijirest.2024.12.3.27.
- [9] H. N. Syaddad, “Perancangan Sistem Keamanan Sepeda Motor Menggunakan Gps Tracker Berbasis Mikrokontroler Pada Kendaraan Bermotor,” *Media J. Inform.*, vol. 11, no. 2, p. 26, Aug. 2020, doi: 10.35194/mji.v11i2.1035.
- [10] D. Kurniawan, M. A. Rojabi, and A. R. Publisher, *Find My Device Google: Revolusi Jaringan Pelacakan Global Berbasis Ekosistem Android*. Afdan Rojabi Publisher, 2026. [Online]. Available: <https://books.google.co.id/books?id=pkHIEQAAQBAJ>
- [11] Ade Rahayu, “Metode Penelitian dan Pengembangan (R&D): Pengertian, Jenis dan Tahapan,” *DIAJAR J. Pendidik. dan Pembelajaran*, vol. 4, no. 3, pp. 459–470, 2025, doi: 10.54259/diajar.v4i3.5092.
- [12] S. T. M. T. Abil Huda *et al.*, *TEKNIK ELEKTRO*. Dunia Penerbitan buku, 2026. [Online]. Available: <https://books.google.co.id/books?id=Zo7REQAAQBAJ>
- [13] Y. Zorin and O. Chepelyuk, “Enhanced single-phase voltage control relay for household consumers with IoT and Bluetooth Low Energy support,” *Bull. NTU “KhPI”. Ser. Probl. Electr. Mach. Appar. Perfect. Theory Pract.*, no. 1 (13), pp. 12–16, Jun. 2025, doi: 10.20998/2079-3944.2025.1.03.
- [14] Dahlan and M. A. Mu’min, “Desain Sistem Keamanan Sepeda Motor Menggunakan Mikrokontroler Arduino dan Sensor Fingerprint ZFM-60 Berbasis Mobile,” *Sci. J. Comput. Sci. Informatics*, vol. 2, no. 1, pp. 40–47, Jan. 2025, doi: 10.34304/scientific.v2i1.343.
- [15] J. Penerapan, T. Informasi, M. N. Kholidah, I. Mualim, and N. A. Sivi, “IT-EXPLORE Analisis jaringan telekomunikasi untuk sistem peringatan dini konflik manusia – gajah di taman nasional Way Kambas,” vol. 05, pp. 86–97, 2026, doi: 10.24246/itexplore.v5i1.2026.pp86-97.