IMPLEMENTASI DAN EVALUASI SISTEM KEAMANAN KENDARAAN LISTRIK RINGAN BERBASIS IOT DENGAN AUTENTIKASI RFID, PELACAKAN GPS, DAN KENDALI *CUT-OFF*

Mohammad Raihan Fahreza[1], Budi Cahyo Wibowo[2]

[1]Program Studi Teknik Elektro, Fakultas Teknik,
Universitas Muria Kudus, Indonesia

[2]Program Studi Teknik Elektro, Fakultas Teknik,
Universitas Muria Kudus, Indonesia

ABSTRAK

Sistem keamanan konvensional pada kendaraan listrik ringan belum mengintegrasikan autentikasi, pelacakan lokasi, notifikasi, dan pemutusan daya jarak jauh dalam satu perangkat. Penelitian ini merancang dan mengevaluasi sistem berbasis *Internet of Things* yang mengintegrasikan ESP32, RFID RC522, GPS Neo-6M, Telegram Bot, dan MOSFET sebagai aktuator *cut-off*. Pengujian mencakup kesalahan posisi GPS, waktu respons Telegram, autentikasi RFID, serta fungsi ON dan OFF. GPS menghasilkan rata-rata kesalahan 8,05 m, median 8,00 m, simpangan baku 3,94 m, dan rentang 3,20–15,20 m. Telegram menghasilkan rata-rata respons 4,37 detik, median 2,67 detik, dan rentang 1,58–15,20 detik. Sistem menerima kartu terdaftar dan menolak kartu tidak terdaftar pada tujuh percobaan, dengan rata-rata respons RFID 2,47 detik. Perintah ON dan OFF berhasil mengubah kondisi MOSFET pada lokasi pengujian hingga 5,88 km selama internet tersedia, sedangkan akun tidak sah ditolak. Sistem beroperasi selama 24 jam tanpa reset atau gangguan fungsi yang teramati. Prototipe mampu mengintegrasikan empat fungsi keamanan, tetapi pengujiannya masih terbatas dan belum memiliki interlock *cut-off* berbasis kecepatan kendaraan.

Kata Kunci: *autentikasi RFID, Internet of Things, kendaraan listrik ringan, pelacakan GPS Neo-6M, sistem keamanan, cut-off.*

ABSTRACT

Conventional security systems for light electric vehicles have not integrated authentication, location tracking, notification, and remote power cut-off into one device. This study designed and evaluated an Internet of Things system integrating an ESP32, RFID RC522, GPS Neo-6M, Telegram Bot, and a MOSFET cut-off actuator. The tests covered GPS positioning error, Telegram response time, RFID authentication, and ON/OFF functions. GPS produced a mean error of 8.05

m, a median of 8.00 m, a standard deviation of 3.94 m, and a range of 3.20–15.20 m. Telegram produced a mean response time of 4.37 s, a median of 2.67 s, and a range of 1.58–15.20 s. The system accepted registered cards and rejected unregistered cards in seven trials, with a mean RFID response time of 2.47 s. ON and OFF commands changed the MOSFET state at test locations up to 5.88 km when Internet access was available, while unauthorized accounts were rejected. The system operated for 24 hours without an observed reset or functional failure. The prototype integrated four security functions, but testing remained limited and no speed-based cut-off interlock was used.

***Keywords**: **Keywords**: GPS Neo-6M tracking, Internet of Things, light electric vehicle, RFID authentication, security system, cut-off control..*

1. PENDAHULUAN

Kementerian Perindustrian Republik Indonesia melaporkan bahwa populasi kendaraan listrik pada 2024 mencapai sekitar 207 ribu unit, meningkat 78% dari sekitar 116 ribu unit pada 2023 [1]. Pusiknas Bareskrim Polri juga mencatat 6.323 kasus pencurian sepeda motor sejak Januari hingga pertengahan Mei 2026 [2]. Data tersebut menegaskan perlunya sistem yang tidak hanya mengandalkan kunci mekanis, tetapi juga menyediakan autentikasi, pelacakan lokasi, notifikasi, dan pemutusan daya jarak jauh.

Internet of Things menghubungkan mikrokontroler, sensor, aktuator, dan aplikasi melalui internet. Pada sistem keamanan kendaraan, RFID mendukung autentikasi, GPS memperkirakan lokasi, aplikasi pesan mengirim notifikasi, dan aktuator mengendalikan daya. Setiap teknologi memiliki batasan: UID RFID dapat diduplikasi, ketelitian GPS dipengaruhi lingkungan dan geometri satelit, sedangkan komunikasi internet bergantung pada kualitas jaringan dan latensi server.

Penelitian terdahulu telah menerapkan sebagian fungsi tersebut. Matsuani [7] menggunakan GPS Tracker berbasis Android tanpa RFID dan *cut-off*. Himawan et al. [15] menggabungkan RFID dan GPS, tetapi belum mengevaluasi *cut-off* MOSFET. Maesa dan Hartono [8] menggunakan GPS Neo-6M dan sensor getar tanpa autentikasi pengguna. Perbandingan yang lebih lengkap disajikan pada Tabel 1.

Studi sebelumnya umumnya berfokus pada fungsi tertentu dan belum mengevaluasi secara terpadu kesalahan GPS, waktu respons komunikasi, keputusan autentikasi RFID, serta *cut-off* melalui internet pada kendaraan listrik ringan. Penelitian ini tidak menawarkan algoritma baru. Kesenjangannya terletak pada integrasi dan evaluasi kuantitatif keempat fungsi tersebut dalam satu prototipe.

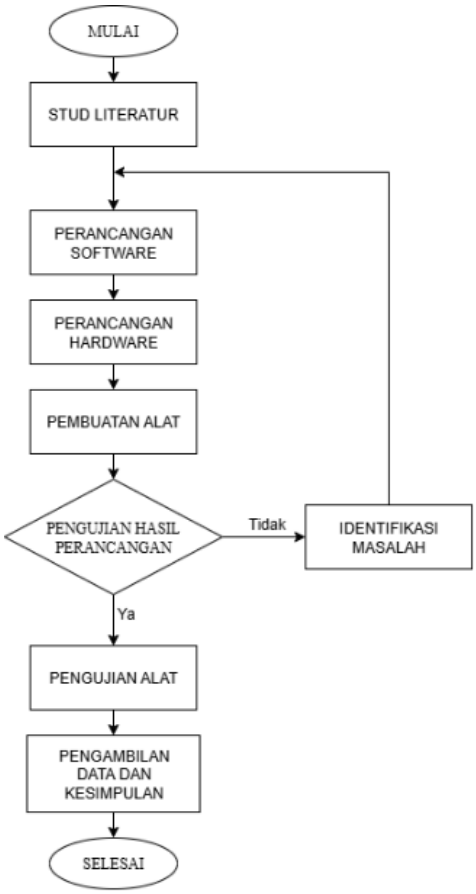
Penelitian ini bertujuan merancang dan mengevaluasi prototipe berbasis ESP32. Kontribusinya ialah integrasi RFID, GPS Neo-6M, Telegram, status *locked*/*unlocked*, dan *cut-off* MOSFET, disertai evaluasi kesalahan posisi, waktu respons, autentikasi, kondisi jaringan, dan pemutusan daya.

Tabel 1. Perbandingan Metode dan Kontribusi Penelitian

Penelitian	**Platform**	**Autentikasi**	**Pelacakan**	**Notifikasi**	***Cut-off***	**Parameter evaluasi**	**Keterbatasan**
Matsuani (2023) [7]	Android	Tidak	GPS	Aplikasi	Tidak	Fungsi GPS	Tanpa autentikasi
Himawan et al. (2022) [15]	Arduino + ESP8266	RFID	GPS	Telegram	Tidak	RFID dan GPS	Belum menggunakan *cut-off* MOSFET
Maesa dan Hartono (2025) [8]	IoT	Tidak	GPS Neo-6M	Telegram	Tidak	Ketelitian GPS	Tanpa autentikasi
Isyanto et al. (2022) [16]	IoT	Tidak	GPS	Telegram	Relay	Respons dan GPS	Tanpa autentikasi RFID
Nuha (2025) [13]	ESP32	NFC	GPS Neo-6M	Smartphone	Engine *cut-off*	Respons sistem	Tanpa RFID dan Telegram
Simanjuntak *et al.* (2025) [18]	ESP32 + FastAPI + Android	Login Aplikasi	GPS	Android	Kendali kendaraan	Fungsional sistem dan komunikasi IoT	Tanpa RFID/NFC
Auwali et al. (2023) [11]	ESP32-CAM	Tidak	Tidak	Telegram	Kontrol kendaraan	Respons sistem	Tanpa RFID dan GPS
Somantri *et al.* (2024) [19]	ESP32	Fingerprint	Tidak	IoT	Engine *cut-off*	Autentikasi fingerprint	Tanpa GPS
Juliarto *et al.* (2024) [20]	ESP32	Blynk	Tidak	Blynk	Kendali kendaraan	Respons kendali IoT	Tanpa GPS & RFID
Ashar dan Saputra (2021) [14]	ESP32 - CAM	RFID (e-KTP)	Tidak	Telegram	Tidak	autentikasi RFID dan notifikasi	Tanpa GPS
Penelitian ini	ESP32	RFID	GPS Neo-6M	Telegram	MOSFET	Error dan waktu respons	Uji keamanan masih terbatas

2. METODE PENELITIAN

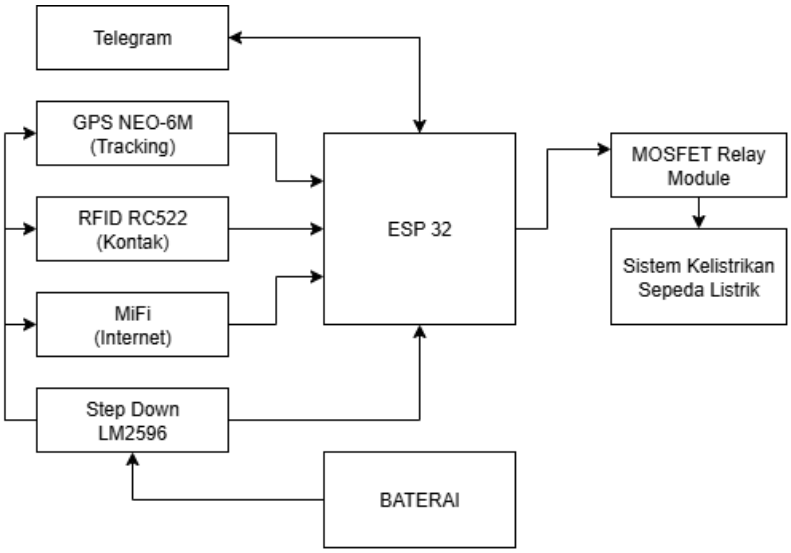
Penelitian Research and Development ini mencakup identifikasi kebutuhan, perancangan perangkat keras dan perangkat lunak, integrasi prototipe, pengujian, dan analisis. Sistem mengintegrasikan ESP32, RFID RC522, GPS Neo-6M, MOSFET, LM2596, MiFi, dan Telegram Bot. Pengujian meliputi kesalahan GPS, respons Telegram, autentikasi RFID,kondisi jaringan, serta kendali ON dan OFF.



Gambar 1. Flowchart Alur Penelitian

A. Arsitektur Sistem Keamanan

ESP32 berfungsi sebagai pusat kendali. RFID RC522 digunakan untuk autentikasi pengguna, GPS Neo-6M untuk memperoleh koordinat kendaraan, Telegram Bot untuk notifikasi dan kendali jarak jauh, serta MOSFET sebagai aktuator pemutus daya. Arsitektur sistem ditunjukkan pada Gambar 2.



Gambar 2. Diagram Blok Sistem

Saat diaktifkan, ESP32 menginisialisasi modul dan terhubung ke Telegram melalui Wi-Fi. Kartu terdaftar dapat mengaktifkan kendaraan, sedangkan kartu lain ditolak. GPS mengirim koordinat dan tautan Google Maps. Pengguna dapat memeriksa status dan lokasi serta menghubungkan atau memutus daya melalui MOSFET.

B. Perancangan Perangkat Keras

Perangkat dirakit di Laboratorium Teknik Elektro Universitas Muria Kudus dan diuji pada Mei-Juni 2026 di Kabupaten Kudus, Jawa Tengah. Pengujian GPS dilakukan saat kendaraan dalam kondisi diam di lingkungan terbuka. Tabel 2–4 menyajikan spesifikasi kendaraan, perangkat, dan koneksi pin, sedangkan Gambar 3 menunjukkan rangkaian.

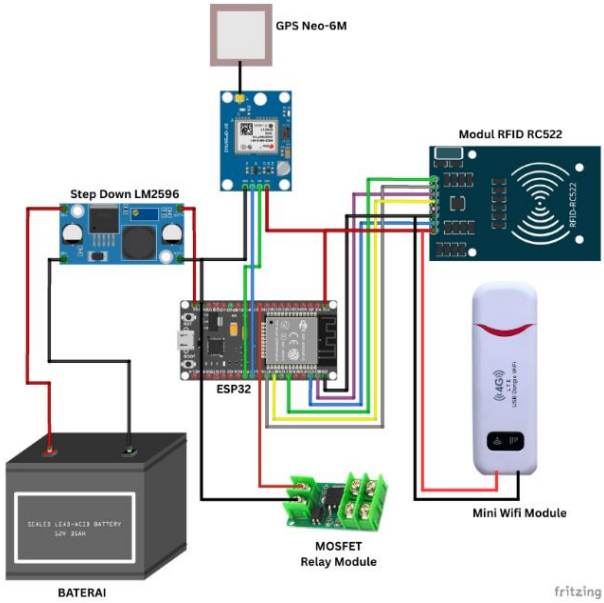
Tabel 2. Spesifikasi Kendaraan

No	Parameter	Keterangan
1	Jenis Kendaraan	Sepeda listrik
2	Tipe Kendaraan	U-Winfly D65
3	Tegangan dan Kapasitas Baterai	48 V / 12 Ah (untuk motor penggerak)
5	Daya Motor	600 W
6	Arus Kerja	±12,5 A
7	Posisi Pemasangan Sistem	Kompartemen bagian depan kendaraan, di bawah stang dan di atas dek kaki

Tabel 3. Spesifikasi Perangkat Penelitian

No	Komponen	Spesifikasi	Fungsi
1	ESP32 DevKit V1	Tegangan kerja 3,3 V, tegangan masukan melalui VIN 5 V, frekuensi clock hingga 240 MHz, Wi-Fi	Pengendali utama

No	Komponen	Spesifikasi	Fungsi
		2,4GHz IEEE 802.11 b/g/n	
2	GPS Neo-6M	Baud rate default 9600 bps, sensitivitas tracking hingga sekitar −161 dBm, akurasi posisi horizontal nominal sekitar 2,5 m pada kondisi optimal	Akuisisi koordinat
3	RFID RC522	Frekuensi kerja 13,56 MHz, tegangan kerja 3,3 V, jarak pembacaan tipikal hingga sekitar 5 cm bergantung kartu dan antena	Autentikasi
4	MOSFET IRF5305s	Logic-level MOSFET, dikendalikan logika 3,3 V dari GPIO ESP32; P-Channel MOSFET; VDS = −55 V; ID = 31 A	Memutus catu daya sistem kontrol
5	LM2596	Tegangan masukan sekitar 4,5–40 V DC, tegangan keluaran adjustable 1,25–37 V DC; pada sistem diatur menjadi 5 V	Penurun tegangan
6	Baterai	Tegangan nominal 12 V	Sumber daya sistem keamanan
7	MiFi	Operator Telkomsel, jaringan 4G LTE	Akses internet



Gambar 3. Wiring Perangkat Keras Sistem Keamanan

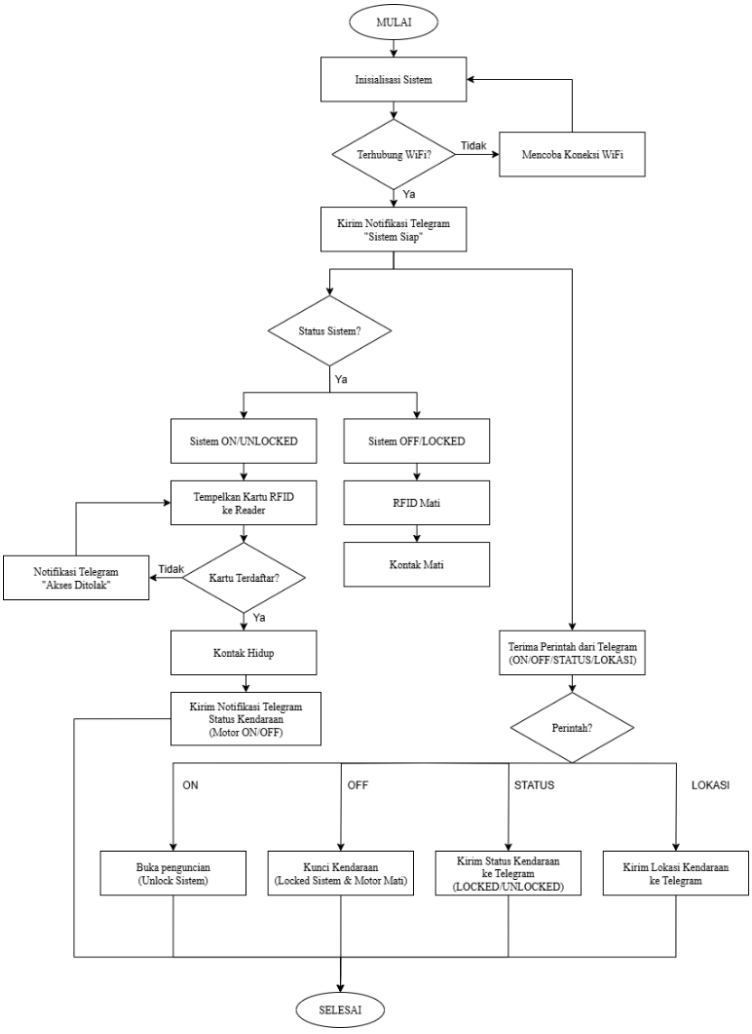
Tabel 4. Koneksi Pin

Perangkat	Pin Perangkat	Koneksi ESP32	Tegangan	Fungsi
GPS Neo-6M	TX	GPIO 16 (RX2)	Logika 3,3 V	Data GPS ke ESP32
GPS Neo-6M	RX	GPIO 17 (TX2)	Logika 3,3 V	Data ESP32 ke GPS
GPS Neo-6M	VCC	5 V / VIN	5 V	Catu daya modul GPS
GPS Neo-6M	GND	GND	0 V	Ground bersama
RFID RC522	SDA/SS	GPIO 5	Logika 3,3 V	Seleksi perangkat SPI
RFID RC522	SCK	GPIO 18	Logika 3,3 V	Clock SPI
RFID RC522	MOSI	GPIO 23	Logika 3,3 V	Data ESP32 ke RFID
RFID RC522	MISO	GPIO 19	Logika 3,3 V	Data RFID ke ESP32
RFID RC522	RST	GPIO 22	Logika 3,3 V	Reset modul RFID
RFID RC522	VCC/3.3 V	3V3 ESP32	3,3 V	Catu daya RFID RC522
RFID RC522	GND	GND	0 V	Ground bersama
MOSFET IRF5305s	IN/Gate	GPIO 4	Logika 3,3 V	Sinyal kendali *cut-off*
MOSFET IRF5305s	VCC/+	5 V	5 V	Catu daya modul
MOSFET IRF5305s	GND/−	GND	0 V	Ground bersama
LM2596	IN+	Positif baterai	12 V	Masukan positif step-down
LM2596	IN−	Negatif baterai	0 V	Masukan negatif/ground
LM2596	OUT+	VIN/5 V sistem	5 V	Keluaran step-down
LM2596	OUT−	GND sistem	0 V	Ground keluaran
ESP32 DevKit V1	VIN/5 V	OUT+ LM2596	5 V	Catu daya ESP32
ESP32 DevKit V1	GND	OUT− LM2596	0 V	Ground ESP32
ESP32 DevKit V1	3V3	VCC RFID RC522	3,3 V	Catu daya RFID RC522

Baterai utama 48 V menyuplai motor, sedangkan baterai 12 V terpisah menyuplai sistem keamanan melalui LM2596 5 V. ESP32 membaca GPS dan RFID, mengendalikan MOSFET, serta berkomunikasi melalui MiFi. Karena tegangan kerja mendekati batas MOSFET, penerapan operasional memerlukan margin tegangan lebih besar, proteksi lonjakan, *fuse*, dan *gate driver* yang sesuai.

C. Perancangan Perangkat Lunak

Perangkat lunak C++ dikembangkan pada Arduino IDE untuk mengelola GPS, RFID, MOSFET, Wi-Fi, dan Telegram. Setelah inisialisasi, sistem membaca kartu, menerima perintah, dan memperbarui lokasi. Kartu terdaftar mengaktifkan MOSFET. Kartu lain ditolak dan memicu notifikasi. Telegram digunakan untuk memeriksa status dan lokasi serta mengaktifkan atau menonaktifkan *cut-off*. Sistem memvalidasi chat ID, menginisialisasi ulang modul dan koneksi setelah restart, serta hanya mengirim lokasi ketika GPS memperoleh koordinat valid.



Gambar 4. Flowchart Perancangan Sistem Perangkat Lunak

Tabel 5. Daftar Perintah dan Respons Telegram Bot

Perintah	Fungsi	Respons sistem
/*locked*	Mengunci akses kendaraan	Status *locked*
/*unlocked*	Membuka akses terotorisasi	Status *unlocked*
/status	Membaca status kendaraan	*Locked*/*unlocked*
/lokasi	Meminta koordinat	Koordinat dan tautan peta
/off	Menonaktifkan MOSFET	Daya terputus
/on	Mengaktifkan MOSFET	Daya terhubung

Perintah /on dan /off dievaluasi saat koneksi internet tersedia.

D. Prosedur Pengujian Sistem

Pengujian sistem mencakup sebagai berikut.

1. Kesalahan posisi GPS terhadap koordinat pembanding Google Maps.
2. Waktu respons perintah Telegram.
3. Ketepatan keputusan dan waktu respons RFID.
4. Pengaruh kondisi jaringan.
5. Keberhasilan perubahan kondisi MOSFET melalui perintah ON dan OFF

Parameter dan indikator keberhasilan masing-masing pengujian disajikan pada Tabel 6.

Tabel 6. Parameter dan Indikator Keberhasilan Pengujian

No	Jenis Pengujian	Parameter yang Diukur	Indikator Keberhasilan
1	GPS Neo-6M	Selisih koordinat (m) terhadap Google Maps	GPS Neo-6M mampu memperoleh koordinat lokasi dan menampilkan lokasi kendaraan pada Google Maps.
2	Komunikasi ESP32–Telegram	Waktu respons (*delay*) pengiriman dan penerimaan pesan	Sistem mampu menerima perintah dan memberikan respons melalui Telegram tanpa kegagalan komunikasi pada pengujian yang dilakukan.
3	RFID RC522	Waktu respons autentikasi dan tingkat keberhasilan pembacaan UID	Sistem mampu menerima UID terdaftar dan menolak UID yang tidak terdaftar sesuai database.
4	Fitur *Cut-off*	Keberhasilan perubahan MOSFET melalui perintah ON dan OFF	MOSFET berubah sesuai perintah saat internet tersedia

Jaringan diuji pada kondisi baik, sedang, lemah, dan terputus berdasarkan RSSI. Operator Telkomsel dan Indosat diuji melalui MiFi 4G LTE di Kabupaten Kudus. Setiap

kombinasi operator dan RSSI diuji tujuh kali, lalu waktu respons dan keberhasilan komunikasi dianalisis secara deskriptif.

Tabel 7. Skenario Pengujian Berdasarkan Kondisi Jaringan

No.	Operator	Kondisi Jaringan	RSSI (dBm)	Perintah yang Diuji
1	Operator A	Baik	-58	/status, /lokasi, /off
2	Operator A	Sedang	-70	/status, /lokasi, /off
3	Operator A	Lemah	-90	/status, /lokasi, /off
4	Operator A	Terputus	-	/status, /lokasi, /off
5	Operator B	Baik	-65	/status, /lokasi, /off
6	Operator B	Sedang	-74	/status, /lokasi, /off
7	Operator B	Lemah	-79	/status, /lokasi, /off
8	Operator B	Terputus	-	/status, /lokasi, /off

Kualitas sinyal dikelompokkan menjadi baik (RSSI > −67 dBm), sedang (−67 sampai −79 dBm), dan lemah (< −80 dBm) berdasarkan pedoman TP-Link [25]. GPS dan RFID masing-masing diuji tujuh kali. Empat perintah Telegram diuji tujuh kali sehingga menghasilkan 28 data, sedangkan perintah OFF diuji pada sepuluh lokasi.

Data GPS diringkas menggunakan rata-rata, median, simpangan baku, minimum, dan maksimum. Telegram dan RFID dievaluasi berdasarkan waktu respons dan ketepatan keputusan, sedangkan *cut-off* dinilai dari perubahan kondisi MOSFET. Kesalahan posisi GPS dihitung dengan persamaan Haversine:

$$a = sin^2\left(\frac{\Delta\varphi}{2}\right) + cos\,(\varphi_1)cos\,(\varphi_2)sin^2\left(\frac{\Delta\lambda}{2}\right) \quad (1)$$

$$d = 2R\arctan 2\left(\sqrt{a}\sqrt{1-a}\right) \quad (2)$$

Keterangan:

d= jarak kesalahan posisi (m);

R= jari-jari bumi, yaitu 6.371.000 m;

φ_1= latitude koordinat GPS dalam radian;

φ_2= latitude koordinat referensi dalam radian;

$\Delta\varphi$= selisih *latitude* dalam radian;

$\Delta\lambda$= selisih *longitude* dalam radian.

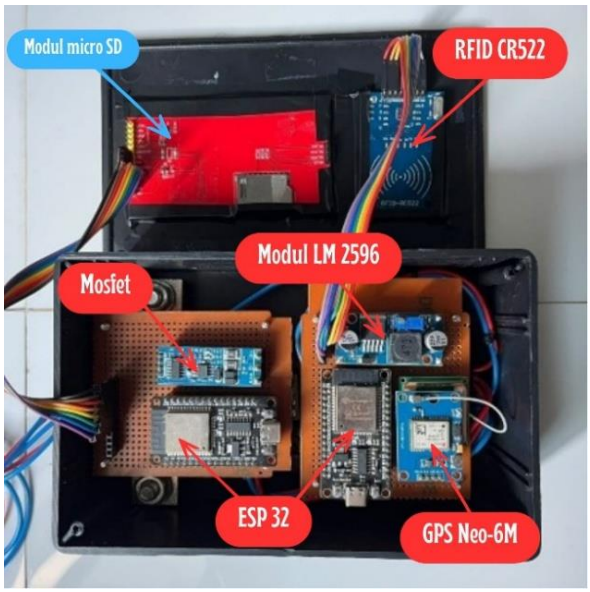
Koordinat pembanding diambil dari pin Google Maps pada telepon pintar di setiap lokasi. Nilainya digunakan dalam persamaan Haversine, tetapi tidak diperlakukan sebagai koordinat pembanding.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan implementasi dan pengujian autentikasi RFID, pelacakan GPS, komunikasi Telegram, dan *cut-off* pada kendaraan listrik ringan.

A. Implementasi Perangkat Keras

ESP32 dipilih karena menyediakan Wi-Fi, UART, dan SPI. RFID RC522 berfungsi sebagai autentikasi lokal, GPS Neo-6M memperoleh koordinat, MOSFET menjalankan *cut-off*, dan LM2596 menurunkan tegangan 12 V menjadi 5 V. Prototipe belum memiliki fuse dan proteksi polaritas sehingga keduanya perlu ditambahkan sebelum penerapan operasional. Hasil implementasi perangkat keras ditunjukkan pada Gambar 5.



Gambar 5. Implementasi perangkat keras

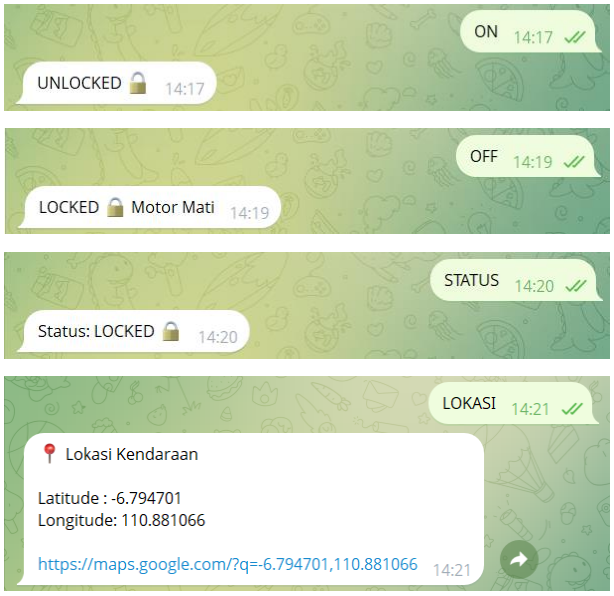
Tabel 8. Spesifikasi Fisik dan Elektrik Implementasi Perangkat

Parameter	Spesifikasi
Dimensi perangkat	20 × 15 × 8 cm
Tipe MOSFET	IRF5305s
Tegangan beban	48 V
Arus beban	±12,5 A
Posisi pemasangan	Kompartemen bagian depan kendaraan, di bawah stang dan di atas dek kaki
Tegangan baterai	48 V
Kapasitas baterai	12 Ah

Seluruh komponen terhubung dan berfungsi. ESP32 membaca RFID dan GPS, mengendalikan MOSFET, serta berkomunikasi melalui MiFi. Sejalan dengan Himawan et al. [15], prototipe mengintegrasikan autentikasi, pelacakan, notifikasi, dan kendali kelistrikan.

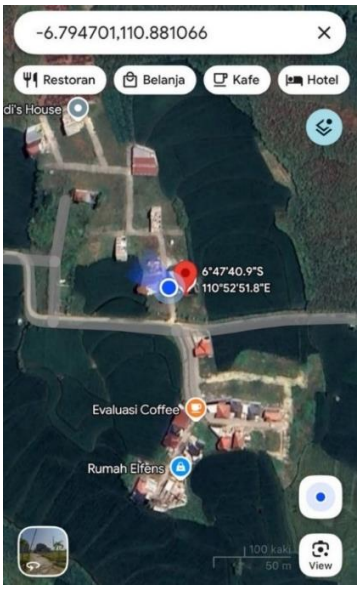
B. Implementasi Perangkat Lunak

Program pada ESP32 mengelola autentikasi RFID, GPS, Telegram, dan *cut-off*.



Gambar 6. Respons Instruksi Telegram

ESP32 memeriksa Telegram secara berkala dan hanya memproses chat ID terdaftar. Dalam status *locked*, RFID tidak dapat mengaktifkan kendaraan sebelum pemilik membuka akses melalui Telegram. Perintah tidak dikenal ditolak. Program memiliki prosedur reconnect yang mempertahankan status terakhir, tetapi keberhasilannya belum diuji secara kuantitatif. Sistem tidak mengirim koordinat lama ketika data GPS belum valid. Kartu terdaftar mengaktifkan MOSFET, sedangkan kartu lain ditolak dan memicu notifikasi. Sistem juga mengirim tautan Google Maps dan menjalankan *cut-off*.



Gambar 7. Tampilan Tautan LOKASI

(Sumber : Google Maps) [10].

Tautan Google Maps pada Gambar 7 menampilkan perkiraan lokasi dari koordinat GPS Neo-6M.

C. Pengujian Akurasi GPS Neo-6M

GPS diuji tujuh kali pada lokasi dan waktu berbeda. Evaluasi awal ini belum cukup untuk menyimpulkan keandalan umum. Kesalahan dihitung dengan Haversine antara koordinat GPS Neo-6M dan Google Maps.

Tabel 9. Hasil pengujian selisih jarak dengan Google Maps

Uji Coba	Koordinat GPS Neo-6M		Koordinat Google Maps		Hasil Selisih (Meter)
	Latitude	*Longitude*	*Latitude*	*Longitude*	
1	-6.7947010	110.8810660	-6.7946940	110.8810000	7,33
2	-6.7949757	110.8784930	-6.7948962	110.8785366	10,07
3	-6.8046900	110.8742510	-6.8047412	110.8741931	8,30
4	-6.7813430	110.8593570	-6.7813854	110.8593008	8,00
5	-6.8073600	110.8420900	-6.8073735	110.8420693	3,20
6	-6.8179520	110.8382360	-6.8179770	110.8382052	4,30
7	-6.8152300	110.8498200	-6.8153121	110.8497156	15,20
Rata-Rata					8,05

Tabel 9 menunjukkan rata-rata kesalahan 8,05 m. GPS dapat memperkirakan lokasi pada tingkat area, tetapi kesalahan maksimum 15,20 m belum memadai untuk membedakan kendaraan pada ruang parkir yang berdekatan.

Variasi kesalahan dipengaruhi lingkungan, geometri satelit, multipath, atmosfer, orientasi antena, jumlah satelit, dan kualitas sinyal. Delapan satelit terdeteksi, tetapi GDOP dan perubahan kondisi penerimaan tidak dicatat sehingga pengaruh setiap faktor tidak dapat dipisahkan. Temuan ini sejalan dengan Maesa dan Hartono [8].



Gambar 8. Grafik Hasil Selisih Jarak antara GPS Neo-6M dengan Google Maps

Tabel 10. Kondisi dan Parameter Pengujian GPS

Parameter	**Keterangan**
Kondisi pengujian	Terbuka
Kondisi kendaraan	Diam
Lama GPS memperoleh posisi	70 detik
Jumlah satelit	8 satelit
Waktu pengambilan	22.00
Perangkat Google Maps	Iphone 13
Koordinat referensi	Google Maps pada titik pengujian
Ketelitian perangkat referensi	3,20-15,20 meter

D. Pengujian Waktu Respons Instruksi Telegram

Waktu respons diukur sejak perintah dikirim hingga respons diterima. Empat perintah, yaitu *locked*, *unlocked*, lokasi, dan status, masing-masing diuji tujuh kali sehingga menghasilkan 28 data disajikan pada Tabel 11.

Tabel 11. Hasil Pengukuran Delay Instruksi dan Respons Telegram

Uji Coba	Respons Waktu (s)			
	LOCKED	***UNLOCKED***	**STATUS**	**LOKASI**
1	2,31	3,08	2,76	5,86
2	2,13	2,76	1,74	4,31
3	1,58	2,63	2,68	2,01
4	2,33	4,29	6,03	14,82
5	1,91	1,83	15,20	1,89
6	10,22	2,65	2,40	2,56
7	1,75	14,43	3,43	2,70
Rata-Rata	**3,18**	**4,52**	**4,89**	**4,88**
Rata-Rata Keseluruhan	**4,37**			

Rata-rata respons Telegram mencapai 4,37 detik. Nilai ini memadai untuk kendali jarak jauh yang tidak menuntut respons seketika, tetapi maksimum 15,20 detik menunjukkan bahwa sistem tidak real-time. Seluruh perintah berhasil diproses ketika internet tersedia. Pengukuran memakai stopwatch telepon pintar dan masih dipengaruhi reaksi pengamat. Penelitian lanjutan perlu menggunakan timestamp otomatis pada telepon dan ESP32. Telegram sBot API menggunakan HTTP polling sekitar 60 ms. Respons dipengaruhi internet, Wi-Fi MiFi, pertukaran paket, server Telegram, dan waktu eksekusi ESP32.

Tabel 12. Statistik Waktu Respons Telegram

Perintah	Rata-rata	Median	Simpangan baku	Minimum	Maksimum
LOCKED	3,18 s	2,13 s	3,12 s	1,58 s	10,22 s
UNLOCKED	4,52 s	2,76 s	4,43 s	1,83 s	14,43 s
STATUS	4,89 s	2,76 s	4,75 s	1,74 s	15,20 s
LOKASI	4,88 s	2,70 s	4,61 s	1,89 s	14,82 s
Keseluruhan	**4,37 s**	**2,67 s**	**4,09 s**	**1,58 s**	15,20 s

Hasil ini merupakan respons komunikasi berbasis jaringan, bukan kinerja real-time. Tabel 7 memuat target RSSI, sedangkan Tabel 13 memuat nilai aktual yang berubah mengikuti jaringan seluler.

Tabel 13. Hasil Pengujian Telegram Berdasarkan Kondisi Jaringan

Operator	Kondisi Jaringan	RSSI (dBm)	Rata-rata Respons (s)	Keberhasilan Perintah	Keterangan
Operator A	Baik	-55	1,58	10/10	Ada koneksi
Operator A	Sedang	-70	2,86	10/10	Ada koneksi
Operator A	Lemah	-82	6,38	10/10	Ada koneksi
Operator A	Terputus	-	–	0/10	Tidak ada koneksi
Operator B	Baik	-62	2,14	10/10	Ada koneksi
Operator B	Sedang	-72	3,74	10/10	Ada koneksi
Operator B	Lemah	-88	8,47	9/10	Ada koneksi
Operator B	Terputus	-	–	0/10	Tidak ada koneksi

Tabel 13 menunjukkan bahwa sinyal lebih baik menghasilkan respons lebih stabil, sedangkan sinyal lemah meningkatkan variasi. Komunikasi gagal ketika internet terputus. Perbedaan antaroperator juga menunjukkan pengaruh layanan jaringan di lokasi pengujian.

Tabel 14. Kondisi dan Parameter Pengukuran Waktu Respons Sistem

Parameter	Keterangan
Alat pencatat waktu	Stopwatch pada smartphone
Ketelitian pengukuran	0,01 detik
Titik awal pengukuran	Saat perintah dikirim melalui Telegram
Titik akhir pengukuran	Saat respons diterima atau tindakan sistem dijalankan
Interval polling Telegram	60 ms
Operator jaringan	Telkomsel
Jenis jaringan	4G LTE
Kondisi sinyal	Baik
Kekuatan sinyal (RSSI)	-68 dBm
Perintah /lokasi	Waktu respons mencakup selang waktu sejak pengguna mengirim perintah melalui Telegram hingga sistem memberikan respons sesuai fungsi yang dijalankan.

E. Pengujian Sistem Autentikasi RFID

RFID diuji tujuh kali dengan kartu terdaftar dan tidak terdaftar untuk menilai ketepatan keputusan serta waktu respons berdasarkan UID ditunjukkan pada Tabel 15.

Tabel 15. Hasil Pengujian Autentikasi Kartu RFID

Uji Coba	UID Kartu	UID Terdaftar	Status Kartu	Status Kartu	Waktu Respons (s)
1	49 FE ** **	Ya	Terdaftar	Akses diterima	1,49
2	49 FE ** **	Ya	Terdaftar	Akses diterima	3,02
3	3B 45 ** **	Tidak	Tidak terdaftar	Akses ditolak	2,64
4	49 FE ** **	Ya	Terdaftar	Akses diterima	2,89
5	49 FE ** **	Ya	Terdaftar	Akses diterima	3,45
6	3B 45 ** **	Tidak	Tidak terdaftar	Akses ditolak	1,76
7	3B 45 ** **	Tidak	Tidak terdaftar	Akses ditolak	2,06
Rata-Rata					**2,47**

Seluruh tujuh keputusan autentikasi benar. Rata-rata respons mencapai 2,47 detik, median 2,64 detik, simpangan baku 0,72 detik, dan rentang 1,49–3,45 detik. Jarak, orientasi kartu, dan pemrosesan ESP32 dapat memengaruhi variasi. Pengujian hanya memakai dua UID dan belum mencakup variasi jarak, orientasi, kerusakan kartu, duplikasi UID, serangan replay, atau banyak kartu. Hasil ini membuktikan fungsi autentikasi dasar, bukan keamanan RFID secara menyeluruh.

F. Pengujian Fitur *Cut-off*

Fitur *cut-off* diuji untuk menilai kemampuan MOSFET menghubungkan dan memutus daya melalui Telegram disajikan pada Tabel 16.

Tabel 16. Hasil Pengujian Keberhasilan Fitur *Cut-off*

Uji Coba	Lokasi Perangkat		Lokasi Kendaraan		Selisih (Meter)	Perintah Telegram	Kondisi MOSFET
	Latitude	*Longitude*	*Latitude*	*Longitude*			
1	-6.7946661	110.8809888	-6.7948962	110.8785366	271,96	OFF	Tidak Aktif
2	-6.7946661	110.8809888	-6.8015402	110.8789044	798,26	OFF	Tidak Aktif
3	-6.7946661	110.8809888	-6.8047412	110.8741931	1348,36	OFF	Tidak Aktif
4	-6.7946661	110.8809888	-6.7836333	110.8659141	2067,73	OFF	Tidak Aktif
5	-6.7946661	110.8809888	-6.7813854	110.8593008	2813,42	OFF	Tidak Aktif
6	-6.7946661	110.8809888	-6.8073735	110.8420693	4523,55	OFF	Tidak Aktif
7	-6.7946661	110.8809888	-6.8179770	110.8382052	5388,22	OFF	Tidak Aktif
8	-6.7946661	110.8809888	-6.8268668	110.8387420	5880,28	OFF	Tidak Aktif

Uji Coba	Lokasi Perangkat		Lokasi Kendaraan		Selisih (Meter)	Perintah Telegram	Kondisi MOSFET
	Latitude	*Longitude*	*Latitude*	*Longitude*			
9	-6.7946661	110.8809888	-6.8153121	110.8497156	4146,45	OFF	Tidak Aktif
10	-6.7946661	110.8809888	-6.8038746	110.8617738	2355,75	OFF	Tidak Aktif

Perintah OFF berhasil pada sepuluh lokasi selama internet tersedia, dengan jarak maksimum 5,88 km. Jarak fisik bukan batas utama karena komunikasi berlangsung melalui internet. Sistem belum memakai kecepatan sebagai syarat OFF sehingga pemutusan perlu ditunda sampai kendaraan berhenti atau berada di bawah batas aman.

Tabel 17. Pengujian Lanjutan Fungsi *Cut-off*

No.	Kondisi Pengujian	Perintah	Waktu Respons (s)	Tegangan Sebelum (V)	Tegangan Setelah (V)	Arus Beban (A)	Hasil
1	Internet aktif	OFF	3,24	50,8	50,6	0,00	Berhasil
2	Internet aktif	ON	2,87	50,6	50,5	12,1	Berhasil
3	Pengulangan lokasi sama	OFF	3,51	50,7	50,5	0,00	Berhasil
4	Pengulangan lokasi sama	ON	3,08	50,5	50,4	12,3	Berhasil
5	Internet terputus	OFF	-	50,7	50,7	12,2	Gagal
6	Akun tidak sah	OFF	-	50,7	50,7	12,2	Ditolak
7	Kendaraan bergerak	OFF	3,76	50,9	50,6	0,00	Berhasil

Tabel 17 menunjukkan bahwa OFF gagal saat internet terputus dan akun tidak sah berhasil ditolak. Namun, daya masih dapat diputus ketika kendaraan bergerak. Prototipe belum layak digunakan secara operasional sebelum dilengkapi interlock berbasis kecepatan atau status kendaraan.

G. Pengujian Konsumsi Daya dan Stabilitas Sistem

Pengukuran dilakukan saat standby, RFID aktif, GPS aktif, Telegram aktif, serta MOSFET OFF dan ON disajikan pada Tabel 18.

Tabel 18. Hasil Pengujian Konsumsi Daya Sistem

Kondisi	Tegangan (V)	Arus (A)	Daya (W)
Standby	50,8	0,18	9,14
RFID aktif	50,7	0,22	11,15
GPS aktif	50,6	0,28	14,17
Telegram aktif	50,5	0,32	16,16
MOSFET OFF	50,7	0,31	15,72
MOSFET ON	50,6	0,35	17,71

Arus pada Tabel 18 diukur dari baterai utama 48 V dan daya dihitung dengan $P = V \times I$. Karena itu, nilai tersebut menggambarkan daya rangkaian utama, bukan konsumsi khusus sistem keamanan. Sistem keamanan memakai baterai 12 V terpisah yang diturunkan menjadi 5 V melalui LM2596. Konsumsi khusus sistem keamanan belum diketahui karena sumber 12 V belum diukur terpisah.

Tabel 19. Hasil Pengujian Stabilitas Sistem

Durasi Pengujian	Kondisi Sistem	Gangguan	Keterangan
24 jam	Normal	Tidak ada	Sistem Stabil

Sistem beroperasi selama 24 jam tanpa reset atau gangguan yang teramati. Namun, kehilangan koneksi, kegagalan modul, jumlah perintah, dan interval observasi belum dicatat secara kuantitatif. Hasil ini belum membuktikan keandalan jangka panjang.

4. PERBANDINGAN DENGAN PENELITIAN TERDAHULU

Tabel 20. Perbandingan dengan penelitian terdahulu

Parameter	Penelitian ini	Penelitian terdahulu	Analisis
Kesalahan/akurasi GPS	Rata-rata error 8,05 m	Himawan et al. (2022) [15]: 8,348 m; Maesa dan Hartono (2025) [8]: error 24,78 m (ruang terbuka) dan 27,94 m (ruang tertutup)	Error GPS mendekati Himawan et al. [15] dan lebih kecil dibanding Maesa dan Hartono [8], dengan perbedaan kondisi pengujian.
Respons Telegram	Rata-rata 4,37 s, rentang 1,58–15,20 s	Kholik et al. (2022) [17]: rata-rata delay perintah Engine ON/OFF 5,01 s	Respons lebih cepat 0,64 s, tetapi masih dipengaruhi kualitas jaringan.
Respons RFID	Rata-rata 2,47 s	Himawan et al. (2022) [15]: 0,31	Respons RFID lebih lambat

Parameter	Penelitian ini	Penelitian terdahulu	Analisis
		s (mati→hidup) dan 0,28 s (hidup→mati)	dan pengujian masih terbatas pada jumlah UID.
Cut-off	Perintah /off berhasil 10/10 pengujian	Kholik et al. (2022) [17]: perintah Engine ON/OFF diuji dengan rata-rata delay 5,01 s	Fungsi ON dan OFF berhasil seluruhnya diuji secara kuantitatif.
Keamanan akses	Kartu terdaftar diterima dan kartu tidak terdaftar ditolak pada 7 pengujian	Himawan et al. (2022) [15]: RFID digunakan untuk menghidupkan/mematikan kendaraan dan sebagai pengganti kunci ganda	Autentikasi berhasil, tetapi pengujian UID dan keamanan akses masih terbatas.

Tabel 20 menunjukkan bahwa kesalahan GPS 8,05 m mendekati Himawan et al. [15] sebesar 8,348 m dan lebih kecil daripada Maesa dan Hartono [8], yaitu 24,78 m di ruang terbuka dan 27,94 m di ruang tertutup. Perbandingan dibatasi oleh perbedaan perangkat, lingkungan, dan prosedur. Respons Telegram 4,37 detik lebih rendah daripada Kholik et al. [17] sebesar 5,01 detik, tetapi maksimum 15,20 detik menegaskan pengaruh jaringan. Respons RFID 2,47 detik lebih lambat daripada Himawan et al. [15], yaitu 0,31 dan 0,28 detik, yang dapat dipengaruhi konfigurasi dan integrasi sistem. OFF berhasil pada sepuluh lokasi, tetapi variasi beban, keamanan komunikasi, dan operasi jangka panjang belum diuji. Dengan demikian, penelitian ini membuktikan fungsi dasar prototipe, bukan keamanan atau keandalan operasional secara menyeluruh.

5. KETERBATASAN PENELITIAN

Penelitian terbatas pada tujuh pengujian GPS, tujuh pengujian tiap perintah Telegram, dan dua UID RFID. Evaluasi jaringan berdasarkan RSSI dan operator belum mencakup latensi, jitter, throughput, atau packet loss. Pengaruh GDOP, cuaca, dan multipath terhadap GPS juga belum diukur terpisah. Pengujian ON/OFF, internet terputus, akun tidak sah, sumber daya, dan stabilitas 24 jam masih terbatas. Sistem belum diuji terhadap duplikasi UID, kehilangan GPS, restart, variasi beban, dan serangan token Telegram. Interlock yang mencegah *cut-off* saat kendaraan bergerak juga belum tersedia.

6. KESIMPULAN

Prototipe berbasis ESP32 berhasil mengintegrasikan RFID, GPS, Telegram, dan *cut-off*. Tujuh pengujian GPS menghasilkan rata-rata kesalahan 8,05 m, median 8,00 m,

simpangan baku 3,94 m, dan rentang 3,20–15,20 m. Hasil ini memadai untuk memperkirakan area, tetapi belum untuk membedakan ruang parkir yang berdekatan.

Empat perintah Telegram menghasilkan rata-rata respons 4,37 detik dengan rentang 1,58–15,20 detik. Sistem menerima kartu terdaftar dan menolak kartu tidak terdaftar pada tujuh percobaan, dengan rata-rata respons RFID 2,47 detik. Perintah ON dan OFF berfungsi saat internet tersedia, dan akun tidak terotorisasi ditolak.

Sistem beroperasi selama 24 jam tanpa gangguan yang teramati, tetapi jumlah pengujian, evaluasi jaringan, dan pengukuran konsumsi khusus sistem keamanan masih terbatas. Prototipe belum layak diterapkan secara operasional karena *cut-off* dapat bekerja saat kendaraan bergerak. Penelitian lanjutan perlu memperbanyak pengujian, menambah variasi UID, mengevaluasi keamanan komunikasi dan daya, serta menerapkan interlock berbasis kecepatan.

DAFTAR PUSTAKA

[1] Kementerian Perindustrian Republik Indonesia, "LG Keluar Konsorsium Baterai EV, Target dan Jadwal Pengurangan Emisi Karbon Tidak Terpengaruh," Apr. 24, 2025. [Online]. Available: https://ilmate.kemenperin.go.id/publikasi/informasi-industri/lg-keluar-konsorsium-baterai-ev-target-dan-jadwal-pengurangan-emisi-karbon-tidak-terpengaruh. [Accessed: Jul. 22, 2026]

[2] Pusat Informasi Kriminal Nasional (Pusiknas) Bareskrim Polri, "Curanmor dan Pasar Gelap Kendaraan Curian," *Pusiknas Bareskrim Polri*, May 26, 2026. [Online]. Available:https://pusiknas.polri.go.id/detail_artikel/curanmor_dan_pasar_gelap_kendaraan_curian. [Accessed: Jul. 25, 2026].

[3] D. M. Yulanto and H. Iskandar, "Studi Analisis Perkembangan Teknologi Kendaraan Listrik Hibrida," *Journal of Automotive Technology Vocational Education*, vol. 2, no. 1, pp. 31–44, 2021, doi: 10.31316/jatve.v2i1.1488.

[4] S. Gulo, M. F. S. Hutabarat, and M. Pangaribuan, "Perancangan Sistem Keamanan Kendaraan Roda Dua Menggunakan RFID Diprogram," *Jurnal Sains dan Teknologi ISTP*, vol. 20, no. 2, pp. 211–220, 2024, doi: 10.59637/jsti.v20i02.373.

[5] M. R. Arif Cahyono, I. Mariza, and Wirawan, "Electric Bike Monitoring and Controlling System Based on *Internet of Things*," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 11, no. 1, pp. 53–60, 2022, doi: 10.22146/jnteti.v11i1.3183.

[6] E. Irawan and A. Muzakir, "Sistem Pengendali Keamanan Sepeda Motor Berbasis IoT (*Internet of Things*) Menggunakan Smartphone Android," *Journal of Information Technology Ampera*, vol. 3, no. 2, pp. 148–158, 2022, doi: 10.51519/journalita.volume3.isssue2.year2022.page148-158.

[7] M. M. Matsuani, "Analisis Efektifitas Pengendalian Sistem Sepeda Listrik Menggunakan GPS Tracker Berbasis Aplikasi Android," *J. IPTEK*, vol. 7, no. 1, pp. 1–8, 2023, doi: 10.31543/jii.v7i1.199.

[8] Fernando Maesa and H. Hartono, "Rancang Bangun Sistem Kontrol dan Monitoring Keamanan Sepeda Motor Berbasis IoT dengan Modul GPS Neo-6M dan Sensor Getar SW-420," *J. SURYA Tek.*, vol. 12, no. 1, pp. 37–43, 2025, doi: 10.37859/jst.v12i1.8532.

[9] B. C. Wibowo, "Prototype of Flood Early Warning System (EWS) Using Telegram Broadcast Message Notification," *J. Media Elektr.*, vol. 21, no. 2, pp. 52–62, 2024, doi: 10.59562/metrik.v21i2.1814.

[10] Google Maps, "Ngembalrejo, Ngembal Rejo, Kabupaten Kudus, Jawa Tengah," 2026, [Online]. Available: https://maps.google.com/?q=-6.794701,110.881066

[11] G. R. Auwali, A. Ahfas, and S. D. Ayuni, "Alat Kontrol dan Pengaman Sepeda Motor Menggunakan ESP32-CAM Berbasis Telegram untuk Meminimalisasi Pencurian," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 3, no. 2, pp. 219–229, 2023, doi: 10.57152/malcom.v3i2.923.

[12] L. A. Prasety, I. Himawan, and R. A. Sihombing, "Sistem Deteksi Dini dan Pelacakan Pencurian Kendaraan Bermotor Menggunakan GPS Neo-6M dan Platform Android," *Jurnal Rekayasa Sistem Informasi dan Teknologi*, vol. 3, no. 4, pp. 550–558, 2026, doi: 10.70248/jrsit.v3i4.3522.

[13] M. R. L. Nuha, "Rancang Bangun Sistem Keamanan Sepeda Motor dengan Engine Cut Off, GPS, dan Kendali NFC Smartphone," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 3S1, 2025, doi: 10.23960/jitet.v13i3S1.7589.

[14] A. A. Ashar and D. H. R. Saputra, "Design and Build a Safe Security System Using RFID With e-KTP as a Tag and Monitoring With IoT-Based ESP32-CAM With Telegram Notifications," *Indonesian Journal of Innovation Studies*, vol. 13, 2021, doi: 10.21070/ijins.v13i.527.

[15] A. Himawan, T. Rismawan, and S. Suhardi, "Sistem Keamanan Sepeda Motor Menggunakan GPS, RFID Dan Pembatas Kecepatan Dengan Arduino Uno Berbasis

IoT," *Coding: Jurnal Komputer dan Aplikasi*, vol. 10, no. 3, pp. 399–410, 2022, doi: 10.26418/coding.v10i03.55398.

[16] H. Isyanto, H. Muchtar, R. Rasma, and A. R. Dinata, "Design of Security System Device for Motorized Vehicles through the Telegram Messenger Application and Updating GPS Locations on Smartphones in Real Time with IoT-based Smart Vehicles," *Journal of Electrical Technology UMY*, vol. 6, no. 2, pp. 67–76, 2022, doi: 10.18196/jet.v6i2.16182.

[17] A. Kholik, I. Ibrahim, and R. Rahmadewi, "Sistem *Internet of Things* dan Transmisi Data Menggunakan Aplikasi Telegram Pada Sistem Keamanan Sepeda Motor," *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, vol. 7, no. 1, pp. 99–111, 2022, doi: 10.30998/string.v7i1.13877.

[18] N. P. Simanjuntak, M. A. Rahman, A. N. Pratama, S. Stelyven, and A. Yulianto, "Perancangan dan Implementasi Sistem Keamanan Kendaraan Berbasis IoT Menggunakan ESP32, FastAPI, dan Aplikasi Android," *Telcomatics*, vol. 10, no. 1, pp. 73–81, 2025, doi: 10.37253/telcomatics.v10i1.10870.

[19] S. Somantri, G. P. Insany, and R. Ryansyah, "Development Of A Motor Vehicle Security System Using Fingerprint Technology With An *Internet of Things* Based Prototype Method," *G-Tech: Jurnal Teknologi Terapan*, vol. 8, no. 1, pp. 593–602, 2024, doi: 10.33379/gtech.v8i1.3879.

[20] M. Juliarto, R. A. Nityasa, and A. D. F. Aditama, "Perancangan Keamanan Kendaraan Tanpa Kunci Dengan Menggunakan ESP32 dan Aplikasi BLYNK Berbasis IoT," *V-MAC (Virtual of Mechanical Engineering Article)*, vol. 9, no. 1, 2024, doi: 10.36526/v-mac.v9i1.3653.

[21] G. P. N. Hakim, M. H. I. Hajar, A. Firdausi, and E. Ramadhan, "Benchmarking in Microcontroller Development Board Power Consumption For Low Power IoT WSN Application," *Jurnal Teknologi Elektro*, vol. 13, no. 1, pp. 25–28, 2022, doi: 10.22441/jte.2022.v13i1.005.

[22] D. Cornei, C. Foșalău, and L. Cornei, "A Study Regarding Power Consumption of an IoT Node for Image Retrieval and Its Optimization," *Buletinul Institutului Politehnic din Iași, Section Electrotechnics, Energetics, Electronics*, vol. 69 (73), no. 1, pp. 61–84, 2023, doi: 10.2478/bipie-2023-0004.

[23] Y. Yang, J. Wang, P. Liu, A. Fu, and Y. Zhang, "Uncovering Access Token Security Flaws In Multiuser Scenario Of Smart Home Platforms," *IEEE Internet of*

Things Journal, vol. 11, no. 22, pp. 36841–36857, 2024, doi: 10.1109/JIOT.2024.3429417.

[24] Z. W. Rohdyawan, M. I. N. Hakim, R. Pratindy, and M. R. Tsani, "IoT-Based Dual-Sensor Vehicle Security System Using Piezoelectric And Glass-Break Detectors With GPS Tracking: Design And Performance Evaluation," *Journal of Vocational, Informatics and Computer Education*, vol. 4, no. 1, pp. 76–88, 2026, doi: 10.66053/voice.v4i1.421.

[25] TP-Link, "How To Improve Your Wireless Signal Strength," *TP-Link Technologies Co., Ltd.* [Online]. Available: https://www.tp-link.com/support/faq/. [Accessed: Jul. 25, 2026].