

RANCANG BANGUN KEAMANAN SEPEDA MOTOR IOT DENGAN BIOMETRIK, GPS, DAN KENDALI KUNCI STANG VIA SMARTPHONE

Ade Kholik Prasetya^{1*}, Anton Brevia Yunanda², Mochamad Sidqon³, Agung Kridoyono⁴

^{1,2}Teknik Informatika, Universitas 17 Agustus 1945 Surabaya, Jl. Semolowaru No.45, Menur Pumpungan, Kec. Sukolilo, Surabaya, Jawa Timur, Indonesia.

Keywords:

Autentikasi Biometrik
ESP32
GPS Tracking
Internet of Things (IoT)
Keamanan Sepeda Motor.

Correspondent Email:

adekholikprasetya12@gmail.com
antonbrevia@untag-sby.ac.id
sidqon@untag-sby.ac.id
akridoyono@untag-sby.ac.id

Abstrak. Meningkatnya kasus pencurian sepeda motor menunjukkan bahwa sistem keamanan konvensional seperti kunci kontak manual dan kunci stang mekanik tidak lagi efektif. Penelitian ini merancang dan mengimplementasikan sistem keamanan sepeda motor berbasis *Internet of Things (IoT)* yang mengintegrasikan autentikasi biometrik, pelacakan GPS, dan kontrol kunci stang otomatis. Autentikasi dilakukan menggunakan sensor sidik jari pada smartphone, sementara pelacakan lokasi kendaraan menggunakan modul GPS Neo-6M. Mekanisme penguncian stang dikendalikan oleh aktuator solenoid yang terhubung ke mikrokontroler ESP32. Seluruh sistem dioperasikan melalui aplikasi smartphone berbasis Kodular dan dilengkapi dengan antarmuka web lokal serta notifikasi Telegram. ESP32 berperan sebagai pusat kendali sistem dengan dukungan koneksi Bluetooth dan WiFi, serta berkomunikasi dengan layanan cloud ThingSpeak untuk penyimpanan data. Pengguna dapat mengaktifkan atau menonaktifkan motor serta mengontrol kunci stang melalui perintah suara atau sentuhan. Pengujian menunjukkan sistem mampu mengenali pengguna dengan cepat, mengontrol kunci stang secara otomatis, serta mendeteksi dan memberi notifikasi ketika terjadi pergerakan mencurigakan. Hasilnya, sistem ini dinyatakan efektif dan layak digunakan sebagai solusi keamanan sepeda motor berbasis IoT yang praktis dan inovatif.



Copyright © [JITET](http://www.jitet.org) (Jurnal Informatika dan Teknik Elektro Terapan). This article is an open access article distributed under terms and conditions of the Creative Commons Attribution (CC BY NC)

Abstract. The increasing number of motorcycle theft cases indicates that conventional security systems such as manual ignition keys and mechanical handlebar locks are no longer effective. This study designs and implements a motorcycle security system based on the Internet of Things (IoT), integrating biometric authentication, GPS tracking, and automatic handlebar lock control. Authentication is performed using a fingerprint sensor on a smartphone, while vehicle tracking utilizes the Neo-6M GPS module. The handlebar locking mechanism is controlled by a solenoid actuator connected to an ESP32 microcontroller. The entire system is operated via a smartphone application built with Kodular, supported by a local web interface and Telegram notifications. The ESP32 functions as the system controller with Bluetooth and WiFi connectivity and communicates with the ThingSpeak cloud service for data storage. Users can activate or deactivate the motorcycle and control the handlebar lock through voice commands or touch inputs. Testing results show that the system quickly recognizes authorized users, automatically manages the handlebar lock based on motorcycle status, and detects suspicious movement when the vehicle is turned off. Overall, the system is proven to be effective and feasible as a practical, innovative, and IoT-based motorcycle security solution.

1. PENDAHULUAN

Maraknya kasus pencurian sepeda motor menjadi perhatian serius bagi para pengendara. Menurut laporan dari Suara Surabaya.Net Radio Suara Surabaya telah menerima 136 laporan motor hilang selama bulan September 2024 untuk wilayah Kota Surabaya dan sekitarnya. Laporan itu disampaikan oleh para pendengar maupun masyarakat yang menjadi korban pencurian motor (curanmor), hingga dilarikan/digelapkan. Kasus pencurian ini tidak hanya mengakibatkan kerugian finansial yang signifikan bagi pemilik kendaraan, tetapi juga menimbulkan ketidaknyamanan serta perasaan tidak aman bagi para pengguna sepeda motor. Fenomena ini menunjukkan bahwa sistem keamanan konvensional belum sepenuhnya efektif dalam mencegah kehilangan kendaraan dan perlu ditingkatkan melalui pendekatan berbasis teknologi modern seperti yang telah dikaji dalam penelitian sebelumnya [1].

Peningkatan keamanan pada kendaraan adalah salah satu solusi yang dibutuhkan untuk pencegahan pencurian sepeda motor. Salah satu sistem keamanan pada sepeda motor seperti sistem kontrol akses biometrik menggunakan sidik jari [2]. Teknologi biometrik ini bekerja dengan mengenali identitas unik pengguna, yaitu sidik jari, yang lebih sulit dipalsukan atau dibobol dibandingkan kunci fisik atau PIN, yang dapat hilang atau diketahui orang lain. Sistem ini memberikan keamanan yang lebih tinggi dengan memastikan bahwa hanya pengguna terdaftar yang bisa mengakses kendaraan. Selain itu, sistem ini dapat diintegrasikan dengan teknologi *Internet of Things* (IoT), sehingga memungkinkan konektivitas yang berkelanjutan antar perangkat, termasuk kendaraan. Dengan adanya IoT, pengendara dapat memantau dan mengelola keamanan kendaraan secara real-time melalui perangkat pintar, seperti smartphone,

sehingga memberikan kemudahan dan ketenangan bagi pengguna dalam menjaga keamanan kendaraan mereka [3]. Penelitian oleh [4] menunjukkan bahwa sistem keyless berbasis Bluetooth memungkinkan kontrol sepeda motor dalam radius tertentu, meskipun memiliki batasan jarak. Untuk konektivitas yang lebih luas dan stabil, penggunaan modul SIM Card 4G terbukti efektif dalam mendukung aplikasi IoT [5].

Penelitian ini bertujuan untuk mengembangkan sistem keamanan kendaraan bermotor berbasis teknologi fingerprint dengan metode prototipe yang terintegrasi IoT, sebagai kelanjutan dari penelitian sebelumnya [1]. Penelitian sebelumnya berfokus pada penerapan autentikasi sidik jari pada kendaraan bermotor, menggunakan NodeMCU ESP32 sebagai mikrokontroler utama untuk menggantikan penggunaan kunci fisik atau kunci konvensional. Sistem ini juga dilengkapi dengan modul GPS untuk pelacakan posisi kendaraan secara real-time yang terhubung dengan aplikasi Android, serta Firebase sebagai database untuk manajemen data secara real-time, yang memberikan pemilik kemampuan untuk mengakses keamanan kendaraan melalui smartphone.

Namun, penelitian ini menemukan bahwa sensor sidik jari yang terpasang langsung pada sepeda motor menghadapi tantangan signifikan dalam ketahanan terhadap cuaca. Sensor yang terpapar langsung pada kendaraan berisiko mengalami kerusakan atau penurunan fungsi saat terkena air hujan, debu, atau kondisi cuaca ekstrem lainnya. Untuk mengatasi masalah ini, penelitian ini menggunakan autentikasi sidik jari melalui aplikasi smartphone sebagai solusi, yang selain melindungi sensor dari paparan cuaca, juga meningkatkan kepraktisan dalam mengakses sistem keamanan kendaraan.

Selain peningkatan ketahanan sensor, beberapa saran pengembangan tambahan diajukan untuk memperluas fungsionalitas dan aksesibilitas sistem keamanan ini, seperti integrasi keyless berbasis Bluetooth untuk kemudahan verifikasi pengguna, optimalisasi jaringan internet dengan modul SIM Card 4G untuk konektivitas yang lebih luas, dan pengembangan antarmuka berbasis web agar pelacakan GPS tidak terbatas pada aplikasi smartphone saja. Studi lain juga menunjukkan bahwa integrasi GPS tracker berbasis NB-IoT dapat memberikan pelacakan lokasi kendaraan secara real-time dengan akurasi tinggi meskipun tergantung pada kekuatan sinyal [6], dan kontrol suara dapat menjadi alternatif akses praktis yang responsif terhadap perintah pengguna [7]. Untuk penguncian fisik, penggunaan solenoid sebagai aktuator telah terbukti memberikan pengamanan yang lebih efektif daripada kunci mekanik, selama ketahanannya terhadap kondisi cuaca tetap dijaga [8].

Berdasarkan saran-saran tersebut, penelitian ini dirancang untuk lebih memaksimalkan sistem keamanan kendaraan berbasis IoT dengan menambahkan fitur kontrol pengunci stang untuk pencegahan fisik pencurian dan kontrol suara sebagai alternatif akses ketika autentikasi sidik jari mengalami kendala, seperti saat jari basah atau dalam kondisi lain yang mengganggu proses autentikasi. Dengan penambahan kedua fitur ini, sistem keamanan yang dikembangkan diharapkan mampu meningkatkan lapisan proteksi dan kenyamanan pengguna, sekaligus memperluas fleksibilitas kontrol bagi pemilik kendaraan.

2. TINJAUAN PUSTAKA

2.1. Sepeda Motor

Sepeda motor merupakan kendaraan bermotor beroda dua yang memiliki sistem kelistrikan untuk mendukung fungsi utama

kendaraan. Komponen kelistrikan penting meliputi spul, kiprok, aki, koil, dan sistem pengapian. Fungsi utama dari sistem ini adalah menyediakan arus untuk menyalakan motor serta mendukung komponen seperti relay dan solenoid [9].

2.2. Bluetooth

Bluetooth adalah teknologi komunikasi nirkabel jarak pendek yang memungkinkan pertukaran data antar perangkat tanpa kabel. Dalam penelitian ini, Bluetooth digunakan untuk menghubungkan mikrokontroler dengan smartphone pengguna sebagai media autentikasi dan kontrol perintah suara [10].

2.3. WiFi

WiFi digunakan dalam sistem untuk menghubungkan mikrokontroler ke internet, memungkinkan pengiriman data lokasi dan status keamanan kendaraan ke cloud atau aplikasi pesan seperti Telegram. WiFi bekerja berdasarkan standar IEEE 802.11 [11].

2.4. Global Positioning System (GPS)

GPS digunakan untuk mendapatkan informasi posisi geografis kendaraan secara real-time. Modul GPS seperti Neo-6M menerima sinyal dari satelit untuk menentukan koordinat lokasi dalam bentuk latitude dan longitude, yang kemudian dikirim ke server [12].

2.5. Internet of Things (IoT)

IoT adalah konsep teknologi yang memungkinkan perangkat fisik seperti sensor dan mikrokontroler untuk terhubung dan saling bertukar data melalui internet. Dalam penelitian ini, IoT digunakan untuk memantau dan mengendalikan sistem keamanan sepeda motor secara real-time dari jarak jauh [13].

2.6. Mikrokontroler ESP32

ESP32 adalah mikrokontroler yang memiliki konektivitas WiFi dan Bluetooth

terintegrasi, sehingga cocok untuk aplikasi IoT. ESP32 digunakan sebagai pusat kendali dalam sistem keamanan motor, mengatur komunikasi antara sensor, relay, dan platform cloud.

2.7. Solenoid Door Lock

Solenoid adalah aktuator elektromagnetik yang digunakan untuk mengontrol kunci stang motor secara elektronik. Saat diberi arus, solenoid menarik mekanisme pengunci sehingga stang terbuka; saat arus dihentikan, stang kembali terkunci [14].

2.8. Biometrik

Autentikasi biometrik berbasis smartphone digunakan dalam sistem ini untuk mengendalikan motor secara aman melalui perintah suara atau pemindaian sidik jari, memastikan hanya pengguna yang sah yang dapat mengakses kendaraan [15].

2.9. ThingSpeak

ThingSpeak adalah platform cloud yang digunakan untuk menyimpan dan memvisualisasikan data dari perangkat IoT. Dalam sistem ini, ThingSpeak digunakan untuk merekam data lokasi kendaraan dan mengaksesnya melalui dashboard secara real-time.

3. METODE PENELITIAN

3.1. Perangkat Penelitian

Penelitian ini menggunakan berbagai *hardware* dan *software* untuk membangun sistem keamanan.

Tabel 3. 1 Perangkat penelitian

No	Komponen	Fungsi
1	ESP32 Dev Kit C	Mikrokontroler
2	Modul Relay 2 Channel	Mengendalikan kelistrikan motor (kontak) dan

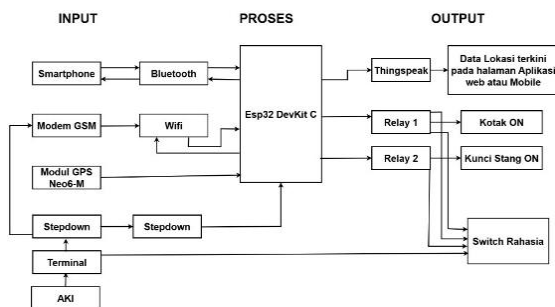
		solenoid kunci stang.
3	Solenoid Lock	Mengunci dan membuka stang motor secara otomatis.
4	Sensor GPS Neo-6M	Mendapatkan lokasi kendaraan secara real-time.
5	Modem GSM	Menghubungkan ESP32 ke internet untuk mengirim data ke ThingSpeak dan Telegram.
6	Step-down LM2596	Menurunkan tegangan dari 12V ke 5V
7	Smartphone (dengan aplikasi MIT App Inventor)	Untuk mengirim perintah (via Bluetooth) dan menampilkan lokasi motor.
8	ThingSpeak Channel	Platform cloud untuk menyimpan dan memantau data lokasi GPS.
9	Bot Telegram	Untuk mengirim notifikasi pencurian ke pengguna.
10	Sepeda Motor Vario CBS 110	Obyek uji sistem keamanan
11	Arduino IDE	Pengembangan sistem ESP32

Dari Tabel 3.1, perangkat terdiri dari komponen perangkat keras yang berfungsi untuk pemantauan, pelacakan, dan pengendalian, serta perangkat lunak yang mendukung pengembangan sistem dan antarmuka pengguna.

3.2. Perancangan Sistem

Perancangan sistem dilakukan sebagai landasan dalam pembangunan sistem agar dapat berfungsi secara efektif sesuai dengan skenario yang telah ditetapkan, tanpa menyimpang dari ruang

lingkup permasalahan penelitian. Diagram blok digunakan untuk menggambarkan prinsip kerja sistem secara menyeluruh, mencakup hubungan dan interaksi antar komponen, di mana setiap komponen memiliki peran fungsional yang saling terintegrasi.

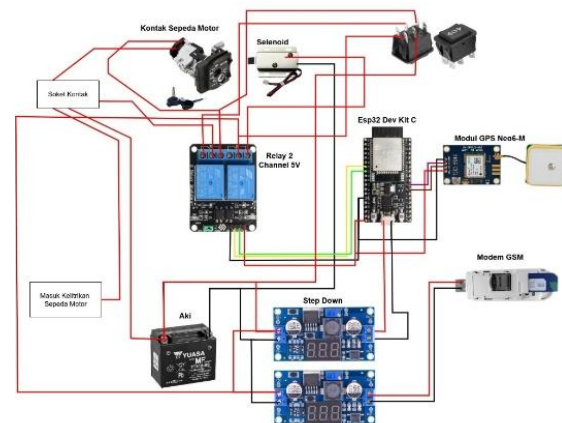


Gambar 3. 1 Blok diagram

Gambar 3.1 menunjukkan bahwa sistem terdiri dari tiga bagian utama: input, proses, dan output. Komponen input seperti smartphone (Bluetooth), modem GSM (WiFi), modul GPS Neo6-M, dan sumber daya dari aki terhubung ke ESP32 DevKit C sebagai pusat kendali. Mikrokontroler ini mengatur output berupa Relay 1 (kotak ON), Relay 2 (kunci stang ON), serta mengirim data lokasi ke Thingspeak yang dapat diakses melalui aplikasi web atau mobile. Sistem juga dilengkapi dengan switch rahasia untuk kontrol manual.

3.3. Rancangan Hardware

Perancangan perangkat keras dilakukan untuk menyatukan seluruh komponen sistem keamanan agar dapat bekerja secara terpadu sesuai dengan fungsi yang telah ditentukan.



Gambar 3. 2 Rancangan perangkat keras

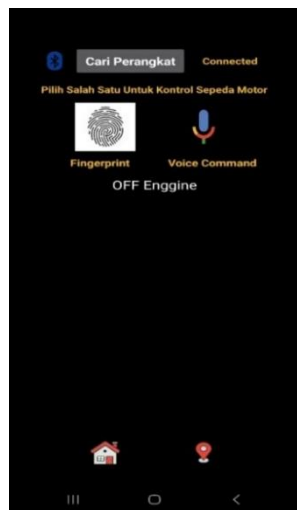
Berdasarkan Gambar 3.2, perancangan hardware dilakukan dengan mengintegrasikan ESP32 Dev Kit C, modul GPS Neo-6M, modem GSM, dan relay 2 channel 5V, yang semuanya mendapat pasokan daya dari aki motor 12V melalui modul step-down. Sistem dirancang agar ESP32 dapat menerima data dari modul GPS dan modem GSM, serta mengendalikan kontak motor dan solenoid pengunci melalui relay, sesuai dengan instruksi dari sistem kendali.

3.4. Rancangan Software

Perancangan perangkat lunak bertujuan untuk memastikan seluruh proses pengembangan aplikasi berjalan terstruktur dan sesuai dengan spesifikasi sistem. Antarmuka pengguna dirancang agar mudah dipahami, ramah pengguna, dan memiliki navigasi yang jelas. Proses perancangan antarmuka ini dilakukan menggunakan platform Kodular.



Gambar 3. 3 Tampilan halaman login



Gambar 3. 4 Tampilan Halaman Home



Gambar 3. 5 Tampilan Halaman GPS

Gambar 3.3 menampilkan tampilan halaman login, Gambar 3.4 menunjukkan

halaman beranda (home), dan Gambar 3.5 memperlihatkan halaman peta (GPS). Ketiga antarmuka tersebut dirancang agar terintegrasi dengan alur sistem serta mendukung fungsionalitas utama aplikasi secara optimal.

4. HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil implementasi dari sistem keamanan sepeda motor berbasis Internet of Things (IoT) yang telah dirancang menggunakan mikrokontroler ESP32, serta pembahasan mengenai kinerja sistem berdasarkan pengujian yang telah dilakukan. Pengujian dilakukan terhadap fungsionalitas utama sistem, antara lain kendali motor melalui Bluetooth, penguncian otomatis stang, pemantauan lokasi menggunakan GPS, serta pengiriman data dan notifikasi melalui jaringan internet.

4.1. Pengujian Autentikasi Biometrik

Autentikasi biometrik dalam sistem ini dilakukan menggunakan fitur sidik jari (fingerprint) pada smartphone yang terintegrasi dengan aplikasi pengendali berbasis Kodular. Tujuan pengujian ini adalah untuk mengetahui sejauh mana akurasi dan responsivitas autentikasi sidik jari dalam membuka akses pengendalian sepeda motor.

Tabel 4. 1 Hasil pengujian autentikasi biometrik

No	Sidik jari	Status	Hasil
1	Sidik jari ke 1	Terdaftar	Berhasil
2	Sidik jari ke 2	Belum Terdaftar	Gagal
3	Sidik Jari ke 3	Belum Terdaftar	Gagal
4	Sidik Jari ke 4	Belum Terdaftar	Gagal
5	Sidik Jari ke 5	Belum Terdaftar	Gagal

6	Sidik Jari ke 6	Terdaftar	Berhasil
7	Sidik Jari ke 7	Belum Terdaftar	Gagal
8	Sidik Jari ke 8	Belum Terdaftar	Gagal
	Sidik Jari ke 9	Belum Terdaftar	Gagal
	Sidik Jari ke 10	Belum Terdaftar	Gagal

4.2. Autentikasi Biometrik, Autentikasi Perintah Suara dan Koneksi Bluetooth untuk Kontrol Perangkat

Pada tahap ini dilakukan pengujian sistem autentikasi dan kontrol perangkat menggunakan metode biometrik (sidik jari), perintah suara, dan koneksi Bluetooth sebagai media komunikasi antara pengguna dan mikrokontroler ESP32.

Autentikasi biometrik digunakan untuk memastikan bahwa hanya pengguna yang terdaftar yang dapat mengakses dan mengendalikan sistem. Proses autentikasi ini terhubung langsung dengan sistem relay untuk mengaktifkan atau menonaktifkan motor serta penguncian stang. Sementara itu, perintah suara digunakan sebagai opsi kontrol yang lebih fleksibel, dan koneksi Bluetooth berfungsi sebagai jalur transmisi data antara aplikasi Android dan perangkat ESP32 secara lokal (tanpa internet).

Tabel berikut menunjukkan hasil pengujian autentikasi biometrik pada berbagai kondisi:

Tabel 4. 2 Hasil pengujian autentikasi biometrik kontrol perangkat

No	Kondisi	Waktu Respon	Hasil
1	Jari Kering (Pengguna Terdaftar)	< 2 detik	Akses diterima, relay aktif
2	Jari Basah (Pengguna Terdaftar)	< 2 detik	Sensor tidak bisa membaca

3	Jari Dingin (Pengguna Terdaftar)	< 2 detik	Akses diterima, sedikit lambat
4	Motor Mati (Pengguna Tidak Terdaftar)	< 2 detik	Akses ditolak
5	Motor Mati (Pengguna Terdaftar)	< 2 detik	Motor menyala (relay aktif)
6	Motor Nyala (Pengguna Terdaftar)	< 2 detik	Motor mati (relay aktif)

Pada tabel 4.2 Hasil pengujian autentikasi biometrik menunjukkan bahwa sistem mampu mengenali pengguna terdaftar dengan cepat dan akurat dalam kondisi jari kering maupun dingin dengan waktu respon kurang dari 2 detik, meskipun pada suhu dingin terjadi sedikit perlambatan, sementara pada kondisi jari basah sensor gagal membaca sidik jari sehingga akses ditolak, dan sistem juga secara konsisten menolak akses dari pengguna yang tidak terdaftar, serta mampu mengaktifkan maupun menonaktifkan relay dengan baik berdasarkan validasi biometrik dari pengguna terdaftar, yang menunjukkan bahwa sistem telah berfungsi secara efektif sebagai pengendali perangkat dalam mendukung keamanan sepeda motor berbasis IoT.

Tabel 4. 3 Pengujian Autentikasi Perintah Suara Kontrol Perangkat

No	Kondisi Pengujian	Waktu Respon	Hasil Sistem
1	“Nyalakan Motor” di ruangan tenang	< 2 detik	Berhasil, akses dibuka

2	“Matikan Motor” di ruangan tenang	< 2 detik	Berhasil, akses dibuka
3	“Nyalakan Motor” di lingkungan bising	< 2 detik	Berhasil, akses dibuka
4	“Matikan Motor” di lingkungan bising	< 2 detik	Berhasil, akses dibuka
5	Perintah suara yang tidak terdaftar	< 2 detik	Gagal, perintah tidak dikenali

Pada tabel 4.3 Hasil pengujian autentikasi perintah suara menunjukkan bahwa sistem mampu merespons perintah "Nyalakan Motor" dan "matikanMotor" dengan cepat (<2 detik) baik dalam kondisi ruangan tenang maupun lingkungan bising seperti jalanan, yang membuktikan bahwa fitur pengenalan suara bekerja secara andal dalam berbagai situasi, sementara saat diberikan perintah yang tidak terdaftar, sistem secara tepat tidak mengenali perintah tersebut dan menolak akses, sehingga menunjukkan bahwa sistem kontrol suara telah berfungsi secara efektif dan selektif dalam mengendalikan perangkat keamanan sepeda motor berbasis IoT.

Tabel 4. 4 Pegujian Koneksi Bluetooth Tanpa Penghalang

No	Jarak (meter)	Kestabilan Koneksi	Keterangan Singkat
1	1	Sangat stabil	Koneksi cepat dan kuat
2	2	Sangat stabil	Respons cepat, tanpa gangguan
3	3	Stabil	Delay ringan,

			masih normal
4	4	Stabil	Perintah tetap diterima
5	5	Cukup stabil	Delay mulai terasa, kadang perlu retry
6	6	Mulai fluktuatif	Respons lambat, risiko gagal meningkat
7	7	Tidak stabil	Delay tinggi, sering lambat
8	8	Hampir tidak stabil	Kadang gagal koneksi
9	9	Sering putus-nyambung	Perlu beberapa kali koneksi ulang
10	10	Cenderung gagal	Umumnya gagal konek

Pada tabel 4.4 menunjukkan bahwa koneksi Bluetooth dalam kondisi ideal (tanpa penghalang) masih optimal hingga 5 meter. Di atas itu, koneksi mulai tidak stabil dan delay meningkat signifikan. Pada 10 meter, koneksi biasanya gagal. Ini sesuai dengan batas wajar Bluetooth Class 2 seperti pada ESP32.

Tabel 4. 5 Pegujian Koneksi Bluetooth Dengan Penghalang

No	Jarak (m)	Kecepatan Deteksi (detik)	Keterangan Singkat
1	1	0.7	Sangat stabil, koneksi cepat dan kuat

2	2	0.8	Sangat stabil, respons cepat
3	3	1.0	Stabil, sedikit delay
4	4	1.2	Stabil, perintah tetap diterima
5	5	1.5	Cukup stabil, mulai terasa delay
6	6	1.8	Mulai fluktuatif, respons lambat
7	7	2.2	Tidak stabil, delay cukup tinggi
8	8	2.5	Hampir tidak stabil, kadang gagal
9	9	3.0	Sering putus-nyambung, sinyal tidak konsisten
10	10	>3.2	Cenderung gagal, koneksi sering tidak berhasil

Tabel pengujian 4.5 di atas menunjukkan pengaruh jarak terhadap koneksi Bluetooth pada sistem keamanan sepeda motor, dengan pintu kamar sebagai penghalang tetap.

Pada jarak 1–3 meter, sistem masih mampu terhubung dengan waktu deteksi yang relatif cepat dan koneksi cukup stabil. Namun mulai dari jarak 4 meter ke atas, terjadi penurunan performa secara signifikan.

Hal ini disebabkan oleh perlemahan sinyal akibat hambatan fisik dan jarak tempuh gelombang radio yang semakin

jauh. Pada jarak lebih dari 6 meter, sistem umumnya tidak lagi mampu membentuk koneksi, menandakan batas praktis dalam skenario ini.

Penggunaan penghalang pintu kamar mencerminkan kondisi rumah nyata, seperti motor yang diparkir dalam garasi atau ruang tertutup, sehingga hasil ini dapat menjadi referensi batas maksimal koneksi aman sistem.

Tabel 4. 6 Pairing oleh Perangkat Asing Tanpa Penghalang

No	Jarak (m)	Status Pairing	Keterangan Singkat
1	1	Berhasil	Pairing sukses, tapi perintah ditolak (bukan aplikasi resmi)
2	2	Berhasil	Terhubung tapi tidak bisa mengendalikan sistem
3	3	Berhasil	Pairing berhasil, kontrol tetap ditolak
4	4	Berhasil	Pairing berhasil, kontrol tetap ditolak
5	5	Gagal	Gagal pairing, sinyal lemah
6	6	Gagal	Gagal pairing, sinyal lemah
7	7	Gagal	Gagal pairing, sinyal lemah
8	8	Gagal	Gagal pairing, sinyal lemah
9	9	Gagal	Gagal pairing, sinyal lemah
10	10	Gagal	Gagal pairing, sinyal lemah

Berdasarkan Tabel 4.6, sistem keamanan berbasis Bluetooth mampu menolak seluruh perintah dari perangkat asing meskipun berhasil melakukan pairing pada jarak 1–4 meter, karena hanya perintah

dari aplikasi resmi atau sesuai format yang akan dieksekusi, sedangkan pada jarak 5–10 meter proses pairing gagal akibat lemahnya sinyal, sehingga sistem ini mengandalkan validasi perintah secara software dan pembatasan jangkauan fisik sebagai lapisan keamanan ganda terhadap akses tidak sah.

Tabel 4. 7 Percobaan Pairing oleh Perangkat Asing dengan Penghalang

No	Jarak (m)	Status Pairing	Keterangan Singkat
1	1	Berhasil	Pairing sukses, tapi kontrol ditolak
2	2	Berhasil	Terhubung tapi tidak bisa mengendalikan sistem
3	3	Berhasil	Pairing berhasil, kontrol tetap ditolak
4	4	Sering gagal	Koneksi tidak stabil, pairing tidak konsisten
5	5	Gagal	Tidak bisa terhubung karena penghalang
6	6	Gagal	Gagal pairing, sinyal melemah
7	7	Gagal total	Tidak ada koneksi sama sekali
8	8	Gagal total	Tidak ada koneksi sama sekali
9	9	Gagal total	Tidak ada koneksi sama sekali
10	10	Gagal total	Tidak ada koneksi sama sekali

Berdasarkan Tabel 4.7, sistem keamanan berbasis Bluetooth menunjukkan proteksi kuat terhadap perangkat asing, di mana pada jarak 1–3 meter pairing masih memungkinkan namun perintah tetap ditolak jika tidak sesuai format, sementara mulai jarak 4 meter pairing menjadi tidak stabil, dan pada 5–10 meter pairing gagal sepenuhnya akibat penghalang fisik seperti pintu kamar, sehingga sistem ini memadukan keamanan software dan pembatasan sinyal fisik untuk perlindungan lebih menyeluruh terhadap akses tidak sah.

4.3. Pengujian Lokasi GPS

Pengujian GPS dilakukan dalam dua kondisi, yaitu di luar ruangan untuk menguji kemampuan menangkap sinyal satelit tanpa hambatan, dan di dalam ruangan untuk melihat pengaruh hambatan fisik terhadap kinerja GPS.

Saat motor dalam kondisi mati, sistem akan menyimpan titik lokasi awal dan memantau pergerakan secara berkala. Jika terdeteksi pergerakan lebih dari 30 meter dari titik awal, sistem akan melakukan verifikasi selama 30 detik. Jika dalam waktu tersebut kendaraan tidak kembali ke posisi awal, maka dianggap sebagai indikasi pencurian.

Sistem kemudian mengirim notifikasi ke bot Telegram dan mengunggah data lokasi ke ThingSpeak. Jika kendaraan tetap diam atau kembali ke posisi semula, maka tidak ada notifikasi yang dikirim.

Tabel 4. 8 Pengujian lokasi GPS

No	Lokasi Uji	Respon Sistem	Kesimpulan
1	Lapangan Terbuka	Data muncul < 5 detik	Lokasi akurat dan konsisten
2	Pinggir Jalan	Data terkirim ± 5 detik	Masih dalam batas toleransi

3	Garasi Terbuka	Delay hingga 10 detik	Masih bisa digunakan dengan toleransi
4	Dalam Rumah	Sering gagal kirim data	Tidak disarankan untuk akurasi GPS
5	Setelah Pindah 30 m	Notifikasi terkirim < 10 detik	Pelacakan bekerja sesuai logika sistem

Berdasarkan Tabel 4.8, sistem pelacakan GPS bekerja andal di area terbuka dengan akurasi $\pm 3-5$ meter dan pengiriman data ke ThingSpeak di bawah 5 detik, namun akurasi menurun di lokasi semi atau tertutup akibat gangguan sinyal, sementara fitur pelacakan pencurian tetap berfungsi dengan baik dalam mendeteksi perpindahan saat motor dalam kondisi OFF, sehingga sistem ini efektif di luar ruangan namun kurang optimal di dalam ruangan.

4.4. Pengujian Kontrol Pengunci Stang Motor

Pengujian ini bertujuan mengevaluasi kinerja aktuator solenoid sebagai pengunci stang motor, dengan fokus pada waktu respons, jumlah siklus kerja, dan konsumsi daya terhadap aki 12V.

Waktu aksi diukur dari saat perintah dikirim melalui aplikasi hingga solenoid mengunci atau membuka stang. Pengujian dilakukan secara berulang untuk menguji konsistensi, serta dilakukan pengukuran arus dan tegangan guna memastikan sistem aman terhadap kapasitas aki motor. Hasil pengujian disajikan dalam tabel berikut:

Tabel 4. 9 Pengujian pengunci stang motor

No	Perintah	Tegangan Aki (V)	Arus Aktif (A)
1	Matikan Motor	12.4	0.88
2	Nyalakan Motor	12.3	0.90
3	Siklus ke-1 (5x)	12.2	0.90
4	Siklus ke-2 (10x)	12.1	0.87
5	Siklus ke-3 (10x)	12.0	0.81
6	Siklus ke-4 (10x)	12.2	0.90
7	Siklus ke-5 (10x)	12.1	0.89
8	Solenoid aktif lama	11.9	0.88

Berdasarkan Tabel 4.9, sistem pengunci stang motor berbasis solenoid menunjukkan respons cepat di bawah 1 detik, performa stabil hingga 10 siklus tanpa penurunan, serta konsumsi daya efisien dengan arus 0.88–0.90 A dan tegangan aki tetap stabil di atas 12V, meskipun penggunaan solenoid secara terus-menerus sebaiknya dihindari untuk menjaga kestabilan daya, sehingga sistem ini dinilai layak dan efektif untuk implementasi pada kendaraan.

4.5. Pengujian Kebutuhan Daya Sistem

Berikut adalah estimasi konsumsi daya dari masing-masing komponen dalam sistem:

Tabel 4. 10 Pengujian kebutuhan daya

No	Komponen	Tegangan Operasi	Arus (mAh)
1	ESP32 Dev Kit C	5V	120
2	Relay 2 Channel	5V	140

3	GPS Neo-6M	5V	40
4	Modem GSM (idle TX)	5V	220
5	Solenoid (idle)	12V	100
Total			620

Untuk mengetahui berapa lama sistem dapat aktif jika hanya bergantung pada aki motor tanpa pengisian ulang, digunakan rumus:

$$t = \frac{Q}{I}$$

Keterangan:

- t = waktu daya tahan aki (jam)
- Q = kapasitas aki dalam satuan mAh
- I = total konsumsi arus sistem per jam (mAh)

Perhitungan:

Aki 12V 4,2 Ah (4200 mAh):

$$t = \frac{4200}{620} = 6.77 \text{ Jam}$$

Dengan demikian, sistem akan mampu tetap aktif antara 6,7 jam tanpa pengisian ulang, tergantung kapasitas aki yang digunakan.

5. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem keamanan sepeda motor berbasis IoT dengan autentikasi biometrik, GPS, dan kendali kunci stang melalui smartphone, maka dapat disimpulkan bahwa:

a. Sistem berhasil dirancang menggunakan modul ESP32 yang mengintegrasikan Bluetooth untuk kendali motor, GPS Neo-

6M untuk pelacakan lokasi, dan perintah suara sebagai autentikasi biometrik melalui smartphone.

b. Sistem dapat mendeteksi kondisi pencurian berdasarkan perubahan lokasi lebih dari 3 meter saat motor dalam kondisi mati. Jika dalam waktu 30 detik tidak kembali ke lokasi awal, sistem secara otomatis mengirimkan notifikasi ke bot Telegram dan memperbarui data ke platform ThingSpeak.

c. Relay digunakan untuk mengontrol arus kontak motor dan solenoid kunci stang. Saat motor dinyalakan melalui perintah suara "Nyalakan motor", sistem membuka kunci stang dan mengaktifkan kontak. Saat diperintah "Matikan motor", sistem mengunci kembali kunci stang dan mulai memantau lokasi.

d. Kelebihan: Sistem memiliki kemampuan kendali motor secara nirkabel melalui Bluetooth, dapat memantau lokasi secara otomatis, serta mampu mengirimkan notifikasi pencurian secara real-time ke Telegram dan ThingSpeak, sehingga memberikan keamanan tambahan bagi pengguna.

e. Kekurangan: Sistem masih bergantung pada sinyal GPS yang tidak stabil saat kondisi cuaca buruk (misalnya hujan). Selain itu, solenoid door lock yang digunakan memerlukan arus terus-menerus saat aktif, sehingga berisiko menimbulkan panas berlebih dan membebani sistem.

f. Pengembangan selanjutnya: Sistem dapat ditingkatkan dengan:

- Menambahkan sensor Hall Effect NJK-5002C untuk mendeteksi pergerakan logam sebagai upaya pencurian, terutama saat motor dalam keadaan mati.

- Mengganti solenoid dengan tipe latching atau menggunakan servo motor, atau menambahkan mekanisme pengunci eksternal (seperti pegas atau grendel) agar solenoid hanya aktif sesaat untuk mengurangi beban arus dan meningkatkan efisiensi energi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, bantuan, dan arahan selama proses penelitian ini berlangsung. Ucapan terima kasih secara khusus disampaikan kepada dosen pembimbing yang telah membimbing dengan penuh kesabaran, serta kepada keluarga dan rekan-rekan yang senantiasa memberikan semangat dan motivasi. Tak lupa, penulis juga menyampaikan apresiasi kepada pihak institusi dan laboratorium yang telah menyediakan fasilitas dalam mendukung kelancaran penelitian ini.

DAFTAR PUSTAKA

- [1] C. Gudiato, C. Cahyaningtyas, and N. P., "G-Tech : Jurnal Teknologi Terapan," *G-Tech : Jurnal Teknologi Terapan*, vol. 8, no. 1, pp. 186–195, 2024, [Online]. Available: <https://ejournal.uniramalang.ac.id/index.php/g-tech/article/view/1823/1229>
- [2] M. N. Afif and M. K. Dermawan, "Penggunaan Alat Biometrik Sidik Jari sebagai Kontrol Akses dalam Analisis CPTED terhadap Risiko Trespassing di Instalasi Gudang Material Korporasi ' X '," vol. 5, no. 4, pp. 819–830, 2024.
- [3] A. Martulandi and D. Setiawan, "Sistem Kehadiran Biometrik Sidik Jari Menggunakan IoT yang Terintegrasi dengan Telegram," *Engineering, Mathematics and Computer Science (EMACS) Journal*, vol. 3, no. 3, pp. 103–107, 2021, doi: 10.21512/emacsjournal.v3i3.7426.
- [4] M. R. Fauzi, "Perancangan Penyalaan Engine Sepeda Motor Berbasis Arduino Melalui Bluetooth Android," *Jurnal Surya Teknik*, vol. 8, no. 1, pp. 265–273, 2021, doi: 10.37859/jst.v8i1.2676.
- [5] I. Fibriani, Widjonarko, A. Bayu, and P. Ciptaning, "Analisa Sistem Monitoring Greenhouse Berbasis Internet of Things (IoT) Pada Jaringan 4G LTE," *Jurnal SinarFe7*, vol. 3, no. 1, pp. 231–236, 2020.
- [6] A. Febriana, A. A. Dahlan, and F. Firdaus, "Rancang Bangun GPS Tracker Pada Kendaraan Bermotor Menggunakan SIM7000 NB-IoT Berbasis Arduino," *Elektron : Jurnal Ilmiah*, vol. 13, pp. 60–67, 2021, doi: 10.30630/eji.13.2.225.
- [7] A. Nurhuda, B. Harpad, and M. S. A. Mubarak, "Kendali Lampu Menggunakan Perintah Suara Berbasis Node Mcu," *Sebatik*, vol. 23, no. 1, pp. 77–83, 2019, doi: 10.46984/sebatik.v23i1.447.
- [8] E. Octavia, R. Dijaya, A. Eviyanti, and N. L. Azizah, "Rancangan Bangun Sistem Keamanan Rumah Kost Berbasis IoT dengan ESP32-Cam," *Indonesian Journal of Applied Technology*, vol. 1, no. 3, p. 16, 2024, doi: 10.47134/ijat.v1i3.3073.
- [9] I. Mawardi, M. Hatta, J. Teknik Mesin Politeknik Negeri Lhokseumawe, and J. Teknik Elektro Politeknik Negeri Lhokseumawe, "PELATIHAN USAHA PERBENGKELAN SEPEDA MOTOR DI KABUPATEN ACEH UTARA," vol. 6, no. 2, 2022.
- [10] A. Jamal, M. Ridha Fauzi, P. Studi Mesin Otomotif, F. Teknik, and U. Muhammadiyah Riau Jl Tuanku Tambusai Ujung No, "Perancangan Penyalaan Engine Sepeda Motor Berbasis Arduino Melalui Bluetooth Android," vol. 8, no. 1, pp. 265–273, 2021.
- [11] M. Arif, "Fakultas Komputer SEJARAH WIFI DAN PERKEMBANGAN WIFI."
- [12] A. Febriana, A. A. Dahlan, and F. Firdaus, "Rancang Bangun GPS Tracker Pada Kendaraan Bermotor Menggunakan SIM7000 NB-IoT Berbasis Arduino," *Elektron : Jurnal Ilmiah*, pp. 60–67, Nov. 2021, doi: 10.30630/eji.13.2.225.
- [13] M. A. Fauzi and S. A. Sukarno, "PENGEMBANGAN SISTEM PENDETEKSI KEBOCORAN GAS LPG BERBASIS IOT: INTEGRASI SENSOR MQ-02 DAN DHT11 UNTUK PEMANTAUAN REAL-TIME," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, Jan. 2025, doi: 10.23960/jitet.v13i1.5980.
- [14] A. Hambali, A. Pranata, and F. Setiawan, "Implementasi IOT pada Smartdoor Lock Menggunakan Sensor Selenoid Berbasis NodeMCU," vol. 4, no. 1, pp. 36–48, 2025, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jsko>
- [15] B. Suharjo, S. Falentino, and ; S Liawatimena, "Perancangan Sistem Keamanan... (Beman Suharjo; dkk) PERANCANGAN SISTEM KEAMANAN

SEPEDA MOTOR DENGAN SISTEM SIDIK
JARI.”