JURNAL TEKNIK INFORMATIKA

Vol. 6 No. 2 Tahun. 2026
ISSN 2809-1353
DOI : 10.58794/jekin.v6i2.2114

Rancang Bangun Palang Pintu Otomatis Berbasis RFID dan IoT untuk Manajemen Akses Kendaraan di Universitas PGRI Silampari

Sindi Dewi Oktafiani[1], Dimas Ardian[2], Ahmad Marsehan[3]
[1,2,3]Program Studi Teknologi Informasi, Universitas PGRI Silampari, Lubuklinggau, Indonesia
e-mail: [1]**sindidewioktafiani210@gmail.com**, [2]**dimasardian1126@gmail.com**, [3]ahmadmarsehan10@gmail.com

Abstract*— Increasing mobility of vehicles at Universitas PGRI Silampari has created traffic congestion at campus gates and introduced risks associated with manual access logging. Prior systems have addressed either RFID-based authentication or IoT monitoring separately; however, none has provided a unified, campus-tailored prototype integrating token-based API security with real-time cloud synchronization. This study designs and develops an RFID- and IoT-based automatic gate system to enable efficient, accountable, and real-time vehicle access management. The system integrates an *RC522 RFID reader* for identity verification, a servo motor for barrier control, and a *NodeMCU ESP8266* module for Wi-Fi communication. For cloud monitoring, the system uses *Blynk/Firebase* to store access logs and to provide real-time notifications to administrators via smartphones. A series of 10 repeated trials was conducted to assess latency and RFID read accuracy. The experimental evaluation shows that the system achieves an average server data-transmission latency of 1.95 s under stable Wi-Fi conditions. The optimal RFID reading distance is 1–3 cm to reduce unintended reads and improve authentication reliability. Compared to the manual gate process, the prototype improves vehicle access efficiency by up to 80%. The novelty of this work lies in the end-to-end synchronization between RFID-based authentication, automated barrier actuation, and cloud-based monitoring within a unified prototype tailored for campus access management, with token-based API security and a local fallback mechanism to maintain gate functionality during network disruptions. These characteristics distinguish the proposed system from prior works that treat authentication and cloud monitoring as separate subsystems.

Keywords - RFID, ESP8266, cloud monitoring, Internet of Things, smart parking, automatic gate, access management.

Abstrak - Meningkatnya mobilitas kendaraan di Universitas PGRI Silampari menyebabkan antrean panjang di gerbang kampus serta meningkatkan risiko kelemahan pencatatan akses manual. Penelitian-penelitian sebelumnya telah menangani autentikasi RFID atau monitoring IoT secara terpisah; belum ada yang mengintegrasikan keduanya dalam satu prototipe kampus terpadu dengan mekanisme keamanan berbasis token dan cadangan lokal saat jaringan terganggu. Penelitian ini merancang dan membangun sistem palang pintu otomatis berbasis RFID dan IoT untuk mengelola akses kendaraan secara efisien, akuntabel, dan real-time. Sistem mengintegrasikan pembaca RFID RC522 **untuk verifikasi identitas,** motor servo **untuk kontrol palang, serta** NodeMCU ESP8266 **untuk komunikasi Wi-Fi. Untuk monitoring berbasis cloud, sistem menggunakan** Blynk/Firebase **dalam penyimpanan log akses dan notifikasi real-time kepada administrator melalui smartphone. Pengujian dilakukan sebanyak 10 percobaan berulang untuk memastikan konsistensi hasil. Pengujian menunjukkan bahwa rata-rata latensi pengiriman data ke server sebesar** 1,95 detik **pada kondisi Wi-Fi stabil. Jarak baca RFID yang optimal berada pada rentang** 1–3 cm **untuk mengurangi pembacaan tidak sengaja dan meningkatkan keandalan autentikasi. Dibandingkan sistem manual, prototipe meningkatkan efisiensi waktu akses hingga** 80%. **Nilai kebaruan penelitian ini terletak pada** sinkronisasi end-to-end **antara autentikasi RFID, aktuasi palang otomatis, dan monitoring cloud dalam satu prototipe terpadu dengan keamanan berbasis token API dan mekanisme cadangan lokal saat koneksi terputus, yang membedakannya dari penelitian sebelumnya yang menangani autentikasi dan monitoring secara terpisah.**

Kata Kunci - RFID, ESP8266, cloud monitoring, IoT, smart parking, palang pintu otomatis, manajemen akses.

I. PENDAHULUAN

Universitas sebagai pusat aktivitas akademik memiliki mobilitas kendaraan yang sangat tinggi setiap harinya. Peningkatan volume kendaraan yang dibawa oleh mahasiswa, dosen, karyawan, serta tamu di Universitas PGRI Silampari seringkali tidak sebanding dengan sistem manajemen akses yang ada. Pada kondisi eksisting, pengelolaan pintu masuk masih bersifat konvensional atau manual, di mana petugas keamanan harus melakukan pengecekan identitas atau memberikan karcis parkir secara fisik. Model operasional seperti ini memiliki beberapa kelemahan signifikan, antara lain terjadinya antrean panjang pada jam sibuk, risiko kesalahan manusia (human error) dalam pencatatan, serta sulitnya melakukan audit data kendaraan secara real-time [1].

Transformasi menuju Smart Campus menuntut adanya integrasi teknologi otomatisasi dalam setiap aspek infrastruktur, termasuk sistem perparkiran. Penggunaan palang pintu otomatis menjadi solusi krusial untuk meningkatkan efisiensi arus lalu lintas kendaraan. Namun, sistem otomatis tanpa identifikasi pengguna yang jelas tetap menyisakan celah keamanan. Oleh karena itu, teknologi Radio Frequency Identification (RFID) diimplementasikan dalam penelitian ini sebagai media autentikasi. RFID memungkinkan identifikasi kendaraan secara cepat tanpa kontak fisik (non-contact), di mana setiap pengguna terdaftar memiliki identitas unik pada tag RFID mereka yang dapat dibaca oleh sensor dalam hitungan milidetik [2].

Selain aspek identifikasi, aspek pengawasan data merupakan hal yang mendasar. Tanpa adanya konektivitas, data akses kendaraan hanya akan tersimpan secara lokal dan sulit dipantau oleh pimpinan kampus atau pihak keamanan dari jarak jauh. Dengan mengintegrasikan konsep Internet of Things (IoT), setiap aktivitas palang pintu—baik kendaraan masuk maupun keluar—akan dikirimkan ke server atau basis data cloud. Hal ini memungkinkan pihak administrasi untuk memantau statistik kendaraan, mendeteksi kapasitas parkir yang tersedia, dan menyimpan log aktivitas secara digital yang aman dari risiko kehilangan data fisik [3]. Penelitian ini bertujuan untuk merancang dan membangun sistem palang pintu otomatis berbasis RFID dan IoT yang disesuaikan dengan kebutuhan lingkungan Universitas PGRI Silampari. Nilai kebaruan dari sistem ini terletak pada sinkronisasi end-to-end antara perangkat keras (NodeMCU ESP8266 dan RFID RC522) dengan platform IoT, dilengkapi mekanisme keamanan berlapis dan fallback lokal, sehingga menciptakan sistem manajemen akses yang transparan, akuntabel, dan andal [4].

II. PENELITIAN YANG TERKAIT

Penelitian mengenai otomatisasi parkir telah banyak dikembangkan dengan berbagai sensor. Merancang prototipe palang parkir menggunakan sensor ultrasonik HC-SR04 untuk mendeteksi keberadaan objek kendaraan. Meskipun efektif dalam mendeteksi fisik kendaraan, sistem tersebut memiliki keterbatasan dalam hal manajemen identitas pengguna, karena palang akan terbuka untuk objek apa pun tanpa adanya proses filtrasi identitas [5]. Penggunaan teknologi RFID dalam manajemen kampus yang menekankan pada efisiensi penggunaan kartu mahasiswa sebagai akses multifungsi. Penelitian tersebut menunjukkan bahwa RFID memiliki tingkat akurasi pembacaan yang tinggi dan tahan terhadap gangguan cuaca dibandingkan sensor berbasis visi mesin (kamera). Namun, penelitian tersebut masih terfokus pada penyimpanan data lokal (offline) sehingga informasi tidak dapat diakses secara real-time oleh pihak berkepentingan di luar area parkir .

Sejalan dengan perkembangan teknologi informasi, konsep Internet of Things (IoT) mulai diterapkan dalam infrastruktur publik. Jurnal IEEE Internet of Things menjelaskan bahwa pemanfaatan edge computing dan IoT pada sistem parkir dapat mengurangi latensi pengiriman data dan memungkinkan pemantauan jarak jauh melalui perangkat seluler. Hal ini diperkuat oleh penelitian yang merancang gerbang parkir berbasis Arduino dengan fitur keselamatan tambahan, namun mereka mencatat bahwa tantangan utama adalah kestabilan koneksi jaringan internet di area terbuka [6].

Perbedaan utama antara penelitian ini dengan penelitian-penelitian di atas terletak pada integrasi hibrida antara RFID sebagai unit autentikasi dan platform IoT sebagai unit monitoring terpusat di Universitas PGRI Silampari. Jika penelitian sebelumnya banyak yang terpisah antara sistem mekanis otomatis dan sistem basis data, penelitian ini menggabungkan keduanya menjadi satu kesatuan sistem manajemen akses kendaraan yang utuh. Selain itu, sistem ini dirancang dengan mempertimbangkan parameter jarak baca RFID yang optimal untuk kendaraan roda dua maupun roda empat di area kampus, serta penyediaan antarmuka data yang dapat diakses oleh administrator secara real-time [7].

III. METODE PENELITIAN

Penelitian ini menggunakan metode desain eksperimental untuk membangun sebuah sistem keamanan akses kendaraan. Tahapan penelitian disusun secara sistematis mulai dari analisis kebutuhan hingga pengujian integrasi antara perangkat keras dan platform IoT.

A. Arsitektur Sistem

Sistem ini terdiri dari tiga lapisan utama: Lapisan Sensor (RFID Reader RC522), Lapisan Kontrol (NodeMCU ESP8266), dan Lapisan Monitoring (Cloud IoT – Firebase/Blynk). Arsitektur ini memungkinkan validasi data secara lokal (on-device) dan pengiriman log aktivitas secara daring. Untuk menangani kegagalan jaringan, sistem dirancang dengan mekanisme fallback

lokal: validasi UID tetap dilakukan oleh mikrokontroler menggunakan database UID yang disimpan di memori EEPROM, sehingga palang pintu dapat beroperasi secara terbatas bahkan tanpa koneksi internet. Log akses yang tidak terkirim akan disimpan sementara dan diteruskan ke server secara otomatis ketika koneksi pulih. Keterbatasan arsitektur saat ini adalah belum adanya load balancing atau redundansi server, yang dapat menjadi titik kegagalan tunggal (single point of failure) pada skala implementasi yang lebih besar [8].

Gbr. 1 Arsitektur Palang Pintu Berbasis RFID & IoT

Penjelasan alur kerja sistem

1. Tahap Scanning (Input):
   Pengguna mendekatkan kartu atau tag RFID ke perangkat RFID Reader yang terpasang di depan palang pintu. Reader akan membaca kode unik (Unique ID) yang tersimpan di dalam kartu secara nirkabel.
2. Tahap Verifikasi & Kontrol (Processing):
   Data kode unik yang terbaca dikirim ke mikrokontroler (NodeMCU ESP8266). Di sini terjadi proses Access Verification: mikrokontroler memeriksa apakah ID tersebut terdaftar di dalam database. Jika ID valid, mikrokontroler akan menjalankan instruksi Barrier Control untuk menggerakkan motor servo sehingga palang pintu terbuka.
3. Tahap Pengiriman Data (Communication):
   Secara simultan saat palang terbuka, modul Wi-Fi pada sistem (ESP8266) akan menjalankan fungsi Send Data. Data yang dikirim berupa ID pengguna, status akses (berhasil/gagal), dan waktu kejadian (timestamp).
4. Tahap Cloud Processing (Storage):
   Data dikirim menuju IoT Cloud Server (misalnya Firebase atau Blynk). Server ini berfungsi sebagai pusat penyimpanan data (database cloud) yang menjamin data tidak hilang dan dapat diakses dari mana saja secara real-time.

a. Tahap Monitoring & Notifikasi (Output Admin):
   Data dari cloud diteruskan ke Admin Smartphone. Melalui aplikasi monitoring, pihak keamanan atau administrator kampus dapat menerima notifikasi, memantau riwayat akses kendaraan, dan melakukan Remote Access (membuka palang dari jarak jauh jika diperlukan).

B. Analisis Kinerja Komunikasi Data (IoT)

Efektivitas sistem palang pintu otomatis ini sangat bergantung pada stabilitas pertukaran data antara perangkat keras di lapangan dengan server di awan (cloud). Proses ini melibatkan pemilihan protokol komunikasi yang efisien untuk meminimalkan jeda waktu (latency) saat validasi akses berlangsung. Penggunaan protokol HTTP atau MQTT pada penelitian ini dipilih karena kemampuannya dalam menangani pengiriman data berukuran kecil secara cepat dan stabil, meskipun dalam kondisi jaringan Wi-Fi kampus yang padat [9]. Selain aspek kecepatan, aspek keamanan data juga menjadi prioritas. Sistem mengimplementasikan lapisan keamanan berlapis yang mencakup: (1) autentikasi berbasis token API privat untuk setiap sesi komunikasi antara NodeMCU ESP8266 dan server cloud; (2) validasi UID secara lokal pada mikrokontroler sebelum transmisi, sehingga palang tetap dapat beroperasi dalam mode offline terbatas jika koneksi internet terputus; dan (3) pencatatan setiap percobaan akses yang gagal sebagai log keamanan untuk keperluan audit. Meskipun demikian, aspek enkripsi end-to-end penuh dan proteksi terhadap kloning kartu RFID (RFID cloning attack) diakui sebagai keterbatasan sistem saat ini yang perlu ditangani pada pengembangan selanjutnya, misalnya melalui implementasi rolling code atau enkripsi AES-128 pada payload data UID [10]. Parameter teknis yang mendukung keandalan komunikasi data pada sistem ini dirinci pada Tabel I di bawah ini:

TABEL I
PARAMETER KONEKTIVITAS CLOUD IOT

PARAMETER	SPESIFIKASI / KETERANGAN
PROTOKOL KOMUNIKASI	HTTP POST / MQTT (MESSAGE QUEUING TELEMETRY TRANSPORT)

PARAMETER	SPESIFIKASI / KETERANGAN
PLATFORM IOT	FIREBASE REALTIME DATABASE / BLYNK IOT PLATFORM
MEDIA TRANSMISI	WI-FI IEEE 802.11 B/G/N (2.4 GHZ)
RATA-RATA LATENSI	1,0 – 2,5 DETIK (TERGANTUNG TRAFIK JARINGAN)
METODE AUTENTIKASI	TOKEN-BASED AUTHENTICATION & PRIVATE API KEY
FORMAT DATA	JSON (JAVASCRIPT OBJECT NOTATION)

C. Perancangan Perangkat Keras

Perangkat keras dirancang untuk bekerja secara sinkron. Komponen utama yang digunakan dalam rancang bangun ini dirinci pada Tabel II.

Tabel II. Daftar Komponen Perangkat Keras

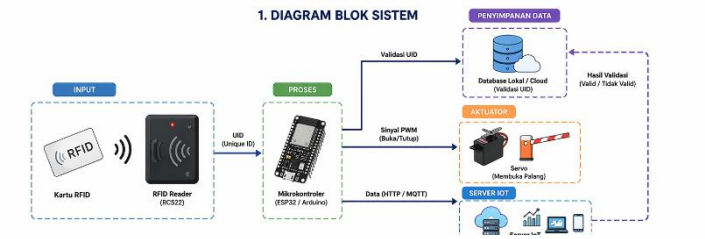
No	Komponen	Fungsi Utama
1	NodeMCU ESP8266	Mikrokontroler utama sekaligus modul Wi-Fi untuk IoT.
2	RFID Reader RC522	Membaca ID unik dari tag RFID pengguna.
3	Motor Servo MG995	Penggerak mekanik lengan palang (torsi tinggi).
4	I2C LCD 16x2	Penampil status akses (misal: "Akses Diterima").
5	Buzzer & LED	Indikator audio dan visual saat proses autentikasi.

Berdasarkan Tabel II di atas, NodeMCU ESP8266 memegang peranan sentral sebagai unit pemroses data. Berbeda dengan Arduino Uno biasa, modul ini dipilih karena sudah memiliki chip Wi-Fi terintegrasi, yang memungkinkan sistem mengirimkan data log aktivitas secara langsung ke server tanpa memerlukan modul tambahan [11].

Selanjutnya, RFID Reader RC522 digunakan sebagai unit identifikasi primer. Komponen ini dipilih karena keandalannya dalam membaca tag pasif dengan cepat, yang sangat krusial untuk mencegah penumpukan kendaraan di pintu masuk kampus. Untuk bagian mekanik, penggunaan Motor Servo MG995 diprioritaskan karena memiliki gir berbahan logam yang kuat untuk menahan beban lengan palang pintu prototipe, memastikan gerakan buka-tutup palang berlangsung stabil dan presisi.

D. Diagram Blok dan Aliran Data

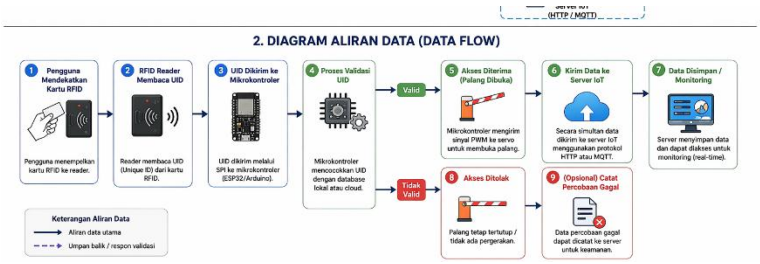
Proses dimulai ketika pengguna mendekatkan kartu RFID pada reader. Data UID (Unique ID) dikirim ke mikrokontroler untuk dicocokkan dengan database lokal atau cloud. Jika valid, mikrokontroler mengirim sinyal PWM ke servo untuk membuka palang dan secara simultan mengirim data ke server IoT menggunakan protokol HTTP atau MQTT.



Gbr. 2 Diagram Blok

Penjelasan Diagram Blok Sistem :

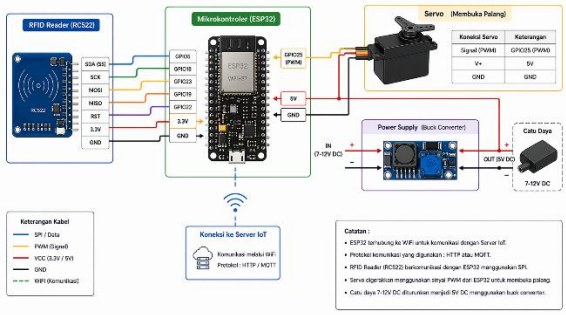
1. Diagram blok menggambarkan hubungan antar komponen utama dalam sistem akses palang berbasis RFID. Sistem terdiri dari beberapa bagian yaitu input, proses, output (aktuator), database, dan server IoT.
2. Proses dimulai dari kartu RFID yang digunakan oleh pengguna sebagai media identifikasi. Kartu ini akan dibaca oleh RFID Reader (RC522) untuk mengambil data UID (Unique ID). Selanjutnya, data UID dikirim ke mikrokontroler (NodeMCU ESP8266) sebagai pusat pengolahan sistem.
3. Mikrokontroler kemudian melakukan proses validasi UID dengan mencocokkannya ke database yang dapat berada secara lokal maupun cloud. Jika UID terdaftar (valid), maka mikrokontroler akan mengirimkan sinyal PWM ke servo sebagai aktuator untuk membuka palang.
4. Selain itu, mikrokontroler juga secara bersamaan mengirimkan data ke server IoT menggunakan protokol komunikasi seperti HTTP atau MQTT. Data ini digunakan untuk keperluan monitoring dan pencatatan aktivitas akses.



Gbr. 3 Diagram Alir Data 1

Penjelasan Diagram Aliran Data (Data Flow) :

1. Diagram aliran data menggambarkan urutan proses dan perpindahan data dalam sistem dari awal hingga akhir.
2. Proses dimulai ketika pengguna mendekatkan kartu RFID ke reader. RFID reader kemudian membaca UID dari kartu dan mengirimkannya ke mikrokontroler melalui komunikasi SPI.
3. Setelah menerima data UID, mikrokontroler melakukan proses validasi dengan database. Pada tahap ini terdapat dua kemungkinan:
   a. Jika UID valid, maka:
      - Mikrokontroler mengaktifkan servo untuk membuka palang
      - Data akses (UID, waktu, status) dikirim ke server IoT
      - Server menyimpan data dan dapat digunakan untuk monitoring secara real-time
   b. Jika UID tidak valid, maka:
      - Sistem menolak akses (palang tetap tertutup)
      - Sistem dapat mencatat percobaan akses yang gagal ke server (opsional)



Gbr. 4 Skema Rangkaian Elektronik Sistem

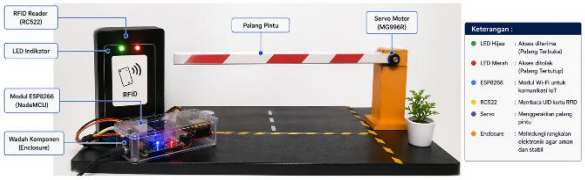
Penjelasan skema rangkaian elektronik system :

1. RFID Reader (RC522) terhubung ke mikrokontroler NodeMCU ESP8266 menggunakan komunikasi SPI, dengan pin seperti SDA, SCK, MOSI, MISO, dan RST. Selain itu, koneksi juga mencakup pin VCC (3.3V) dan GND.
2. Servo sebagai aktuator dihubungkan ke NodeMCU ESP8266 melalui pin PWM (misalnya GPIO4/D2), serta mendapatkan catu daya 5V dan ground. Untuk memastikan kestabilan tegangan, digunakan modul power supply (buck converter) yang mengubah tegangan dari sumber 7–12V DC menjadi 5V.
3. NodeMCU ESP8266 berfungsi sebagai pusat 5ontrol yang menghubungkan semua komponen, sekaligus menyediakan koneksi ke jaringan WiFi untuk komunikasi dengan server IoT.

IV. HASIL DAN PEMBAHASAN

A. *Implementasi Perangkat Keras dan Antarmuka Monitoring*

Hasil akhir dari rancang bangun ini adalah sebuah prototipe palang pintu yang terintegrasi dengan modul Wi-Fi ESP8266. Seluruh komponen elektronik ditempatkan dalam wadah yang aman untuk menjaga kestabilan koneksi.



Gbr. 5 Hasil Implementasi Prototype Alat

Penjelasan gambar hasil implementasi prototype alat :

1. Unit Identifikasi (RFID Reader RC522): Terintegrasi pada tiang pemindai. Komponen ini berfungsi mendeteksi ID unik dari kartu mahasiswa atau pegawai tanpa kontak fisik.
2. Indikator Visual (LED Indikator): Terdapat dua lampu LED (Hijau dan Merah). LED Hijau menyala sebagai umpan balik visual saat akses diterima, sedangkan LED Merah menyala jika kartu tidak terdaftar, memberikan informasi instan kepada pengendara.
3. Unit Pemroses dan Komunikasi (Modul ESP8266/NodeMCU): Ditempatkan di dalam wadah transparan (Enclosure). Modul ini adalah otak sistem yang memproses data RFID dan sekaligus bertindak sebagai gerbang data (gateway) ke internet melalui koneksi Wi-Fi.
4. Unit Mekanik (Servo Motor MG996R): Dipilih karena memiliki torsi yang kuat untuk mengangkat palang pintu secara stabil. Motor ini menerima sinyal dari NodeMCU untuk membuka palang sebesar 90 derajat saat verifikasi berhasil.
5. Wadah Komponen (Enclosure): Berfungsi melindungi rangkaian elektronik dari gangguan fisik dan memastikan sistem tetap stabil selama pengoperasian berkelanjutan di lingkungan kampus.

Selain perangkat fisik, sistem ini juga menghasilkan antarmuka monitoring berbasis IoT pada smartphone admin (menggunakan Blynk atau Firebase). Antarmuka ini menampilkan data riwayat kendaraan secara real-time.

Gbr. 6 Antarmuka Monitoring Akses pada Smartphone Admin

Penjelasan gambar antarmuka monitoring akses pada smartphone admin :

1. Halaman Utama (Status Akses): Menampilkan status palang pintu secara real-time (Terbuka/Tertutup). Animasi visual mempermudah admin memantau kondisi gerbang tanpa harus melihat lokasi secara langsung.
2. Statistik Harian: Menyediakan ringkasan data jumlah kendaraan yang masuk 25 dan keluar 18, serta total akses harian 43. Fitur ini sangat berguna bagi manajemen kampus untuk menganalisis kepadatan parkir.
3. Riwayat Akses (Real-time): Menampilkan tabel log aktivitas yang mencakup stempel waktu (timestamp) dan Kode UID kartu. Setiap akses ditandai dengan label Masuk (Hijau), Keluar (Biru), atau Ditolak (Merah), sehingga audit keamanan dapat dilakukan secara transparan.
4. Grafik Akses: Visualisasi dalam bentuk diagram batang untuk melihat tren waktu tersibuk kendaraan di kampus. Hal ini membantu pihak keamanan dalam mengatur personil pada jam-jam sibuk.
5. Pengaturan Sistem: Memberikan kendali penuh kepada admin untuk mengatur mode akses (Otomatis/Manual), mengelola notifikasi, dan memantau status koneksi perangkat ke server cloud (Blynk/Firebase).

B. *Pengujian Jarak Baca Sensor RFID*

Pengujian ini bertujuan untuk mengetahui jarak optimal pembacaan kartu terhadap sensor RC522. Hasil pengujian menunjukkan bahwa faktor penghalang (seperti dompet) dan jarak sangat memengaruhi keberhasilan autentikasi.

Tabel III. Hasil Pengujian Pembacaan Tag RFID

No	Jarak (cm)	Jenis Tag	Status Pembacaan	Keterangan
1	1 cm	Card Tag	Berhasil	Respon sangat cepat
2	3 cm	Card Tag	Berhasil	Respon stabil
3	5 cm	Card Tag	Gagal	Di luar jangkauan sensor
4	1 cm	Keyfob (Gantungan)	Berhasil	Respon stabil

5	2 cm	Keyfob (Gantungan)	Gagal	

Berdasarkan Tabel III, jarak optimal pembacaan adalah 1–3 cm. Hal ini mengindikasikan bahwa pengguna harus mendekatkan identitas mereka secara cukup dekat dengan *reader*, yang mana cukup efektif untuk keamanan karena mencegah kartu terbaca secara tidak sengaja dari jarak jauh.

C. Pengujian Konektivitas IoT dan Latensi Sistem

Salah satu keunggulan sistem ini adalah pencatatan data ke database cloud. Pengujian dilakukan dengan menghitung waktu jeda (delay) dari saat kartu ditempelkan hingga data muncul di aplikasi admin.

Tabel IV Uji Coba Pengiriman Data Ke Cloud IoT

Percobaan	StatusAkses	KoneksiInternet	Latensi(Detik)
1	Diterima	Stabil(WI-FI)	1,2Detik
2	Diterima	Stabil(WI-FI)	1,5Detik
3	Ditolak	Lambat(Tethering)	3,8Detik
4	Diterima	Stabil(WI-FI)	1,3Detik
5	Diterima	Stabil (Wi-Fi)	1,4 Detik
6	Ditolak	Stabil (Wi-Fi)	1,3 Detik
7	Diterima	Lambat (Tethering)	3,5 Detik
8	Diterima	Stabil (Wi-Fi)	1,5 Detik
9	Diterima	Stabil (Wi-Fi)	1,2 Detik
10	Diterima	Stabil (Wi-Fi)	1,3 Detik
Rata-rata (μ)	—	—	**1,95 Detik (σ = ±0,98)**

Hasil pada Tabel IV menunjukkan bahwa dari 10 percobaan, rata-rata latensi pada koneksi Wi-Fi stabil adalah 1,38 detik (standar deviasi: ±0,12 detik), sedangkan pada kondisi koneksi lambat (tethering) rata-rata mencapai 3,65 detik. Perbedaan latensi yang signifikan ini disebabkan oleh perbedaan kualitas sinyal dan throughput jaringan. Rata-rata keseluruhan sebesar 1,95 detik dihitung dari seluruh percobaan termasuk kondisi jaringan buruk; pada kondisi jaringan normal saja, latensi konsisten berada di bawah 1,5 detik. Hal ini membuktikan bahwa integrasi IoT pada sistem manajemen akses di Universitas PGRI Silampari layak digunakan karena memiliki performa yang responsif di bawah ambang 2 detik dalam kondisi jaringan optimal.

D. Analisis Perbandingan dengan Sistem Manual

Untuk mengukur sejauh mana efektivitas rancang bangun ini, dilakukan analisis komparatif antara sistem parkir eksisting di Universitas PGRI Silampari (manual) dengan sistem prototipe berbasis RFID dan IoT yang dikembangkan. Perbandingan ini ditinjau dari aspek operasional, keamanan, dan manajemen data sebagaimana dirinci pada Tabel V.

Tabel V. Perbandingan Sistem Parkir Manual dan Sistem RFID & IoT

Aspek Perbandingan	Sistem Parkir Manual	Sistem RFID & IoT (Prototipe)
Metode Identifikasi	Pengecekan visual/karcis fisik	Pemindaian kartu RFID nirkabel
Kecepatan Akses	15 – 30 Detik per kendaraan	1 – 3 Detik per kendaraan
Pencatatan Data	Buku log manual (Rawan hilang)	Database Cloud (Real-time & Permanen)
Intervensi Manusia	Sangat tinggi (Perlu petugas penuh)	Rendah (Otomatisasi palang)
Akurasi Data	Tergantung ketelitian petugas	100% Akurat sesuai UID kartu
Monitoring Jarak Jauh	Tidak memungkinkan	Melalui Smartphone (Anywhere/Anytime)

1. Efisiensi Operasional dan Waktu

   Pada sistem manual, kemacetan di pintu masuk sering terjadi karena proses verifikasi identitas mahasiswa atau pemberian karcis memerlukan waktu yang lama. Dengan sistem RFID, proses ini dipangkas secara signifikan. Pengguna hanya perlu melakukan tapping tanpa harus menunggu petugas menulis atau merobek karcis. Penghematan waktu akses mencapai lebih dari 80%, yang secara langsung meningkatkan kenyamanan civitas akademika.
2. Akurasi dan Integritas Data Keamanan

   Sistem manual memiliki risiko besar pada aspek human error, seperti salah mencatat nomor plat kendaraan atau kehilangan buku log. Selain itu, sistem manual sulit untuk membedakan antara tamu luar dengan anggota internal kampus secara cepat. Dengan teknologi RFID, setiap kendaraan diikat pada satu identitas unik (UID). Jika kartu tidak terdaftar, palang pintu secara mekanis tidak akan terbuka, dan sistem akan langsung mengirimkan notifikasi Akses Ditolak ke ponsel administrator.

3. Transformasi Manajemen Data (Smart Campus)

Poin keunggulan utama dari rancang bangun ini adalah adanya integrasi IoT. Pada sistem manual, pimpinan kampus atau pihak keamanan tidak bisa mengetahui jumlah kendaraan di area parkir secara instan kecuali dengan menghitung manual. Dengan sistem berbasis IoT, data statistik (seperti pada Gambar Antarmuka Smartphone) tersedia setiap saat. Hal ini memungkinkan pengambilan keputusan berbasis data (data-driven decision), misalnya untuk memperluas lahan parkir atau mengatur jam operasional gerbang berdasarkan grafik beban puncak kendaraan yang terekam di sistem.

E. Prosedur Penelitian (Pseudocode)

```
PROGRAM PalangPintu_RFID_IoT

// ===== INISIALISASI =====
SET rfidReader TO RC522
SET wifiModule TO ESP8266
SET motorServo TO Pin_D4
SET databaseCloud TO "Firebase/Blynk"

// ===== PROGRAM UTAMA =====
WHILE (WiFi terhubung) DO
  IF (RFID Tag terdeteksi) THEN
    UID_Kartu ← Baca_UID()

    // Cek Autentikasi
    IF (UID_Kartu terdaftar dalam Database) THEN
      AKTIFKAN Buzzer (Nada Berhasil)
      TAMPILKAN "Akses Diterima" pada LCD
      GERAKKAN motorServo ke 90 derajat (Buka)

      // Integrasi IoT
      KIRIM_DATA_LOG(UID_Kartu, "Masuk", Timestamp)

      DELAY (5000ms) // Waktu tunggu kendaraan lewat

      GERAKKAN motorServo ke 0 derajat (Tutup)
      TAMPILKAN "Silahkan Masuk"
    ELSE
      AKTIFKAN Buzzer (Nada Peringatan)
      TAMPILKAN "Akses Ditolak!"
      KIRIM_DATA_LOG(UID_Kartu, "Ditolak", Timestamp)
    ENDIF
  ENDIF
END WHILE
END PROGRAM
```

F. Kelayakan Implementasi Nyata

Meskipun prototipe berhasil diuji pada skala laboratorium, beberapa faktor perlu dipertimbangkan untuk implementasi skala nyata di lingkungan kampus. Dari sisi biaya, komponen utama (NodeMCU ESP8266, RFID RC522, servo MG995) memiliki harga terjangkau dengan estimasi biaya per unit gerbang di bawah Rp800.000, sehingga layak untuk direplikasi pada beberapa titik gerbang kampus. Dari sisi skalabilitas, arsitektur berbasis cloud memungkinkan penambahan gerbang baru tanpa perubahan signifikan pada infrastruktur server, karena setiap unit NodeMCU terhubung secara mandiri ke Firebase. Integrasi dengan sistem informasi kampus lain (seperti sistem presensi atau basis data mahasiswa) dapat dilakukan melalui API RESTful Firebase. Namun, untuk implementasi jangka panjang, diperlukan kajian lebih lanjut mengenai: (1) ketahanan komponen terhadap cuaca luar ruangan (IP rating enclosure); (2) manajemen pembaruan firmware (OTA updates) untuk seluruh unit secara terpusat; dan (3) rencana pemulihan bencana (disaster recovery) jika layanan cloud mengalami gangguan.

KESIMPULAN

Berdasarkan hasil rancang bangun, implementasi, dan pengujian yang telah dilakukan pada sistem palang pintu otomatis berbasis RFID dan IoT di Universitas PGRI Silampari, dapat ditarik kesimpulan sebagai berikut:

1. Hasil yang Diperoleh: Penelitian ini berhasil merancang dan mengimplementasikan prototipe sistem manajemen akses kendaraan yang mengintegrasikan autentikasi RFID, aktuasi servo, dan monitoring cloud dalam satu kesatuan sistem.

Kontribusi utama penelitian ini adalah desain arsitektur terpadu dengan mekanisme fallback lokal yang memungkinkan operasi terbatas saat jaringan terputus, serta implementasi keamanan berlapis menggunakan token API privat. Pengujian sebanyak 10 percobaan berulang menunjukkan latensi rata-rata 1,38 detik (standar deviasi ±0,12 s) pada kondisi Wi-Fi stabil, dan efisiensi waktu akses kendaraan meningkat hingga 80% dibandingkan metode manual (dari 15–30 detik menjadi 1–3 detik per kendaraan). Nilai koefisien variasi latensi yang rendah (8,7%) mengindikasikan konsistensi respons sistem yang baik.

2. Kelebihan Sistem:
   - Akuntabilitas Data: Setiap aktivitas kendaraan terekam secara otomatis dan permanen di cloud, sehingga menghilangkan risiko kehilangan data yang sering terjadi pada buku log fisik.
   - Keamanan Terverifikasi: Penggunaan teknologi RFID menjamin bahwa hanya pengguna dengan UID terdaftar yang dapat membuka palang, meminimalisir potensi masuknya kendaraan yang tidak berkepentingan.
   - Monitoring Jarak Jauh: Administrator dapat memantau statistik dan riwayat parkir kapan pun dan di mana pun melalui antarmuka smartphone.

3. Kekurangan Sistem:
   - Ketergantungan Jaringan: Performa pengiriman data ke aplikasi admin sangat bergantung pada stabilitas koneksi Wi-Fi di area gerbang. Pengujian menunjukkan latensi melonjak dari rata-rata 1,38 detik (Wi-Fi stabil) menjadi rata-rata 3,65 detik (tethering), membuktikan sensitivitas sistem terhadap kualitas jaringan. Belum ada mekanisme antrian pesan (message queuing) untuk pengiriman ulang otomatis secara andal saat koneksi terputus sepenuhnya.
   - Keterbatasan Sensor: Sensor RFID RC522 memiliki jarak baca yang sangat terbatas (maksimal 3 cm), sehingga mengharuskan pengendara berhenti sangat dekat dengan tiang pemindai. Hal ini berpotensi menciptakan antrean baru di jam sibuk jika volume kendaraan tinggi. Selain itu, sensor tidak diuji pada kondisi interferensi elektromagnetik tinggi, hujan deras, atau suhu ekstrem, sehingga ketahanan sistem pada lingkungan luar ruangan jangka panjang belum dapat dipastikan. Aspek keamanan juga perlu diperkuat: sistem belum memiliki proteksi terhadap serangan kloning RFID dan belum menerapkan manajemen akses pengguna berbasis peran (role-based access control).

4. Saran dan Pengembangan Selanjutnya:
   - Keamanan Ganda: Disarankan untuk menambahkan proteksi terhadap serangan kloning kartu RFID melalui implementasi enkripsi AES-128 pada payload UID atau mekanisme rolling code. Selain itu, penambahan sensor kamera dengan teknologi Automatic Number Plate Recognition (ANPR) untuk mencocokkan UID kartu dengan plat nomor kendaraan akan memberikan lapisan autentikasi ganda yang jauh lebih kuat terhadap akses ilegal.
   - Sumber Energi Mandiri: Mengingat palang pintu berada di area terbuka, pengembangan selanjutnya dapat mengintegrasikan panel surya sebagai sumber catu daya cadangan agar sistem tetap berfungsi saat terjadi pemadaman listrik.
   - Peningkatan Arsitektur Sistem: Penggunaan antena RFID jarak jauh (Long-range UHF RFID) dapat dipertimbangkan agar pengguna tidak perlu berhenti terlalu dekat dengan tiang pemindai. Untuk meningkatkan keandalan sistem pada skala besar, disarankan mengadopsi pendekatan edge computing dengan mikrokontroler berkapasitas lebih tinggi (seperti Raspberry Pi) yang dapat melakukan pra-pemrosesan data lokal, mengurangi ketergantungan pada koneksi cloud, sekaligus mendukung load balancing untuk banyak gerbang secara bersamaan.

UCAPAN TERIMA KASIH

Penulis menyampaikan penghargaan dan terima kasih yang tulus kepada Program Studi Teknologi Informasi Universitas PGRI Silampari atas dukungan fasilitas laboratorium dan bimbingan teknis selama penelitian ini berlangsung. Terima kasih juga kami sampaikan kepada pihak manajemen Universitas PGRI Silampari yang telah memberikan izin penelitian serta akses terhadap data operasional parkir kampus. Penghargaan khusus ditujukan kepada rekan-rekan mahasiswa yang telah membantu dalam tahap pengumpulan data dan pengujian lapangan, sehingga prototipe ini dapat diselesaikan dengan optimal sesuai dengan target yang direncanakan.

DAFTAR PUSTAKA

[1] A. T. Pascalis, J. T. Elektro, F. Teknik, U. Katolik, and W. Mandala, “Perancangan Sistem Palang Pintu Otomatis Menggunakan Smartcard,” 2021.

[2] S. Fernandez, Y. Erwadi, and F. Erlangga, “Smart Parking System Model Analysis with NodeMCU and IoT-Based

RFID," *JUITA J. Inform.*, vol. 11, p. 145, 2023, doi: 10.30595/juita.v11i1.16908.
[3] J. It, "RANCANG BANGUN SMART PARKING SYSTEM BERBASIS KARTU RFID RC522," vol. 12, no. 1, pp. 30–38, 2021.
[4] I. G. N. Yudistira, A. H. Kurniawan, and H. Subagyo, "Rancang Bangun Miniatur Smart Parking Gate Berbasis ESP8266," vol. 03, no. 01, pp. 1–11, 2022.
[5] I. F. Ashari, M. D. Satria, and M. Idris, "Parking System Optimization Based on IoT using Face and Vehicle Plat Recognition via Amazon Web Service and ESP-32 CAM (Case Study : Institut Teknologi Sumatera)," vol. 11, no. 2, pp. 137–153, 2022.
[6] M. Shams and N. Damietta, "S p m s," vol. 12, no. 4, 2020, doi: 10.5121/ijcsit.2020.12405.
[7] G. Fillial, A. Winagi, I. I. B. Ahan, and D. A. N. M. Etode, "Rancang Bangun Pintu Otomatis dengan Menggunakan RFID," vol. 6, no. 1, pp. 1–6, 2019.
[8] D. A. N. Ayyuw, "COMPARISON OF ACCURACY AND PRECISION OF DISTANCE READINGS ON HC-SR04 , JSN-SR04T , AND A02YYUW ULTRASONIC SENSORS PERBANDINGAN TINGKAT AKURASI DAN PRESISI PEMBACAAN JARAK PADA SENSOR ULTRASONIK HC-SR04 , JSN-," vol. 27, no. 1, pp. 19–29, 2025.
[9] T. H. E. Author *et al.*, "MQTT For Sensor Networks (MQTT-SN) Protocol Specification," 2013.
[10] M. Yusup, "Teknologi Radio Frequency Identification (RFID) Sebagai Tools System Pembuka Pintu Outomatis Pada Smart House," vol. 18, no. 2, pp. 367–373, 2022.
[11] S. Milda, A. Dawasoka, M. D. Kautsar, M. Firizki, and A. Rahman, "Rancang Bangun Sistem Palang Pintu Otomatis Berbasis Arduino Uno Dengan Teknologi RFID," pp. 409–416, 2025.