

Sistem Keamanan Pintu Menggunakan Sensor Reed Switch dengan Notifikasi Discord

Rizki Dini Hari*, Hermanto, Kamdan

Fakultas Teknik, Komputer dan Desain, Program Studi Teknik Informatika, Universitas Nusa Putra, Sukabumi
Jl. Raya Cibolang Cisaat - Sukabumi No.21, Cibolang Kaler, Kec. Cisaat, Kabupaten Sukabumi, Jawa Barat, Indonesia

Email: ^{1,*}rizki.dinihari_ti21@nusaputra.ac.id, ²hermanto@nusaputra.ac.id, ³kamdan@nusaputra.ac.id,

Email Penulis Korespondensi: rizki.dinihari_ti21@nusaputra.ac.id

Submitted: 13/07/2025; Accepted: 31/07/2025; Published: 31/07/2025

Abstrak—Sistem keamanan merupakan komponen krusial dalam menciptakan lingkungan sekolah yang aman dan kondusif. Penelitian ini bertujuan untuk merancang dan membangun sebuah prototipe sistem keamanan pintu otomatis di SMPN 1 Warungkiara. Sistem ini mengintegrasikan sensor reed switch untuk mendeteksi status pintu, serta teknologi RFID dan fingerprint sebagai media autentikasi akses. Notifikasi keamanan dikirimkan secara real-time melalui platform Discord menggunakan mikrokontroler NodeMCU ESP8266 yang terhubung ke jaringan Wi-Fi, terutama untuk aktivitas mencurigakan di luar jam operasional. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan studi kasus, sementara pengembangan sistem menerapkan model prototyping. Tahapan pengembangan meliputi komunikasi kebutuhan, perancangan cepat, pembuatan prototipe, dan evaluasi oleh pengguna. Hasil pengujian menunjukkan prototipe sistem dapat berfungsi dengan baik dan efektif. Sensor mampu mendeteksi status pintu secara akurat, proses autentikasi menggunakan RFID dan fingerprint berjalan sesuai rancangan, dan notifikasi ke Discord terkirim secara instan. Implementasi sistem ini diharapkan dapat meningkatkan pengawasan keamanan secara digital, meminimalisir risiko, serta mendukung terciptanya proses belajar mengajar yang lebih aman dan nyaman di lingkungan sekolah.

Kata Kunci: Sistem Keamanan; Internet of Things (IoT); Reed Switch; RFID; Fingerprint; Discord; NodeMCU

Abstract—A security system is a crucial component in creating a safe and conducive school environment. This research aims to design and build a prototype of an automatic door security system at SMPN 1 Warungkiara. The system integrates a reed switch sensor to detect the door's status, along with RFID and fingerprint technology as access authentication media. Security notifications are sent in real-time via the Discord platform using a NodeMCU ESP8266 microcontroller connected to a Wi-Fi network, especially for suspicious activities outside operational hours. The research method employed is qualitative with a case study approach, while the system development applies the prototyping model. The development stages include requirements communication, quick design, prototype construction, and user evaluation. The test results indicate that the system prototype functions well and effectively. The sensor accurately detects the door's status, the authentication process using RFID and fingerprint operates as designed, and notifications to Discord are sent instantly. The implementation of this system is expected to enhance digital security monitoring, minimize risks, and support the creation of a safer and more comfortable teaching and learning process within the school environment.

Keywords: Security System; Internet of Things; Reed Switch; RFID; Fingerprint; Discord; NodeMCU

1. PENDAHULUAN

Perkembangan teknologi komunikasi telah membawa perubahan besar dalam dunia pendidikan[1]. Pemanfaatan teknologi seperti Internet of Things (IoT) membuka peluang untuk meningkatkan keamanan lingkungan sekolah secara signifikan. Di SMPN 1 Warungkiara, sistem keamanan pintu yang ada saat ini masih bersifat konvensional, mengandalkan kunci manual atau pengawasan terbatas. Keterbatasan fundamental ini menciptakan berbagai celah keamanan yang signifikan. Sistem kunci manual sangat rentan terhadap risiko kehilangan atau duplikasi kunci tanpa izin, yang dapat membahayakan seluruh aset sekolah. Selain itu, tidak ada jejak audit digital, sehingga mustahil untuk melacak siapa yang masuk dan kapan, menyulitkan investigasi jika terjadi insiden. Situasi ini berpotensi merugikan pihak sekolah, tidak hanya dari segi kehilangan aset berharga seperti peralatan laboratorium komputer dan dokumen administratif, tetapi juga dapat menciptakan gangguan serius terhadap kegiatan belajar mengajar yang seharusnya berjalan kondusif.

Untuk mengatasi masalah tersebut, diperlukan sebuah sistem keamanan terdigitalisasi yang lebih efektif, proaktif, dan mampu memberikan lapisan keamanan modern[2]. Penggunaan RFID dan fingerprint berfungsi sebagai metode autentikasi ganda yang aman dan efisien, di mana hanya pengguna terdaftar yang dapat memperoleh akses[3]. Sensor reed switch ditambahkan untuk memantau status fisik pintu (terbuka/tertutup) secara real-time. Keunggulan utama sistem ini adalah kemampuannya mengirimkan notifikasi instan melalui platform Discord saat terdeteksi aktivitas mencurigakan, seperti upaya pembobolan di luar jam operasional[4].

Beberapa penelitian terkait telah dilakukan sebelumnya dan menjadi landasan bagi pengembangan sistem ini. Penelitian oleh Syahputra, dkk. (2024) merancang sistem keamanan pintu menggunakan identifikasi sidik jari dengan notifikasi berbasis Telegram[5]. Persamaannya terletak pada penggunaan biometrik, namun perbedaannya adalah platform notifikasi yang digunakan dan penelitian ini menambahkan autentikasi RFID dan menggunakan notifikasi discord. Faturrachman dan Yustiana (2021) juga berfokus pada keamanan pintu berbasis IoT dan sidik jari untuk lingkungan rumah. Penelitian ini mengembangkannya dengan menambahkan faktor autentikasi kedua (RFID) untuk keamanan berlapis dan menerapkannya pada konteks institusi sekolah yang memiliki kebutuhan

pengawasan berbeda[6]. Sementara itu, Alfonsius, dkk. (2024) mengembangkan sistem keamanan pintu menggunakan RFID dan keypad dengan mikrokontroler Arduino Nano. Perbedaan signifikan dalam penelitian ini adalah penggunaan sensor sidik jari yang lebih aman dibandingkan keypad, serta pemanfaatan NodeMCU ESP8266 yang memiliki modul Wi-Fi terintegrasi untuk konektivitas IoT yang lebih efisien dalam mengirim notifikasi[7]. Terakhir, penelitian Yulisman, dkk. (2021) yang menerapkan pintu otomatis berbasis E-KTP (RFID) untuk hotel menunjukkan relevansi dalam teknologi akses. Namun, penelitian ini mengadaptasi konsep tersebut untuk tujuan keamanan sekolah dengan menambahkan fitur krusial seperti deteksi intrusi melalui reed switch dan sistem peringatan dini melalui Discord, yang lebih menekankan pada aspek keamanan daripada kemudahan akses komersial[8].

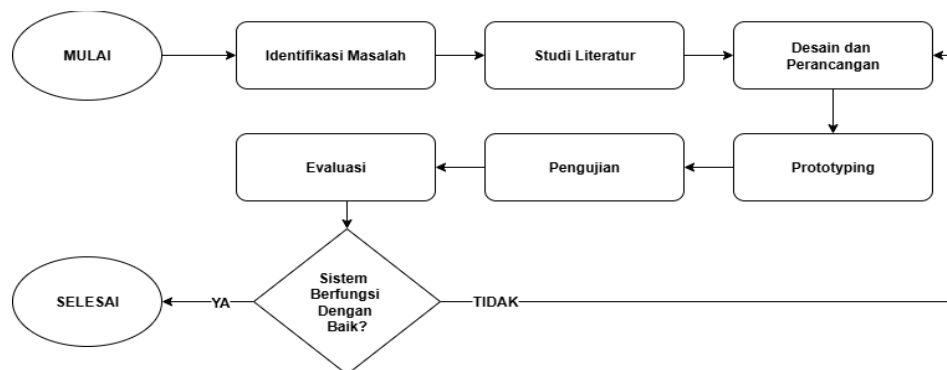
Berdasarkan latar belakang dan analisis tersebut, tujuan dari penelitian ini adalah: 1) Merancang dan mengimplementasikan sistem keamanan pintu otomatis di SMPN 1 Warungkiara yang mampu memantau status buka/tutup pintu secara real-time menggunakan sensor reed switch. 2) Membangun mekanisme pengiriman notifikasi instan melalui platform Discord kepada pihak yang berwenang apabila terjadi perubahan status pintu yang tidak sah atau terdeteksi upaya pembobolan. 3) Mengintegrasikan komponen perangkat keras dengan perangkat lunak untuk menciptakan sistem yang berfungsi secara sinergis.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kualitatif yang berfokus pada eksplorasi mendalam dan deskripsi fenomena dari berbagai sumber, seperti wawancara dan observasi langsung untuk memberikan pemahaman yang luas terhadap masalah yang sedang diteliti[9]. Meskipun menggunakan metode kualitatif, penelitian ini juga menggunakan sistem secara protoipe sebagai dasar dalam pengembangan dan implementasi alat. Pada penelitian ini menggunakan teknik pengumpulan data primer, Penelitian kualitatif merupakan penelitian yang bersifat deskriptif dan analisis[10]. Deskriptif dalam penelitian kualitatif berarti menggambarkan dan menjabarkan peristiwa, fenomena dan situasi sosial yang diteliti[11]. Analisis berarti memaknai dan menginterpretasikan serta membandingkan data hasil penelitian. Maka dari itu penelitian ini menggunakan teknik pengumpulan data dengan melakukan wawancara dan observasi[12]. Alur proses untuk tahapn penelitian dapat di lihat pada gambar 1 berikut

2.1 Tahapan Penelitian

Tahapan penelitian adalah level atau tingkatan dalam penelitian yang dilakukan secara terstruktur, runtut, baku, logis dan juga sistematis.



Gambar 1. Tahapan Penelitian

Dari Gambar 1 tahapan tersebut dapat dijelaskan sebagai berikut:

a. Studi Literatur

Pada tahap awal penelitian, dilakukan studi literatur yang merupakan proses untuk menghimpun berbagai data dan sumber yang berkaitan dengan topik riset atau penelitian. Berbagai sumber informasi seperti jurnal, buku, dokumen, internet, dan koleksi perpustakaan dimanfaatkan dalam proses ini. Pada intinya studi literatur adalah sebuah pendekatan riset yang berfokus pada penelaahan referensi teoritis untuk menjawab masalah yang sedang diteliti[13]. Pada penelitian ini studi literatur berfungsi untuk memahami perkembangan mikrokontroler ESP8266 yang digunakan untuk mengontrol pendeteksi kebakaran. Selain itu untuk meninjau berbagai penelitian tentang integrasi IoT, dan studi literatur ini berfungsi untuk menemukan perbedaan pada penelitian sebelumnya agar Solusi yang di buat bermanfaat dan dapat digunakan dengan sebaik baiknya[14].

b. Perancangan

Tahap perancangan merupakan fase krusial di mana cetak biru sistem keamanan ini dibentuk. Perancangan ini meliputi spesifikasi teknis untuk komponen perangkat keras (hardware), serta arsitektur dan alur logika untuk perangkat lunak (software). Tujuan dari tahap ini adalah untuk memastikan semua komponen dapat berinteraksi secara sinergis untuk menciptakan sistem yang andal dan responsif. Desain ini mencakup dua komponen utama yang dijelaskan di bawah ini[15].

1. Desain Alat

Desain perangkat keras difokuskan pada pemilihan dan integrasi komponen fisik untuk membangun prototipe yang fungsional. Arsitektur perangkat keras dirancang dengan pendekatan dual-controller untuk optimalisasi pemrosesan data[16].

- a) Mikrokontroler: Sistem ini menggunakan dua unit NodeMCU ESP8266 sebagai otak pemrosesan. Pemilihan mikrokontroler ini didasarkan pada keunggulannya yang memiliki modul Wi-Fi built-in, yang merupakan syarat esensial untuk dapat terhubung ke internet dan mengirimkan notifikasi ke platform Discord[17]. Tugas dibagi antara dua papan: satu NodeMCU (versi Lolin V3) berfungsi sebagai pengendali utama yang menangani sensor RFID, reed switch, dan modul relay, sementara satu NodeMCU lainnya (versi Amica 12E) didedikasikan khusus untuk memproses data dari sensor fingerprint.
- b) Sensor dan Autentikasi: Untuk mendeteksi status pintu secara akurat, digunakan sebuah sensor reed switch. Sensor ini terdiri dari dua bagian magnetik yang dipasang di kusen dan daun pintu. Sensor dihubungkan ke salah satu pin digital NodeMCU yang dikonfigurasi sebagai INPUT_PULLUP untuk memastikan pembacaan status buka/tutup yang stabil dan konsisten. Untuk autentikasi akses, sistem ini dilengkapi dengan modul RFID RC522 untuk akses menggunakan kartu dan sebuah sensor fingerprint untuk keamanan biometrik.
- c) Sumber Daya (Power Supply): Sistem ini memerlukan dua sumber daya terpisah untuk operasional yang stabil. Mikrokontroler NodeMCU dan komponen bertegangan rendah lainnya ditenagai oleh adaptor DC 5V 2A yang terhubung melalui port micro-USB. Sementara itu, Solenoid Door Lock yang berfungsi sebagai aktuatur pengunci pintu memerlukan tegangan yang lebih tinggi, sehingga ditenagai oleh adaptor 12V secara terpisah.

2. Desain Sistem

Desain sistem atau perangkat lunak bertujuan untuk menulis logika yang mengatur bagaimana perangkat keras beroperasi dan berkomunikasi, terutama dalam hal pemrosesan data sensor dan pengiriman notifikasi[18].

- a) Alur Logika Program (Flowchart): Logika program dirancang menggunakan alur kerja yang jelas[19]. Saat sistem dinyalakan, program pertama-tama akan melakukan inisialisasi dan mencoba terhubung ke jaringan Wi-Fi yang tersedia. Setelah berhasil terhubung, mikrokontroler akan masuk ke dalam loop utama di mana ia secara terus-menerus memindai input dari sensor RFID, fingerprint, dan reed switch. Jika ada autentikasi yang sah, program akan mengaktifkan relay untuk membuka kunci. Namun, jika sensor reed switch mendeteksi pintu terbuka tanpa didahului oleh autentikasi yang sah, program akan mengidentifikasinya sebagai upaya pembobolan dan memicu alur notifikasi. Program juga dirancang untuk menangani kesalahan, seperti kegagalan koneksi Wi-Fi.
- b) Integrasi API Discord: Untuk mengirim notifikasi, sistem diintegrasikan dengan API Discord. Proses ini dimulai dengan membuat sebuah Bot khusus di platform Discord menggunakan BotFather untuk mendapatkan Token API yang unik. Selanjutnya ID Chat dari kanal atau pengguna yang akan menerima notifikasi diidentifikasi[20]. Di dalam kode program NodeMCU, sebuah fungsi khusus dibuat untuk mengirimkan permintaan HTTP POST ke endpoint API Discord. Permintaan ini berisi Token API untuk autentikasi dan pesan notifikasi yang akan dikirim.
- c) Format Notifikasi: Format pesan notifikasi dirancang agar informatif dan mudah dipahami oleh petugas keamanan. Ketika terdeteksi upaya pembobolan, sistem akan mengirimkan pesan yang jelas dan lugas seperti "PINTU DIBUKA PAKSA!" atau "Peringatan! Pintu Laboratorium Terbuka!". Pesan ini juga dapat dikembangkan untuk menyertakan stempel waktu (timestamp) kejadian guna mempermudah pelacakan dan audit keamanan.

c. Prototyping

Penelitian ini menerapkan metode prototyping, sebuah pendekatan pengembangan sistem yang iteratif. Prosesnya diawali dengan tahap Komunikasi untuk memahami kebutuhan pengguna di SMPN 1 Warungkiara, yang kemudian dilanjutkan dengan Perancangan Cepat untuk arsitektur perangkat keras dan lunak. Setelah itu, sebuah Prototipe fungsional dirakit dan diprogram, yang pada akhirnya masuk ke tahap Penyerahan dan Umpan Balik. Pada tahap akhir ini, prototipe diserahkan kepada pengguna untuk dievaluasi, memungkinkan adanya perbaikan berulang hingga sistem dinilai berhasil dan sesuai dengan kebutuhan yang telah ditetapkan[7].

d. Pengujian

Setelah unit prototipe fungsional berhasil dirakit dan diprogram, penelitian memasuki tahap krusial berikutnya, yaitu Pengujian. Tahap ini bertujuan untuk memvalidasi dan memverifikasi apakah sistem yang telah dibangun dapat beroperasi sesuai dengan rancangan dan tujuan awal[21]. Proses pengujian dilakukan secara sistematis melalui serangkaian skenario yang dirancang untuk mengevaluasi setiap komponen dan fitur secara individual maupun terintegrasi. Pengujian dibagi menjadi tiga fokus utama:

1. Pengujian Fungsionalitas Sensor dan Alarm: Pengujian pertama difokuskan pada komponen deteksi intrusi utama, yaitu sensor reed switch dan buzzer. Skenario pengujian meliputi simulasi pembukaan pintu secara paksa untuk memastikan sensor dapat secara akurat mendeteksi perubahan status dan berhasil memicu

buzzer sebagai alarm suara. Selain itu, diuji juga bahwa alarm tidak akan berbunyi ketika pintu dibuka secara sah setelah autentikasi berhasil, guna menghindari alarm palsu.

2. **Pengujian Sistem Autentikasi dan Akses:** Pengujian ini mengevaluasi keandalan sistem autentikasi ganda. Dilakukan percobaan menggunakan kartu RFID yang valid (terdaftar) dan tidak valid untuk memastikan modul RFID RC522 dan program dapat membedakannya dengan benar. Hal yang sama dilakukan pada sensor fingerprint, di mana sidik jari yang terdaftar dan tidak terdaftar diuji untuk memverifikasi akurasi sensor biometrik. Pengujian juga mencakup fungsi akses dari dalam ruangan menggunakan push button dan skenario kegagalan daya untuk memastikan sistem bersifat fail-secure (pintu tetap terkunci saat listrik padam).
3. **Pengujian Fungsionalitas Notifikasi Discord:** Fokus pengujian terakhir adalah pada sistem notifikasi. Skenario ini memastikan bahwa setiap kali terdeteksi pembukaan paksa, sistem dapat secara instan dan andal mengirimkan pesan peringatan ke kanal Discord yang telah ditentukan. Kecepatan pengiriman, keakuratan isi pesan (misalnya, "PINTU DIBUKA PAKSA!"), dan ketahanan sistem terhadap kondisi seperti koneksi internet yang lambat atau pemicuan alarm berulang kali (uji spam) juga dievaluasi dalam tahap ini untuk memastikan efektivitas notifikasi sebagai sistem peringatan dini.
- e. **Evaluasi**
Evaluasi adalah fase analisis yang dilakukan setelah pengujian, di mana semua data hasil uji dianalisis untuk menentukan apakah sistem telah berhasil memenuhi tujuan awal penelitian[6]. Pada tahap ini, keberhasilan setiap fitur mulai dari akurasi sensor, keandalan autentikasi, hingga efektivitas notifikasi dinilai secara kritis. Proses ini menjadi titik penentu: jika sistem terbukti berfungsi dengan baik, sebagaimana ditunjukkan oleh status "LULUS" pada semua skenario uji dalam penelitian ini, maka penelitian dapat dilanjutkan ke tahap kesimpulan. Sebaliknya, jika ditemukan kegagalan, alur penelitian akan kembali ke tahap perancangan atau protoyping untuk dilakukan perbaikan[8].

2.2 Alat dan Bahan

Untuk merealisasikan sistem keamanan pintu ini, diperlukan serangkaian komponen perangkat keras (hardware) dan perangkat lunak (software) yang dipilih secara spesifik berdasarkan fungsinya. Komponen-komponen ini terbagi menjadi tiga kategori utama: unit pemrosesan, perangkat input (sensor), dan perangkat output (aktuator). Rincian lengkap mengenai alat dan bahan yang digunakan dalam penelitian ini disajikan pada Tabel 1.

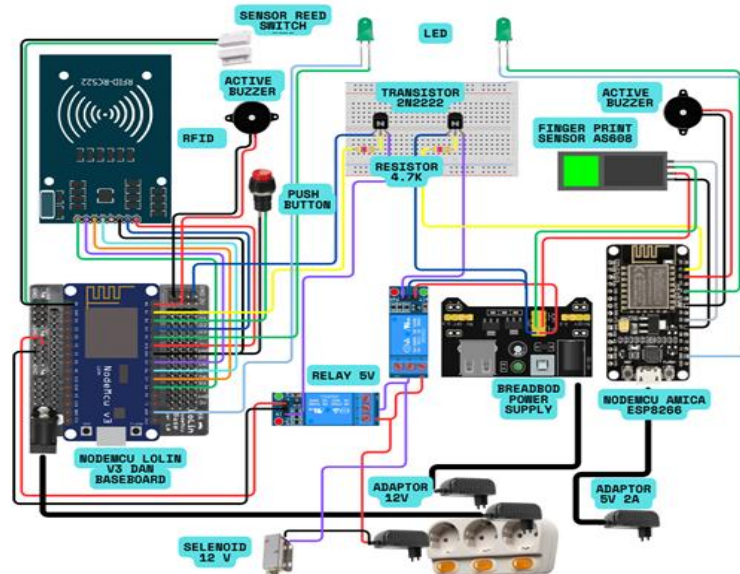
Tabel 1. Alat dan Bahan

No	Nama Bahan	Jumlah Bahan
1	NodeMCU ESP8266 Amica	1 Unit
2	NodeMCU ESP8266 LolinV3	1 Unit
3	Reed Switch	1 Unit
4	Buzzer	1 Unit
5	Lampu LED	2 Unit
6	Breadboard	2 Unit
7	RFID – RC522	1 Unit
8	Sensor Fingerprint	1 Unit
9	Solenoid Door Lock	1 Unit
10	Transistor 2n2222	2 Unit
11	Resistor 4.7k	2 Unit
12	Relay 5v	2 Unit
13	Adaptor 12V	3 Unit
14	Adaptor 5V 2A	1 Unit
15	Breadboard Power Supply 5v & 3.3v	1 Unit
16	Push Button	1 Unit
17	Kabel Jumper Female/male	1 Pcs
18	Kabel Micro USB	1 Unit

2.3 Skematik Alat

Skematik ini menggambarkan arsitektur sebuah sistem kunci pintu pintar yang secara unik dibangun di atas dua mikrokontroler NodeMCU yang bekerja paralel untuk membagi tugas secara spesifik[22]. Untuk mendukung operasinya, sistem ini ditenagai oleh dua adaptor terpisah: sebuah Adaptor 5V yang menyuplai daya ke seluruh komponen elektronik seperti kedua NodeMCU dan jajaran sensor melalui modul power supply breadboard dan sebuah Adaptor 12V yang dayanya didedikasikan khusus untuk menggerakkan Solenoid Lock. Pembagian tugas di antara kedua otak sistem ini sangat jelas: NodeMCU AMICA (kanan) bertindak sebagai pengendali utama, bertanggung jawab atas otentikasi biometrik melalui Sensor Sidik Jari dan secara langsung mengaktifkan Relay 5V untuk membuka kunci, sambil memberikan umpan balik visual dan suara via LED dan buzzer. Sementara itu, NodeMCU V3 (kiri) berfungsi sebagai pengendali sekunder yang mengelola otentikasi alternatif via RFID Reader,

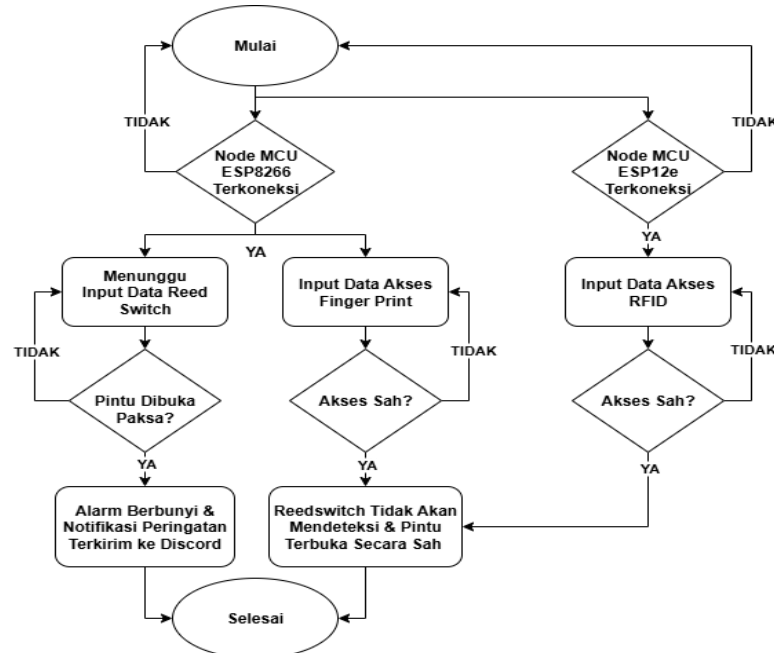
sekaligus memonitor status fisik pintu melalui Sensor Reed Switch dan menerima input manual dari Push Button. Dengan demikian, otentikasi yang berhasil dari salah satu jalur akan memicu aksi utama, yaitu pengaktifan relay oleh NodeMCU kanan untuk membuka kunci pintu. Berikut Gambar 2 skematik alat perancangan alur kerja sistem keamanan pintu.



Gambar 2. Skematik Alat

2.4 Perancangan Alur Kerja Sistem Keamanan Pintu

Perancangan alur kerja sistem baru merupakan gambaran proses terhadap sistem yang akan dibangun. Dimulai dari proses awal sistem dijalankan sampai dengan proses akhir dari sistem.



Gambar 3. Alur Kerja Sistem Keamanan Pintu

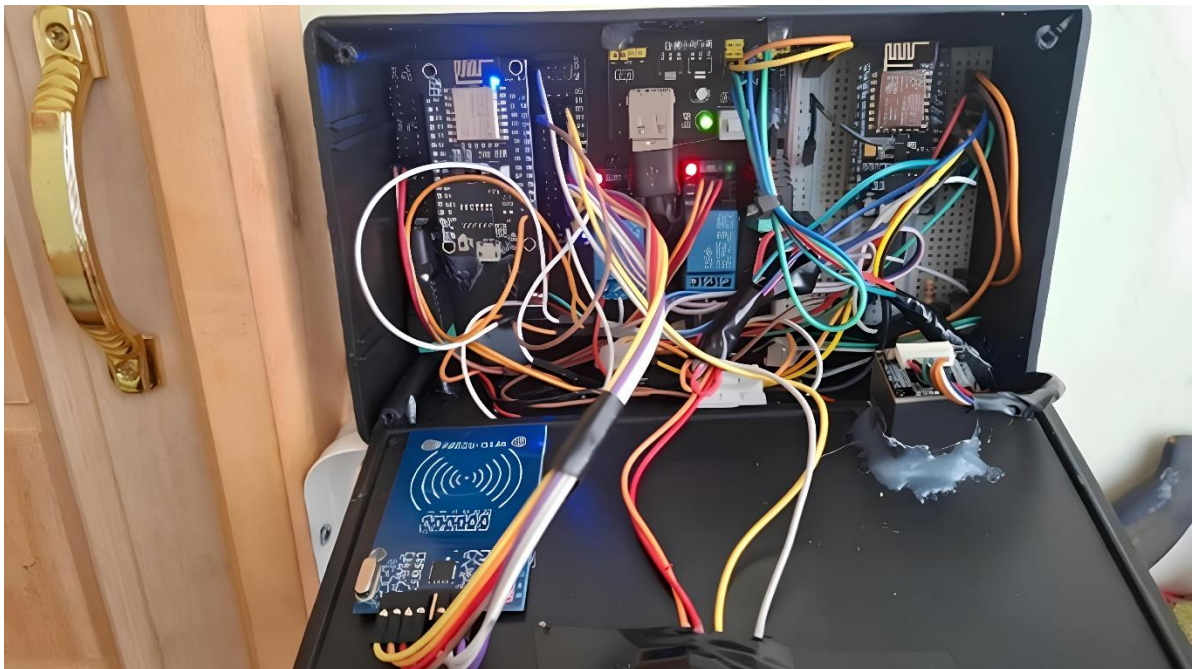
Gambar 3 merupakan alur kerja sistem keamanan pintu pintar dengan memulai operasinya dari titik "Mulai". Langkah pertama yang fundamental adalah melakukan verifikasi koneksi dengan mikrokontroler NodeMCU, baik itu varian ESP8266 maupun ESP12e. Hanya setelah koneksi berhasil terjalin, sistem akan melanjutkan ke fungsi-fungsi utamanya. Setelah tahap inisialisasi, alur kerja sistem ini secara unik terbagi menjadi tiga cabang proses yang berjalan secara paralel dan independen. Ketiga cabang ini mewakili fungsi inti dari sistem: satu untuk deteksi pembobolan melalui Reed Switch, dan dua lainnya untuk proses autentikasi akses melalui Fingerprint dan RFID. Pada jalur autentikasi, ketika seorang pengguna mencoba mengakses pintu menggunakan sidik jari atau kartu RFID, sistem akan menerima data input tersebut. Data ini kemudian akan divalidasi melalui tahap keputusan "Akses Sah?". Jika akses terbukti valid, sistem tidak hanya membuka pintu, tetapi juga secara

cerdas memastikan bahwa sensor Reed Switch tidak akan salah menafsirkan pembukaan ini sebagai upaya paksa, sesuai dengan status "Reedswitch Tidak Akan Mendeteksi & Pintu Terbuka Secara Sah". Jika akses tidak sah, alur untuk proses tersebut akan berhenti. Secara bersamaan, jalur keamanan yang berpusat pada Reed Switch terus aktif memantau kondisi pintu. Alur ini secara spesifik dirancang untuk menjawab pertanyaan "Pintu Dibuka Paksa?". Apabila sistem mendeteksi adanya pembukaan pintu yang tidak melalui proses autentikasi yang sah, maka sistem akan langsung mengambil tindakan. Responsnya adalah dengan membunyikan alarm fisik dan secara simultan mengirimkan notifikasi peringatan real-time ke server Discord. Sebagai penutup dari setiap alur, baik itu setelah akses yang berhasil maupun setelah alarm peringatan terkirim, semua cabang proses akan bermuara pada titik akhir "Selesai". Ini mengindikasikan bahwa dalam desain flowchart ini, setiap siklus operasi (akses ataupun peringatan) dianggap sebagai satu tugas yang tuntas, sebelum sistem mengakhiri alurnya.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Alat

Tahap implementasi merupakan fase realisasi fisik dari rancangan sistem dan alur kerja yang telah dibuat sebelumnya[23]. Pada tahap ini, seluruh komponen elektronik utama meliputi mikrokontroler NodeMCU ESP8266, sensor sidik jari, pembaca kartu RFID, dan modul relay sebagai saklar elektrik dirangkai secara cermat menjadi satu kesatuan unit fungsional. Proses ini melibatkan penyambungan setiap modul menggunakan kabel jumper, mengikuti konfigurasi pin yang telah ditentukan pada tahap perancangan untuk memastikan semua komponen dapat berkomunikasi dengan benar. Untuk menciptakan prototipe yang ringkas, aman, dan terlindungi, keseluruhan rangkaian elektronik ini ditempatkan di dalam sebuah boks proyek. Hasil akhir dari proses perakitan ini adalah sebuah perangkat kunci pintu pintar yang terintegrasi, yang wujud fisiknya dapat dilihat pada Gambar 4.



Gambar 4. Implementasi Alat Keamanan Pintu

3.2 Hasil Pengujian

Hasil pengujian menggambarkan seluruh hasil uji coba yang dilakukan kepada sistem. Pada proses pengujian akan memastikan setiap proses pada sistem berjalan dengan baik atau tidak.

Tabel 2. Hasil Pengujian

No.	Skenario Pengujian	Langkah-langkah	Hasil yang Diharapkan	Hasil Aktual	Status
1.	Akses Berhasil via RFID	Menempelkan kartu RFID yang telah terdaftar pada sensor RC522	Kunci Solenoid terbuka. Lampu Indikator Terbuka Menyala	Kunci Solenoid terbuka. Lampu Indikator Terbuka Menyala	LULUS
2.	Akses Ditolak via RFID	Menempelkan kartu RFID yang tidak	Kunci Solenoid tetap terkunci	Kunci Solenoid tetap terkunci	LULUS

No.	Skenario Pengujian	Langkah-langkah	Hasil yang Diharapkan	Hasil Aktual	Status
		terdaftar pada sensor RC522			
3.	Akses Berhasil via Sidik Jari	Menempelkan jari yang telah terdaftar pada sensor sidik jari.	Kunci Solenoid terbuka. Lampu Indikator Terbuka Menyala	Kunci Solenoid terbuka. Lampu Indikator Terbuka Menyala	LULUS
4.	Akses Ditolak via Sidik Jari	Menempelkan jari yang tidak terdaftar pada sensor sidik jari.	Kunci Solenoid tetap terkunci	Kunci Solenoid tetap terkunci	LULUS
5.	Deteksi Pembukaan Paksa	Membuka pintu secara fisik (memisahkan sensor reed switch) tanpa autentikasi sebelumnya	Kunci Solenoid tetap terkunci. Alarm buzzer berbunyi terus-menerus. Notifikasi "PINTU DIBUKA PAKSA!" terkirim ke Discord	Kunci Solenoid tetap terkunci. Alarm buzzer berbunyi terus-menerus. Notifikasi "PINTU DIBUKA PAKSA!" terkirim ke Discord	LULUS
6.	Fungsi Offline	Memutuskan koneksi internet (Wi-Fi), lalu mencoba akses berhasil dengan RFID/sidik jari	Kunci Solenoid terbuka Notifikasi ke Discord gagal terkirim	Kunci Solenoid terbuka Notifikasi ke Discord gagal terkirim	LULUS

Pada Tabel 2 hasil pengujian tersebut menunjukkan bahwa sistem kunci pintu pintar (smart lock) telah berhasil melewati seluruh skenario pengujian dan berfungsi sesuai dengan rancangan. Sistem ini terbukti andal dalam menjalankan fungsi utamanya, di mana akses berhasil diberikan menggunakan RFID dan sidik jari yang telah terdaftar, yang ditandai dengan terbukanya kunci solenoid dan menyala lampu indikator. Sebaliknya, sistem juga secara efektif menolak akses ketika kartu RFID atau sidik jari yang tidak terdaftar digunakan, sehingga pintu tetap terkunci. Dari segi keamanan, fitur deteksi pembukaan paksa bekerja dengan sempurna, saat pintu dibuka secara ilegal, kunci tetap mengunci, alarm buzzer berbunyi, dan notifikasi darurat berhasil terkirim ke Discord. Lebih lanjut, pengujian fungsi offline mengkonfirmasi bahwa sistem tetap dapat diandalkan bahkan tanpa koneksi internet, di mana akses masuk tetap berfungsi normal meskipun notifikasi online gagal terkirim. Secara keseluruhan, hasil "LULUS" di semua kategori membuktikan bahwa sistem ini aman, akurat, dan fungsional dalam berbagai kondisi.

3.2.1 Pengujian Akses RFID

Pengujian akses RFID dilakukan untuk memastikan bahwa sistem keamanan pintu berbasis Radio Frequency Identification (RFID) dapat berfungsi sesuai dengan rancangan. Pengujian ini berfokus pada kecepatan pembacaan kartu, akurasi identifikasi pengguna, serta respon sistem dalam memberikan izin atau penolakan akses.



Gambar 5. Pengujian Akses RFID

Gambar 5 adalah dokumentasi salah satu skenario pengujian fungsionalitas sistem, yaitu autentikasi akses menggunakan kartu RFID. Pada gambar tersebut, terlihat seorang pengguna sedang menempelkan kartu RFID

yang telah terdaftar pada sensor perangkat. Sistem secara langsung merespons dengan menyalakan lampu indikator LED berwarna hijau. Indikator visual ini menandakan bahwa kartu telah berhasil dikenali dan divalidasi oleh sistem, yang selanjutnya akan memicu relay untuk membuka solenoid lock dan memberikan akses masuk.

3.2.2 Pengujian Akses Finger Print

Pengujian akses fingerprint dilakukan untuk memastikan sistem keamanan pintu berbasis sidik jari dapat berjalan sesuai dengan perancangan. Pengujian ini difokuskan pada akurasi pembacaan sidik jari, kecepatan autentikasi, serta kemampuan sistem dalam membedakan sidik jari yang terdaftar dan tidak terdaftar.

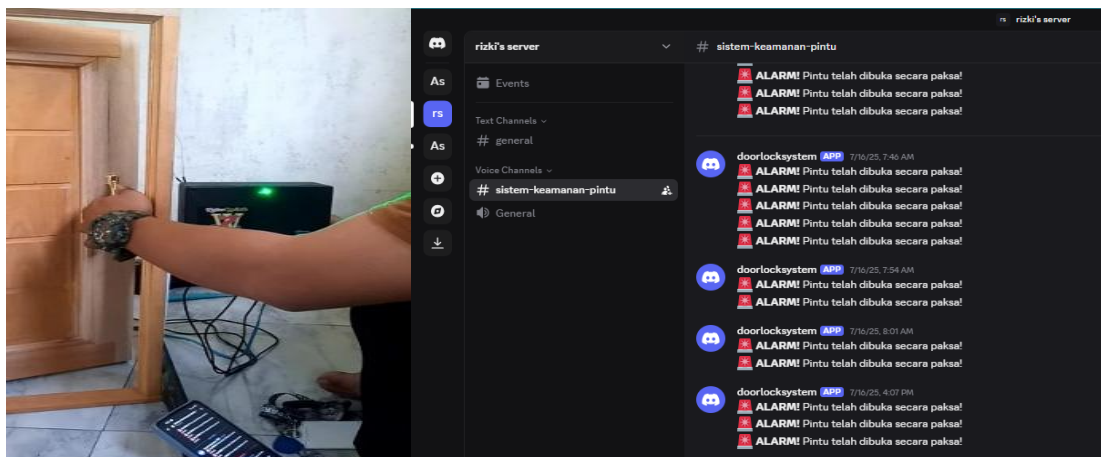


Gambar 6. Pengujian Akses Fingerprint

Pengujian selanjutnya adalah verifikasi akses menggunakan sidik jari, seperti yang didokumentasikan pada Gambar 6. Dalam skenario ini, pengguna menempatkan ibu jarinya pada sensor fingerprint yang terpasang di perangkat. Respons positif dari sistem ditunjukkan dengan menyalanya lampu indikator LED berwarna hijau. Hal ini menandakan bahwa sidik jari pengguna berhasil diidentifikasi sebagai data biometrik yang sah dan terdaftar dalam sistem, sehingga akses diberikan dengan mengaktifkan solenoid lock.

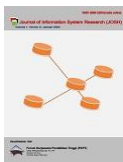
3.4.1 Pengujian Sensor Reedswitch Membuka Paksa Pintu

Pengujian sensor reed switch dilakukan untuk memastikan bahwa sistem keamanan pintu mampu mendeteksi kondisi abnormal, khususnya saat pintu dibuka secara paksa tanpa melalui prosedur autentikasi resmi. Reed switch dipasang pada bagian pintu dan kusen, yang akan saling terhubung ketika pintu dalam keadaan tertutup.



Gambar 7. Pengujian Sensor Reedswitch Membuka Paksa Pintu

Gambar 7 menampilkan pengujian krusial dari sistem keamanan, yaitu simulasi pembukaan pintu secara paksa untuk menguji fungsionalitas sensor reed switch dan sistem notifikasi. Gambar pertama menunjukkan aksi fisik di mana pintu dibuka tanpa melalui proses autentikasi. Aksi ini menyebabkan sensor reed switch mendeteksi adanya perubahan status yang tidak sah. Sebagai respons langsung, sistem secara otomatis memicu protokol alarm dan mengirimkan serangkaian notifikasi peringatan ke kanal Discord #sistem-keamanan-pintu, seperti yang terdokumentasi pada gambar kedua. Pesan notifikasi yang jelas dan berulang “ALARM! Pintu telah dibuka secara



paksa!" membuktikan bahwa sistem berhasil berfungsi sebagai sistem peringatan dini yang andal dan responsif terhadap potensi ancaman.

4. KESIMPULAN

Penelitian ini berhasil secara konkret merancang dan mengimplementasikan sebuah prototipe sistem keamanan pintu otomatis yang fungsional dan andal, dengan studi kasus di SMPN 1 Warungkiara, sebagai solusi atas keterbatasan sistem keamanan konvensional. Sistem ini dibangun di atas platform Internet of Things (IoT), memanfaatkan dua mikrokontroler NodeMCU ESP8266 dalam arsitektur dual-controller untuk optimalisasi pemrosesan data. Satu NodeMCU didedikasikan untuk menangani sensor sidik jari, sementara yang lainnya mengelola sensor reed switch dan pembaca RFID, yang berfungsi sebagai metode autentikasi ganda untuk memastikan hanya pengguna terdaftar yang dapat memperoleh akses. Keunggulan utama dari sistem ini adalah kemampuannya untuk memberikan respons keamanan berlapis saat mendeteksi anomali. Berdasarkan hasil pengujian yang sistematis, prototipe ini terbukti bekerja tanpa cela di semua skenario yang diujikan. Sensor reed switch secara akurat mendeteksi status buka-tutup pintu dan berhasil memicu alarm ketika terjadi upaya pembukaan paksa. Saat pembobolan disimulasikan, sistem secara simultan menjaga kunci solenoid tetap terkunci, membunyikan alarm buzzer di lokasi, dan mengirimkan notifikasi peringatan "PINTU DIBUKA PAKSA!" secara instan ke kanal Discord yang telah ditentukan. Platform Discord dipilih karena efektivitasnya dalam memastikan pihak berwenang menerima peringatan di mana pun mereka berada. Sebuah temuan penting dari pengujian adalah ketahanan sistem dalam kondisi offline, di mana fungsi akses dan alarm lokal tetap beroperasi normal meski koneksi internet terputus. Dengan demikian, penelitian ini tidak hanya menghasilkan solusi keamanan yang inovatif dan terjangkau, tetapi juga berhasil mengubah paradigma keamanan di lingkungan sekolah dari reaktif menjadi proaktif melalui pengawasan digital yang responsif.

REFERENCES

- [1] M. U. Batoebara and A. N. Pasaribu, "Perkembangan Teknologi Komunikasi dan Informasi di Media baru," *Jurnal Prosiding Ilmu Sosial dan Ilmu Politik Universitas Dharmawangsa*, Jul. 2021, doi: <https://doi.org/10.46576/spu.v1i0.93>.
- [2] A. N. Mas Erwan, M. N. H. Muzaffar Alfian, and M. S. Mohamad Adenan, "Smart Door Lock," *International Journal of Recent Technology and Applied Science*, vol. 3, no. 1, pp. 1–15, Mar. 2021, doi: [10.36079/iamintang.ijortas-0301.194](https://doi.org/10.36079/iamintang.ijortas-0301.194).
- [3] A. A. Zainuddin et al., "Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology," *Malaysian Journal of Science and Advanced Technology*, pp. 360–365, Aug. 2024, doi: [10.56532/mjsat.v4i4.335](https://doi.org/10.56532/mjsat.v4i4.335).
- [4] A. Widiyatmoko and I. Suharjo, "Smart Temperature and Humidity Monitoring pada Data center Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta Berbasis Raspberry Pi 5 dan Notifikasi Discord," *Jurnal Kridatama Sains dan Teknologi*, vol. 7, no. 2, 2025, doi: <https://doi.org/10.53863/kst.v7i02.1742>.
- [5] F. Ferella, S. Paembonan, and H. Abduh, "Prototype Sistem Kontrol Rumah Pintar Menggunakan Kamera Berbasis Internet of Things (IoT)," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, Jan. 2025, doi: [10.23960/jitet.v13i1.6025](https://doi.org/10.23960/jitet.v13i1.6025).
- [6] M. Faturrachman and I. Yustiana, "Sistem Keamanan Pintu Rumah dengan Sidik Jari Berbasis Internet of Things (IOT)," *JTIUST*, vol. 6, no. 2, 2021, doi: <https://doi.org/10.54367/jtiust.v6i2.1517>.
- [7] E. Alfonsius, A. S. Ruitan, and D. Liuw, "Pengembangan Sistem Keamanan Pintu Menggunakan Metode Prototype Berbasis RFID dan Keypad 4x4 dengan Arduino Nano," *Jurnal Ilmiah Informatika dan Ilmu Komputer (JIMA-ILKOM)*, vol. 3, no. 2, pp. 110–123, Sep. 2024, doi: [10.58602/jima-ilkom.v3i2.33](https://doi.org/10.58602/jima-ilkom.v3i2.33).
- [8] Yulisman, N. Iman, E. Sabna, and H. Fonda, "Sistem Pintu Otomatis Menggunakan E-KTP Berbasis Internet of Things (IoT) pada Kamar Hotel," *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, vol. 1, no. 2, pp. 85–91, Oct. 2021, doi: [10.54259/satesi.v1i2.60](https://doi.org/10.54259/satesi.v1i2.60).
- [9] M. Rijal Fadli, "Memahami Desain Metode Penelitian Kualitatif," *Humanika*, vol. 21, no. 1, pp. 33–54, 2021, doi: [10.21831/hum.v21i1](https://doi.org/10.21831/hum.v21i1).
- [10] D. Assyakurrohm, D. Ikhrum, R. A. Sirodj, and M. W. Afgani, "Metode Studi Kasus dalam Penelitian Kualitatif," *Jurnal Pendidikan Sains dan Komputer*, vol. 3, no. 01, pp. 1–9, Dec. 2022, doi: [10.47709/jpsk.v3i01.1951](https://doi.org/10.47709/jpsk.v3i01.1951).
- [11] I. C. Simanjuntak, K. Khotimah, F. F. Afza, A. N. Rafiansyah, and O. D. Radianto, "Analisis Hubungan Penggunaan Sosial Media dengan Peran Mahasiswa di Masyarakat," *Jurnal Sains Student Research*, vol. 2, no. 3, pp. 29–36, 2024, doi: [10.61722/jssr.v2i3.1238](https://doi.org/10.61722/jssr.v2i3.1238).
- [12] Ardiansyah, Risnita, and S. M. Jailani, "Teknik Pengumpulan Data dan Instrumen Penelitian Ilmiah," *Jurnal Pendidikan Islam*, vol. 1, no. 2, 2023, doi: <https://doi.org/10.61104/ihsan.v1i2.57>.
- [13] B. A. Habsy, N. Mufidha, C. Shelomita, I. Rahayu, and Moch. I. Muckorobin, "Filsafat Dasar dalam Konseling Psikoanalisis : Studi Literatur," *Indonesian Journal of Educational Counseling*, vol. 7, no. 2, pp. 189–199, Jul. 2023, doi: [10.30653/001.202372.266](https://doi.org/10.30653/001.202372.266).
- [14] A. Febrianto and R. A. Siroj, "Studi Literatur: Landasan Dalam Memilih Metode Penelitian yang Tepat," *Journal Educational Research and Development*, vol. 01, no. 02, pp. 259–263, 2024, doi: <https://doi.org/10.62379/jerd.v1i2.142>.
- [15] M. Alparisi, "Perancangan Sistem Keamanan Berkas Berbasis IoT Menggunakan Fingerprint dengan Notifikasi via Telegram," *Jurnal Informatika dan Komputer (INFOKOM)*, vol. Volume 9, Nomor 1, Jun. 2021, doi: <https://doi.org/10.56689/infokom.v9i1.480>.
- [16] F. Husniya, M. Ulum, A. K. Wibisono, and R. Alfita, "Rancang Bangun Sistem Pengaman Pintu Menggunakan RFID dan Fingerprint," *Jurnal FORTECH*, vol. 2, no. 1, 2021, doi: <https://doi.org/10.32492/fortech.v2i1.232>.
- [17] F. Palaha, Machdalena, Ermawaati, and D. Engla Harda Arya, "Analisa Traffic Data Esp8266 pada Kontrol dan



- Monitoring Daya Lisrik Menggunakan Aplikasi Blynk Berbasis Arduino Nano,” Jurnal Nasional Komputasi dan Teknologi Informasi, vol. 4, no. 6, 2021, doi: 10.32672/jnkti.v4i6.3646.
- [18] Y. Erdani, R. A. Pratama, B. A. Ahad, and G. I. F. Fadila, “Desain Sistem Kontrol Container Station Menggunakan Metode Waterfall Berbasis Internet of Things (IoT),” G-Tech: Jurnal Teknologi Terapan, vol. 8, no. 3, pp. 1415–1430, Jul. 2024, doi: 10.33379/gtech.v8i3.4315.
- [19] N. N. E. Smrti, I. P. G. S. Andisasana, N. K. D. T. Rahayu, Adnan, and P. Putu, “Flowgorithm Sebagai Penunjang Pembelajaran Algoritma dan Pemrograman,” Jurnal Bangkit Indonesia, vol. 2, no. 1, 2023, doi: <https://doi.org/10.52771/bangkitindonesia.v12i1.218>.
- [20] R. Kurniawan Sugeng, “Implementasi Zabbix Monitoring dengan Integrasi Sistem Notifikasi Discord, Teams, Telegram untuk Monitoring Infrastruktur Jaringan pada PT. Pundi Mas Berjaya (PMB),” The 6th National Conference for Community Service Project, vol. 6, no. 1, 2024. doi: <https://doi.org/10.37253/nacospro.v6i1.9721>.
- [21] U. Saputra et al., “Analisa Pengujian Sistem Informasi Website E-Commerce Bali-Store Menggunakan Metode Black Box Testing,” Jurnal Teknologi Informasi, vol. 2, no. 1, 2023, doi: <https://doi.org/10.35308/jti.v2i2.7847>.
- [22] Y. Susanto, M. Taringan, and Yulhendri, “Pengukuran dan Pendataan Zat Cair Toluene dengan Akses Rfid Berbasis Nodemcu Esp8266 yang Termonitor Melalui Web,” SINTAMA: Jurnal Sistem Informasi, Akuntansi dan Manajemen, vol. 2, no. 3, 2022, doi: <https://doi.org/10.54951/sintama.v2i3.392>.
- [23] J. P. Hendrik Sitorus and M. Sakban, “Perancangan Sistem Informasi Penjualan Berbasis Web pada Toko Mandiri 88 Pematangsiantar,” Jurnal Bisantra Informatika (JBI), vol. 5, no. 2, 2021, doi: <https://doi.org/10.31004/riggs.v4i1.359>.