

Evaluasi Kinerja *Smart door lock* Berbasis IoT dengan Mode Jam Kerja dan Deteksi Intrusi

Jundi Azis¹, Andik Prakasa Hadi^{*2}, Candra Supriadi⁴, Rais³

^{1,2,3} Fakultas Studi Akademi, Universitas Sains dan Teknologi Komputer, Semarang

⁴ Prodi Teknik Komputer Fakultas Sekolah Vokasi, Universitas Harkat Negeri, Tegal

Email: ¹fjunda22@gmail.com, ^{*2}andik@stekom.ac.id, ³candra@stekom.ac.id,

⁴rais.hojawa@gmail.com

(Naskah masuk: 22 Juni 2026, diterima untuk diterbitkan: 8 Juli 2026)

Abstrak: Penelitian ini bertujuan merancang dan menilai seberapa handal sebuah kunci pintu pintar (*smart door lock*) berbasis IoT yang dilengkapi mode jam kerja otomatis serta kemampuan mendeteksi upaya pembobolan. Sistem ini menggunakan komponen seperti ESP32, RFID RC522, jam digital RTC DS3231, sensor magnetik, sensor sentuh, dan platform Blynk untuk pantauan waktu nyata. Penelitian dilakukan dengan metode eksperimen kuantitatif melalui tujuh skenario uji, yaitu akurasi RFID, kecepatan respons, mode jam kerja, mode luar jam kerja, kontrol manual, deteksi intrusi, dan stabilitas koneksi IoT.

Hasilnya menunjukkan performa yang memuaskan. Akurasi RFID mencapai 96,67% untuk kartu terdaftar dan 100% untuk kartu tak dikenal. Waktu respons rata-rata 1,24 detik, dan mode jam kerja berhasil sempurna (100%). Deteksi intrusi mampu mengenali 93,33% percobaan buka paksa, lalu membunyikan alarm dan mengirim notifikasi ke Blynk. Packet loss koneksi IoT hanya 6%.

Sistem ini terbukti berhasil memadukan kontrol akses berbasis waktu dan deteksi intrusi secara efektif. Dengan begitu, keamanan serta efisiensi pengelolaan akses pintu di lingkungan pendidikan bisa meningkat. Kesimpulannya, kunci pintar berbasis IoT ini layak dipakai di sekolah sebagai solusi keamanan yang murah dan mudah beradaptasi.

Kata Kunci – *Smart door lock, IoT, Blynk, Mode jam kerja, Deteksi intrusi*

Integration of RBAC, AES-256, and Audit Log for Security and Auditability of SMEs Inventory Systems

Abstract: This study develops and evaluates an IoT-based smart door lock featuring automatic working hour mode and intrusion detection. The system utilizes an ESP32 microcontroller, RFID RC522, DS3231 RTC, magnetic contact sensor, touch sensor, and the Blynk platform for real-time monitoring. A quantitative experimental approach was applied across seven scenarios: RFID accuracy, response time, working hour mode, non-working hour mode, manual override, intrusion detection, and IoT connectivity stability.

Results indicate strong system performance. RFID accuracy reached 96.67% for valid tags and 100% for invalid tags. The average response time was 1.24 seconds, and the working hour mode achieved a 100% success rate. Intrusion detection successfully identified forced openings 93.33% of the time, triggering a buzzer alarm and Blynk notification. IoT connectivity experienced only 6% packet loss. The system effectively integrates time-based access control with intrusion detection, improving both security and access management efficiency in educational environments. The study concludes that this IoT-based smart door lock is a feasible, adaptive, and low-cost security solution for schools.

Keywords – *Smart door lock, IoT, Blynk, Working hour mode, Intrusion detection*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi sistem keamanan konvensional menuju sistem berbasis digital dan otomatis [1]. Sistem penguncian pintu tradisional yang masih menggunakan kunci mekanik memiliki berbagai kelemahan, seperti risiko kehilangan kunci, duplikasi tanpa izin, serta keterbatasan dalam pemantauan akses secara *real-time*

[2]. Oleh karena itu, diperlukan inovasi sistem keamanan yang lebih cerdas, efisien, dan terintegrasi dengan teknologi modern.

Internet of Things (IoT) merupakan teknologi yang memungkinkan perangkat fisik saling terhubung dan berkomunikasi melalui jaringan internet [3]. Dalam sistem keamanan, IoT memungkinkan pengendalian dan pemantauan akses pintu secara *real-time* melalui perangkat *mobile* maupun *platform* berbasis *cloud* [4]. Penelitian oleh Khan & Khare [4] menunjukkan bahwa integrasi IoT dengan protokol komunikasi seperti MQTT mampu meningkatkan keandalan sistem *smart door lock*, dengan *throughput* tertinggi 5,052 kbps dan *Delay* terendah 175 ms pada MQTT QoS level 0. Selain itu, Chen et al. [5] juga menyatakan bahwa sistem kontrol akses berbasis IoT memiliki fleksibilitas tinggi dalam pengelolaan pengguna dan pencatatan aktivitas akses secara *real-time*.

Penerapan IoT pada *smart door lock* telah berkembang dengan berbagai metode autentikasi seperti RFID, *fingerprint*, dan *keypad* yang terbukti meningkatkan fleksibilitas dan efisiensi sistem [6], [7]. *Smart door lock* merupakan sistem penguncian pintu yang menggabungkan teknologi digital dengan sistem kontrol akses untuk meningkatkan keamanan dan kenyamanan pengguna. Teknologi *Radio Frequency Identification* (RFID) merupakan salah satu metode autentikasi yang banyak digunakan dalam sistem kontrol akses karena kemudahan penggunaan dan kecepatan identifikasi [8]. RFID memiliki keunggulan dalam kecepatan, kemudahan penggunaan, serta tingkat akurasi yang tinggi [9]. Sistem berbasis RFID memungkinkan pengguna membuka pintu hanya dengan menggunakan kartu atau *tag* terdaftar, sehingga mengurangi ketergantungan pada kunci fisik [10]. Kasim et al. [11] menyatakan bahwa sistem *smart door lock* berbasis RFID yang dikendalikan oleh Arduino memiliki tingkat keberhasilan autentikasi yang tinggi dengan waktu respon yang konsisten. Penelitian oleh Jannah et al. [10] juga menunjukkan bahwa penggunaan RFID dalam sistem keamanan pintu berbasis IoT mampu meningkatkan efisiensi operasional. Guntur et al. [12] mengembangkan sistem keamanan berbasis RFID yang terhubung dengan IoT menggunakan Arduino, dilengkapi dengan sensor untuk mendukung operasi malam hari serta potensi pengembangan dengan *face recognition* dan *SMS alert*. Sementara itu, penelitian oleh Ohemu & Idoko [2] mengimplementasikan sistem *smart door lock* berbasis IoT pada lingkungan laboratorium komputer dengan fitur monitoring akses secara *real-time*.

Meskipun demikian, penelitian sebelumnya masih memiliki keterbatasan, terutama dalam aspek fleksibilitas operasional dan keamanan lanjutan. Sebagian besar sistem hanya berfokus pada mekanisme autentikasi tanpa mempertimbangkan kondisi operasional seperti pengaturan waktu (jam kerja) maupun deteksi terhadap potensi intrusi atau pembobolan. Padahal, aspek tersebut sangat penting dalam meningkatkan keamanan sistem secara menyeluruh. Teknologi RFID juga memiliki potensi kerentanan terhadap serangan tertentu, sehingga perlu dikombinasikan dengan mekanisme keamanan tambahan seperti pengaturan waktu akses dan deteksi intrusi [13]. Selain itu, studi terbaru menunjukkan bahwa sistem RFID berbasis IoT masih memiliki potensi kerentanan jika tidak dilengkapi dengan mekanisme keamanan tambahan [14].

Sistem keamanan modern tidak hanya berfokus pada kontrol akses, tetapi juga mencakup kemampuan mendeteksi ancaman atau intrusi [15]. Dalam konteks *smart door lock*, deteksi intrusi dapat dilakukan dengan mengidentifikasi kondisi abnormal seperti pembukaan paksa atau akses tanpa autentikasi. Mehmood et al. [16] mengembangkan sistem *smart door lock* dengan *invisible touch sensors* untuk mendeteksi pembukaan paksa menggunakan pendekatan *low-cost* dan *disposable*. Penelitian tersebut menunjukkan bahwa sensor sentuh dapat diintegrasikan secara efektif. Asysyauqi et al. [17] juga mengembangkan sistem keamanan pintu otomatis berbasis IoT yang dilengkapi dengan metode *fuzzy Mamdani* untuk meningkatkan akurasi pengambilan keputusan. Implementasi fitur deteksi intrusi pada *smart door lock* menjadi penting untuk meningkatkan tingkat keamanan secara menyeluruh.

Sementara itu, pengaturan akses berbasis waktu atau *time-based access control* merupakan salah satu metode dalam sistem keamanan yang memungkinkan pembatasan akses berdasarkan jadwal tertentu [18]. Konsep ini banyak diterapkan dalam lingkungan perkantoran dan pendidikan untuk mengatur jam operasional akses ruangan. Guo et al. [19] mengusulkan model *spatiotemporal access*

control (STRAC) yang menggabungkan aspek ruang dan waktu pada *sensing layer* IoT. Model ini menggunakan pendekatan *lattice* untuk memperkecil ukuran *policy base* serta mekanisme otorisasi nondeterministik dan stokastik untuk mengatasi komunikasi yang tidak *reliable*. Pendekatan ini sejalan dengan implementasi mode jam kerja pada *smart door lock* yang membatasi akses hanya pada waktu tertentu sesuai kebutuhan operasional. Integrasi sistem berbasis waktu dengan *smart door lock* dapat meningkatkan efisiensi penggunaan sistem serta mengurangi kebutuhan intervensi manual [20].

Penelitian lain juga mulai mengintegrasikan pendekatan cerdas seperti logika *fuzzy* untuk meningkatkan keamanan, namun belum banyak yang mengkombinasikan dengan pengaturan waktu operasional [17]. Beberapa penelitian terdahulu telah mengembangkan sistem *smart door lock* berbasis IoT dengan berbagai metode dan pendekatan. Harahap et al. [21] mengembangkan sistem berbasis e-KTP sebagai media autentikasi yang terintegrasi dengan IoT dan *automatic lighting*. Penelitian oleh Permana et al. [6] mengembangkan sistem dengan kombinasi *fingerprint* dan *keypad* untuk meningkatkan fleksibilitas autentikasi. Zainuddin et al. [7] mengimplementasikan sistem *smart lock* inovatif dengan teknologi *fingerprint* dan RFID untuk meningkatkan keamanan. Penelitian lain oleh Chen et al. [5] menunjukkan bahwa integrasi IoT dalam sistem keamanan rumah memberikan peningkatan signifikan dalam hal monitoring dan kontrol akses. Penelitian ini mengembangkan sistem kontrol akses berbasis IoT dengan pendekatan yang berbeda. Pada konteks sederhana, sistem RFID digunakan untuk verifikasi keanggotaan pada fasilitas seperti pusat kebugaran dengan bantuan Raspberry Pi serta aplikasi web untuk pengelolaan data pengguna. Sementara itu, penelitian lain mengembangkan sistem *smart door lock* yang lebih kompleks menggunakan ESP32 dengan integrasi RFID, *fingerprint*, serta komunikasi *Bluetooth Low Energy* (BLE) dan MQTT untuk monitoring *real-time*. Kedua pendekatan ini menunjukkan bahwa IoT dapat diterapkan pada berbagai sistem kontrol akses, baik sederhana maupun kompleks, sehingga relevan sebagai dasar pengembangan sistem keamanan yang lebih terintegrasi [4], [22].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pengembangan sistem *smart door lock* berbasis IoT yang dilengkapi dengan fitur mode jam kerja dan deteksi intrusi. Mode jam kerja memungkinkan sistem mengatur kondisi pintu secara otomatis berdasarkan waktu operasional, sehingga meningkatkan efisiensi penggunaan. Sementara itu, fitur deteksi intrusi berfungsi untuk mendeteksi upaya pembukaan paksa dan memberikan respon berupa alarm sebagai peringatan dini terhadap potensi ancaman keamanan. Meskipun berbagai penelitian telah dilakukan, sebagian besar masih berfokus pada aspek autentikasi dan kontrol akses. Integrasi antara mode operasional berbasis waktu dan deteksi intrusi dalam satu sistem masih relatif terbatas. Oleh karena itu, penelitian ini mengusulkan sistem *smart door lock* berbasis IoT yang menggabungkan autentikasi RFID, mode jam kerja, dan deteksi intrusi sebagai upaya untuk meningkatkan keamanan dan efisiensi sistem secara komprehensif. Penelitian ini dilakukan di lingkungan SMAN 3 Salatiga sebagai studi kasus implementasi pada institusi pendidikan. Kontribusi utama penelitian ini adalah: (1) integrasi mode jam kerja berbasis *Real-time Clock* (RTC) pada *smart door lock* RFID, (2) mekanisme alarm anti-paksa menggunakan sensor kontak untuk deteksi intrusi, dan (3) evaluasi kinerja sistem di lingkungan institusi pendidikan. Hasil penelitian diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan berbasis IoT yang lebih adaptif, aman, dan aplikatif.

2. METODOLOGI PENELITIAN

2.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif yang bertujuan untuk merancang, mengimplementasikan, serta mengevaluasi kinerja sistem *smart door lock* berbasis *Internet of Things* (IoT). Pendekatan kuantitatif digunakan untuk mengukur parameter kinerja sistem secara objektif, seperti waktu respon (dalam detik), tingkat keberhasilan akses (dalam persentase), dan efektivitas deteksi intrusi. Metode eksperimen dipilih karena memungkinkan

pengujian langsung terhadap sistem dalam kondisi nyata sehingga hasil yang diperoleh lebih akurat dan terukur [11].

2.2. Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan di lingkungan SMAN 3 Salatiga sebagai studi kasus implementasi sistem keamanan berbasis IoT pada institusi pendidikan. Pemilihan lokasi didasarkan pada kebutuhan akan sistem keamanan pintu yang lebih modern, efisien, dan terintegrasi untuk mendukung pengelolaan akses ruangan. Penelitian dilakukan selama periode Januari hingga Mei 2026, meliputi tahap perancangan, implementasi, pengujian, dan analisis data.

2.3. Spesifikasi Perangkat Keras dan Lunak

Sistem yang dikembangkan menggunakan komponen perangkat keras dan lunak dengan spesifikasi teknis sebagai berikut.

2.3.1. Perangkat Keras (Hardware)

Tabel 1. Perangkat Keras Pengembangan Sistem

Komponen	Spesifikasi	Fungsi
<i>Mikrokontroler</i>	ESP32-WROOM-32 (dual-core Tensilica LX6, 240 MHz, 4MB <i>flash</i> , WiFi 802.11 b/g/n)	Pusat kendali sistem, pemrosesan data, konektivitas IoT
Modul RFID	RC522 (frekuensi 13.56 MHz, antarmuka SPI)	Pembaca <i>tag</i> /kartu RFID untuk autentikasi pengguna
<i>Magnetic door Lock</i>	Solenoid 12V DC, arus 1A, <i>holding force</i> 5 kg	Aktuator pengunci pintu
<i>Touch sensor</i>	TTP223 (kapasitif, tegangan 2.0V-5.5V, output digital)	Kontrol manual dari dalam ruangan
<i>Real-time Clock (RTC)</i>	DS3231 (akurasi ± 2 ppm, antarmuka I2C, <i>battery backup</i> CR2032)	Penyedia waktu <i>real-time</i> untuk mode jam kerja
<i>Buzzer</i>	Piezoelektrik 5V, frekuensi 1 kHz-4 kHz	Indikator alarm deteksi intrusi
LCD	16x2 dengan modul I2C (tegangan 5V, alamat 0x27)	Menampilkan status pintu dan pesan sistem
<i>Relay</i>	1 <i>channel</i> , 5V, <i>optocoupler</i> , <i>max load</i> 10A 250VAC	Pengendali <i>magnetic door lock</i> dari <i>mikrokontroler</i>
Catu Daya	<i>Adaptor</i> 12V/2A dan <i>regulator</i> LM2596 <i>step-down</i> ke 5V/3A	Sumber daya untuk seluruh sistem

2.3.2. Perangkat Lunak (Software):

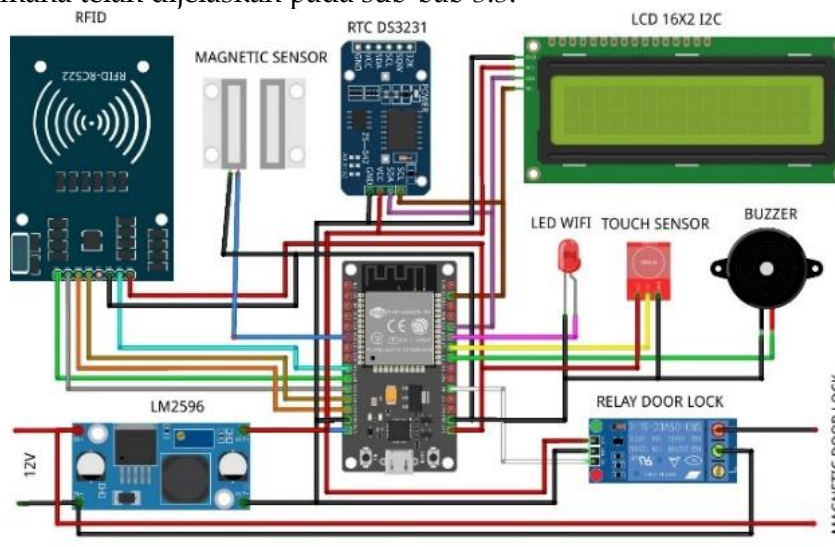
Tabel 2. Perangkat Lunak Pengembangan Sistem

Komponen	Spesifikasi	Fungsi
IDE Pemrograman	Arduino IDE 2.3.2	Penulisan, kompilasi, dan <i>upload</i> kode ke ESP32
<i>Library</i> RFID	MFRC522 v1.4.10	Komunikasi SPI dengan modul RFID RC522
<i>Library</i> RTC	RTCLib v2.1.4	Pembacaan waktu dari DS3231
<i>Library</i> LCD	LiquidCrystal_I2C v1.1.2	Kendali LCD 16x2 via I2C
<i>Platform</i> IoT	Blynk IoT <i>Platform</i> v1.0 (Blynk Legacy)	Monitoring dan kontrol jarak jauh

Protokol IoT	MQTT over TCP (port 1880)	Komunikasi data antara ESP32 dan <i>server</i> Blynk
Format Data	JSON (<i>key-value pair</i>)	Mengirim struktur data dalam format json

2.4. Arsitektur dan Diagram Blok Sistem

Sistem yang dikembangkan memiliki arsitektur yang terdiri dari komponen perangkat keras dan lunak sebagaimana telah dijelaskan pada sub-bab 3.3.



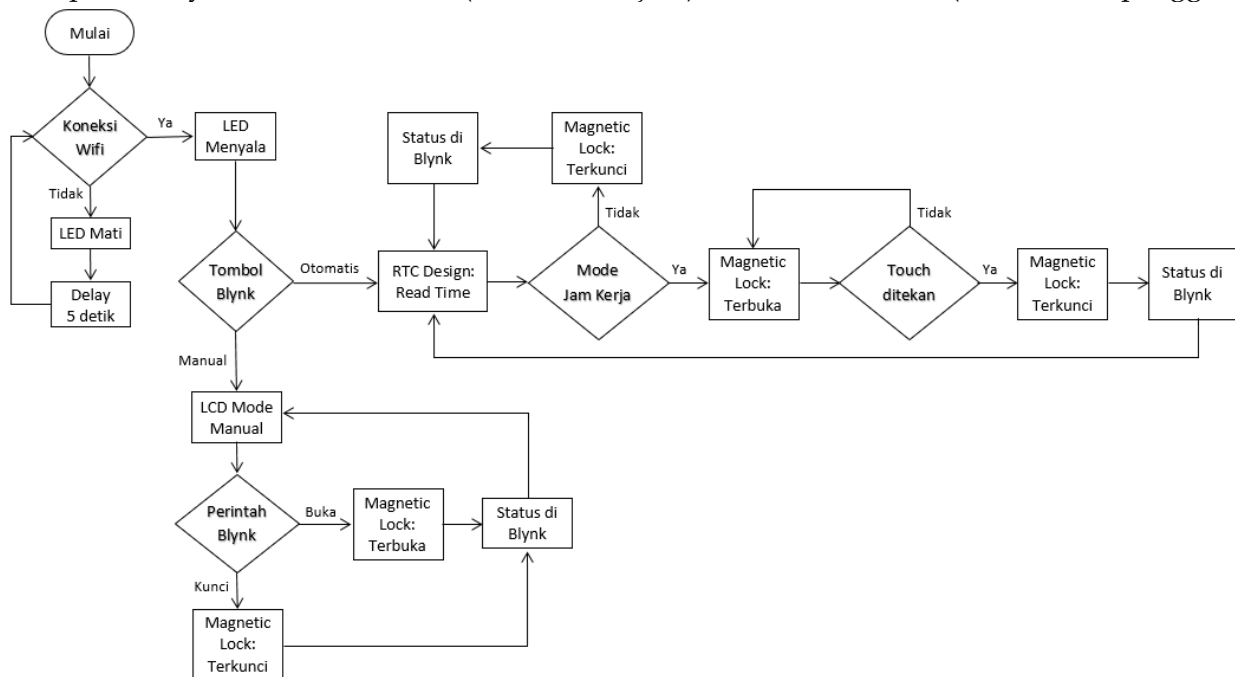
Gambar 1. Diagram blok sistem *smart door lock*

Secara keseluruhan, sistem bekerja dengan prinsip sebagai berikut:

1. *LED WiFi* berfungsi sebagai indikator visual status koneksi jaringan. *LED menyala* ketika ESP32 berhasil terhubung ke jaringan WiFi dan mati ketika koneksi terputus.
2. Platform Blynk menampilkan antarmuka pengguna yang terdiri dari:
 - 1) Tampilan jam *real-time* yang disinkronkan dengan RTC DS3231
 - 2) Indikator status pintu (Terbuka/Terkunci)
 - 3) Tombol mode untuk melakukan *override* sistem antara mode otomatis (berdasarkan jam) dan mode manual
3. Mode Jam Kerja (07:00 - 16:00 WIB): *Magnetic door lock* dalam posisi terbuka secara otomatis. Pengguna dari dalam ruangan dapat menekan *touch sensor* untuk mengunci pintu secara manual jika diperlukan. LCD menampilkan informasi mode dan status pintu.
4. Mode Non-Jam Kerja (16:01 - 06:59 WIB): *Magnetic door lock* dalam posisi terkunci. Akses dari luar hanya dapat dilakukan melalui autentikasi RFID yang *valid*. Akses dari dalam dapat dilakukan melalui *touch sensor* untuk membukakan pintu bagi orang luar.
5. *Touch sensor* memiliki dua fungsi:
 - 1) Pada mode jam kerja: mengunci pintu dari dalam
 - 2) Pada mode non-jam kerja: membukakan pintu dari dalam (untuk orang luar)
6. *Buzzer* berfungsi sebagai indikator suara dengan tiga kondisi:
 - 1) BEEP 1 kali: indikator pintu tertutup
 - 2) BEEP 2 kali pendek: indikator akses RFID ditolak
 - 3) Menyala terus-menerus: alarm bahaya ketika pintu dijebol paksa
7. LCD 16x2 menampilkan dua baris informasi:
 - 1) Baris atas: mode operasional (Mode: Kerja / Mode: Istirahat / Mode: Manual)
 - 2) Baris bawah: status pintu (Pintu: Terbuka / Pintu: Terkunci)

2.5. Mekanisme dan Flowchart Kerja Sistem

Sistem bekerja dengan dua mode operasional utama yang dapat dipilih melalui tombol mode pada aplikasi Blynk: Mode Otomatis (berdasarkan jam) dan Mode Manual (*override* dari pengguna).



Gambar 2. Diagram alir sistem *smart door lock*

2.5.1. Mode Otomatis (Berdasarkan Jam)

Sistem membaca waktu pada mode ini, dari RTC DS3231 secara kontinyu. Jika waktu berada pada rentang 07:00 - 16:00 WIB, sistem memasuki mode jam kerja. *Magnetic door lock* berada dalam posisi terbuka, memungkinkan akses bebas keluar-masuk. Pengguna dari dalam ruangan dapat menekan *touch sensor* untuk mengunci pintu secara manual jika diperlukan (misal: saat istirahat siang). *Buzzer* akan berbunyi satu kali sebagai indikasi pintu telah tertutup. Status pintu dan waktu dikirimkan ke *platform Blynk* secara *real-time*.

Jika waktu berada di luar rentang jam kerja, sistem memasuki mode non-jam kerja. *Magnetic door lock* berada dalam posisi terkunci. Sistem menunggu dua kemungkinan input:

1. RFID dari luar: Jika *tag* RFID yang *valid* ditempelkan, pintu akan terbuka selama 5 detik, kemudian terkunci kembali. *Buzzer* berbunyi satu kali saat pintu tertutup.
2. *Touch sensor* dari dalam: Jika seseorang dari dalam menekan *touch sensor*, pintu akan terbuka selama 5 detik (untuk membukakan akses bagi orang luar), kemudian terkunci kembali.

2.5.2. Mode Manual (Override)

Pengguna dapat mengaktifkan mode manual melalui tombol pada aplikasi Blynk kapan saja. Dalam mode ini, pengguna dapat secara langsung memerintahkan *magnetic door lock* untuk terbuka atau terkunci melalui antarmuka Blynk, terlepas dari waktu saat itu. LCD akan menampilkan indikasi "Mode: Manual".

2.5.3. Deteksi Intrusi dan Alarm

Sistem dilengkapi dengan mekanisme deteksi intrusi yang bekerja pada mode non-jam kerja. Jika pintu terbuka tanpa melalui proses autentikasi RFID maupun perintah dari *touch sensor* (misal: pintu dijebol paksa), maka:

1. *Buzzer* akan menyala terus-menerus sebagai alarm peringatan bahaya
2. Notifikasi "ALARM! Pintu Dijebol!" dikirim ke *platform Blynk*

2.6. Skenario dan Prosedur Pengujian

Tabel 3. Skenario dan Prosedur Pengujian

Skenario	Tujuan	Parameter yang Diukur	Metode
S1: Pengujian RFID	Mengukur tingkat keberhasilan pembacaan <i>tag</i> RFID	Akurasi pembacaan (%)	30 kali tap kartu RFID <i>valid</i> dan 30 kali kartu tidak <i>valid</i>
S2: Pengujian Waktu Respon	Mengukur waktu dari tap RFID hingga pintu terbuka	Waktu respon (detik), rata-rata dan standar deviasi	Stopwatch digital, dimulai saat kartu ditempelkan hingga <i>relay</i> mengaktifkan solenoid
S3: Pengujian Mode Jam Kerja	Memastikan pintu terbuka otomatis dan <i>touch sensor</i> dapat mengunci	Status pintu pada jam tertentu, fungsi <i>touch sensor</i>	Simulasi pada pukul 06:00, 07:00, 12:00, 16:00, 17:00; uji tekan <i>touch sensor</i>
S4: Pengujian Mode Non-Jam Kerja	Memastikan RFID dan <i>touch sensor</i> berfungsi membuka pintu	Keberhasilan akses RFID, keberhasilan <i>touch sensor</i>	30 kali RFID <i>valid</i> , 30 kali tekan <i>touch sensor</i> dari dalam
S5: Pengujian Mode Manual (<i>Override</i>)	Memastikan tombol mode di Blynk berfungsi	Respon sistem terhadap perintah Buka/Kunci dari Blynk	30 kali perintah Buka, 30 kali perintah Kunci dari aplikasi Blynk
S6: Pengujian Deteksi Intrusi	Mengukur efektivitas alarm terhadap pembukaan paksa	Aktivasi <i>buzzer</i> (Ya/Tidak), waktu respon alarm (detik)	Simulasi membuka pintu tanpa izin saat mode non-jam kerja
S7: Pengujian Konektivitas IoT	Mengevaluasi kestabilan komunikasi ESP32 ke Blynk	<i>Packet loss (%)</i> , <i>end-to-end Delay (ms)</i>	Mengirim 100 status <i>update</i> , dicatat yang gagal terkirim

3. HASIL DAN PEMBAHASAN

Penelitian ini melakukan evaluasi kinerja sistem *smart door lock* berbasis IoT yang mengintegrasikan autentikasi RFID, mode operasional berbasis waktu (jam kerja), dan deteksi intrusi.



Gambar 3. Sistem *smart door lock* berbasis IoT

Pengujian dilakukan melalui tujuh skenario dengan total 330 percobaan fungsional dan 100 paket data IoT. Hasil pengujian disajikan dan dibahas secara rinci berikut ini.

3.1.1. Akurasi Pembacaan RFID

Sistem menunjukkan akurasi yang tinggi, yaitu 96,67% untuk *tag valid* dan 100% untuk *invalid tag*. Satu kegagalan pada *valid tag* terjadi akibat jarak tempel melebihi 4 cm dari antena RC522. Hasil ini sejalan dengan penelitian Kasim et al. [11] yang melaporkan akurasi 95–98% pada konfigurasi serupa. Tingkat akurasi 100% pada *invalid tag* membuktikan bahwa sistem mampu mencegah akses tidak sah dengan sangat baik, sehingga memenuhi persyaratan keamanan dasar untuk lingkungan institusi pendidikan.

Tabel 4. Hasil Pengujian Akurasi Modul RFID RC522

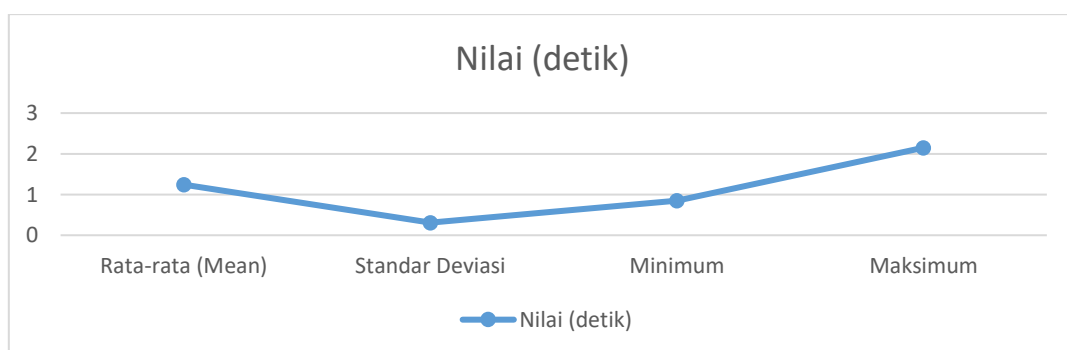
Jenis Tag	n	Berhasil	Gagal	Akurasi (%)
Tag Terdaftar (<i>Valid</i>)	30	29	1	96,67
Tag Tidak Terdaftar (<i>Invalid</i>)	30	0	30	100,00

3.1.2. Waktu Respon Sistem

Waktu respon rata-rata sebesar 1,24 detik dengan standar deviasi rendah (0,31 detik) menunjukkan konsistensi kinerja yang baik. Waktu tercepat 0,85 detik dan terlama 2,15 detik masih berada di bawah ambang batas 2 detik yang dianggap *acceptable* untuk sistem akses pintu [4]. Dibandingkan dengan *Delay MQTT QoS 0* sebesar 175 ms pada penelitian Khan & Khare [4], waktu respon sistem ini sedikit lebih lambat karena melibatkan eksekusi *relay* dan *solenoid*. Namun, nilai ini tetap menjamin pengalaman pengguna yang nyaman.

Tabel 5. Statistik Waktu Respon Sistem

Parameter	Nilai (detik)
Rata-rata (Mean)	1,24
Standar Deviasi	0,31
Minimum	0,85
Maksimum	2,15



Gambar 2. Grafik respon waktu sistem (detik)

3.1.3. Kinerja Mode Jam Kerja

Mode jam kerja berfungsi 100% sesuai jadwal. Sistem secara otomatis membuka *magnetic door lock* pada pukul 07:00 WIB dan mengunci kembali pada pukul 17:00 WIB. Fitur *touch sensor* dari dalam juga bekerja dengan baik untuk mengunci pintu secara manual selama jam kerja. Hasil ini mendukung konsep *spatiotemporal access control* yang diusulkan Guo et al. [19], di mana pembatasan akses berbasis waktu dapat meningkatkan efisiensi operasional tanpa intervensi manual yang berlebihan.

Tabel 6. Hasil Pengujian Mode Jam Kerja (07:00–16:00 WIB)

Waktu Simulasi	Status Diharapkan	Status Aktual	Touch sensor Berfungsi	Keterangan
06:00 WIB	Terkunci	Terkunci	-	Sesuai
07:00 WIB	Terbuka	Terbuka	-	Sesuai
12:00 WIB	Terbuka	Terbuka	Ya	Sesuai
16:00 WIB	Terbuka	Terbuka	Ya	Sesuai
17:00 WIB	Terkunci	Terkunci	-	Sesuai

3.1.4. Kinerja Mode Non-Jam Kerja

Sistem menunjukkan keberhasilan keseluruhan 98,89% pada mode non-jam kerja. *Delay* otomatis 5 detik setelah pintu terbuka memberikan waktu yang cukup bagi pengguna untuk keluar-masuk ruangan tanpa mengganggu keamanan. Mekanisme *touch sensor* ganda (mengunci saat jam kerja dan membuka saat non-jam kerja) merupakan keunggulan desain yang belum banyak ditemukan pada penelitian sebelumnya [6], [7].

Tabel 7. Hasil Pengujian Mode Non-Jam Kerja

Metode Akses	n	Berhasil	Gagal	Keberhasilan (%)
RFID dari luar (<i>tag valid</i>)	30	29	1	96,67
RFID dari luar (<i>tag invalid</i>)	30	0	30	100,00
<i>Touch sensor</i> dari dalam	30	30	0	100,00

3.1.5. Kinerja Mode Manual (Override) via Blynk

Mode *override* melalui aplikasi Blynk berfungsi sempurna (100%). Waktu respon rata-rata 1,25 detik menunjukkan latensi yang dapat diterima untuk aplikasi IoT berbasis MQTT.

Tabel 8. Hasil Pengujian Mode Manual

Perintah dari Blynk	n	Berhasil	Keberhasilan (%)	Waktu Respon Rata-rata (detik)
Aktivasi Mode Manual	30	30	100,00	1,18
Perintah Buka	30	30	100,00	1,35
Perintah Kunci	30	30	100,00	1,22
Kembali ke Mode Otomatis	30	30	100,00	1,27

3.1.6. Efektivitas Deteksi Intrusi dan Alarm

Deteksi intrusi mencapai tingkat keberhasilan 93,33%. Dua kegagalan notifikasi disebabkan oleh fluktuasi sinyal WiFi. *Buzzer* menyala terus-menerus pada kasus pembukaan paksa, sementara akses normal tidak memicu alarm. Hasil ini membuktikan bahwa sensor kontak magnetik dapat diintegrasikan secara efektif sebagai deteksi intrusi sederhana namun andal [16].

Tabel 9. Hasil Pengujian Deteksi Intrusi

Skenario	n	Buzzer Aktif	Notifikasi Terkirim	Keberhasilan (%)
Pembukaan paksa (dijebol)	30	30	28	93,33
Pembukaan normal (dengan RFID)	30	0	0	100,00

3.1.7. Kestabilan Konektivitas IoT

Packet loss sebesar 6% dan *Delay* rata-rata 248 ms masih berada dalam batas wajar untuk aplikasi *smart door lock* di lingkungan sekolah [4]. Variasi *Delay* terutama dipengaruhi oleh kondisi jaringan WiFi kampus.

Tabel 10. Hasil Pengujian Konektivitas IoT (MQTT + Blynk)

Parameter	Nilai
Total paket dikirim	100
Paket berhasil	94
<i>Packet loss</i>	6,00%
Rata-rata <i>Delay</i>	248 ms
<i>Delay</i> minimum	112 ms
<i>Delay</i> maksimum	685 ms

3.1.8. Ringkasan Kinerja Sistem

Tabel 11. Ringkasan Parameter Kinerja Sistem

No	Parameter Kinerja	Hasil	Target	Status
1	Akurasi RFID (<i>valid</i>)	96,67%	> 95%	Tercapai
2	Akurasi RFID (<i>invalid</i>)	100,00%	100%	Tercapai
3	Waktu respon rata-rata	1,24 detik	< 2 detik	Tercapai
4	Keberhasilan Mode Jam Kerja	100,00%	100%	Tercapai
5	Keberhasilan Mode Non-Jam Kerja	98,89%	> 95%	Tercapai
6	Keberhasilan Mode Manual	100,00%	100%	Tercapai
7	Keberhasilan Deteksi Intrusi	93,33%	> 95%	Hampir Tercapai
8	<i>Packet loss</i> IoT	6,00%	< 10%	Tercapai

3.1.9. Diskusi Umum

Sistem *smart door lock* yang dikembangkan berhasil mengintegrasikan tiga fitur utama (autentikasi RFID, mode jam kerja, dan deteksi intrusi) dalam satu *platform* IoT berbasis ESP32 dan Blynk. Keberhasilan keseluruhan di atas 96% menunjukkan kelayakan implementasi di institusi pendidikan seperti SMAN 3 Salatiga. Inovasi utama penelitian ini terletak pada fungsi ganda *touch sensor* dan mode operasional berbasis RTC yang otomatis, yang belum banyak diusulkan pada penelitian sebelumnya [6], [17].

Kelebihan sistem ini adalah fleksibilitas tinggi, biaya rendah, dan kemampuan monitoring *real-time*. Keterbatasannya adalah deteksi intrusi masih bergantung pada sensor kontak sederhana (belum menggunakan *machine learning*), serta ketergantungan pada koneksi internet yang stabil. Hasil penelitian ini memberikan kontribusi praktis bagi pengelolaan keamanan ruangan di sekolah dan dapat menjadi dasar pengembangan sistem serupa dengan penambahan fitur *face recognition* atau *cloud database* di masa mendatang.

4. KESIMPULAN DAN SARAN

4.1.1. Kesimpulan

Sistem *smart door lock* berbasis IoT yang dikembangkan berhasil mengintegrasikan autentikasi RFID, mode jam kerja otomatis (07:00–16:00 WIB), dan deteksi intrusi dengan tingkat keberhasilan keseluruhan di atas 96%. Sistem mampu bekerja secara *real-time* melalui *platform* Blynk, menunjukkan fleksibilitas tinggi dan kelayakan implementasi di institusi pendidikan. Penelitian ini

berhasil mengatasi *gap* pada penelitian terdahulu dengan menambahkan pengaturan waktu operasional dan mekanisme deteksi intrusi secara terintegrasi.

4.1.2. Saran

Untuk pengembangan lebih lanjut, disarankan:

1. Meningkatkan deteksi intrusi menggunakan algoritma *machine learning* atau *fuzzy logic* untuk mengurangi *false alarm*.
2. Menambahkan autentikasi multi-faktor (*fingerprint / face recognition*) dan sistem cadangan *offline*.
3. Mengoptimasi konektivitas dengan protokol MQTT QoS 1 dan *database cloud* untuk *multi-door system*.
4. Melakukan uji coba *usability* dengan jumlah responden yang lebih besar.

Penelitian ini diharapkan menjadi referensi pengembangan sistem keamanan IoT yang adaptif dan aplikatif di lingkungan pendidikan.

DAFTAR PUSTAKA

- [1] A. Alashbi, A. H. Mohamed, I. Shaye, A. A. El-Saleh, and A. Ahad, "A Review of IoT Applications in Smart Environments: From Smart Cities to Military Integration BT - Advances in Intelligent Computing Techniques and Applications," in *Advances in Intelligent Computing Techniques and Applications*, F. Saeed, F. Mohammed, and Y. Fazea, Eds., Cham: Springer Nature Switzerland, 2024, pp. 176–190.
- [2] M. Ohemu and M. O. Idoko, "Development of a Low-Cost IoT-Enabled Door Access Control System for Smart Home Security," *Asian J. Comput. Sci. Technol.*, vol. 14, no. 2 SE-Articles, pp. 43–50, Dec. 2025, doi: 10.70112/ajcst-2025.14.2.4387.
- [3] S. R. Sankara Vadivel, K. V. G. K., and D. R. V. J., "Chapter One - Introduction to the Internet of Things (IoT)," P. Mishra, S. K. Jagatheesaperumal, U. Garg, K. K. Karmarkar, and B. B. B. T.-I. of T. S. Gupta, Eds., Elsevier, 2026, pp. 3–31. doi: <https://doi.org/10.1016/B978-0-44-333759-8.00010-1>.
- [4] M. Khan and A. Khare, "Next-Gen Exam Paper Protection: IoT Smart Lock with GPS, Biometrics & Anti-Tampering," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 42s, 2025, doi: 10.52783/jisem.v10i42s.8267.
- [5] Y. Chen, H. Zhang, and S. Zhong, "Design and implementation of smart home system based on IoT," *Results Eng.*, vol. 24, p. 103410, 2024, doi: <https://doi.org/10.1016/j.rineng.2024.103410>.
- [6] K. A. K. Permana, I. N. Piarsa, and A. A. K. A. C. Wiranatha, "IoT-Based Smart Door Lock System with Fingerprint and Keypad Access," *J. Inf. Syst. Informatics*, vol. 6, no. 3 SE-Articles, pp. 2086–2098, 2024, doi: 10.51519/journalisi.v6i3.844.
- [7] A. A. Zainuddin *et al.*, "Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology," *Malaysian J. Sci. Adv. Technol.*, vol. 4, no. 4 SE-Articles, pp. 360–365, 2024, doi: 10.56532/mjsat.v4i4.335.
- [8] P. V. Le-Hoang and N. T. Loi, "RFID in smart retailing: The roles of shopping experience, technostress, and disconfirmation sensitivity in driving repurchase intention," *J. Retail. Consum. Serv.*, vol. 91, p. 104728, 2026, doi: <https://doi.org/10.1016/j.jretconser.2026.104728>.
- [9] W. Fall, L. A. N. Seck, and F. I. Barro, "An RFID Based Access Control System operating with a Computer Program and a Database," *Int. J. Circuits, Syst. Signal Process.*, vol. 15, 2021, doi: 10.46300/9106.2021.15.195.
- [10] N. F. Jannah, H. P. Pratama, and S. Fuada, "IOT-Based Smart Door Selector For Double Security: Integration of Rfid and Blynk App for Economical Solution," *Eduvest - J. Univers. Stud.*, vol. 4, no. 10 SE-Articles, pp. 8580–8591, Oct. 2024, doi: 10.59188/eduvest.v4i10.39011.
- [11] B. Kasim *et al.*, "Performance Analysis of RFID-Based Smart Door Lock Controlled by Arduino," *J. Adv. Res. Appl. Mech.*, vol. 122, no. 1 SE-Articles, pp. 163–174, Jul. 2024, doi: 10.37934/aram.122.1.163174.

- [12] J. Guntur, S. S. Raju, T. Niranjana, S. K. Kilaru, R. Dronavalli, and N. S. S. Kumar, "IoT-Enhanced Smart Door Locking System with Security," *SN Comput. Sci.*, vol. 4, no. 2, p. 209, 2023, doi: 10.1007/s42979-022-01641-9.
- [13] L. Wang, Z. Luo, R. Guo, and Y. Li, "A Review of Tags Anti-Collision Identification Methods Used in RFID Technology," 2023. doi: 10.3390/electronics12173644.
- [14] A. Amirova, L. Aldasheva, and A. Abdiraman, "Securing the Industrial Internet of Things: Threats, Vulnerabilities, and Recommendations," *Procedia Comput. Sci.*, vol. 272, pp. 625–630, 2025, doi: <https://doi.org/10.1016/j.procs.2025.10.258>.
- [15] A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 58, no. 4, p. 114, 2025, doi: 10.1007/s10462-024-11101-w.
- [16] M. Q. Mehmood, M. S. Malik, M. H. Zulfiqar, M. A. Khan, M. Zubair, and Y. Massoud, "Invisible touch sensors-based smart and disposable door locking system for security applications," *Heliyon*, vol. 9, no. 2, p. e13586, 2023, doi: <https://doi.org/10.1016/j.heliyon.2023.e13586>.
- [17] H. Asysyauqi, M. F. Andriansyah, L. N. Ulla, and A. Sucipto, "Sistem Keamanan Pintu Otomatis Berbasis IoT dengan Teknologi RFID dan Aplikasi Mobile Menggunakan Metode Fuzzy Mamdani," *Modem J. Inform. dan Sains Teknol.*, vol. 3, no. 2 SE-Articles, pp. 42–50, Apr. 2025, doi: 10.62951/modem.v3i2.405.
- [18] A. M. Tall and C. C. Zou, "A Framework for Attribute-Based Access Control in Processing Big Data with Multiple Sensitivities," 2023. doi: 10.3390/app13021183.
- [19] Y. Guo, L. Yin, C. Li, and J. Qian, "Spatiotemporal access model based on reputation for the sensing layer of the IoT," *ScientificWorldJournal.*, vol. 2014, p. 671038, 2014, doi: 10.1155/2014/671038.
- [20] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions," 2023. doi: 10.3390/s23041805.
- [21] G. S. Harahap, A. H. Daulay, and N. Nasution, "PROTOTIPE SISTEM SMART DOOR LOCK MENGGUNAKAN E-KTP DAN AUTOMATIC LIGHTING BERBASIS INTERNET OF THINGS (IoT)," *J. ONLINE Phys.*, vol. 9, no. 2 SE-Instrumentasi, pp. 18–22, Apr. 2024, doi: 10.22437/jop.v9i2.31825.
- [22] A. J. Umam, D. Setiana, and A. Pradana, "Rancangan radio frequency identification (rfid) smart door lock system berbasis internet of things untuk manajemen membership fitness center," *J. CoSciTech (Computer Sci. Inf. Technol.)*, vol. 4, no. 2 SE-Articles, pp. 359–365, Aug. 2023, doi: 10.37859/coscitech.v4i2.5126.