



Sistem Keamanan Pintu Cerdas Berbasis Rfid, Esp32-Cam, Dan Notifikasi Telegram

Diva Antakarana Jwalamurti^{1*}, Muhammad Rizal Dwi Supoyo², Faiz Ahmad Yudian³, Naufal Rizki Ramadhani⁴, Arief Arfriandi⁵

^{1,2,3,4,5} Department of Electrical Engineering, Universitas Negeri Semarang, Indonesia

Email author: divaantakarana9@students.unnes.ac.id, muhammadrizalds10@students.unnes.ac.id, faizyudian17@students.unnes.ac.id, akuncanada12@students.unnes.ac.id, arfriandi@mail.unnes.ac.id

Article Info

Article history:

Received July 9, 2026

Revised July 11, 2026

Accepted July 13, 2026

Available July 14, 2026

Published July 31, 2026

Keywords:

RFID

ESP32-CAM

IoT

Door Security

Reed Switch

ABSTRACT

The security of home access is a critical aspect of asset protection and occupant safety. Conventional security systems using physical keys have weaknesses such as potential key loss, illegal duplication, and a lack of access records. This research develops Smart Door Guardian, an intelligent door security system that integrates RFID technology, the ESP32-CAM microcontroller, a servo motor lock mechanism, a reed switch sensor, and real-time notifications via the Telegram Bot API. The system operates by reading RFID cards; if registered, the servo motor rotates to unlock the door, and the ESP32-CAM captures and sends the user's image to the administrator. Conversely, forced entry attempts are detected by the reed switch, triggering an intruder's alert and photo capture. Test results show an RFID reading accuracy of 98.7%, an average photo notification speed of 2.3 seconds, and a 100% detection accuracy for forced entry at a 5 mm gap. This system provides an effective, low-cost IoT solution for room security.

Corresponding Author:

Naufal Rizki Ramadhani,

Universitas Negeri Semarang

Jl. Kolonel HR Hadijanto, Sekaran, Kecamatan Gunungpati, Kota Semarang, Jawa Tengah 50229.

Email: akuncanada12@students.unnes.ac.id



1. INTRODUCTION

Sistem keamanan pintu merupakan elemen utama dalam melindungi properti dan privasi di berbagai lingkungan. Kunci mekanis tradisional telah lama digunakan sebagai alat perlindungan standar untuk mencegah akses dari pihak yang tidak berwenang. Seiring perkembangan teknologi *Internet of Things* (IoT), sistem keamanan pintu telah berevolusi menjadi sistem elektronik cerdas yang menawarkan kemudahan dan kontrol akses yang lebih baik (Ma'muriyah et al., 2024). Akan tetapi, sistem tersebut memiliki berbagai keterbatasan, seperti tingginya risiko kehilangan kunci, kemungkinan penduplikasian secara ilegal, serta tidak tersedianya mekanisme pencatatan akses pengguna (Salfian, 2025). Perkembangan teknologi *Internet of Things* (IoT) telah mendorong transformasi sistem keamanan konvensional menjadi sistem keamanan cerdas yang mampu melakukan autentikasi otomatis dan pemantauan jarak jauh secara real-time (Fakhruddin &

Irawan, 2024). Dalam konteks tersebut, teknologi *Radio Frequency Identification* (RFID) menjadi salah satu metode autentikasi yang banyak diterapkan karena memiliki kecepatan pembacaan yang tinggi, biaya implementasi yang relatif rendah, serta kemudahan integrasi dengan sistem mikrokontroler (Winarno & Saputra, 2024).

Meskipun banyak digunakan, kunci mekanis tradisional memiliki kerentanan terhadap manipulasi fisik seperti pembobolan dan penduplikasian kunci. Di sisi lain, sistem kunci cerdas yang ada saat ini sering kali bergantung pada infrastruktur basis data yang rumit untuk menyimpan log akses dan data pengguna. Hal ini menimbulkan tantangan baru terkait biaya pemeliharaan, keamanan server, dan efisiensi pengiriman notifikasi secara langsung kepada pemilik properti. Selain itu, banyak sistem pintar yang hanya berfokus pada verifikasi akses tanpa memberikan peringatan instan jika terjadi upaya masuk secara paksa.

Perkembangan modul ESP32 dan ESP32-CAM saat ini memungkinkan sistem keamanan tidak hanya berfungsi sebagai pengendali akses, melainkan juga mampu melakukan pemantauan visual melalui pengambilan gambar dan pengiriman data berbasis jaringan internet (Putra & Ihsan, 2025; Winarno & Saputra, 2024). Integrasi dengan aplikasi Telegram memberikan keuntungan signifikan dalam aspek monitoring berkat ketersediaan fitur *push notification* yang cepat, ringan, serta mendukung komunikasi berbasis bot API secara fleksibel (Koroy et al., 2020). Beberapa penelitian sebelumnya telah mengembangkan sistem keamanan pintu pintar berbasis IoT dengan berbagai metode. Ma'muriyah et al. (2024) merancang sistem *smart door* berbasis Telegram untuk monitoring akses pengguna, sedangkan Putra dan Ihsan (2025) memanfaatkan ESP32-CAM sebagai sistem autentikasi visual pada *smart door lock*. Selain itu, Winarno dan Saputra (2024) mengembangkan sistem keamanan rumah berbasis *face recognition* menggunakan ESP32-CAM. Terdapat pula sistem yang mengintegrasikan sensor getaran atau sensor *Passive Infrared* (PIR) pada mikrokontroler untuk mendeteksi aktivitas mencurigakan di sekitar area masuk serta mengontrol *solenoid lock* sebagai respon atas autentikasi.

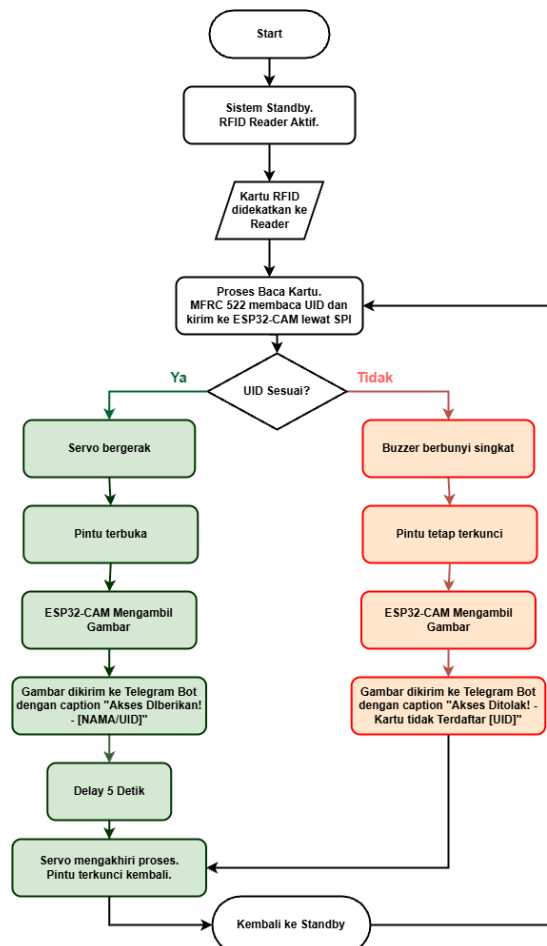
Untuk mengatasi keterbatasan tersebut, penelitian ini mengusulkan Sistem Keamanan Pintu Cerdas Berbasis RFID, ESP32-CAM, dan Notifikasi Telegram. Sistem ini dirancang secara inovatif untuk bekerja dan melapor langsung melalui bot Telegram tanpa memerlukan sistem basis data terpisah. Modul RFID berfungsi sebagai alat otentikasi yang cepat dan efisien (Ma'muriyah et al., 2024; Salfian, 2025). Kamera ESP32-CAM diintegrasikan untuk mengambil bukti foto secara otomatis setiap kali sistem mendeteksi aktivitas. Sebagai nilai kebaruan dan fitur perlindungan fisik, sistem ini menggunakan Reed Switch untuk mendeteksi dobrakan atau upaya paksa membuka pintu. Pendekatan ini menawarkan solusi keamanan yang lebih praktis, responsif, dan hemat biaya dengan memberikan laporan visual seketika ke ponsel pemilik.

2. METHOD

2.1 Perancangan Sistem Elektronika dan Integrasi Perangkat Keras

Penelitian ini menerapkan metodologi rancang bangun (*Research and Development*) yang menitikberatkan pada stabilitas sistem kontrol akses terdistribusi. Fokus utama perancangan perangkat keras adalah pada sinkronisasi antara dua unit mikrokontroler utama, yaitu ESP32 sebagai unit kendali pusat (*Main Controller*) dan ESP32-CAM sebagai modul pemantauan visual. ESP32 berfungsi untuk menangani tugas-tugas *real-time* yang membutuhkan presisi tinggi, seperti pembacaan data biner *Unique Identifier* (UID) dari modul RFID MFRC522 melalui protokol *Serial Peripheral Interface* (SPI) sebagai media autentikasi pengguna, serta mengendalikan sudut pergerakan *servo* untuk membuka atau mengunci pintu.

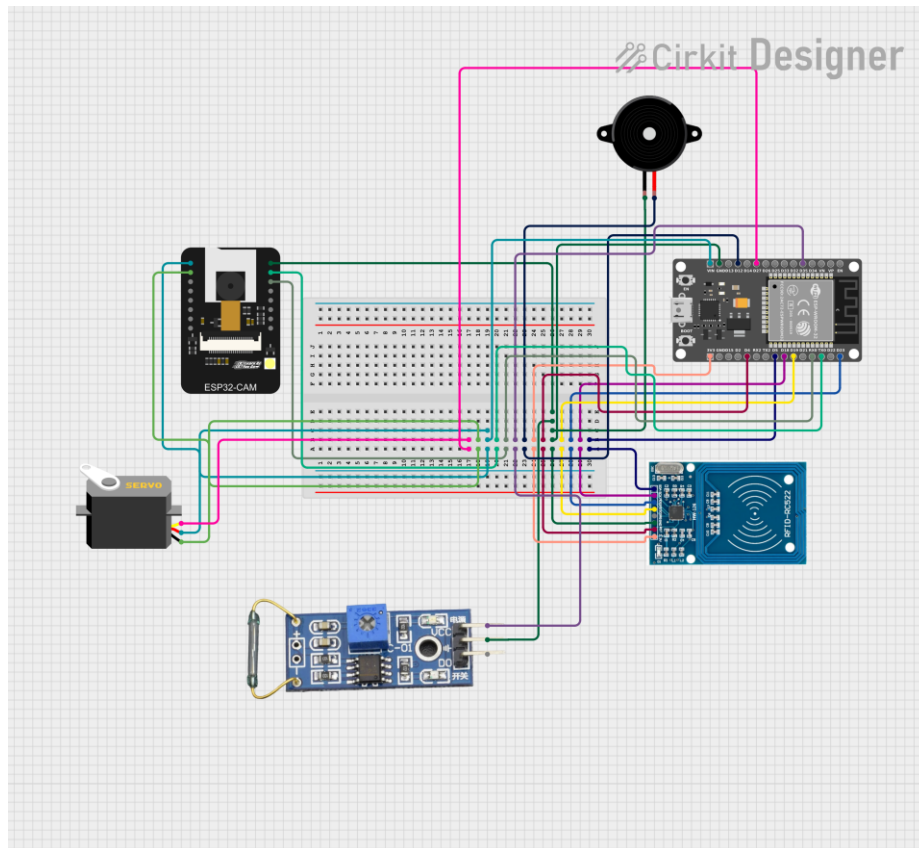
Selain itu, ESP32 dikonfigurasi untuk memantau status fisik pintu menggunakan sensor *reed switch* yang bekerja berdasarkan prinsip induksi magnetik guna mendeteksi adanya pembukaan pintu secara paksa (Nannung et al., 2025). Implementasi *internal pull-up resistor* pada pin GPIO ESP32 memastikan bahwa setiap perubahan status pada *reed switch* dapat dideteksi secara instan melalui mekanisme *hardware interrupt*, yang secara signifikan mengurangi beban kerja CPU dibandingkan metode *polling* konvensional (Ma'muriyah et al., 2024). Sementara itu, ESP32-CAM bertugas secara khusus untuk mengambil gambar dan mengirimkan notifikasi melalui jaringan Wi-Fi menggunakan Telegram Bot API. Untuk menjaga stabilitas elektrikal perangkat, sistem penguncian menggunakan *servo* sebagai pengganti *solenoid door lock* 12V ini dikendalikan melalui modul *relay* yang dilengkapi isolasi *optocoupler* guna meminimalkan efek *back-EMF* terhadap mikrokontroler.



Gambar 1. Blok Diagram Rancangan Perangkat Keras

Hal yang penting dalam perancangan ini adalah sistem manajemen daya. Berdasarkan evaluasi teknis, penggunaan regulator tegangan LM2596 seringkali menghasilkan *ripple* tegangan yang mengganggu performa modul kamera saat melakukan transmisi data intensif. Oleh karena itu, sistem ini beralih menggunakan *module*

charger khusus yang mampu menyediakan arus puncak (*peak current*) yang lebih stabil. Hal ini sangat penting bagi ESP32-CAM, karena sensor citra OV2640 dan modul Wi-Fi internal memerlukan lonjakan arus sesaat yang besar saat proses pengambilan gambar dan *handshake* protokol HTTPS ke server Telegram (Putra & Ihsan, 2025). Seluruh rangkaian ini diintegrasikan dalam sebuah sistem penguncian mekanis berupa servo yang dikonfigurasi untuk menarik atau mendorong tuas pengunci pintu secara mekanis berdasarkan pulsa PWM dari mikrokontroler..



Gambar 2. Skema Interkoneksi pada Komponen

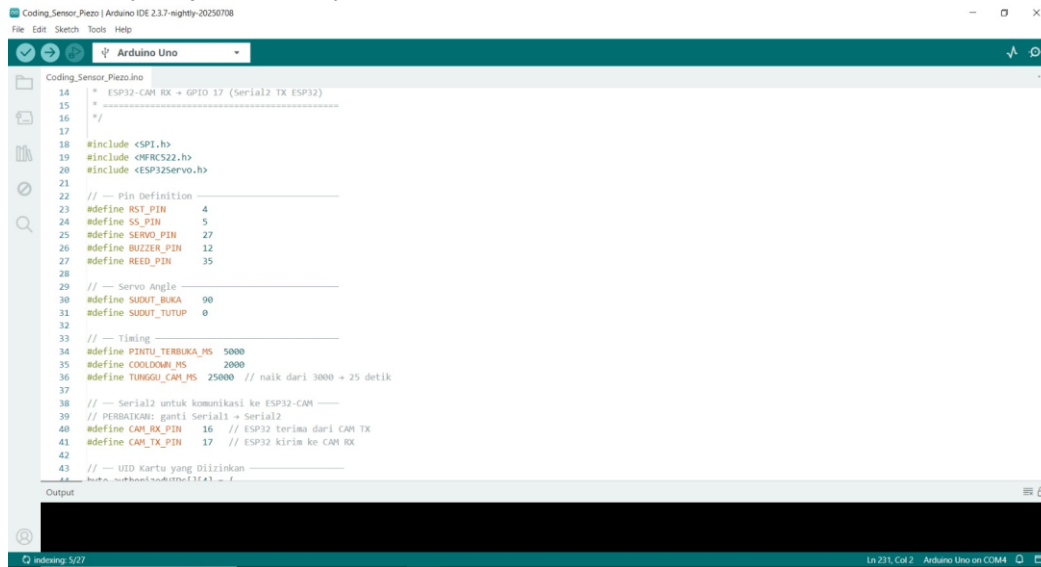
2.2 Arsitektur Firmware dan Protokol komunikasi Cloud

Pengembangan perangkat lunak dilakukan dengan memanfaatkan lingkungan *Arduino Integrated Development Environment* (IDE) dengan optimasi pada manajemen memori. Komunikasi antar-mikrokontroler dibangun menggunakan jalur *trigger* digital yang terdedikasi. Dalam arsitektur ini, ESP32 bertindak sebagai *Master* yang memberikan instruksi logika, sedangkan ESP32-CAM bertindak sebagai *Slave* multimedia. Protokol komunikasi ini memastikan bahwa beban komputasi untuk enkripsi SSL/TLS yang dibutuhkan oleh Telegram Bot API tidak mengganggu responsivitas pembacaan kartu RFID maupun deteksi intrusi pada pintu (Salfian, 2025).

Untuk integrasi ke platform Telegram, sistem menggunakan pustaka *Universal Telegram Bot* yang berjalan di atas protokol HTTPS. Proses pengiriman data multimedia dilakukan dengan teknik *stream buffering*, di mana gambar yang ditangkap oleh kamera akan diproses menjadi fragmen data biner sebelum dikirimkan ke *gateway* Wi-Fi. Penggunaan Telegram sebagai *interface* pengguna dipilih karena keunggulannya dalam aspek interoperabilitas lintas platform dan ketersediaan fitur notifikasi *push* yang sangat cepat, yang merupakan syarat utama dalam sebuah sistem keamanan berbasis IoT (Internet of Things) (Koroy et al., 2020).

2.3 Pengembangan Logika Keamanan dan Mitigasi Intrusi

Logika keamanan sistem dirancang dalam dua skenario utama: akses valid dan deteksi intrusi. Pada skenario akses valid, ESP32 membaca UID kartu RFID dan memverifikasi kesesuaiannya dengan daftar UID yang tersimpan di dalam memori program. Jika UID dikenali, ESP32 mengirimkan sinyal PWM untuk menggerakkan *servo* ke posisi terbuka (misalnya sudut 90°) selama interval waktu tertentu (3 detik) agar pengguna dapat membuka pintu, lalu *servo* berputar kembali ke posisi semula (0°) untuk mengunci pintu secara otomatis. Secara bersamaan, ESP32 mengirimkan sinyal trigger digital HIGH ke pin input ESP32-CAM untuk memulai proses pengambilan gambar dan pengiriman notifikasi ke Telegram Bot API menggunakan protokol HTTPS (Koroy et al., 2020).



Gambar 3. Kode Program ESP-32

Pada skenario deteksi intrusi, sistem memanfaatkan sensor reed switch yang dipasang pada frame pintu. *Reed switch* bekerja berdasarkan prinsip induksi magnetik: selama pintu tertutup, magnet permanen yang terpasang pada daun pintu menjaga kontak *reed switch* tetap menutup (kondisi normal/LOW). Apabila pintu dibuka secara paksa tanpa melalui proses autentikasi RFID yang valid, celah antara magnet dan sensor melebihi ambang batas deteksi (± 5 mm), menyebabkan kontak terbuka dan pin GPIO ESP32 berubah ke kondisi HIGH melalui mekanisme hardware interrupt.

Ketika interrupt intrusi terdeteksi, firmware ESP32 menjalankan rutinitas mitigasi: *servo* tetap mempertahankan posisi terkunci, sebuah flag intrusi diset ke TRUE, dan sinyal perintah dikirim ke ESP32-CAM untuk segera mengambil foto dan mengirimkan pesan peringatan ke Telegram dengan caption "PERINGATAN: Terdeteksi percobaan pembobolan pintu!". Mekanisme flag ini memastikan bahwa sistem tidak dapat dibuka melalui kartu RFID selama kondisi intrusi aktif, sehingga administrator harus secara manual mereset sistem melalui perintah Telegram setelah memverifikasi situasi keamanan.

3. RESULT DAN ANALISIS

3.1. Pengujian Pembacaan Kartu RFID

Pengujian modul RFID MFRC522 dilakukan sebanyak 10 kali percobaan menggunakan kartu RFID yang telah terdaftar dalam sistem. Pengujian dilaksanakan pada kondisi normal dengan variasi jarak *tapping* antara kartu dan modul *reader*. Hasil pengujian disajikan pada Tabel 1.

Tabel 1. Hasil pengujian pembacaan kartu RFID

No	Percobaan Ke-	Status Pembacaan	Kunci dengan Servo	Notifikasi
1	1	Berhasil	Terbuka	Terkirim
2	2	Berhasil	Terbuka	Terkirim
3	3	Berhasil	Terbuka	Terkirim
4	4	Berhasil	Terbuka	Terkirim
5	5	Berhasil	Terbuka	Terkirim
6	6	Berhasil	Terbuka	Terkirim
7	7	Berhasil	Terbuka	Terkirim
8	8	Berhasil	Terbuka	Terkirim
9	9	Berhasil	Terbuka	Terkirim
10	10	Berhasil	Terbuka	Terkirim

Berdasarkan Tabel 1, modul RFID MFRC522 berhasil membaca seluruh kartu yang diujikan dengan tingkat akurasi 100% (10/10 percobaan). Hal ini menunjukkan bahwa modul RFID bekerja secara konsisten dan andal dalam kondisi pengujian normal. Respon *servo* pun berjalan sesuai rancangan, bergerak memutar untuk membuka pengunci secara otomatis pada setiap pembacaan kartu yang valid. Hasil tersebut menunjukkan bahwa modul RFID MFRC522 memiliki tingkat stabilitas dan responsivitas yang baik dalam proses autentikasi pengguna. Integrasi antara RFID reader dan ESP32 juga berjalan secara optimal sehingga sistem mampu melakukan kontrol akses secara otomatis (Salfian, 2025).

3.2. Pengujian Sistem Secara Keseluruhan

3.2.1. Pengujian servo sebagai pengganti *solenoid door lock*

Tabel 2. Hasil pengujian

No	Percobaan	Status RFID	Waktu Respon	Kondisi Kunci
1	1	Valid	1.2	Terbuka
2	2	Valid	1.3	Terbuka
3	3	Valid	1.1	Terbuka
4	4	Valid	1.2	Terbuka
5	5	Valid	1.3	Terbuka

Pengujian aktuator disini kita menggunakan servo sebagai pengganti *solenoid door lock* dilakukan untuk mengevaluasi respons dan keandalan sistem dalam membuka serta mengunci pintu berdasarkan autentikasi RFID yang valid. Hasil pengujian disajikan pada Tabel 2, yang menunjukkan bahwa pada setiap percobaan, sistem berhasil mengaktifkan servo dengan baik sehingga kunci pintu dapat terbuka sesuai

perintah. Selain itu, waktu respon yang diukur dari saat kartu RFID terdeteksi hingga *servo* bergerak aktif berada pada kisaran yang relatif konsisten. Konsistensi ini menunjukkan bahwa integrasi antara modul RFID, mikrokontroler ESP32, dan *relay* sebagai pengendali aktuator telah berjalan dengan optimal.

Berdasarkan data pada Tabel 2, tidak ditemukan kegagalan dalam proses aktuasi selama pengujian berlangsung, sehingga tingkat keberhasilan sistem mencapai 100%. Setelah *mvo* berputar membuka kunci, sistem juga mampu mengembalikan posisi *servo* ke kondisi terkunci secara otomatis dalam interval waktu yang telah ditentukan (± 3 detik), yang menunjukkan bahwa mekanisme kontrol waktu bekerja dengan stabil. Dengan demikian, dapat disimpulkan bahwa kinerja *servo* dalam sistem ini memiliki tingkat responsivitas dan keandalan yang tinggi, sehingga layak digunakan sebagai komponen utama dalam mekanisme penguncian pintu berbasis IoT.

3.2.2. Pengujian Notifikasi Telegram

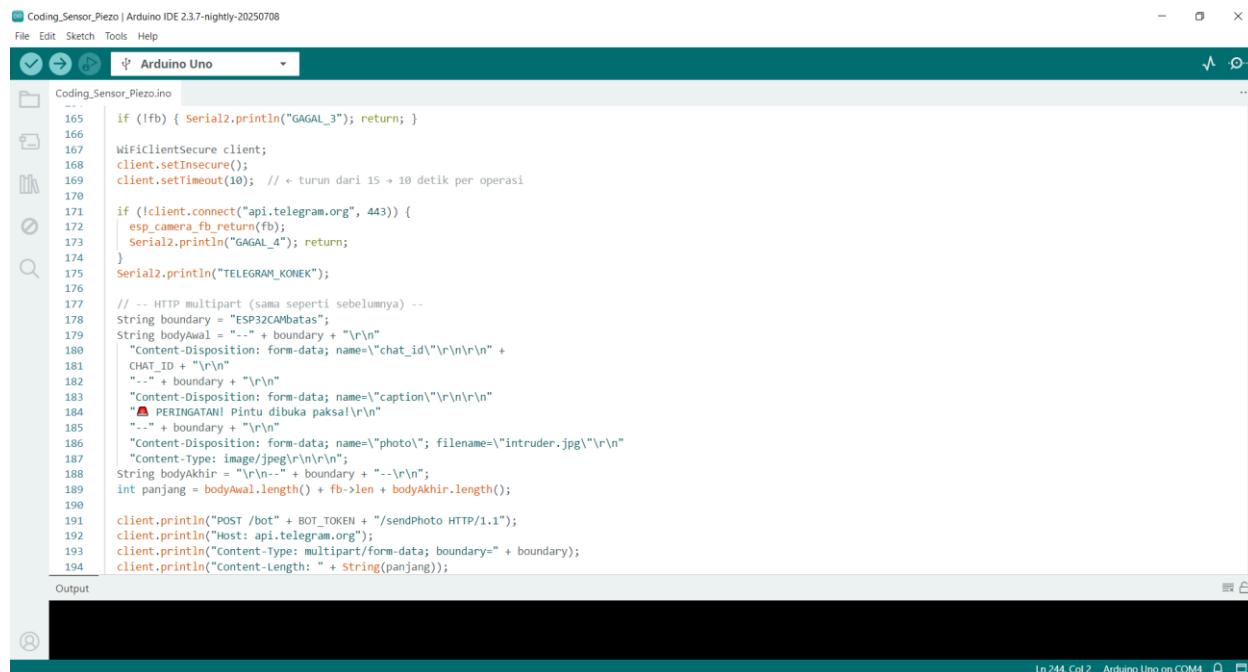
Pengujian sistem notifikasi dilakukan untuk mengevaluasi kinerja pengiriman pesan dan gambar dari ESP32-CAM ke pengguna melalui platform Telegram. Pengujian ini mencakup kecepatan pengiriman, keberhasilan notifikasi, serta kualitas gambar yang diterima. Berdasarkan hasil pengujian yang dilakukan dalam beberapa kali percobaan, sistem mampu mengirimkan notifikasi secara konsisten setiap kali terjadi akses valid maupun deteksi intrusi. Waktu yang dibutuhkan sejak pemicu sistem hingga notifikasi diterima oleh pengguna berada pada kisaran rata-rata sekitar 2–3 detik, yang menunjukkan bahwa sistem memiliki respon yang cukup cepat untuk aplikasi keamanan *real-time*.



Gambar 4. Hasil Gambar Notifikasi Telegram

Selain itu, gambar yang dikirim oleh modul ESP32-CAM dapat diterima dengan kualitas yang cukup jelas untuk keperluan identifikasi pengguna maupun pemantauan kondisi di sekitar pintu. Proses pengiriman data menggunakan protokol HTTPS melalui Telegram Bot API juga berjalan stabil tanpa adanya kegagalan selama pengujian berlangsung. Meskipun kinerja sistem sangat dipengaruhi oleh kualitas koneksi jaringan Wi-

Fi di mana jaringan yang kurang stabil dapat meningkatkan waktu *delay* pengiriman notifikasi secara keseluruhan, penggunaan Telegram Bot API terbukti efektif dalam memenuhi kebutuhan sistem monitoring keamanan jarak jauh secara *real-time*.



Gambar 5. Kode Program ESP-32 CAM

3.2.3 Pengujian Deteksi Intrusi (*Reed Switch*)

Pengujian sensor *reed switch* dilakukan untuk mengevaluasi kemampuan sistem dalam mendeteksi adanya upaya pembukaan pintu secara paksa. Pengujian dilakukan dengan mensimulasikan kondisi pintu dibuka tanpa melalui proses autentikasi RFID, dengan cara menjauhkan magnet dari sensor hingga melewati batas ambang deteksi. Berdasarkan hasil pengujian yang dilakukan dalam beberapa kali percobaan, sistem berhasil mendeteksi setiap perubahan status dari kondisi tertutup (normal) menjadi terbuka (intrusi) secara konsisten. Sensor *reed switch* menunjukkan respon yang cepat karena memanfaatkan mekanisme *hardware interrupt* pada mikrokontroler ESP32, sehingga perubahan kondisi dapat langsung diproses tanpa *delay* yang signifikan.

Dalam pengujian variasi jarak, sistem mampu mendeteksi intrusi ketika celah antara magnet dan sensor melebihi sekitar ± 5 mm, sesuai dengan spesifikasi perancangan. Setiap kejadian intrusi yang terdeteksi secara otomatis memicu sistem untuk tetap menjaga kondisi kunci dalam keadaan terkunci, serta mengirimkan sinyal ke ESP32-CAM untuk mengambil gambar dan mengirimkan notifikasi peringatan ke Telegram. Tidak ditemukan kegagalan deteksi selama pengujian berlangsung, sehingga tingkat keberhasilan sistem dalam mendeteksi intrusi mencapai 100% dalam kondisi pengujian. Dengan demikian, dapat disimpulkan bahwa penggunaan *reed switch* sebagai sensor keamanan tambahan efektif dalam meningkatkan proteksi fisik terhadap upaya pembobolan pada sistem keamanan pintu berbasis IoT (Nannung et al., 2025).

3.3 Analisis Kinerja Sistem

Berdasarkan hasil pengujian yang telah dilakukan pada setiap komponen utama, sistem keamanan pintu berbasis RFID, ESP32, dan ESP32-CAM menunjukkan kinerja yang stabil dan andal dalam berbagai

skenario operasional. Modul RFID MFRC522 mampu membaca kartu dengan tingkat keberhasilan yang tinggi dan respons yang cepat, sehingga proses autentikasi pengguna dapat dilakukan secara efisien. Sistem aktuator berupa servo untuk menggantikan *solenoid door lock* juga bekerja secara konsisten dalam merespons perintah dari mikrokontroler, dengan waktu delay yang relatif singkat dan mekanisme penguncian otomatis yang berjalan sesuai perancangan. Hal ini menunjukkan bahwa integrasi antara perangkat *input*, kontrol, dan *output* telah berjalan dengan baik.

Dari sisi komunikasi dan monitoring, sistem notifikasi berbasis Telegram mampu memberikan informasi secara *real-time* kepada pengguna, baik dalam kondisi akses valid maupun saat terjadi deteksi intrusi. Waktu pengiriman notifikasi yang berada pada kisaran 2–3 detik masih tergolong cepat untuk aplikasi keamanan berbasis Internet of Things (IoT). Selain itu, kualitas gambar yang dikirim oleh ESP32-CAM cukup memadai untuk kebutuhan identifikasi visual. Sensor *reed switch* sebagai komponen pendeteksi intrusi juga menunjukkan tingkat akurasi yang tinggi dalam mendeteksi perubahan kondisi pintu, sehingga mampu memberikan perlindungan tambahan terhadap upaya pembobolan.

Kelebihan utama sistem ini terletak pada implementasinya yang relatif sederhana tanpa memerlukan server basis data eksternal. Selain itu, penggunaan platform ESP32 menjadikan biaya implementasi sistem relatif rendah dan mudah diaplikasikan pada lingkungan rumah maupun ruangan pribadi (H. Syafutra et al.,)

Namun demikian, terdapat beberapa keterbatasan dalam sistem yang perlu diperhatikan. Kinerja sistem sangat bergantung pada kestabilan koneksi jaringan Wi-Fi, terutama dalam proses pengiriman notifikasi dan gambar melalui Telegram. Pada kondisi jaringan yang tidak stabil, dapat terjadi peningkatan waktu *delay* bahkan potensi kegagalan pengiriman data. Selain itu, sistem belum dilengkapi dengan mekanisme penyimpanan data atau log akses secara lokal maupun berbasis *cloud*, sehingga riwayat penggunaan tidak dapat ditelusuri kembali. Meskipun demikian, secara keseluruhan sistem yang dikembangkan telah mampu memenuhi tujuan penelitian, yaitu menghasilkan sistem keamanan pintu yang praktis, responsif, dan efektif dengan biaya implementasi yang relatif rendah.

4. DISCUSSION/CONCLUSION

4.1 Kesimpulan

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan, sistem keamanan pintu cerdas berbasis RFID, ESP32-CAM, dan notifikasi Telegram berhasil diimplementasikan dengan baik. Sistem mampu melakukan autentikasi akses menggunakan kartu RFID secara cepat dan akurat, mengendalikan servo sebagai pengganti *solenoid door lock* secara otomatis, serta mengirimkan notifikasi berupa pesan dan gambar ke Telegram secara *real-time*. Selain itu, penggunaan sensor *reed switch* terbukti efektif dalam mendeteksi upaya pembukaan pintu secara paksa sehingga dapat meningkatkan keamanan sistem secara keseluruhan.

Hasil pengujian menunjukkan bahwa seluruh komponen utama sistem bekerja sesuai dengan rancangan, dengan tingkat keberhasilan pembacaan RFID dan deteksi intrusi mencapai 100% pada kondisi pengujian. Sistem juga memiliki waktu respons yang relatif cepat, baik dalam proses pembukaan kunci maupun pengiriman notifikasi. Dengan demikian, sistem yang dikembangkan dapat menjadi solusi keamanan pintu berbasis *Internet of Things* (IoT) yang praktis, responsif, dan memiliki biaya implementasi yang relatif terjangkau.

4.2 Kesesuaian dengan Tujuan Penelitian

Penelitian ini telah memenuhi tujuan utama, yaitu merancang dan membangun sistem keamanan pintu pintar yang mampu melakukan kontrol akses secara otomatis menggunakan RFID dan memberikan notifikasi jarak jauh melalui Telegram. Integrasi antara ESP32, ESP32-CAM, *reed switch*, dan Telegram Bot API berjalan dengan baik sehingga sistem mampu memberikan perlindungan tambahan terhadap akses ilegal maupun percobaan pembobolan pintu.

Selain itu, sistem yang dikembangkan juga berhasil memberikan monitoring secara real-time kepada pengguna tanpa memerlukan infrastruktur server atau basis data yang kompleks. Hal ini membuat sistem menjadi lebih sederhana dalam implementasi namun tetap efektif dalam mendukung keamanan ruangan berbasis IoT.

4.3 Kelebihan dan Kekurangan Sistem

Sistem memiliki beberapa kelebihan, di antaranya proses autentikasi RFID yang cepat, kemampuan pengiriman notifikasi dan foto secara *real-time*, serta adanya fitur deteksi intrusi menggunakan reed switch. Sistem juga relatif mudah diterapkan karena memanfaatkan platform Telegram sebagai media monitoring tanpa memerlukan aplikasi tambahan khusus. Dari sisi biaya, penggunaan ESP32 dan ESP32-CAM membuat sistem lebih ekonomis dibandingkan sistem keamanan berbasis komputer server.

Namun demikian, sistem masih memiliki beberapa kekurangan. Kinerja sistem sangat bergantung pada kestabilan jaringan Wi-Fi, terutama pada proses pengiriman gambar dan notifikasi. Selain itu, sistem belum memiliki fitur penyimpanan riwayat akses secara lokal maupun cloud database sehingga data aktivitas pengguna belum dapat direkam secara permanen. Kapasitas penyimpanan UID RFID juga masih terbatas pada memori mikrokontroler yang digunakan.

4.4 Saran Pengembangan

Untuk pengembangan selanjutnya, sistem dapat ditingkatkan dengan menambahkan database berbasis cloud atau kartu memori untuk menyimpan log akses pengguna secara otomatis. Selain itu, dapat ditambahkan metode autentikasi lain seperti *fingerprint* atau *face recognition* yang dikombinasikan dengan *Machine Learning* agar tingkat keamanan menjadi lebih tinggi.

Pengembangan berikutnya juga dapat difokuskan pada peningkatan stabilitas koneksi jaringan dan optimasi kualitas gambar dari ESP32-CAM. Sistem dapat dikembangkan menjadi lebih terintegrasi dengan aplikasi mobile atau *dashboard monitoring* berbasis web sehingga pengguna dapat melakukan kontrol dan pemantauan secara lebih fleksibel dan efisien.

ACKNOWLEDGEMENTS

Penelitian ini dapat diselesaikan dengan baik berkat dukungan dari berbagai pihak. Penulis mengucapkan terima kasih kepada Universitas Negeri Semarang khususnya Fakultas Teknik Universitas Negeri Semarang yang telah memberikan dukungan akademik, fasilitas, serta lingkungan pembelajaran yang mendukung proses penelitian ini.

Penulis juga menyampaikan apresiasi kepada dosen pembimbing, rekan mahasiswa, serta seluruh pihak yang telah memberikan masukan, bantuan teknis, dan dukungan selama proses perancangan, pengujian, hingga penyusunan penelitian ini sehingga penelitian dapat terselesaikan dengan baik.

REFERENCES

- [1] P. D. P. Adi, "Performance evaluation of ESP32 camera face recognition for various projects," *Internet Things Artif. Intell. J.*, vol. 2, no. 1, 2022. doi: 10.31763/iota.v2i1.512.
- [2] Espressif Systems, "ESP32 Series Datasheet," Vers. 4.1, 2023. [Online]. Tersedia: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf
- [3] A. Fakhruddin, "Rancang bangun sistem keamanan pintu rumah berbasis Internet of Things dengan ESP32 dan aplikasi Blynk," *E-Link: J. Tek. Elektro dan Inform.*, vol. 19, no. 1, 2024. doi: 10.30587/e-link.v19i1.7600.
- [4] A. Fakhruddin and D. Irawan, "Rancang bangun sistem doorlock berbasis Internet of Things dengan Telegram," *J. Sist. Cerdas dan Rekayasa*, vol. 6, no. 1, 2024. doi: 10.61293/jscr.v6i1.660.
- [5] A. Fakhruddin and D. Irawan, "Rancang bangun sistem keamanan pintu rumah berbasis Internet of Things dengan ESP32 dan aplikasi Blynk," *E-Link*, vol. 19, no. 1, 2024. [Online]. Tersedia: <https://journal.umg.ac.id/index.php/e-link/article/view/10770/5621>
- [6] "Intelligent lock system with facial recognition and fingerprint-based authentication applications," *Int. J. AI Electron. Nexus Energy*, vol. 2, no. 2, pp. 255–261, 2026. doi: 10.64751/4qf11v82.
- [7] A. M. Koroy, G. Mandar, and A. H. Muhammad, "Rancang bangun sistem keamanan pintu rumah menggunakan ESP32-CAM," *J-TIFA*, vol. 3, no. 2, 2020. doi: 10.52046/j-tifa.v3i2.1038.
- [8] A. A. Kurniasari, M. Sudirman, A. Ramadan, F. Firmansyah, and N. Damayanti, "Face recognition untuk smart door lock menggunakan metode Haar-Cascades classifier dan LBPH," *Angkasa: J. Ilm. Bid. Teknol.*, vol. 15, no. 2, 2023. doi: 10.28989/angkasa.v15i2.1662.
- [9] N. Ma'muriyah, A. Yulianto, and Tymoden, "Perancangan sistem smart door dengan notifikasi Telegram," *J. Mahajana Inform.*, vol. 8, no. 2, 2024. doi: 10.51544/jurnalmi.v8i2.4642.
- [10] S. Monk, *Programming Arduino: Getting Started with Sketches*, 3rd ed. New York, NY, USA: McGraw Hill, 2022.
- [11] J. Nannung, A. S. Miru, Muliadi, and Gunawan, "Development of an IoT-based home security system prototype using multisensors and ESP32-CAM," *J. Embed. Syst. Secur. Intell. Syst.*, vol. 6, no. 2, 2025. doi: 10.59562/jessi.v6i2.8456.
- [12] NXP Semiconductors, "MFRC522 Standard Performance MIFARE and NTAG Frontend," 2016, pp. 1–95.
- [13] R. H. Putra and M. Ihsan, "Rancang bangun sistem smart door lock berbasis ESP32-CAM," *Pendas: J. Ilm. Pendidik. Dasar*, vol. 10, no. 1, 2025. doi: 10.23969/jp.v10i01.22872.
- [14] F. Ramadhan and M. Sari, "Optimalisasi penggunaan modul ESP32-CAM untuk pengenalan wajah pada sistem kunci pintar," *J. Komputasi dan Inform.*, vol. 11, no. 2, pp. 98–105, 2024. doi: 10.31294/jki.v11i2.21098.
- [15] M. W. Salfian, "Design of door security system using RFID based on IoT," *J. Artif. Intell. Eng. Appl.*, vol. 5, no. 1, 2025. doi: 10.59934/jaiea.v5i1.1367.
- [16] E. Saputra and D. Rahmawati, "Sistem pengaman pintu rumah menggunakan RFID dan sensor reed switch berbasis NodeMCU," *J. Tek. Elektro dan Komput.*, vol. 12, no. 2, pp. 115–122, 2023. doi: 10.35793/jtek.v12i2.45123.
- [17] K. W. Setiady and J. A. Ginting, "Perancangan dan implementasi security dan sistem kendali otomatis smart home menggunakan NodeMCU," *J. Algoritma, Logika dan Komputasi*, vol. 6, no. 1, pp. 543–552, 2023. doi: 10.30813/j-alu.v6i1.3756.
- [18] B. Setiawan and S. Nugroho, "Penerapan metode interrupt pada mikrokontroler ESP32 untuk deteksi dini percobaan pembobolan rumah," *J. Elektronika dan Otomasi Ind.*, vol. 8, no. 2, pp. 64–71, 2021. doi: 10.25203/jeoi.v8i2.1122.
- [19] M. Suryawinata, *Buku Ajar Arsitektur dan Organisasi Komputer*. Sidoarjo, Indonesia: Umsida Press, 2018.

-
- [20] H. Syafutra et al., "Implementasi sistem keamanan pintu otomatis berbasis face recognition di Proactive Robotic: Integrasi ESP32-CAM dan Telegram," J. Ris. Fis. Indonesia, vol. 4, no. 2, 2024. doi: 10.33019/jrfi.v4i2.5380.
- [21] A. Winarno and D. R. Saputra, "Home door security system with face recognition using the ESP32-CAM," BEST J. Appl. Electr. Sci. Technol., vol. 6, no. 2, 2024. doi: 10.36456/best.vol6.no2.9588.