

Implementasi *Radio Frequency Identification* (RFID) dan *Optical Character Recognition* (OCR) pada Prototipe Sistem Gerbang Otomatis

Mohamad Rizal Fitrian¹⁾, Dion Ogi^{2,*}

1) Badan Siber dan Sandi Negara, mohamad.rizal@bssn.go.id

2) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, dion.ogi@poltekssn.ac.id

Riwayat Artikel

Dikirim 14 November 2024
Diterima 23 April 2025
Diterbitkan 25 April 2025

Kata kunci:

RFID
OCR
Raspberry Pi
AES-128
Firebase
sistem gerbang otomatis

Keywords:

RFID
OCR
Raspberry Pi
AES-128
Firebase
automatic gate system

Abstrak

Penelitian ini bertujuan untuk membangun prototipe sistem gerbang otomatis yang menerapkan autentikasi ganda berbasis *Radio Frequency Identification* (RFID) dan *Optical Character Recognition* (OCR) untuk pembacaan plat nomor kendaraan. Sistem ini menggunakan *single-board computer* (SBC) sebagai pusat kendali yang terintegrasi dengan modul RFID dan kamera SBC. Proses autentikasi dilakukan melalui pencocokan UID kartu RFID dengan database, serta pencocokan hasil OCR dari plat nomor kendaraan dengan data yang terenkripsi di *database cloud*. Pengujian dilakukan untuk mengukur akurasi pembacaan karakter plat nomor kendaraan dan waktu autentikasi. Hasil menunjukkan bahwa tingkat keberhasilan autentikasi pengguna hanya mencapai 15%, dengan rata-rata waktu proses autentikasi 35,42 detik. Akurasi pembacaan karakter plat nomor kendaraan dengan latar hitam sebesar 60,17% dan latar merah sebesar 79,82%. Kinerja sistem dipengaruhi oleh ketepatan algoritma OCR dan keterbatasan perangkat keras. Penelitian ini menunjukkan bahwa sistem dapat dikembangkan lebih lanjut dengan peningkatan pada pemrosesan citra dan optimalisasi waktu proses.

Abstract

This study aims to develop a prototype of an automatic gate system that implements dual authentication based on *Radio Frequency Identification* (RFID) and *Optical Character Recognition* (OCR) for vehicle license plate identification. The system employs a *single-board computer* (SBC) as the central controller, integrated with an RFID module and SBC camera. Authentication is carried out by matching the RFID card's UID with data stored in the database, followed by OCR-based verification of the vehicle's license plate against encrypted records stored in *Firestore cloud*. The system was evaluated in terms of character recognition accuracy and authentication time. Results showed a user authentication success rate of only 15%, with an average authentication time of 35.42 seconds. The accuracy of character recognition reached 60.17% for black-background plates and 79.82% for red-background plates. System performance was influenced by the accuracy of the OCR algorithm and hardware limitations. The findings suggest that future development should focus on improving image processing and reducing processing time.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan kebutuhan terhadap sistem keamanan yang lebih efisien dan otomatis. Salah satu bentuk implementasi teknologi tersebut adalah sistem kontrol akses berbasis kendaraan, yang kini banyak diterapkan di area-area terbatas seperti perkantoran, kampus, dan kawasan industri. Sistem ini mengintegrasikan berbagai teknologi, seperti *Radio Frequency Identification* (RFID), *Optical Character Recognition* (OCR), dan *Internet of Things* (IoT), untuk meningkatkan efisiensi, akurasi, dan keamanan dalam proses autentikasi pengguna [1], [2].

Kendati demikian, sistem keamanan tradisional berbasis satu faktor autentikasi seperti *password* atau kartu akses, dinilai kurang andal dalam menghadapi berbagai ancaman seperti *spoofing* dan pencurian identitas [3], [4]. Oleh karena itu, diperlukan pendekatan keamanan yang lebih kompleks dan berlapis, seperti penerapan *two-factor authentication* (2FA) atau bahkan *multi-factor authentication* (MFA), yang menggabungkan faktor "apa yang dimiliki" (RFID) dan "apa yang diketahui/terdeteksi" (plat nomor kendaraan melalui OCR) [5], [6]. Pendekatan ini dapat mengurangi risiko keamanan serta meningkatkan keandalan sistem kontrol akses.

Implementasi sistem berbasis RFID telah banyak dikembangkan dalam berbagai aplikasi seperti kontrol parkir, manajemen gudang, dan sistem *smart gate* [7], [8], [9]. Di sisi lain, OCR telah menjadi komponen penting dalam pengenalan nomor plat kendaraan secara otomatis (*Automatic Number Plate Recognition*/ANPR), terutama dengan dukungan perangkat komputasi mini seperti Raspberry Pi dan pustaka pemrosesan citra OpenCV [10], [11], [12]. Dengan OCR, karakter pada plat nomor kendaraan dapat diekstraksi dan diidentifikasi untuk keperluan autentikasi secara otomatis tanpa campur tangan manusia [13].

Meski demikian, terdapat sejumlah tantangan teknis dalam implementasi sistem semacam ini, terutama terkait dengan akurasi pembacaan OCR yang dapat dipengaruhi oleh kondisi pencahayaan, sudut kamera, jarak pengambilan gambar, serta jenis plat nomor kendaraan (latar merah, hitam, putih, dan lain-lain.) [2], [14]. Selain itu, integrasi antara RFID dan OCR sebagai bagian dari sistem kontrol akses perlu dirancang secara cermat agar mampu mendeteksi pengguna sah secara efisien, sekaligus menolak akses bagi pihak yang tidak berwenang.

Beberapa penelitian sebelumnya telah mengembangkan prototipe sistem pengenalan kendaraan untuk aplikasi kontrol akses berbasis ANPR [1], [15]. Namun, pendekatan yang menggabungkan OCR dan RFID dalam satu sistem autentikasi masih terbatas, khususnya yang diterapkan pada sistem gerbang otomatis di lingkungan institusional. Maka dari itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan prototipe sistem gerbang otomatis yang menggabungkan teknologi RFID dan OCR sebagai metode autentikasi dua faktor, serta melakukan pengujian terhadap performa dan akurasinya.

2. LANDASAN TEORI

2.1. Sistem Kendali Akses Berbasis RFID

Radio Frequency Identification (RFID) merupakan teknologi yang memungkinkan identifikasi objek atau individu secara otomatis melalui gelombang radio. Dalam sistem kendali akses, RFID banyak digunakan sebagai komponen autentikasi karena kemampuannya membaca data dari tag tanpa kontak langsung dan dengan waktu respon yang cepat [7], [9]. Teknologi RFID memiliki keunggulan dalam hal kepraktisan dan efisiensi, namun rentan terhadap serangan seperti *cloning tag* atau *sniffing* [16]. Oleh karena itu, dalam implementasi sistem keamanan, RFID perlu dikombinasikan dengan teknologi lain untuk meningkatkan ketahanan terhadap ancaman tersebut.

Penggunaan RFID dalam sistem kontrol parkir dan manajemen akses telah dibahas dalam sejumlah studi. Misalnya, Chisowa et al. [7] mengembangkan sistem autentikasi dua faktor berbasis RFID dan ANPR untuk kontrol parkir kendaraan. Studi lain juga menunjukkan bahwa integrasi RFID dengan sistem IoT dapat meningkatkan fleksibilitas dan skalabilitas sistem keamanan [8].

2.2. Optical Character Recognition (OCR) untuk ANPR

Optical Character Recognition (OCR) merupakan teknik yang digunakan untuk mengubah teks dalam bentuk citra menjadi data digital yang dapat dikenali oleh sistem komputer. Dalam konteks ANPR (*Automatic Number Plate Recognition*), OCR digunakan untuk membaca dan mengenali karakter pada plat nomor kendaraan [10]. Teknologi ini menjadi populer berkat kemajuan di bidang pemrosesan citra digital, terutama dengan dukungan pustaka seperti OpenCV dan perangkat seperti Raspberry Pi [11], [12].

Beberapa penelitian telah mengembangkan sistem ANPR berbasis OCR, di antaranya oleh Samantaray et al. [17], yang menggunakan Python dan OpenCV untuk mengenali plat nomor kendaraan. Studi lain oleh Jasmine [15] dan Mujawar & Vadi [11] menunjukkan bahwa Raspberry Pi dapat dimanfaatkan secara efektif untuk membangun sistem ANPR real-time dengan tingkat akurasi yang cukup baik. Namun, performa OCR sangat dipengaruhi oleh kondisi pencahayaan, sudut pengambilan gambar, jenis plat nomor kendaraan, dan kualitas kamera [2], [13].

2.3. Two-Factor Authentication (2FA) dan Keamanannya

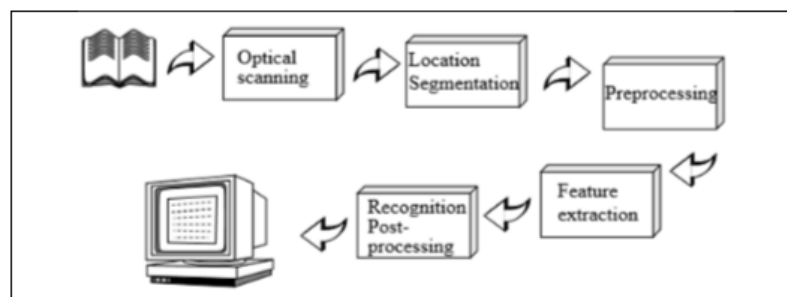
Two-Factor Authentication (2FA) merupakan metode autentikasi yang menggabungkan dua jenis faktor untuk memverifikasi identitas pengguna, misalnya kombinasi antara faktor kepemilikan (RFID) dan faktor biometrik atau pengenalan visual (OCR plat nomor kendaraan). Penerapan 2FA memberikan tingkat keamanan yang lebih tinggi dibandingkan autentikasi satu faktor (1FA) karena mempersulit akses bagi pihak yang tidak berwenang [5], [6].

Dalam konteks sistem akses otomatis, Dasgupta et al. [18] menekankan pentingnya strategi pemilihan faktor autentikasi yang adaptif untuk meningkatkan keamanan tanpa mengorbankan kenyamanan pengguna. Di sisi lain, Mohsin et al. [19] membandingkan 2FA dengan *multi-factor authentication* (MFA) dalam lingkungan *mobile cloud*, dan menyimpulkan bahwa meskipun MFA memberikan keamanan yang lebih tinggi, 2FA sering kali lebih praktis untuk implementasi skala kecil hingga menengah.

2.4. Integrasi RFID dan OCR dalam Sistem Otomatisasi

Beberapa studi telah mulai mengeksplorasi integrasi antara RFID dan OCR dalam sistem otomatisasi, meskipun jumlahnya masih terbatas. Yusuf et al. [8] menunjukkan bagaimana kriptografi dan kontrol akses dapat diterapkan pada sistem IoT berbasis RFID untuk manajemen inventori. Di sisi lain, Kahie et al. [1] dan Ullah et al. [2] menyajikan pendekatan pengenalan plat nomor kendaraan untuk sistem akses berbasis ANPR, tetapi belum menggabungkannya secara langsung dengan RFID sebagai lapisan autentikasi tambahan.

Dengan demikian, dapat disimpulkan bahwa meskipun teknologi RFID dan OCR telah banyak diterapkan secara terpisah dalam sistem kontrol akses, integrasi keduanya dalam satu sistem autentikasi dua faktor untuk gerbang otomatis masih merupakan topik yang relevan untuk diteliti dan dikembangkan lebih lanjut. Berdasarkan kajian literatur di atas, integrasi antara teknologi RFID dan OCR dalam sistem autentikasi dua faktor untuk kontrol akses kendaraan dapat menjadi pendekatan yang menjanjikan untuk meningkatkan keamanan dan efisiensi. Gambar 1 berikut menggambarkan skema OCR yang digunakan dalam penelitian ini.



Gambar 1. Optical Character Recognition [17]

2.5. Ancaman Keamanan terhadap Sistem Gerbang Otomatis

Sistem gerbang otomatis yang mengandalkan teknologi seperti RFID dan OCR tidak luput dari potensi serangan keamanan. Beberapa ancaman yang sering terjadi antara lain serangan *tag cloning*, *replay attack*, dan *spoofing* baik terhadap data RFID maupun citra plat nomor kendaraan.

RFID, meskipun praktis, memiliki kelemahan terhadap serangan seperti *cloning* atau *eavesdropping*, yaitu ketika penyerang dapat merekam sinyal dari tag RFID dan menggunakannya kembali untuk mendapatkan akses ilegal [13]. Hal ini menunjukkan pentingnya penggunaan enkripsi pada data yang ditransmisikan oleh tag RFID serta validasi autentikasi ganda.

Sementara itu, pada sistem pengenalan plat nomor berbasis OCR, ancaman *presentation attack* seperti penggunaan gambar atau video kendaraan tertentu dapat mengecoh sistem visual. Senapatha dan Tamtama [3] mengulas bagaimana serangan semacam ini mengganggu sistem pengenalan wajah, dan prinsip serupa bisa diterapkan untuk memahami kerentanan OCR dalam ANPR. Selain itu, kondisi lingkungan seperti pencahayaan rendah atau plat nomor kendaraan yang rusak juga dapat mengakibatkan kesalahan identifikasi [2].

Samantaray et al. [17] dan Dasgupta et al. [18] menekankan bahwa penguatan sistem autentikasi perlu mempertimbangkan baik ancaman teknis maupun konteks penggunaannya. Dalam implementasi 2FA, pemilihan kombinasi autentikasi harus seimbang antara keamanan, efisiensi, dan kenyamanan pengguna.

Dengan mempertimbangkan berbagai ancaman tersebut, maka integrasi dua teknologi (RFID dan OCR) dalam sistem autentikasi dua faktor dapat menjadi solusi yang memperkuat lapisan keamanan dalam sistem gerbang otomatis, selama dirancang dengan mempertimbangkan aspek kriptografi, validasi input, dan deteksi anomali.

3. HASIL DAN PEMBAHASAN

Penelitian ini mengimplementasikan sistem gerbang otomatis dengan autentikasi dua faktor berbasis RFID dan OCR untuk meningkatkan keamanan akses kendaraan. Sistem ini dirancang dalam tiga komponen utama, yaitu: komponen pengguna (*user side*), sistem kontrol pada gerbang (*gate controller*), serta *server backend* untuk penyimpanan dan validasi data.

3.1. Analisis Kebutuhan

Analisis kebutuhan dilakukan dengan studi literatur dan observasi untuk mendapatkan berbagai informasi terkait proses bisnisnya sehingga dapat dirumuskan kebutuhan-kebutuhan dalam sistem yang akan dibangun, yang ditampilkan dalam Tabel 1 dan Tabel 2. Sedangkan kebutuhan sistem baik perangkat keras maupun perangkat lunak yang digunakan untuk membangun sistem gerbang otomatis ditampilkan dalam Tabel 3 dan Tabel 4.

Tabel 1. Kebutuhan Fungsional Sistem Gerbang Otomatis

Nomor	Kebutuhan Fungsional Sistem
1	Sistem harus mampu melakukan autentikasi RFID dan pengenalan plat nomor kendaraan.
2	Sistem harus mampu menyediakan fitur registrasi pengguna pada <i>database</i> .
3	Sistem harus mampu menyediakan fitur hapus pengguna pada <i>database</i> .
4	Sistem harus mampu menyediakan log riwayat aktivitas pengguna pada <i>database</i> .

Tabel 2. Kebutuhan Non-fungsional Sistem Gerbang Otomatis

Nomor	Kebutuhan Non-fungsional Sistem
1	Database yang digunakan adalah Google Firebase <i>realtime database</i> .
2	Pembangunan sistem menggunakan Raspberry Pi Model 4B, MFRC522 RFID Reader, RFID Card, dan Pi Camera.
3	Pengamanan data pada <i>database</i> menggunakan AES 128.

Tabel 3. Daftar Perangkat Keras yang Digunakan

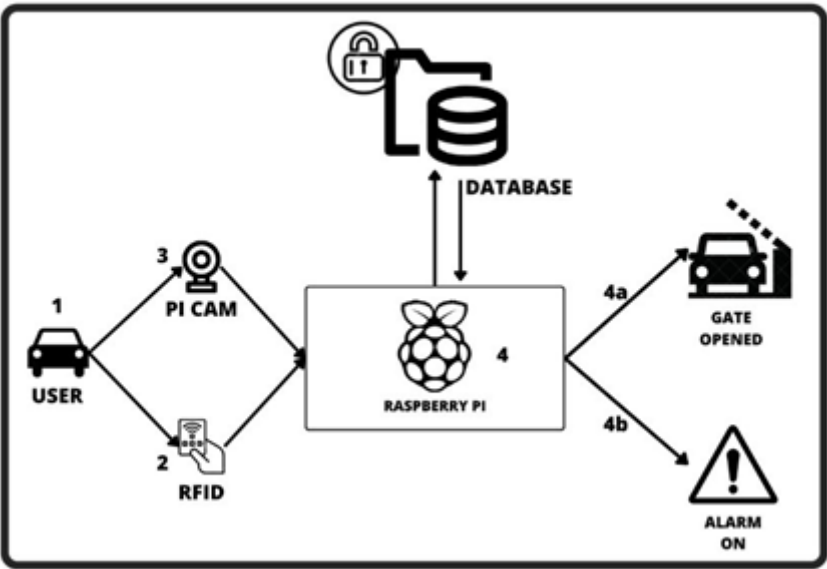
Nomor	Perangkat Keras
1	Raspberry Pi Model 4B, sebagai pusat pengolahan data yang digunakan untuk implementasi perangkat keras, melakukan proses autentikasi.
2	RFID Reader, untuk membaca informasi dari kartu RFID
3	RFID Card, untuk menyimpan data UID pengguna.
4	Pi Camera, untuk menangkap gambar plat nomor kendaraan.

Tabel 4. Daftar Perangkat Lunak yang Digunakan

Nomor	Perangkat Lunak
1	Sistem Operasi, sistem operasi yang digunakan adalah Debian Buster untuk Raspberry Pi Model 4B.
2	Bahasa Pemrograman, bahasa pemrograman yang akan digunakan untuk implementasi sistem adalah Python.
3	Library, library yang diperlukan untuk mengaktifkan dan mengontrol perangkat keras seperti RPi.GPIO, OpenCV, MFRC522, Firebase, dan Pytesseract.
4	Thonny Python, untuk melakukan editor kode program pada Raspberry.
5	Google Firebase, database digunakan untuk menyimpan data.

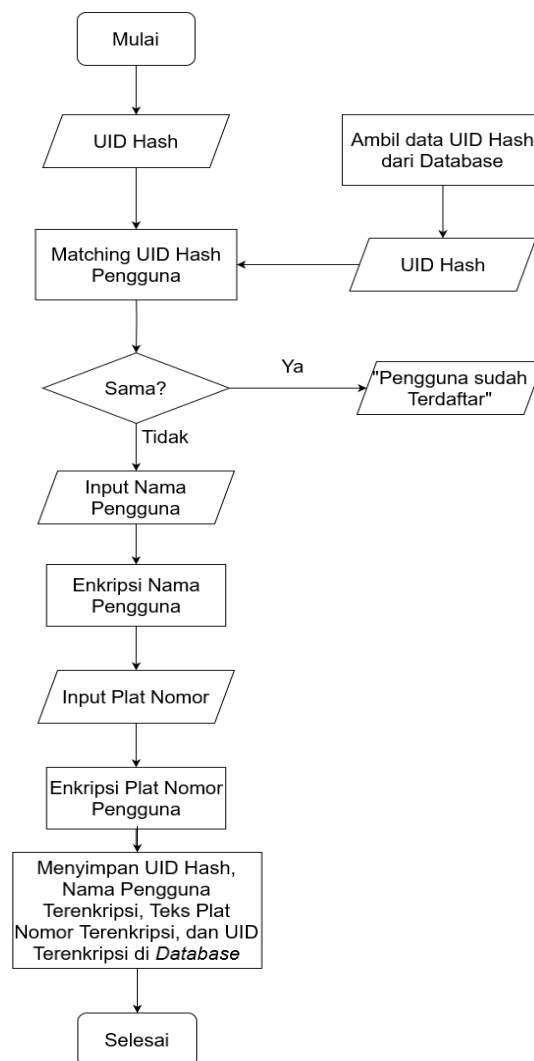
3.2. Arsitektur Sistem

Sistem ini terdiri dari dua tahapan autentikasi. Pertama, pengguna melakukan pemindaian kartu RFID melalui pembaca RFID. Jika kartu dikenali sebagai kartu yang valid, maka sistem akan melanjutkan ke tahap kedua, yaitu deteksi dan pembacaan plat nomor kendaraan menggunakan Pi Cam dan algoritma OCR. Jika kedua autentikasi berhasil, maka palang gerbang akan terbuka secara otomatis.



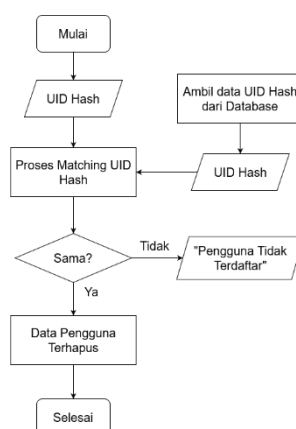
Gambar 2. Arsitektur Sistem Gerbang Otomatis

Gambar 2 menunjukkan arsitektur sistem yang dikembangkan. Dari gambaran umum sistem tersebut, dijabarkan proses kerja sistem menggunakan pemodelan *flowchart* dengan 3 fitur proses kerja sebagai berikut. Gambar 3 menunjukkan bahwa fungsi Registrasi dimulai dengan proses pengambilan nilai UID dari tag RFID, dilanjutkan dengan pemeriksaan *database* untuk mengetahui keberadaan data yang sama. Proses berikutnya adalah menginput data pengguna dan mengenkripsi sebelum menyimpannya pada *database*.

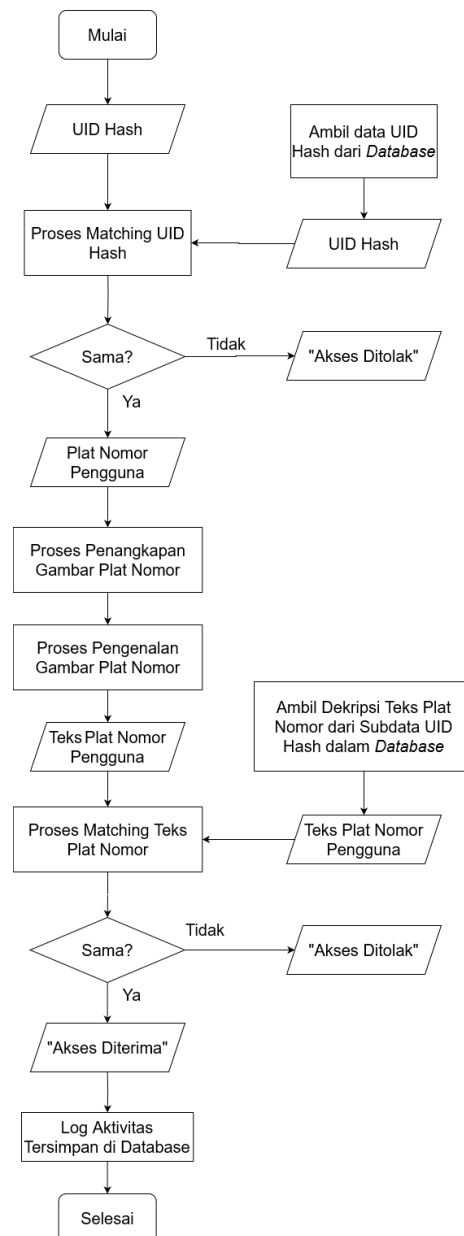


Gambar 3. Diagram Alur Fungsi Registrasi

Dari Gambar 4 berikut diketahui bahwa fungsi Penghapusan Data dimulai dengan proses pengambilan nilai UID dari tag RFID, dilanjutkan dengan pemeriksaan *database* untuk mengetahui keberadaan data.



Gambar 4. Fungsi Penghapusan Data

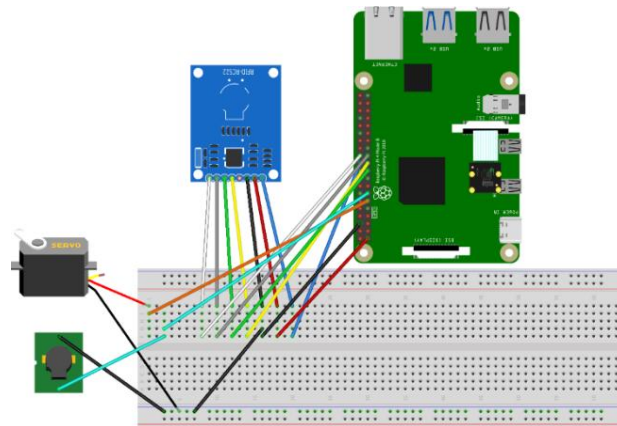


Gambar 5. Fungsi Autentikasi dan Log

Gambar 5 menunjukkan fungsi Autentikasi yang diawali dengan proses pengambilan nilai UID dari tag RFID, dilanjutkan dengan proses pencocokan dengan data yang ada pada *database*. Jika sama maka dilanjutkan dengan proses dekripsi data plat nomor kendaraan dari *database* dan pencocokan dengan data yang diperoleh dari foto tangkapan Pi Cam. Jika sama maka akses pengguna diterima dan aktifitas pengguna dicatat lalu disimpan pada *database*.

3.3. Implementasi Sistem

Sistem gerbang otomatis menerapkan autentikasi menggunakan perangkat keras yang sudah dianalisis berdasarkan kebutuhan fungsional dan non-fungsional. Sistem gerbang otomatis dibangun pada Raspberry Pi yang terintegrasi dengan MFRC522 Reader untuk autentikasi menggunakan RFID Card dan modul Pi Cam untuk autentikasi menggunakan pengenalan plat nomor kendaraan. Sebagai *output* dari sistem gerbang otomatis menggunakan *servo* untuk indikasi bahwa akses diterima dan *buzzer* untuk indikasi bahwa akses ditolak. Gambar 6 merupakan gambar konfigurasi perangkat keras yang digunakan.



Gambar 6. Konfigurasi Perangkat Keras

Sistem yang bekerja mengimplementasikan autentikasi RFID pada sistem gerbang otomatis dan menggunakan pengenalan plat nomor kendaraan berbasis OCR menggunakan Google Firebase. Firebase Database adalah layanan penyimpanan data *cloud*. Firebase Database digunakan untuk menyimpan data pengguna dan log data.

Data pengguna seperti identitas berupa nama pengguna, nomor UID pengguna, dan nomor plat kendaraan disimpan dalam bentuk *JSON object* pada *database*. Setiap pengguna memiliki dokumen tersendiri pada *database* yang diberi nama berdasarkan nomor UID pengguna. Dokumen tersebut berisi data pengguna seperti pada entitas berupa nama pengguna dan nomor plat kendaraan pengguna. Selain itu, data log juga disimpan dalam *database*. Setiap kali pengguna melakukan autentikasi menggunakan RFID dan OCR, data log akan disimpan dengan format *JSON* pada *database*. Data log berisi informasi tentang waktu masuk, nama pengguna, dan nomor plat kendaraan pengguna.

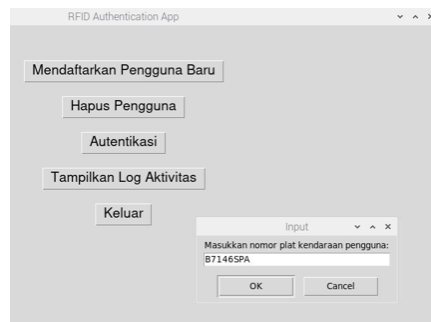
Setelah konfigurasi perangkat keras dan database dilakukan maka pemrograman untuk membangun fungsi-fungsi sistem dilakukan. Tampilan dari hasil pemrograman sistem dapat dilihat pada Gambar 7 hingga Gambar 13.



Gambar 7. Tampilan Proses Input Tag RFID

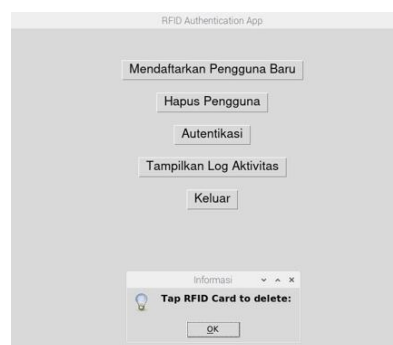


Gambar 8. Tampilan Proses Input Nama Pengguna

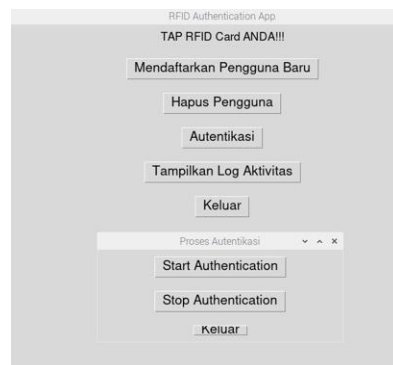


Gambar 9. Tampilan Input Nomor Plat Kendaraan

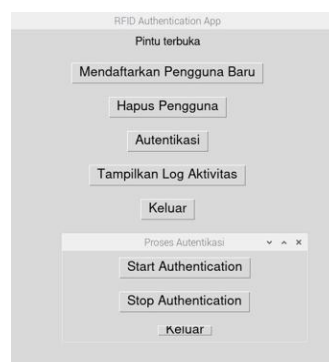
Gambar 7 menunjukkan proses input tag pengguna sebagai langkah awal registrasi pengguna sistem. Langkah berikutnya menginput nama pengguna dan nomor plat kendaraannya sebagai mana ditunjukkan oleh Gambar 8 dan Gambar 9. Data nama dan nomor plat kendaraan selanjutnya dienkripsi dengan AES-128 sebelum disimpan pada Firebase. Gambar 10 menunjukkan proses hapus data pengguna, jika suatu saat pengguna tidak lagi ada.



Gambar 10. Tampilan Proses Hapus Pengguna



Gambar 11. Tampilan Autentikasi Tag RFID



Gambar 12. Tampilan Notifikasi Autentikasi Berhasil



Gambar 13. Tampilan Log Aktivitas

Gambar 11 menunjukkan proses input tag pengguna sebagai langkah autentikasi pengguna sistem, dilanjutkan dengan pengenalan nomor plat kendaraan. Jika hasil pencocokan nilai Hash UID tag RFID dan pencocokan nomor plat kendaraan berhasil maka sistem memberikan notifikasi bahwa pintu gerbang terbuka seperti ditunjukkan pada Gambar 12. Log aktifitas keluar masuk yang melalui sistem ini tercatat dan disimpan secara aman pada Firebase, ditunjukkan oleh Gambar 13.

3.4. Pengujian Sistem

Sistem yang dihasilkan dari tahapan implementasi kemudian diuji untuk mengetahui apakah fungsionalitas dan non-fungsionalitas sistem sudah sesuai dengan yang diharapkan. Adapun pengujian yang dilakukan pengujian sistem yang meliputi *Unit Testing*, *Integration Testing*, *System Testing*, dan *Security Testing*.

Pengujian sistem dilakukan untuk mengevaluasi hal-hal sebagai berikut:

1. Keberhasilan autentikasi pengguna melalui UID RFID dan OCR plat nomor kendaraan.
2. Akurasi sistem dalam mengenali karakter pada plat nomor kendaraan.
3. Waktu rata-rata proses autentikasi dari awal hingga keputusan akses.

Langkah-langkah pengujian meliputi:

1. Menyiapkan beberapa kartu RFID dan kendaraan dengan berbagai jenis plat nomor (latar hitam dan merah).
2. Melakukan proses autentikasi sebanyak 20 kali untuk setiap jenis plat nomor kendaraan.
3. Mencatat jumlah keberhasilan autentikasi (akses diterima) dan kegagalan (akses ditolak).
4. Menghitung akurasi pengenalan karakter pada plat nomor kendaraan secara manual dengan membandingkan hasil OCR terhadap plat nomor kendaraan yang asli.
5. Mencatat waktu proses autentikasi mulai dari pembacaan tag RFID hingga gerbang terbuka atau akses ditolak.

Pengujian *security testing* dilakukan dengan menguji sistem implementasi autentikasi pada sistem gerbang otomatis yang datanya dienkripsi dalam *database*. *Security testing* dilakukan dengan melakukan *test vector* pada algoritma AES128 yang digunakan untuk mengenkripsi data. *Test vector* dilakukan untuk memastikan bahwa proses enkripsi dan dekripsi yang dilakukan sudah sesuai.

3.4.1. Hasil Pengujian Sistem

Berdasarkan hasil *unit testing* setiap tahapan dalam keseluruhan skema, dapat disimpulkan bahwa semua proses pada sistem yang telah dibangun dapat dilakukan dan memberikan hasil yang sesuai dengan harapan yang diinginkan. Dari hasil pengujian *integration testing* yang tercatat, dapat disimpulkan bahwa keseluruhan fungsi untuk mengintegrasikan antarmuka dengan setiap komponen yang berbeda dalam sistem, semuanya beroperasi dengan baik.

Pengujian *system testing* dilakukan dengan menguji kesesuaian kebutuhan fungsional dan non-fungsional yang telah ditetapkan. Hasil pengujian menunjukkan bahwa seluruh kebutuhan fungsional dan non-fungsional telah berhasil diimplementasikan dan berjalan dengan baik. Tabel 5,

Tabel 6, dan Tabel 7 menyajikan hasil pengujian terhadap akurasi, tingkat keberhasilan autentikasi dan waktu respon sistem.

Tabel 5. Hasil Pengujian Akurasi Pengenalan Plat Nomor Kendaraan

Jenis Plat Nomor Kendaraan	Jumlah Karakter	Karakter Terbaca	Akurasi (%)
Latar hitam	120	72	60,17
Latar merah	120	96	79,82

Tabel 6. Hasil Pengujian Keberhasilan Autentikasi

Total Pengujian	Autentikasi Berhasil	Autentikasi Gagal	Keberhasilan (%)
20	3	17	15

Tabel 7. Waktu Proses Autentikasi

Jenis Autentikasi	Waktu Proses (detik)	Waktu Rata-rata (detik)
Autentikasi Berhasil	106,25	35,42
Autentikasi Gagal	624,87	36,76

3.4.2. Hasil Security Testing

Hasil pengujian *Security Testing* dengan *Test Vector* menggunakan AES 128 ditunjukkan pada Tabel 8.

Tabel 8. Hasil Pengujian *Test Vector* Implementasi AES 128

Teks Asli	Teks Terenkripsi	Vector	Hasil
e2e59e3fa6	qXwlaXg+P0eDskGw1bceww==	qXwlaXg+P0eDskGw1bceww==	Sesuai
29da03f00	mydVfRsxZ8sCZ2EvZasLrQ==	mydVfRsxZ8sCZ2EvZasLrQ==	Sesuai

4. KESIMPULAN

Berdasarkan hasil-hasil pengujian di atas maka dapat disimpulkan keberhasilan autentikasi sebesar 15%. Akurasi pengenalan plat nomor dari setiap karakter pada plat nomor berlatar belakang hitam adalah rata-rata 60,17% dan plat nomor berlatar belakang merah adalah rata-rata 79,82%. Performa waktu rata-rata keberhasilan proses autentikasi adalah 35,42 detik. Akurasi pengenalan karakter pada plat nomor kendaraan masih di bawah ekspektasi, kemungkinan disebabkan oleh keterbatasan algoritma OCR yang digunakan. Selain itu, waktu proses autentikasi yang cukup lama disebabkan oleh keterbatasan performa dari Raspberry Pi sebagai pusat pengolahan.

Terdapat dua aspek yang perlu diperbaiki pada implementasi autentikasi RFID pada prototipe sistem gerbang otomatis yang menerapkan pengenalan plat nomor kendaraan OCR. Pertama, akurasi dalam mengenali karakter plat nomor kendaraan, yang dapat ditingkatkan melalui teknik pengolahan citra lanjutan dan pemilihan algoritma OCR yang lebih tepat. Kedua, optimalisasi kinerja sistem untuk mengurangi waktu proses, termasuk dengan mempertimbangkan penggunaan perangkat keras dengan spesifikasi lebih tinggi.

REFERENSI

- [1] S. A. Kahie, A. A. Nor, A. H. Hasan, A. M. Abdi, L. M. Hassan, and M. A. Mohamud, "A smart access control for restricted buildings using vehicle number plates recognition system," in 2021 1st International Conference on Emerging Smart Technologies and Applications, eSmarTA 2021, Institute of Electrical and Electronics Engineer Inc., Aug. 2021. doi:10.1109/eSmarTA52612.2021.9515752.
- [2] F. Ullah et al., "Barrier access control using sensors platform and vehicle license plate characters recognition", *Sensors (Switzerland)*, vol. 19, no. 13, Jul. 2019, doi: 10.3390/s19133015.
- [3] I. K. D. Senapatha and G. I. W. Tamtama, "Studi Literatur Presentation Attack dan Set Data Anti-Spoof Wajah", *Jurnal Teknik Elektro*, vol. 14, no. 1, pp. 10–17, Jun. 2022, doi: 10.15294/jte.v14i1.36108.
- [4] S. Bhattacharjee, A. Mohammadi, A. Anjos, and S. Marcel, "Recent advances in face presentation attack detection", in *Advances in Computer Vision and Pattern Recognition*, Springer London, 2019, pp. 207–228. doi: 10.1007/978-3-319-92627-8_10.

- [5] R. Krishnan Konoth, V. van der Veen, and H. Bos, "How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication". [Online]. Available: <http://twofactorauth.org>
- [6] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication", *Commun ACM*, vol. 58, no. 7, pp. 78–87, Jul. 2015, doi: 10.1145/2699390.
- [7] M. Yusuf, A. Arizal, I. R. Hikmah, "Implementation Cryptography and Access Control on IoT-Based Warehouse Inventory Management System", *Teknik Informatika dan Rekayasa Komputer*, vol. 22, no. 1, 37–50, 2022, doi: 10.30812/matrik.v22i1.1849.
- [8] Y. Miao, Q. Tong, R. H. Deng, K. K. R. Choo, X. Liu, and H. Li, "Verifiable Searchable Encryption Framework Against Insider Keyword-Guessing Attack in Cloud Storage", *IEEE Transactions on Cloud Computing*, vol. 10, no. 2, pp. 835–848, 2022, doi: 10.1109/TCC.2020.2989296.
- [9] W. Huang, Y. Zhang, and Y. Feng, "ACD: An adaptable approach for RFID cloning attack detection", *Sensors (Switzerland)*, vol. 20, no. 8, Apr. 2020, doi: 10.3390/s20082378.
- [10] F. Chisowa Chazanga, J. Phiri, and S. Namukolo, "Development of a Two Factor Authentication for Vehicle Parking Space Control based on Automatic Number Plate Recognition and Radio Frequency Identification", 2019. [Online]. Available: www.ijacsa.thesai.org
- [11] S. S. Mujawar and S. Vadi, "Raspberry Pi And Opencv For License Plate Recognition In Realtime," [Online]. Available: www.irjmets.com
- [12] U. Salimah, V. Maharani, and R. Nursyanti, "Automatic License Plate Recognition Using Optical Character Recognition", *IOP Conf Ser Mater Sci Eng*, vol. 1115, no. 1, p. 012023, Mar. 2021, doi: 10.1088/1757-899x/1115/1/012023.
- [13] W. A. Jabbar, C. W. Wei, N. A. A. M. Azmi, and N. A. Haironnazli, "An IoT Raspberry Pi-based parking management system for smart campus[Formula presented]", *Internet of Things (Netherlands)*, vol. 14, Jun. 2021, doi: 10.1016/j.iot.2021.100387.
- [14] A. Fadlil and D. Prayogi, "Face Recognition Using Machine Learning Algorithm Based on Raspberry Pi 4b", *International Journal of Artificial Intelligence Research*, vol. ISSN, no. 1, pp. 2579–7298, 2022, doi: 10.29099/ijair.v7i1.321.
- [15] Jsl. Jasmine, "Accurate Vehicle Number Plate Recognition And Real Time Identification Using Raspberry Pi", *International Research Journal of Engineering and Technology*, 2018, [Online]. Available: www.irjet.net.
- [16] A. Dwi Saputra and M. Syafrullah, "Algoritme Aes-256 untuk Keamanan Basis Data Penilaian Pegawai pada PT. Buana Jaya Korindo", 2022.
- [17] M. Samantaray, A. K. Biswal, D. Singh, D. Samanta, M. Karuppiyah, and N. P. Joseph, "Optical Character Recognition (OCR) based Vehicle's License Plate Recognition System Using Python and OpenCV", in *Proceedings of the 5th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 849–853. doi: 10.1109/ICECA52323.2021.9676015.
- [18] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication", *Comput Secur*, vol. 63, pp. 85–116, Nov. 2016, doi: 10.1016/j.cose.2016.09.004.
- [19] J. K. Mohsin, L. Han, M. Hammoudeh, and R. Hegarty, "Two factor vs multi-factor, an authentication battle in mobile cloud computing environments", in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jul. 2017. doi: 10.1145/3102304.3102343.