

RANCANG BANGUN SISTEM LOG AKSES KE RUANG SERVER BERBASIS IoT MENGGUNAKAN PENGENALAN WAJAH

Janto Junior Rembet¹, Graciella Regita Maharani Kaligis², Folansky Vladimir
Bambulu³, Eliezer Mangoting Rongre⁴, Yonatan Parassa⁵

^{1,2,3,4,5} Politeknik Negeri Manado

¹janto.jr42@gmail.com, ²regitakaligis2004@gmail.com,

³folanskyvladimirbambulu@gmail.com, ⁴eliezermangoting@gmail.com,

⁵yonatan.pa@gmail.com

ABSTRACT

This study aims to design and implement an Internet of Things (IoT)-based server room access logging system using facial recognition technology. Conventional security systems such as mechanical locks and access cards have several limitations, including vulnerability to loss, duplication, and unauthorized access, as well as the absence of automatic activity logging. Therefore, this research proposes an integrated system that combines facial recognition for authentication with real-time access logging and monitoring. The system utilizes ESP32-CAM as an image acquisition device, while face detection is performed using the Haar Cascade method and identification is conducted using cosine similarity. Data collection was carried out by capturing 50 facial images per registered user at a distance of approximately 30 cm with variations in facial angles. The system was tested under real operational conditions, showing an average accuracy of 91% with a response time of approximately 1–2 seconds. In addition, the system successfully records access activities, including access status and user data, which can be monitored through a web-based interface. The results indicate that the proposed system can improve server room security by providing automated authentication, access control, and real-time monitoring in an integrated manner.

Keywords: IoT, facial recognition, access control, ESP32-CAM, security system

ABSTRAK

Penelitian ini bertujuan untuk merancang dan membangun sistem log akses ruang server berbasis Internet of Things (IoT) menggunakan teknologi pengenalan wajah. Sistem keamanan konvensional seperti kunci mekanis dan kartu akses memiliki berbagai kelemahan, seperti rentan terhadap kehilangan, duplikasi, serta tidak mampu mencatat aktivitas akses secara otomatis. Oleh karena itu, penelitian ini mengusulkan sistem terintegrasi yang menggabungkan autentikasi berbasis pengenalan wajah dengan pencatatan dan monitoring akses secara real-time. Sistem menggunakan ESP32-CAM sebagai perangkat akuisisi citra, dengan metode Haar Cascade untuk deteksi wajah dan cosine similarity untuk proses identifikasi. Pengumpulan data dilakukan dengan merekam 50 citra wajah untuk setiap pengguna terdaftar pada jarak sekitar 30 cm dengan variasi sudut wajah. Hasil pengujian menunjukkan bahwa sistem memiliki rata-rata akurasi sebesar 91% dengan waktu respon sekitar 1–2 detik. Selain itu, sistem mampu mencatat aktivitas akses secara otomatis yang dapat dimonitor melalui antarmuka berbasis web. Hasil penelitian menunjukkan bahwa sistem yang dikembangkan mampu meningkatkan keamanan ruang server dengan menyediakan autentikasi, kontrol akses, dan monitoring secara otomatis dan terintegrasi.

Kata Kunci: IoT, pengenalan wajah, kontrol akses, ESP32-CAM, sistem keamanan

A. Pendahuluan

Keamanan sistem informasi menjadi aspek yang sangat krusial dalam era digital, khususnya pada pengelolaan ruang server sebagai pusat penyimpanan dan pengolahan data. Salah satu permasalahan utama dalam sistem keamanan fisik adalah penggunaan metode konvensional seperti kunci mekanis dan kartu akses yang masih rentan terhadap kehilangan, duplikasi, serta akses tidak sah. Penelitian sebelumnya menunjukkan bahwa metode tradisional tersebut memiliki kelemahan signifikan karena tidak mampu memberikan kontrol akses yang adaptif serta tidak menyediakan pencatatan aktivitas pengguna secara otomatis (Obasi & Tahir, 2025). Selain itu, kebutuhan akan sistem keamanan yang mampu bekerja secara real-time semakin meningkat seiring berkembangnya infrastruktur digital berbasis jaringan.

Untuk mengatasi masalah-masalah di atas, penerapan Internet of Things (IoT) dan teknologi biometrik telah semakin meluas dari tahun ke tahun dalam sistem keamanan modern. IoT memungkinkan perangkat untuk saling berkomunikasi dan berbagi data secara *real time*,

sehingga meningkatkan efisiensi pemantauan dan pengendalian akses (Koteswaramma et al., 2022). Sebaliknya, teknologi biometrik seperti pengenalan wajah dianggap lebih aman daripada metode tradisional karena mengandalkan ciri-ciri unik manusia yang sulit dipalsukan. Obasi & Tahir (2025) menemukan bahwa sistem berbasis pengenalan wajah dapat meningkatkan keamanan dan mengurangi kemungkinan akses tanpa izin dibandingkan dengan sistem berbasis PIN atau kunci mekanis. Jadi, integrasi IoT dan pengenalan wajah merupakan cara yang efektif untuk meningkatkan sistem keamanan di ruang-ruang terbatas seperti ruang server.

Beberapa penelitian sebelumnya telah mengembangkan sistem keamanan berbasis IoT dan pengenalan wajah. Penelitian oleh Ariansyah et al. (2021) mengembangkan sistem kontrol akses pintu berbasis IoT dengan pengenalan wajah yang mampu mengidentifikasi pengguna melalui proses pengolahan citra digital dan membuka akses secara otomatis. Penelitian lain menunjukkan bahwa penggunaan ESP32-CAM sebagai

perangkat utama memungkinkan implementasi sistem keamanan berbasis pengenalan wajah dengan biaya rendah dan kemampuan *real-time* (Bolimera et al., 2025). Selain itu, Syafutra et al. (2024) mengintegrasikan sistem pengenalan wajah dengan notifikasi berbasis Telegram untuk meningkatkan kemampuan monitoring jarak jauh. Hasil penelitian Nannung et al. (2025) juga menunjukkan bahwa sistem berbasis ESP32-CAM mampu mencapai akurasi pengenalan wajah hingga lebih dari 95% dalam kondisi tertentu.

Namun, setelah menelaah studi-studi tersebut, jelas bahwa masih ada beberapa celah penelitian yang perlu diisi. Sebagian besar studi masih berfokus pada cara menyusun sistem keamanan untuk rumah pintar atau prototipe sederhana sehingga belum banyak diterapkan di lingkungan institusional yang membutuhkan tingkat keamanan tinggi. Studi-studi sebelumnya juga sebagian besar membahas fungsi autentikasi pengguna tanpa menghubungkannya dengan pencatatan akses otomatis. Selain itu, belum banyak sistem yang menyediakan pemantauan akses terpusat secara *real-time*, yang sangat

penting untuk pengelolaan ruang server.

Mengingat adanya kesenjangan tersebut, keunikan penelitian ini terletak pada pengembangan sistem pencatatan akses ruang server berbasis IoT yang terintegrasi dengan teknologi pengenalan wajah. Sistem ini tidak hanya berfungsi sebagai sistem autentikasi, tetapi juga dapat secara otomatis mencatat aktivitas akses serta menyediakan pemantauan secara *real-time*. Konsep ini sejalan dengan perkembangan sistem keamanan modern berbasis IoT yang mengintegrasikan autentikasi, kontrol akses, dan pencatatan aktivitas ke dalam satu sistem terpadu (Khadafi et al., 2024).

Dengan demikian, fokus penelitian ini adalah merancang dan membangun sistem yang mampu: (1) melakukan autentikasi pengguna menggunakan teknologi pengenalan wajah, (2) mengontrol akses masuk ke ruang server secara otomatis, serta (3) mencatat dan memonitor aktivitas akses secara *real-time* berbasis IoT pada lingkungan BLSDM Komdigi Manado (Harun & Zainal, n.d.).

B. Metode Penelitian

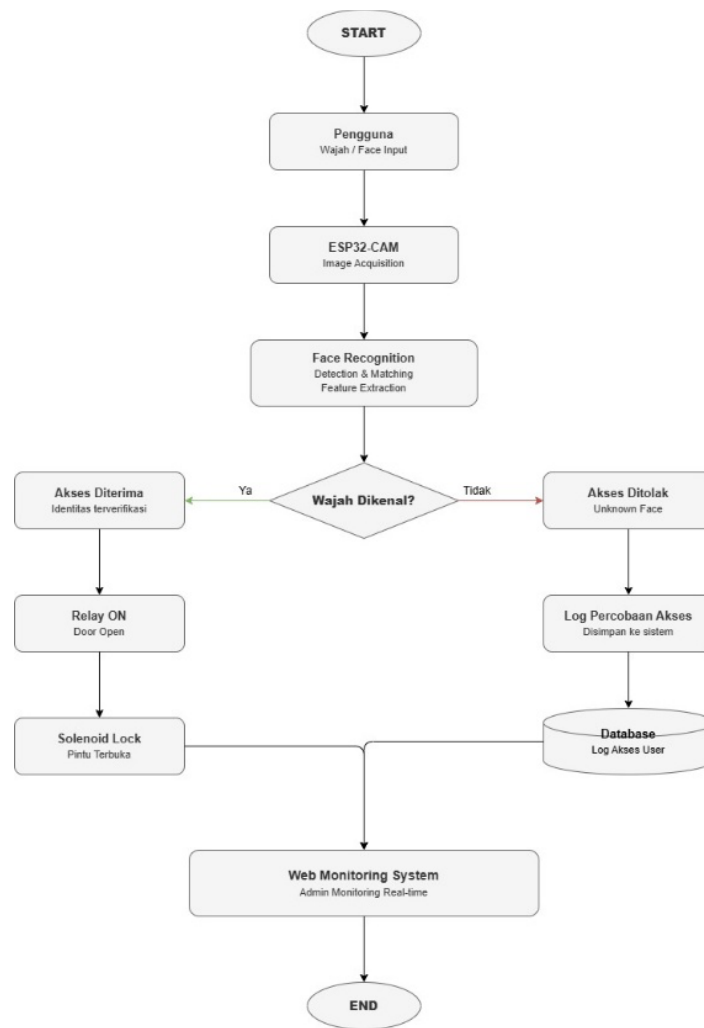
Tujuan utama penelitian ini adalah untuk mengembangkan dan menguji sistem pencatatan akses ruang server berbasis IoT dengan teknologi pengenalan wajah. Metode yang digunakan adalah metode *Research and Development* (R&D) dengan pendekatan prototipe. Tahapan penelitian meliputi: analisis kebutuhan, perancangan sistem, implementasi perangkat keras dan perangkat lunak, serta pengujian dan evaluasi hasil. Metode prototipe dipilih agar perancangan sistem dapat diuji secara bertahap dalam lingkungan nyata dan disesuaikan dengan kebutuhan operasional ruang server.

Metode penelitian yang digunakan meliputi observasi lapangan, studi pustaka, dan eksperimen terkontrol. Observasi dilakukan di ruang server BLSDM Komdigi Manado untuk mengidentifikasi pola akses, kondisi pintu, serta kebutuhan sistem pencatatan akses. Studi pustaka

dilakukan untuk merangkum pendekatan yang telah digunakan dalam penelitian sebelumnya, khususnya sistem akses berbasis IoT dan pengenalan wajah. Untuk mengevaluasi kinerja sistem, eksperimen dilakukan dalam skenario dengan pengguna terdaftar dan tidak terdaftar.

Pada tahap pengumpulan data wajah, setiap subjek yang terdaftar direkam sebanyak 50 citra per orang dari jarak sekitar 30 cm, dengan variasi sudut wajah frontal dan sedikit kemiringan untuk meningkatkan generalisasi model pengenalan wajah. Pengambilan citra dilakukan pada kondisi pencahayaan ruang yang relatif stabil untuk meminimalkan *noise* pada proses deteksi dan ekstraksi fitur wajah. Data wajah yang telah terkumpul kemudian disimpan sebagai *template* pada sistem untuk proses pencocokan saat verifikasi akses (Chen, 2023).

2.1. Arsitektur Sistem



Gambar 1. Arsitektur Sistem

Gambar 1 menunjukkan arsitektur sistem yang terdiri dari beberapa komponen utama, yaitu pengguna sebagai sumber input, modul ESP32-CAM sebagai perangkat akuisisi citra, modul pengenalan wajah sebagai unit pemrosesan, serta sistem kontrol akses yang terintegrasi dengan relay dan *solenoid door lock*. Proses dimulai ketika kamera menangkap citra wajah pengguna, kemudian data citra

diproses melalui tahapan deteksi wajah, ekstraksi fitur, dan pencocokan dengan basis data.

Apabila wajah dikenali, sistem akan mengaktifkan relay sehingga *solenoid door lock* membuka pintu, dan data akses akan dicatat ke dalam basis data. Sebaliknya, jika wajah tidak dikenali, sistem akan menolak akses dan tetap mencatat percobaan tersebut sebagai log keamanan. Seluruh data yang tersimpan dapat

dimonitor melalui sistem berbasis web secara *real-time* oleh administrator (Cesar et al., 2024).

2.2. Metode Pengenalan Wajah

Metode pengenalan wajah pada penelitian ini menggunakan pendekatan berbasis *Haar Cascade Classifier* untuk proses deteksi wajah yang dikombinasikan dengan teknik pencocokan citra sederhana untuk identifikasi pengguna. Pendekatan ini dipilih karena memiliki kebutuhan komputasi yang rendah serta mampu bekerja secara *real-time* pada perangkat *embedded* seperti ESP32-CAM, sehingga sesuai untuk implementasi sistem keamanan berbasis IoT (Win et al., 2021).

Pada tahap awal, sistem melakukan deteksi wajah dengan menggunakan algoritma Haar Cascade, yang didasarkan pada metode Viola-Jones. Metode ini memanfaatkan fitur mirip Haar dan teknik *integral image* untuk mempercepat proses deteksi objek dalam gambar. Penggunaan

pengklasifikasi bertingkat memungkinkan proses klasifikasi dilakukan secara bertahap, sehingga hanya area gambar yang berpotensi menjadi wajah yang diproses lebih lanjut. Pendekatan ini banyak digunakan dalam sistem deteksi wajah pada perangkat waktu nyata dengan sumber daya terbatas (Sutikno et al., 2024).

Setelah wajah berhasil dideteksi, sistem melakukan proses ekstraksi fitur dari citra wajah dalam bentuk representasi berbasis intensitas piksel *grayscale*. Pendekatan ini dipilih karena tidak memerlukan proses pelatihan model yang kompleks, sehingga lebih ringan dan sesuai untuk perangkat *embedded* seperti ESP32-CAM (Putra et al., 2021).

Proses identifikasi dilakukan dengan membandingkan citra wajah masukan dengan data wajah dalam basis data menggunakan metode *cosine similarity* (Sirait & Siddik, 2025). Persamaan *cosine similarity* dinyatakan sebagai Persamaan 1.

$$S = \frac{\vec{F}_i \cdot \vec{F}_d}{\|\vec{F}_i\| \times \|\vec{F}_d\|}$$

Persamaan 1. Cosine Similarity

di mana F_i merupakan vektor fitur wajah masukan dan F^d merupakan vektor fitur wajah dalam basis data. Jika nilai kemiripan melebihi ambang batas (*threshold*), maka wajah dianggap dikenali; jika tidak, maka akses ditolak. Pemilihan metode Haar Cascade didasarkan pada efisiensi komputasi dan kemampuannya untuk dijalankan secara *real-time*, meskipun memiliki keterbatasan terhadap variasi pencahayaan dan pose wajah (Andreas et al., 2019).

2.3. Implementasi Sistem

Implementasi sistem dilakukan dengan mengintegrasikan perangkat keras dan perangkat lunak dalam satu sistem keamanan berbasis IoT yang mampu melakukan pengenalan wajah serta pencatatan log akses secara *real-time*. Perangkat utama yang digunakan adalah ESP32-CAM sebagai modul akuisisi citra yang terhubung ke jaringan Wi-Fi untuk mengirimkan data ke server. Citra wajah yang ditangkap kemudian diproses pada server menggunakan algoritma Haar Cascade melalui pustaka OpenCV untuk mendeteksi wajah berdasarkan fitur *Haar-like* dan teknik *integral image*. Pendekatan ini

banyak digunakan pada sistem *embedded* karena efisiensi komputasinya serta kemampuannya dalam mendukung deteksi wajah secara *real-time* (Silalahi et al., 2024).

Setelah wajah berhasil dideteksi, sistem melakukan proses identifikasi dengan membandingkan citra wajah dengan data yang tersimpan dalam basis data. Jika wajah dikenali, sistem akan mengaktifkan perangkat output seperti relay untuk membuka akses, sedangkan jika tidak dikenali maka akses akan ditolak. Seluruh aktivitas akses dicatat dalam sistem log yang mencakup informasi waktu, status akses, serta citra wajah untuk keperluan monitoring dan audit keamanan. Integrasi antara deteksi wajah, kontrol akses, dan pencatatan log dalam satu sistem terpusat terbukti mampu meningkatkan efektivitas sistem keamanan berbasis IoT (Nur et al., 2024).

C. Hasil Penelitian dan Pembahasan

3.1. Hasil Implementasi Sistem

Sistem yang dikembangkan dalam penelitian ini telah berhasil diimplementasikan melalui integrasi komponen perangkat keras dan perangkat lunak menjadi satu sistem

terpadu. Perangkat keras utama terdiri dari modul ESP32-CAM untuk pengambilan gambar, relay untuk mengendalikan aktuator, dan *solenoid doorlock* untuk mekanisme penguncian pintu. Sementara itu, perangkat lunak dilengkapi dengan sistem pengenalan wajah berbasis OpenCV, basis data untuk penyimpanan data, serta antarmuka web untuk pemantauan.

Proses operasional sistem dimulai saat pengguna berdiri di depan pintu ruang server. Kamera pada ESP32-CAM merekam gambar wajah secara langsung dan mengirimkannya ke server melalui koneksi Wi-Fi. Setelah itu, sistem menjalankan deteksi wajah menggunakan algoritma Haar Cascade. Ketika wajah teridentifikasi, sistem mengekstrak fitur dan membandingkannya dengan data wajah di basis data menggunakan metode cosine similarity.

Jika hasil pencocokan menunjukkan tingkat kesamaan yang melebihi *threshold* yang ditetapkan, sistem mengenali pengguna sebagai pengguna terdaftar dan mengaktifkan relay untuk membuka kunci pintu. Di sisi lain, jika wajah tidak terdeteksi,

sistem menolak akses dan pintu tetap terkunci.

Selain mengatur akses, sistem juga secara otomatis merekam semua kegiatan ke dalam basis data log. Informasi yang direkam mencakup waktu akses, status akses (berhasil atau gagal), serta gambar wajah pengguna. Data ini dapat diakses secara langsung melalui antarmuka berbasis web oleh administrator untuk keperluan pemantauan dan audit keamanan.

3.2. Hasil Pengujian Sistem

Pengujian sistem dilakukan untuk mengevaluasi kinerja sistem dalam hal akurasi pengenalan wajah, waktu respon, serta kemampuan pencatatan log akses. Pengujian dilakukan dalam kondisi lingkungan yang menyerupai kondisi nyata operasional ruang server.

3.2.1. Pengujian Akurasi Pengenalan Wajah

Pengujian dilakukan terhadap 10 skenario pengguna dengan kondisi pencahayaan dan posisi yang bervariasi, masing-masing sebanyak 50 kali percobaan. Hasil pengujian ditunjukkan pada Tabel 1.

Tabel 1. Hasil Pengujian Akurasi Pengenalan Wajah

No	Status Pengguna	Jumlah Percobaan	Berhasil	Gagal	Akurasi (%)
1	Terdaftar	50	48	2	96%
2	Terdaftar	50	45	5	90%
3	Terdaftar	50	48	2	96%
4	Terdaftar	50	44	6	88%
5	Terdaftar	50	47	3	94%
6	Terdaftar	50	43	7	86%
7	Tidak Terdaftar	50	45	5	90%
8	Tidak Terdaftar	50	46	4	92%
9	Tidak Terdaftar	50	47	3	94%
10	Tidak Terdaftar	50	43	7	86%

Hasil pengujian menunjukkan bahwa sistem mampu mengenali wajah pengguna terdaftar dengan tingkat keberhasilan rata-rata sebesar 91%.

Pengujian waktu respon dilakukan untuk mengukur durasi yang dibutuhkan sistem mulai dari pengambilan citra hingga keputusan akses diberikan. Hasil pengujian ditunjukkan pada Tabel 2.

3.2.2. Pengujian Waktu Respon

Tabel 2. Hasil Pengujian Waktu Respon

No	Percobaan	Waktu Respon (detik)
1	1	1,5
2	2	1,8
3	3	1,7
4	4	2,0
5	5	1,6
6	6	1,9
7	7	1,8
8	8	1,7
9	9	2,1
10	10	1,6

Berdasarkan hasil pengujian, diperoleh waktu respon tercepat ± 1 detik, waktu respon terlama $\pm 2,5$ detik, dan rata-rata waktu respon $\pm 1,8$ detik.

Nilai tersebut mengindikasikan bahwa sistem mampu memberikan respons autentikasi yang cukup cepat untuk kebutuhan operasional ruang server.

3.2.3. Pengujian Sistem Pencatatan Log Akses

Sistem log mencatat seluruh aktivitas akses secara otomatis ke dalam basis data. Contoh data log akses ditunjukkan pada Tabel 3.

Tabel 3. Contoh Data Log Akses

No	Waktu	Nama User	Status Akses	Keterangan
1	2026-05-01 10:01:10	Chris	Berhasil	Wajah dikenali
2	2026-05-01 10:05:22	Unknown	Gagal	Tidak terdaftar
3	2026-05-01 10:10:45	Arsyad	Berhasil	Wajah dikenali
4	2026-05-01 10:15:30	Unknown	Gagal	Wajah tidak cocok
5	2026-05-02 10:20:11	Nita	Berhasil	Wajah dikenali

Sistem log ini memberikan nilai tambah dibandingkan sistem konvensional karena memungkinkan pelacakan aktivitas pengguna secara historis untuk keperluan audit keamanan.

3.3. Analisis dan Pembahasan

Berdasarkan hasil implementasi dan pengujian, sistem yang dikembangkan menunjukkan kinerja yang baik dalam memenuhi tujuan penelitian. Dari sisi deteksi wajah, penggunaan metode Haar Cascade terbukti mampu bekerja secara *real-time* dengan kebutuhan komputasi yang rendah, menjadikannya sesuai untuk perangkat *embedded* seperti ESP32-CAM. Namun, metode ini memiliki keterbatasan dalam menghadapi variasi kondisi lingkungan, terutama pencahayaan

rendah dan sudut wajah yang ekstrem.

Pada tahap identifikasi, metode *cosine similarity* memberikan hasil yang cukup baik untuk sistem dengan jumlah pengguna terbatas. Nilai *threshold* yang digunakan berperan penting dalam menentukan tingkat akurasi sistem. Penentuan *threshold* yang terlalu rendah dapat menyebabkan *false acceptance*, sedangkan yang terlalu tinggi dapat menyebabkan *false rejection*.

Integrasi sistem berbasis IoT memungkinkan seluruh komponen sistem saling terhubung dan bekerja secara otomatis. Kemampuan monitoring secara *real-time* melalui antarmuka web memberikan kemudahan bagi administrator dalam mengawasi aktivitas akses ruang server.

Dibandingkan sistem keamanan konvensional, sistem yang dikembangkan memiliki beberapa keunggulan, antara lain: (1) tidak memerlukan media fisik seperti kartu atau kunci; (2) menggunakan identitas biometrik yang sulit dipalsukan; (3) mampu mencatat aktivitas akses secara otomatis; dan (4) mendukung monitoring jarak jauh secara *real-time*.

Namun demikian, sistem ini masih memiliki beberapa keterbatasan, yaitu: (1) sensitif terhadap perubahan kondisi pencahayaan; (2) kinerja menurun pada sudut wajah yang ekstrem; (3) bergantung pada koneksi jaringan; dan (4) skalabilitas masih terbatas untuk jumlah pengguna yang besar.

Secara keseluruhan, sistem yang dikembangkan berhasil meningkatkan aspek keamanan ruang server melalui integrasi teknologi IoT dan pengenalan wajah, sekaligus berfungsi sebagai sistem pencatatan dan monitoring yang mendukung pengelolaan keamanan secara lebih efektif dan efisien.

D. Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian, dapat disimpulkan bahwa sistem log akses

ruang server berbasis IoT menggunakan teknologi pengenalan wajah berhasil dikembangkan dan mampu berfungsi dengan baik sesuai tujuan penelitian. Sistem ini mampu melakukan proses autentikasi pengguna melalui deteksi dan identifikasi wajah menggunakan metode Haar Cascade, serta mengontrol akses pintu secara otomatis melalui integrasi dengan perangkat relay dan *solenoid door lock*. Selain itu, sistem dapat mencatat seluruh aktivitas akses secara *real-time* ke dalam basis data, sehingga mendukung proses monitoring dan audit keamanan secara terpusat.

Hasil pengujian menunjukkan bahwa sistem memiliki rata-rata akurasi sebesar 91% dengan waktu respon sekitar 1–2 detik, yang mengindikasikan kinerja sistem cukup baik dalam kondisi operasional tertentu. Dengan demikian, sistem yang dikembangkan mampu meningkatkan keamanan ruang server dibandingkan metode konvensional, serta memberikan solusi yang lebih efektif, otomatis, dan terintegrasi dalam pengelolaan akses berbasis teknologi IoT.

DAFTAR PUSTAKA

- Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door security system for home monitoring based on ESP32. *Procedia Computer Science*, 157, 673–682. <https://doi.org/10.1016/j.procs.2019.08.218>
- Ariansyah, W., Ilham, D. N., Khairuman, & Candra, R. A. (2021). Opening doors using Internet of Things (IoT) based face recognition. *Brilliance: Research of Artificial Intelligence*, 1(2). <https://doi.org/10.47709/brilliance.v1i2.1095>
- Bolimera, R., Karthick, S., Karthikeya, S., Kumar, V. A., & Siddhartha, R. S. (2025). ESP32-CAM face detection automatic door lock. *International Journal of Data Science, IoT and Management Systems*, 4(4(2)), 107–111. [https://doi.org/10.64751/ijdim.2025.v4.n4\(2\).pp107-111](https://doi.org/10.64751/ijdim.2025.v4.n4(2).pp107-111)
- Cesar, F., Jahuira, A., Salas, D. C., & Suarez, J. T. (2024). IoT-based smart glasses assistance system with facial recognition. *International Journal of Electrical and Electronics Engineering*, 11(12), 287–294. <https://doi.org/10.14445/23488379/IJEEE-V11I12P126>
- Chen, Z. (2023). A study on the CNN-based face recognition across various facial angles. *Applied and Computational Engineering*, 35, 265–271. <https://doi.org/10.54254/2755-2721/35/20230404>
- Harun, N. B., & Zainal, M. S. B. (n.d.). Development of face recognition smart door lock system using ESP32-CAM and Telegram application as media control and monitoring. *Progress in Engineering Application and Technology*, 4(2), 35–48. <https://publisher.uthm.edu.my/periodicals/index.php/peat/article/view/10586>
- Khadafi, M., Pardede, A. M. H., & Sembiring, H. (2024). Design of a guest face detection tool using ESP32-CAM based on Internet of Things (IoT). *Journal of Artificial Intelligence Engineering and Applications*, 4(1), 124–130. <https://doi.org/10.59934/jaiea.v4i1.578>
- Koteswaramma, N., Ananthula, N., Raju, N., Rajeshwari, R., & Mounika, B. (2022). IoT based door access control system using ESP32cam. [Conference Proceedings].
- Nannung, J., Miru, A. S., Muliadi, & Gunawan. (2025). Development of an IoT-based home security system prototype using multisensors and ESP32-CAM. *Journal of Embedded Systems, Security and Intelligent Systems*, 6(2), 168–177. <https://doi.org/10.59562/jessi.v6i2.8456>
- Nur, M., Sulistyowati, H. S., Nurrohman, A., & Saleh, U. B. (2024). Penerapan face recognition untuk model smart security. *Jurnal Informatika dan Sistem Informasi*, 2(1), 152–166.
- Obasi, C., & Tahir, K. M. (2025). A real-time smart door access control system using Haar Cascade Classifier and embedded vision. *International Journal of Data Informatics and Intelligent Computing*, 4(3), 14–22. <https://doi.org/10.59461/ijdiic.v4i3.208>

- Putra, A., Susilo, M., Darlis, D., & Nurmantris, D. A. (2021). Pengenalan wajah berbasis ESP32-CAM untuk sistem kunci sepeda motor. *Jurnal Teknik Elektro*, 8(2), 1091–1103.
- Sirait, A., & Siddik, M. (2025). Implementasi algoritma cosine similarity dalam pengenalan. *JOISIE (Journal of Information Systems and Informatics Engineering)*, 9(1), 1–17. <https://doi.org/10.35145/joisie.v9i1.4772>
- Silalahi, L. M., Simanjuntak, I. U. V., Rizki, R. B., & Fajri, N. (2024). Penerapan metode Haar Cascade terhadap objek botol menggunakan ESP32-Cam. *Jurnal Pendidikan dan Teknologi Indonesia*, 4(6), 269–276. <https://doi.org/10.52436/1.jpti.457>
- Sutikno, T., Ainur, M., Ubaidillah, F., Arsadiando, W., & Purnama, H. S. (2024). Fingerprint based smart door lock system using Arduino and smartphone application. *Computer Science and Information Technologies*, 5(1), 91–98. <https://doi.org/10.11591/csit.v5i1.pp91-98>
- Syafutra, H., Aziz, T. M. N., Novianty, I., Irmansyah, I., Chusnu, M., & Prayoga, D. (2024). Implementasi sistem keamanan pintu otomatis berbasis face recognition di Proactive Robotic: Integrasi ESP32-Cam dan Telegram. *Jurnal Riset Fisika Indonesia*, 4(2), 65–74. <https://doi.org/10.33019/jrfi.v4i2.5380>
- Win, H. P. P., Khine, P. T. T., & Tun, K. N. N. (2021). Face recognition system based on convolution neural networks. *International Journal of Image, Graphics and Signal Processing*, 13(6), 23–29. <https://doi.org/10.5815/ijigsp.2021.06.03>