Jurnal Infortech
Volume 7 No. 2 Desember 2025
E-ISSN: 2715-8160

Sistem Keamanan Rumah Berbasis IoT dengan Pengenalan Wajah Manusia dan Hewan Peliharaan Secara *Real-Time*

Fahrizal[1], Yumi Novita Dewi[2*], Taransa Agasya Tutupoly[3]

[1]Sistem Informasi, Universitas Bina Sarana Informatika, Jakarta, Indonesia.
[2*,3]Informatika, Universitas Bina Sarana Informatika, Jakarta, Indonesia.
e-mail: [1]fahrizal@bsi.ac.id, [2*]yumi.ymd@bsi.ac.id, [3]taransa.tly@bsi.ac.id

Diterima	Direvisi	Disetujui
19-11-2025	22-11-2025	22-12-2025

Abstrak – Sistem keamanan rumah konvensional memiliki keterbatasan dari segi efisiensi dan keamanan karena masih bergantung pada metode autentikasi manual seperti kunci dan kartu akses, yang rentan terhadap penyalahgunaan serta duplikasi tanpa izin. Untuk mengatasi keterbatasan tersebut, penelitian ini mengusulkan sistem keamanan rumah berbasis biometrik yang mengintegrasikan *Machine Learning* (ML) dan *Internet of Things* (IoT) untuk pengenalan wajah dan klasifikasi hewan peliharaan secara *real-time*. Sistem yang diusulkan menerapkan arsitektur *client–server* ini, dimana proses pengenalan yang membutuhkan komputasi tinggi dijalankan pada server Ubuntu menggunakan Python, OpenCV, dan TensorFlow. Metode Haar Cascade digunakan untuk mendeteksi wajah manusia, sedangkan *Convolutional Neural Network* (CNN) diterapkan untuk mengklasifikasikan hewan peliharaan, sehingga sistem mampu membedakan pengguna yang berwenang, individu yang tidak berwenang, serta hewan peliharaan di dalam rumah. Hasil autentikasi dikirimkan melalui protokol HTTP pada jaringan WiFi lokal ke mikrokontroler ESP32, yang selanjutnya mengendalikan mekanisme kunci pintu elektronik. Hasil pengujian menunjukkan bahwa sistem mencapai akurasi pengenalan wajah sebesar 90% dan akurasi klasifikasi hewan peliharaan sebesar 98%, dengan waktu respons rata-rata berkisar antara 1,5 hingga 1,8 detik pada kondisi jaringan yang stabil. Hasil ini membuktikan bahwa sistem yang diusulkan bersifat andal, responsif, tanpa kontak, serta sesuai untuk diterapkan pada aplikasi keamanan smart home.

Kata Kunci: Pengenalan Biometrik, Visi Komputer, ESP32, Internet of Things (IoT), Machine Learning.

Abstract – *Conventional home security systems are limited in efficiency and safety due to their dependence on manual authentication methods such as keys and access cards, which are vulnerable to misuse and unauthorized duplication. To overcome these limitations, this study presents a biometric-based home security system that integrates Machine Learning (ML) and the Internet of Things (IoT) for real-time face recognition and pet classification. The proposed system adopts a client–server architecture, where computationally intensive recognition tasks are executed on an Ubuntu server using Python, OpenCV, and TensorFlow. Haar Cascade classifiers are utilized for human face detection, while a Convolutional Neural Network (CNN) is implemented to classify pets, enabling the system to distinguish between authorized users, unauthorized individuals, and household animals. Authentication results are transmitted via the HTTP protocol over a local WiFi network to an ESP32 microcontroller, which controls an electronic door lock mechanism. Experimental evaluations indicate that the system achieves a face recognition accuracy of 90% and a pet classification accuracy of 98%, with an average response time ranging from 1.5 to 1.8 seconds under stable network conditions. These results demonstrate that the proposed system is reliable, responsive, contactless, and well-suited for smart home security applications.*

Keywords: Biometric Recognition, Computer Vision, ESP32, Internet of Things (IoT), Machine Learning.

PENDAHULUAN

Kemajuan teknologi digital telah mendorong terjadinya transformasi signifikan pada sistem keamanan rumah, seiring dengan meningkatnya kebutuhan akan solusi yang aman, praktis, dan terintegrasi. Metode keamanan konvensional, seperti kunci mekanis, kartu magnetik, dan *Personal Identification Number* (PIN), dinilai kurang efektif karena rentan terhadap peretasan dan penyalahgunaan (Al Farid & Firmansyah, 2022). Selain itu, metode tersebut masih bergantung pada interaksi manual, sehingga kurang efisien dalam memenuhi tuntutan masyarakat modern yang memerlukan tingkat otomatisasi dan konektivitas yang tinggi (Vardakis et al., 2024).

Teknologi biometrik hadir sebagai alternatif autentikasi yang lebih andal dengan memanfaatkan

karakteristik unik individu yang sulit untuk dipalsukan. Diantara berbagai metode biometrik, pengenalan wajah semakin banyak digunakan karena bersifat tanpa kontak, mudah diimplementasikan, serta kompatibel dengan perangkat kamera standar (Tribuana et al., 2024). Penelitian terdahulu menunjukkan bahwa penerapan *Convolutional Neural Networks* (CNN) mampu meningkatkan akurasi pengenalan wajah pada sistem kontrol akses pintu otomatis (Goodfellow et al., 2016; Lee & Choi, 2023). Selain itu, CNN juga terbukti efektif dalam mengklasifikasikan objek lain, termasuk hewan peliharaan, sehingga memungkinkan pengembangan sistem keamanan rumah yang lebih adaptif (Fahrizal, 2020).

Meskipun demikian, sebagian besar penelitian sebelumnya masih berfokus pada pengujian berbasis perangkat lunak atau simulasi tanpa integrasi menyeluruh dengan perangkat fisik (Lin & Hsu, 2023). Keterbatasan ini menjadi perhatian penting karena sistem keamanan biometrik yang ideal tidak hanya harus mampu melakukan pengenalan objek, tetapi juga mengeksekusi tindakan fisik, seperti membuka kunci pintu atau mengaktifkan sistem alarm. Selain itu, beberapa pendekatan yang ada memerlukan sumber daya komputasi yang tinggi, sehingga kurang sesuai untuk diterapkan pada lingkungan rumah tangga dengan keterbatasan perangkat IoT (Zhao et al., 2023).

Sebagai upaya untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan sistem keamanan rumah berbasis biometrik yang mengintegrasikan *Machine Learning* (ML) dan *Internet of Things* (IoT) dalam suatu arsitektur yang sederhana dan efisien. Sistem ini dirancang untuk melakukan pengenalan wajah manusia dan hewan peliharaan secara waktu nyata (*real-time*) menggunakan teknik visi komputer, serta mengendalikan kunci pintu elektronik melalui mikrokontroler ESP32 yang terhubung melalui jaringan WiFi lokal. Pendekatan ini selaras dengan konsep *Artificial Intelligence of Things* (AIoT), yang mengombinasikan kecerdasan buatan dengan perangkat IoT guna menghasilkan sistem keamanan yang adaptif dan responsif (Garg et al., 2022).

METODE PENELITIAN

a. Arsitektur Sistem

Penelitian ini menerapkan arsitektur *client–server* yang memisahkan proses analisis citra dari pengendalian perangkat fisik. Sistem terdiri atas dua komponen utama, yaitu unit pengenalan biometrik berbasis komputer yang berjalan pada sistem operasi Ubuntu dan unit *Internet of Things* (IoT) yang berbasis mikrokontroler ESP32.

Unit pengenalan biometrik berfungsi sebagai server pemrosesan yang melakukan akuisisi citra secara waktu nyata (real-time) melalui kamera IP. Deteksi wajah manusia dilakukan menggunakan algoritma *Haar Cascade* karena kecepatan pemrosesannya yang tinggi dan sesuai untuk aplikasi real-time, sedangkan klasifikasi hewan peliharaan dilakukan menggunakan model *Convolutional Neural Network* (CNN) untuk mengekstraksi fitur visual yang lebih kompleks. Hasil identifikasi kemudian dikirimkan ke unit IoT melalui protokol HTTP menggunakan jaringan WiFi lokal.

Mikrokontroler ESP32 berperan sebagai node aktuator yang menerima perintah dari server dan mengendalikan modul relay untuk mengunci atau membuka kunci pintu elektronik. Arsitektur ini dirancang secara modular dan berskala, sehingga memungkinkan pengembangan sistem lebih lanjut tanpa memerlukan perubahan struktur yang signifikan. Hubungan antar komponen sistem ditunjukkan pada Gambar 1.

Sumber: Hasil Rangcangan Penulis

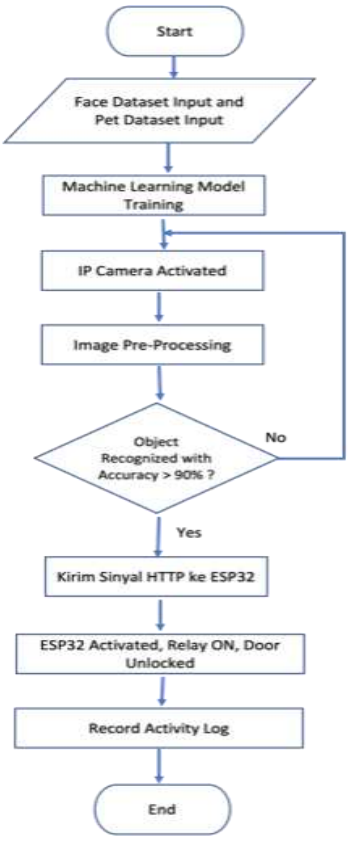
Gambar 1. Diagram Arsitektur Sistem

Pendekatan ini sejalan dengan konsep *Artificial Intelligence of Things* (AIoT), yaitu integrasi kecerdasan buatan dengan jaringan perangkat cerdas untuk menghasilkan sistem yang adaptif, efisien, dan aman dalam lingkungan rumah pintar (Garg et al., 2022).

b. Alur Kerja Sistem

Alur kerja sistem diawali dengan proses akuisisi citra oleh kamera IP yang terhubung ke server. Citra yang diperoleh selanjutnya diproses untuk mendeteksi keberadaan wajah manusia atau hewan peliharaan. Apabila objek yang teridentifikasi sesuai dengan data yang telah terdaftar dan memenuhi ambang batas kepercayaan (*confidence threshold*), sistem akan mengirimkan perintah ke mikrokontroler ESP32 melalui jaringan WiFi lokal.

Mikrokontroler ESP32 kemudian mengaktifkan modul relay untuk membuka kunci pintu elektronik dalam durasi waktu tertentu sebelum kembali ke kondisi awal. Alur kerja sistem ditunjukkan pada Gambar 2.



Sumber: Hasil Rangcangan Penulis

Gambar 2. Diagram Alir Sistem

c. Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh komponen perangkat lunak dan perangkat keras berfungsi sesuai dengan perancangan serta mencapai kinerja yang diharapkan. Pengujian difokuskan pada tiga aspek utama, yaitu pengujian fungsional, pengujian akurasi model pembelajaran mesin, dan pengujian waktu tanggap sistem *Internet of Things* (IoT).

d. Pengujian Fungsional

Pengujian fungsional dilakukan dengan menggunakan metode pengujian kotak hitam (*black box testing*) untuk mengevaluasi fungsi sistem berdasarkan hubungan antara masukan dan keluaran tanpa meninjau kode sumber. Skenario pengujian meliputi pengenalan wajah manusia yang telah terdaftar, pengenalan hewan peliharaan yang telah terdaftar, serta penolakan akses terhadap objek yang tidak dikenali. Pendekatan ini mengacu pada praktik evaluasi sistem keamanan berbasis *Internet of Things* (IoT) (Al Farid & Firmansyah, 2022).

e. Pengujian Akurasi Model Pembelajaran Mesin

Pengujian ini bertujuan untuk menilai kemampuan model dalam mengenali dan mengklasifikasikan objek biometrik secara akurat. Evaluasi dilakukan menggunakan kumpulan data wajah manusia dan hewan peliharaan dengan variasi sudut pengambilan citra serta kondisi pencahayaan. Kinerja model diukur menggunakan metrik akurasi dan matriks kebingungan (*confusion matrix*) untuk menilai kemampuan generalisasi model terhadap data baru, (Goodfellow et al., 2016).

f. Pengujian Waktu Tanggap Sistem *Internet of Things*

Pengujian waktu tanggap bertujuan untuk mengukur kecepatan sistem dalam mengeksekusi perintah, mulai dari proses identifikasi hingga tindakan fisik pada perangkat. Waktu tanggap dihitung berdasarkan selisih penanda waktu (*timestamp*) antara proses identifikasi pada peladen dan aktivasi modul relai pada mikrokontroler ESP32. Hasil pengujian menunjukkan bahwa sistem memiliki latensi yang rendah dengan rata-rata waktu tanggap kurang dari dua detik. Temuan ini sejalan dengan kinerja sistem *Artificial Intelligence of Things* (AIoT) berbasis ESP32 (Vardakis et al., 2024).

HASIL DAN PEMBAHASAN

Penelitian ini menyajikan sebuah sistem keamanan rumah yang mengintegrasikan pembelajaran mesin (*Machine Learning*) dan *Internet of Things* (IoT) untuk mengenali wajah manusia dan hewan peliharaan secara otomatis sebagai dasar pengendalian akses pintu. Sistem ini terdiri atas dua komponen utama, yaitu peladen berbasis Ubuntu sebagai unit pemrosesan data dan mikrokontroler ESP32 sebagai pengendali perangkat fisik. Kamera IP digunakan untuk menangkap citra, sedangkan mikrokontroler ESP32 mengoperasikan modul relai untuk mengunci atau membuka kunci pintu elektronik.

Perangkat lunak sistem dikembangkan menggunakan bahasa pemrograman Python dengan pustaka *OpenCV* dan *TensorFlow*. Deteksi wajah dilakukan menggunakan algoritma *Haar Cascade* karena kecepatan pemrosesannya yang tinggi, sedangkan klasifikasi hewan peliharaan menggunakan model *Convolutional Neural Network* (CNN) untuk mengekstraksi fitur visual yang lebih kompleks.

Hasil identifikasi dikirimkan ke mikrokontroler ESP32 melalui protokol HTTP. Apabila objek yang terdaftar terdeteksi dengan tingkat kepercayaan di atas 90%, modul relai akan diaktifkan selama tiga detik untuk membuka kunci pintu, kemudian secara otomatis kembali ke kondisi awal.

Implementasi perangkat keras menunjukkan bahwa sistem dapat beroperasi secara waktu nyata dan stabil pada jaringan WiFi lokal dengan frekuensi 2,4 GHz, dengan keterlambatan komunikasi yang minimal. Pengujian fungsional menggunakan metode pengujian kotak hitam (*black box testing*) menunjukkan bahwa seluruh fungsi sistem berjalan sesuai dengan perancangan. Kamera IP mampu menangkap citra dengan baik pada berbagai kondisi pencahayaan, pintu terbuka secara otomatis untuk objek yang terdaftar, serta akses ditolak untuk objek

yang tidak dikenali. Hasil pengujian fungsional dirangkum pada Tabel 1.

Tabel 1. Hasil Pengujian Fungsional

No	*Test Scenario*	*Input*	*Expected Output*	*Actual Result*	*Status*
1	*Registered user face*	*Face image*	*Door opens automatically*	*Door opened as expected*	*Pass*
2	*Registered pet*	*Pet image*	*Door opens automatically*	*Door opened as expected*	*Pass*
3	*Unregistered object*	*Random image*	*Door remains locked*	*No action on relay*	*Pass*
4	*WiFi disconnected*	*Face image*	*Error notification & log*	*Notification displayed, system on standby*	*Pass*
5	*Partially blocked camera*	*Face image*	*Not detected*	*No action*	*Pass*

Sumber: Hasil Rangcangan Penulis

Pengujian akurasi sistem dilakukan menggunakan 200 citra wajah manusia dan 200 citra hewan peliharaan dengan variasi kondisi pencahayaan dan jarak. Hasil pengujian menunjukkan bahwa algoritma Haar Cascade mencapai tingkat akurasi sebesar 90% dalam pengenalan wajah manusia, sedangkan model CNN mencapai akurasi sebesar 98% dalam pengenalan hewan peliharaan. Hasil pengujian akurasi model disajikan pada Tabel 2.

Tabel 2. Hasil Pengujian Akurasi Model

Object Type	*Algorithm*	*Test Dataset*	*Correct Detection*	*Accuracy (%)*
Human face	*Haar Cascade*	*200*	*180*	*90%*
Pet (Cat/Dog)	*CNN*	*200*	*196*	*98%*

Sumber: Hasil Rangcangan Penulis

Selain itu, pengujian waktu tanggap dilakukan untuk mengevaluasi kinerja sistem secara keseluruhan. Pada kondisi jaringan yang stabil, waktu tanggap rata-rata dari proses deteksi hingga aktivasi modul relai berada pada rentang 1,5 hingga 1,8 detik. Pada kondisi jaringan yang mengalami gangguan atau ketika jarak perangkat melebihi 10 meter dari perute (*router*), waktu tanggap meningkat hingga sekitar 2,1 detik, namun sistem tetap beroperasi secara andal. Ringkasan hasil pengujian waktu tanggap dan kestabilan sistem ditampilkan pada Tabel 3.

Tabel 3. Waktu Tanggap dan Kestabilan Sistem IoT

Network Condition	*Avg. Response Time (s)*	*Variation*	*Stability (%)*	*Notes*
Stable WiFi (2.4GHz)	*1.52*	*±0.10*	*100*	*Very stable*
WiFi with interference	*1.87*	*±0.25*	*95*	*Slight delay*
Distance >10m from router	*2.14*	*±0.31*	*91*	*Slower response*
Mobile hotspot mode	*1.74*	*±0.19*	*96*	*Fairly stable*

Sumber: Hasil Rangcangan Penulis

Sistem ini memenuhi tiga indikator kinerja utama, yaitu tingkat akurasi pengenalan yang tinggi, waktu tanggap yang mendekati waktu nyata, serta komunikasi yang stabil. Kinerja sistem dipengaruhi oleh kondisi pencahayaan dan jarak kamera; pencahayaan rendah atau jarak lebih dari tiga meter dapat menurunkan tingkat kepercayaan model akibat berkurangnya detail citra. Stabilitas jaringan juga memengaruhi pengoperasian sistem; apabila koneksi WiFi terputus, sistem tidak akan mengaktifkan pintu dan akan menampilkan pesan kesalahan, kemudian kembali berfungsi normal setelah koneksi dipulihkan. Hal ini menunjukkan bahwa sistem memiliki toleransi kesalahan dan mekanisme pengamanan (*fail-safe*) yang sesuai untuk penggunaan di lingkungan rumah tangga.

Secara keseluruhan, sistem yang dikembangkan menunjukkan bahwa integrasi pembelajaran mesin dengan *Internet of Things* mampu meningkatkan tingkat keamanan rumah secara signifikan. Sistem ini beroperasi secara akurat, memiliki waktu respons yang cepat, mudah diimplementasikan, serta berpotensi untuk dikembangkan lebih lanjut sebagai solusi keamanan rumah pintar yang efisien dan ekonomis.

KESIMPULAN

Penelitian ini berhasil mengembangkan sebuah sistem keamanan rumah yang mengintegrasikan pembelajaran mesin (*Machine Learning*) dan *Internet of Things* (IoT), yang mampu mengenali wajah manusia dan hewan peliharaan secara otomatis untuk mengendalikan akses pintu. Sistem ini mengombinasikan algoritma Haar Cascade, *Convolutional Neural Network* (CNN), dan mikrokontroler ESP32, serta beroperasi secara waktu nyata tanpa bergantung pada layanan komputasi awan (*cloud*). Sistem mencapai tingkat akurasi sebesar 90% untuk pengenalan wajah manusia dan 98% untuk pengenalan hewan peliharaan, dengan waktu tanggap berkisar antara 1,5 hingga 1,8 detik. Hasil pengujian menunjukkan bahwa sistem memiliki kestabilan yang baik, mampu menolak akses terhadap objek yang tidak dikenali, serta menawarkan solusi yang efisien dan andal untuk penerapan pada aplikasi rumah pintar.

REFERENSI

Tribuana, D., Aditya, R., & Nugraha, H. (2024). *Face recognition for smart door security access using convolutional neural network*. TELKOMNIKA Telecommunication Computing Electronics and Control, 22(3), 1098–1106. https://doi.org/10.12928/telkomnika.v22i3.34567

Al Farid, M. I., & Firmansyah, B. (2022). *Rancang bangun keamanan rumah menggunakan sensor wajah berbasis IoT*. Jurnal Teknologi Informasi dan Komputer (JUNIF), 4(2), 55–63. https://doi.org/10.33330/junif.v4i2.1783Han, J., & Kamber, M. (2006). *Data Mining: Concepts and Techniques*. *Soft Computing* (Vol. 54). https://doi.org/10.1007/978-3-642-19721-5

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Fahrizal, F. (2021). *Face recognition security based on Ubuntu using Python*. Jurnal Informatika Komputer dan Aplikasi (JIKA), 6(2), 45–51. https://doi.org/10.33330/jika.v6i2.1287

Lin, J., & Hsu, C. (2023). *AIoT-based real-time human detection and access control system*. Sensors, 23(4), 2191. https://doi.org/10.3390/s23042191

Zhao, L., Wang, J., & Liu, Y. (2023). *Low-latency CNN for real-time object detection in embedded IoT systems*. IEEE Access, 11, 45291–45303. https://doi.org/10.1109/ACCESS.2023.3265812

Nguyen, T., & Kim, J. (2022). *Hybrid deep learning for smart surveillance and facial authentication in IoT-based homes*. Applied Sciences, 12(21), 11102. https://doi.org/10.3390/app122111102

Lee, C. H., & Choi, H. (2023). *Development of a smart door lock system integrated with CNN-based face recognition*. Journal of Ambient Intelligence and Humanized Computing, 14(5), 6239–6251. https://doi.org/10.1007/s12652-022-04359-7

Ryu, S., & Kang, D. (2024). *Implementation of CNN-based image recognition system on ESP32 for IoT applications*. IEEE Sensors Journal, 24(3), 1597–1605. https://doi.org/10.1109/JSEN.2023.3340256

Nurhadi, M., & Setiawan, R. (2023). *Integrasi ESP32 dan Python untuk kontrol otomatis rumah cerdas berbasis jaringan lokal*. Jurnal Teknologi dan Sistem Komputer, 11(1), 65–73. https://doi.org/10.14710/jtsiskom.11.1.65-73

Park, S., & Lee, Y. (2024). *YOLOv8 and MobileNetV3 comparison for efficient embedded vision systems*. IEEE Access, 12, 77718–77729. https://doi.org/10.1109/ACCESS.2024.3411569

O'Reilly, A. (2021). *Practical Python for Machine Learning and Computer Vision*. O'Reilly Media. ISBN: 9781492074946