Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/index
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893

Analisis Kinerja *Smart Door Hybrid Haar Cascade* dan *ArcFace* pada *Raspberry*

DOI: http://dx.doi.org/10.35889/jutisi.v15i2.3537

Gautama Wijaya[1*], Stefanus Eko Prasetyo[2], Haeruddin[3], Kevin[4]
Teknologi Informasi, Universitas International Batam, Batam, Indonesia
*e-mail *Corresponding Author*: gautama.wijaya@uib.ac.id

Abstract

Implementing biometric security systems on deep learning devices faces a major challenge in balancing identity verification accuracy with computational resource efficiency. This study presents a performance analysis of a Raspberry Pi 5-based Smartdoor system integrating the detection speed of Haar Cascade with the recognition accuracy of ArcFace. System performance was evaluated based on RAM usage, CPU load, FPS stability, and access Success Rate parameters. Empirical evaluation results indicate that integrating Deep learning ArcFace increased RAM usage by 33.7% and CPU load from 33% to 53%. However, due to the processing capacity of the Raspberry Pi 5, the system maintained stable real-time performance with an average of 18.3 FPS. In terms of security, the Hybrid method proved superior with an access success rate of 73.7%, surpassing the conventional Haar Cascade method which only reached 68.4%. This study concludes that the Hybrid method is a viable solution for home security systems, where the increased computational load is justified by a significant improvement in identity verification reliability.

Keyword: *Raspberry Pi 5; Smartdoor; Haar Cascade; ArcFace; Computational Performance.*

Abstrak

Implementasi sistem keamanan biometrik pada perangkat *deep learning* menghadapi tantangan utama dalam menyeimbangkan akurasi verifikasi dengan efisiensi sumber daya. Penelitian ini menyajikan analisis kinerja sistem *Smartdoor* berbasis Raspberry Pi 5 yang mengintegrasikan kecepatan deteksi *Haar Cascade* dengan akurasi pengenalan wajah *ArcFace*. Kinerja sistem dievaluasi berdasarkan parameter penggunaan RAM, beban CPU, stabilitas FPS, dan tingkat keberhasilan akses. Hasil evaluasi empiris menunjukkan bahwa integrasi *Deep learning ArcFace* meningkatkan penggunaan RAM sebesar 33,7% dan beban CPU dari 33% menjadi 53%. Namun, berkat kapasitas pemrosesan Raspberry Pi 5, sistem mampu mempertahankan stabilitas kinerja *real-time* dengan rata-rata 18,3 FPS. Dari segi keamanan, metode *Hybrid* terbukti lebih unggul dengan akurasi pengenalan wajah sebesar 73,7%, melampaui metode konvensional *Haar Cascade* yang hanya mencapai 68,4%. Penelitian ini menyimpulkan bahwa metode *Hybrid* merupakan solusi yang layak untuk sistem keamanan rumah, di mana peningkatan beban komputasi terbayar dengan peningkatan reliabilitas verifikasi identitas yang signifikan.

Kata kunci: *Raspberry Pi 5; Pintu Pintar; Haar Cascade; ArcFace; Kinerja Komputasi.*

1. Pendahuluan

Perkembangan *Internet of Things* (IoT) telah mendorong transformasi sistem keamanan rumah menuju konsep Smart Home berbasis autentikasi digital. Sistem keamanan modern tidak lagi hanya dituntut mampu mendeteksi keberadaan objek, tetapi juga harus mampu melakukan verifikasi identitas secara presisi dan *real-time*. Penelitian oleh Wijaya dan Yulianto [1] menunjukkan bahwa sistem *Smartdoor* berbasis RFID mampu meningkatkan kontrol akses, namun masih memiliki celah keamanan karena token fisik dapat hilang, tertinggal, atau digandakan. Oleh karena itu, teknologi biometrik seperti pengenalan wajah (*face recognition*) menjadi solusi yang lebih aman karena melekat langsung pada identitas biologis pengguna[2].

Implementasi pengenalan wajah pada perangkat *deep learning* menghadapi keterbatasan sumber daya komputasi. Metode konvensional seperti *Haar Cascade* telah lama dikenal efisien dan cepat untuk deteksi wajah secara *real-time* [3], [4]. Mccullagh [5]. menegaskan bahwa *Haar Cascade* sangat efektif untuk *face detection*, namun tidak mampu melakukan verifikasi identitas karena tidak melakukan ekstraksi fitur mendalam. Suradi et al. [6] juga menunjukkan bahwa meskipun *Haar Cascade* unggul dalam kecepatan inferensi, akurasinya menurun dalam kondisi variasi pencahayaan dan jumlah subjek yang meningkat. Saragih [7] membuktikan bahwa metode ini ringan dijalankan pada Python, tetapi tetap memiliki keterbatasan pada aspek pengenalan wajah.

Sebaliknya, pendekatan *Deep learning* modern menawarkan peningkatan signifikan dalam akurasi. Sim dan Yulianto[8] menunjukkan bahwa model deteksi berbasis *Deep learning* seperti YOLOv5 dan YOLOv8 mampu meningkatkan presisi dan F1-score secara signifikan. Dalam konteks pengenalan wajah, Sari dan Hendrik [9]. membuktikan bahwa *ArcFace* unggul dibanding CNN dan FaceNet melalui mekanisme *Additive Angular Margin Loss*. Temuan tersebut diperkuat oleh Nurlita et al. [10] yang menunjukkan bahwa *ArcFace* lebih tangguh dalam menghadapi variasi pose wajah dibanding Dlib. Namun demikian, Dang [11]dan Kishore et al. [12] menyatakan bahwa model *Deep learning* kompleks menuntut beban komputasi tinggi yang berisiko menurunkan stabilitas FPS pada perangkat *deep learning*.

Beberapa penelitian telah mencoba mengatasi trade-off antara efisiensi dan akurasi melalui pendekatan hybrid. Alfan et al.[13] serta Ramadini dan Haryatmi [14] menggabungkan *Haar Cascade* dengan LBPH untuk sistem berbasis *Raspberry Pi* generasi lama. Meskipun ringan dan efisien, metode statistik seperti LBPH dinilai belum memenuhi standar keamanan biometrik modern yang membutuhkan presisi tinggi. Abdullahu dan Wache [15] mengusulkan arsitektur hybrid berbasis VGG16 dan SVM untuk aplikasi IoT, namun kompleksitas parameter model tersebut cukup besar sehingga berpotensi membebani *edge device*.

Meskipun berbagai pendekatan telah dikembangkan, belum terdapat penelitian yang secara komprehensif menguji integrasi detektor ultra-cepat *Haar Cascade* dengan pengenal berbasis *Deep learning ArcFace* pada *platform Raspberry Pi* 5, khususnya dengan analisis empiris terhadap parameter komputasi dan akurasi secara simultan. Kesenjangan ini menunjukkan perlunya evaluasi terhadap kemampuan perangkat keras generasi terbaru dalam menangani algoritma biometrik *State-of-the-Art.*

Penelitian ini mengusulkan pendekatan hybrid yang mengintegrasikan *Haar Cascade* sebagai detektor awal (pre-filter) dengan *ArcFace* sebagai modul verifikasi identitas dalam satu pipeline dua tahap. Implementasi dilakukan pada Raspberry Pi 5 yang didukung prosesor *Broadcom* BCM2712 [16] untuk mengevaluasi kemampuan perangkat *deep learning* generasi terbaru dalam menangani beban komputasi biometrik berbasis *Deep learning* . Berbeda dengan penelitian sebelumnya yang umumnya menggunakan metode pengenalan wajah ringan atau perangkat keras generasi lama [13], [14] penelitian ini secara empiris menganalisis dampak integrasi *ArcFace* terhadap penggunaan RAM, beban CPU, stabilitas FPS, serta tingkat keberhasilan akses dalam kondisi operasional nyata. Dengan demikian, kontribusi penelitian ini terletak pada evaluasi komprehensif *trade-off* antara efisiensi komputasi dan peningkatan akurasi keamanan pada sistem *Smartdoor* berbasis Raspberry Pi 5.

2. Metodologi

Penelitian ini menerapkan metode eksperimental kuantitatif untuk mengevaluasi kinerja arsitektur keamanan biometrik pada platform *deep learning*. Fokus utama eksperimen adalah melakukan komparasi *head-to-head* antara efisiensi algoritma deteksi standar (*Haar Cascade*) dengan algoritma *hybrid* (*Haar Cascade + ArcFace*). Pengukuran dilakukan terhadap parameter beban komputasi (CPU, RAM) dan responsivitas sistem (FPS) dalam kondisi operasional waktu nyata.

2.1 Arsitektur Perangkat Keras dan Lunak

Infrastruktur perangkat keras dibangun di atas *Single Board Computer* (SBC) generasi terbaru, Raspberry Pi 5 Model B (varian RAM 8GB). Pemilihan platform ini didasarkan pada keunggulan arsitektur *System on Chip* (SoC) Broadcom BCM2712. Prosesor ini memiliki empat inti (*quad-core*) 64-bit Arm Cortex-A76 dengan kecepatan *clock* mencapai 2.4GHz. Sesuai dengan dokumentasi teknis [16], arsitektur ini menawarkan lonjakan kinerja CPU hingga 2-3 kali lipat dibandingkan pendahulunya (Raspberry Pi 4). Kapasitas pemrosesan ini menjadi prasyarat

teknis yang krusial untuk menangani operasi matriks intensif pada algoritma *Deep learning* tanpa menyebabkan latensi berlebih. Selain itu, dukungan memori LPDDR4X dan GPU VideoCore VII memastikan *throughput* data citra dapat diproses secara efisien.

Dari sisi perangkat lunak, sistem beroperasi pada lingkungan Raspberry Pi OS (*Bookworm*) 64-bit untuk memaksimalkan instruksi set ARMv8. Implementasi kode dibangun menggunakan bahasa Python 3.11 dengan dukungan pustaka komputasi numerik yang teroptimasi. Pustaka OpenCV (ver. 4.x) digunakan untuk akuisisi citra dan pra-pemrosesan *Haar Cascade*, sedangkan ONNX *Runtime* digunakan sebagai mesin inferensi (*inference engine*) untuk menjalankan model *ArcFace* yang telah dilatih sebelumnya. Antarmuka pengguna (*User Interface*) untuk pemantauan *streaming* video dikembangkan berbasis web menggunakan kerangka kerja Flask.

2.2 Desain Alur Kerja Algoritma *Hybrid*

Penelitian ini mengimplementasikan arsitektur pemrosesan citra dua tahap (*two-stage pipeline*) yang dirancang untuk mengintegrasikan efisiensi deteksi *Haar Cascade* dengan presisi verifikasi *ArcFace*. Alur kerja sistem dimulai dengan akuisisi data visual beresolusi 640x480 piksel. Pada tahap awal, *Haar Cascade* berfungsi sebagai "gerbang logika" atau filter seleksi; jika tidak ada objek wajah yang terdeteksi, sistem secara otomatis memutus aliran proses ke tahap selanjutnya. Mekanisme ini krusial untuk mencegah pemborosan siklus CPU pada pemrosesan *frame* kosong.

Apabila wajah terdeteksi, area *Region of Interest* (ROI) akan *crop* dan di *resize* menjadi 112x112 piksel guna memenuhi spesifikasi *input layer* model *Deep learning ArcFace*. Model kemudian mengekstraksi fitur biometrik menjadi vektor *embedding* 512-dimensi untuk dicocokkan dengan basis data. Guna memitigasi latensi komputasi dan menjaga stabilitas FPS, diterapkan strategi optimasi temporal berupa mekanisme *Frame Skipping* (n=5). Dalam skema ini, proses inferensi berat *ArcFace* hanya dieksekusi setiap 5 *frame* sekali, sementara deteksi ringan *Haar Cascade* tetap berjalan kontinu pada setiap *frame* untuk menjaga responsivitas pelacakan (*tracking*) yang mulus.

2.3 Skenario Pengujian dan Parameter Evaluasi

Pengujian sistem dilakukan dalam dua skenario utama untuk melihat perbedaan kinerja antara metode deteksi standar dan metode hybrid. Skenario pertama adalah Haar Only, di mana sistem hanya menjalankan modul deteksi wajah menggunakan Haar Cascade tanpa proses verifikasi identitas. Skenario ini digunakan sebagai baseline untuk mengetahui kecepatan deteksi serta beban komputasi minimum sistem.

Skenario kedua adalah *Hybrid System*, yang mengaktifkan seluruh alur pemrosesan, mulai dari deteksi wajah, *cropping* dan *resizing* citra menjadi 112×112 piksel, inferensi *ArcFace*, hingga mekanisme kontrol akses pintu. Skenario ini digunakan untuk mengukur dampak integrasi *ArcFace* terhadap kecepatan sistem, akurasi pengenalan wajah, serta penggunaan sumber daya komputasi. Pengujian dilakukan dalam beberapa kondisi pencahayaan, yaitu pencahayaan normal (*indoor*), *backlight*, dan *low-light*, untuk melihat stabilitas sistem dalam situasi berbeda. Setiap skenario diuji sebanyak 19 kali agar hasil yang diperoleh cukup representatif dan tidak bergantung pada satu kondisi saja.

2.4 Parameter dan Teknik Pengambilan Data

Pengambilan data dilakukan secara *real-time* menggunakan modul logging berbasis Python yang berjalan di latar belakang sistem selama pengujian berlangsung. Beberapa parameter input dikondisikan tetap agar hasil antar skenario dapat dibandingkan secara adil, yaitu resolusi kamera 640×480 piksel, ukuran input model *ArcFace* 112×112 piksel, serta mekanisme frame skipping setiap 5 frame untuk menjaga stabilitas sistem. Setiap skenario diuji selama 5 menit dengan variasi kondisi pencahayaan yang meliputi kondisi normal (indoor), *backlight*, dan *low-light*.

Parameter output yang diukur mencakup kecepatan deteksi dan pemrosesan wajah yang direpresentasikan dalam bentuk FPS (Frame Per Second) serta waktu pemrosesan rata-rata per frame. Selain itu, akurasi pengenalan wajah diukur menggunakan Success Rate yang dihitung dari jumlah keberhasilan akses dibandingkan total percobaan, serta dicatat pula jumlah kesalahan seperti False Negative dan False Positive. Dari sisi kinerja perangkat, sistem juga memonitor penggunaan RAM (MB) dan beban CPU (%) untuk melihat dampak integrasi

ArcFace terhadap sumber daya komputasi. Untuk menghindari *overhead* pencatatan data yang dapat memengaruhi performa, proses *logging* dilakukan dengan teknik sampling setiap 30 frame, dan nilai akhir yang digunakan dalam analisis merupakan rata-rata selama periode pengujian.

3. Hasil dan Pembahasan

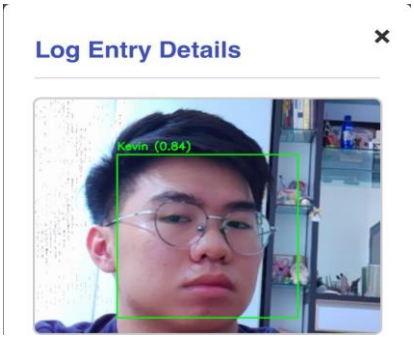
Bab ini menyajikan evaluasi terhadap kinerja sistem *Smartdoor* berbasis arsitektur *hybrid*. Fokus utama analisis diarahkan pada pembuktian kuantitatif mengenai efektivitas integrasi *Haar Cascade* dan *ArcFace* dalam menyeimbangkan *trade-off* antara akurasi keamanan dan efisiensi komputasi pada perangkat *deep learning* modern.

Pengujian pada bab ini difokuskan pada pengukuran dua parameter utama sebagaimana disebutkan pada abstrak, yaitu kecepatan deteksi dan akurasi pengenalan wajah. Eksperimen dilakukan sebanyak 19 percobaan pada masing-masing skenario (*Haar Only* dan *Hybrid*) dengan variasi kondisi pencahayaan normal, *backlight*, dan *low-light* untuk memastikan hasil yang diperoleh cukup representatif dan mencerminkan kondisi operasional nyata.

3.1 Implementasi dan Pemrosesan Data Wajah

Implementasi sistem berhasil direalisasikan dalam satu alur kerja yang kontinu sesuai rancangan hybrid. Proses dimulai dengan akuisisi citra visual dari kamera dengan resolusi standar 640×480 piksel. Pada tahap ini, algoritma Haar Cascade berperan sebagai penapis awal yang secara instan mendeteksi koordinat wajah dan mengabaikan area latar belakang yang tidak relevan.

Citra wajah yang terdeteksi kemudian di-crop dan diubah ukurannya menjadi 112×112 piksel untuk memenuhi spesifikasi input model *ArcFace*. Proses ini dilakukan secara efisien sehingga tidak menimbulkan latensi berarti sebelum tahap pengenalan wajah dilakukan.



Gambar 1. Terdeteksi

3.2 Hasil Pengujian Kinerja Komputasi

Pengujian stabilitas sistem dilakukan melalui mekanisme pencatatan data secara *real-time* dengan interval satu detik. Data ini berfungsi sebagai bukti empiris untuk memvalidasi responsivitas perangkat keras terhadap beban algoritma. Cuplikan data mentah saat sistem beroperasi pada kedua skenario (Haar Only dan Hybrid) disajikan secara terperinci dalam Tabel, yang menjadi landasan utama analisis komparatif ini.

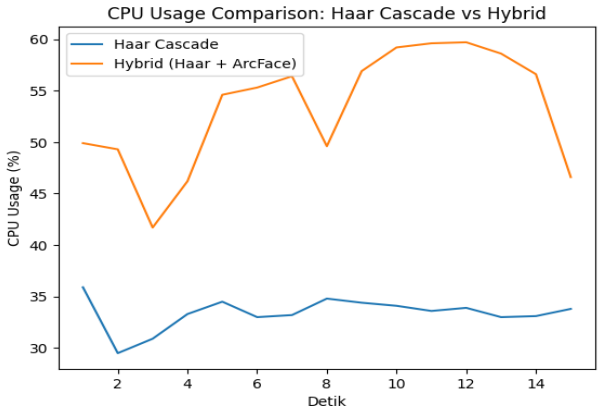
Table 1 Haar Cascade

FPS	RAM (MB)	CPU (%)	Status
20	257.2	35.9	CLOSED
19.9	257.2	29.5	CLOSED
20.2	257.2	30.9	OPEN
20	257.2	33.3	OPEN
20	257.2	34.5	OPEN
20	257.2	33	OPEN
20	257.2	33.2	OPEN
20	257.2	34.8	OPEN

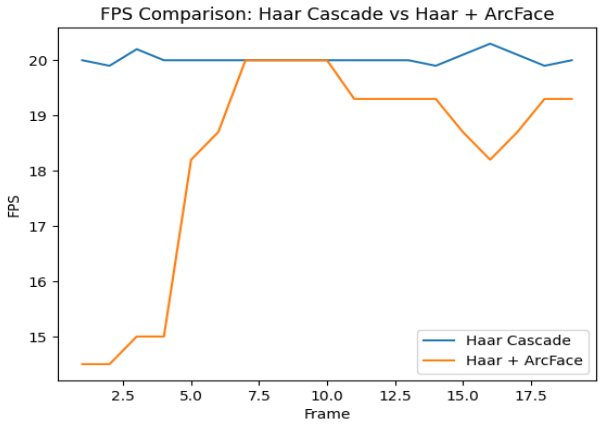
FPS	RAM (MB)	CPU (%)	Status
20	257.22	34.4	OPEN
20	257.22	34.1	OPEN
20	257.22	33.6	OPEN
20	257.22	33.9	CLOSED
20	257.22	33	CLOSED
20	257.22	33.1	CLOSED
19.9	257.22	33.8	CLOSED
20.1	257.22	30.7	OPEN
20.3	257.22	30.3	OPEN
20.1	257.22	32.8	OPEN
19.9	257.22	33.5	OPEN

Table 2 Haar dan *ArcFace*

FPS	RAM (MB)	CPU (%)	Status
14.5	343.66	49.9	OPEN
14.5	343.66	49.3	OPEN
15	343.66	41.7	OPEN
15	343.66	15	CLOSED
18.2	343.66	13.7	CLOSED
18.7	344.72	46.2	CLOSED
20	343.66	54.6	OPEN
20	343.66	55.3	OPEN
20	344.72	56.4	OPEN
20	343.66	49.6	OPEN
19.3	344.72	56.9	OPEN
19.3	343.66	59.2	OPEN
19.3	343.66	59.6	OPEN
19.3	343.66	59.7	OPEN
18.7	343.66	58.6	OPEN
18.2	343.66	56.6	OPEN
18.7	343.66	46.6	OPEN
19.3	343.66	47.3	CLOSED
19.3	343.66	40.1	CLOSED



Gambar 2 Perbandingan CPU



Gambar 3 Perbandingan FPS

Berdasarkan visualisasi data tersebut, terlihat korelasi linear yang signifikan antara peningkatan beban kerja dengan kompleksitas fitur keamanan. Transisi dari metode standar ke *Hybrid* menyebabkan kenaikan penggunaan RAM sebesar 33,7% (dari rata-rata 257 MB menjadi 344 MB) serta lonjakan beban CPU dari 33% menjadi 53%. Peningkatan beban ini merupakan konsekuensi logis dan tak terhindarkan karena sistem diharuskan memuat model *Deep learning ArcFace* (.onnx) ke dalam memori aktif dan melakukan operasi matematika matriks berdimensi tinggi untuk proses verifikasi identitas.

Meskipun terjadi lonjakan beban CPU yang mengindikasikan peningkatan konsumsi daya, spesifikasi perangkat keras Raspberry Pi 5 terbukti menjadi faktor penentu keberhasilan sistem ini. Prosesor Broadcom BCM2712 dengan arsitektur *Quad-core Cortex-A76* berkecepatan 2.4GHz menunjukkan kapasitas pemrosesan yang sangat besar. CPU mampu menangani algoritma berat dengan menyisakan sumber daya yang cukup sehingga tidak terjadi kemacetan data. Ketangguhan ini dibuktikan dengan stabilitas *frame rate* yang terjaga. Berdasarkan kalkulasi nilai tengah (*mean*), sistem mencatatkan angka stabil di 18,3 FPS, hanya mengalami penurunan marjinal sekitar 8,5% dari *baseline* 20 FPS. Nilai FPS tersebut merepresentasikan hasil pengukuran kecepatan deteksi dan pemrosesan wajah pada masing-masing skenario pengujian. Meskipun terjadi peningkatan beban komputasi akibat integrasi *ArcFace*, sistem tetap mampu mempertahankan performa dalam kategori *real-time* sehingga responsivitas deteksi tidak terganggu secara signifikan.

Trade-off berupa kenaikan beban komputasi tersebut dinilai sangat sepadan demi mendapatkan peningkatan fungsionalitas keamanan yang substansial. Sistem tidak lagi sekadar mendeteksi keberadaan objek wajah, melainkan mampu memvalidasi identitas pemilik rumah secara biometrik. Keunggulan ini tercermin dari analisis akurasi, di mana metode *Hybrid* mencatatkan tingkat keberhasilan akses (*Success Rate*) sebesar 73,7%, mengungguli metode standar yang hanya mencapai 68,4%. Nilai keberhasilan akses tersebut diperoleh dari total 19 percobaan pada setiap skenario dan merepresentasikan hasil pengukuran akurasi pengenalan wajah dalam berbagai kondisi pencahayaan. Data ini menunjukkan bahwa integrasi *ArcFace* memberikan peningkatan akurasi yang konsisten meskipun sistem dijalankan pada perangkat *deep learning* dengan keterbatasan sumber daya. Selisih akurasi sebesar 5,3% ini dicapai berkat tahapan normalisasi wajah dalam alur kerja *ArcFace* yang memperbaiki orientasi wajah sebelum pencocokan, membuat sistem jauh lebih toleran terhadap variasi posisi kepala dibandingkan metode konvensional.

3.3 Pembahasan dan Analisis *Trade-off*

Analisis mendalam terhadap skenario *baseline* (Haar Only) mengungkap bahwa sistem beroperasi dengan jejak karbon yang sangat minimal. Penggunaan CPU yang hanya berkisar di angka rata-rata 33,0% menandakan efisiensi energi yang tinggi, yang secara teoritis sangat menguntungkan untuk skenario perangkat bertenaga baterai. Namun, efisiensi ini memiliki limitasi fungsional yang krusial: sistem kehilangan fitur keamanan utamanya. Dalam mode ini, sistem hanya mampu melakukan deteksi objek ("ada wajah") tanpa kemampuan verifikasi ("siapa wajah tersebut"), sehingga tidak memenuhi standar keamanan untuk sebuah pintu pintar yang membutuhkan otentikasi spesifik.

Implementasi metode *Hybrid* hadir untuk menutup celah keamanan tersebut, meskipun membawa konsekuensi pada peningkatan beban komputasi yang masif. Aktivasi modul pengenalan wajah menyebabkan lonjakan beban CPU yang signifikan hingga mencapai rata-rata 53,0% (naik sekitar 60,6% dari *baseline*). Secara teknis, peningkatan intensitas komputasi pada prosesor ini berbanding lurus dengan peningkatan konsumsi arus listrik. Peningkatan ini adalah "biaya" yang harus dibayar sistem untuk menjalankan operasi matriks kompleks demi memvalidasi identitas pengguna.

Meskipun metode *Hybrid* menuntut sumber daya lebih besar, pengujian membuktikan ketangguhan arsitektur Raspberry Pi 5 dalam menangani beban tersebut. Perangkat keras terbukti mampu menyerap lonjakan komputasi tanpa mengalami saturasi atau penurunan kinerja. Indikator utamanya terlihat pada stabilitas laju bingkai yang tetap tinggi di angka rata-rata 18,3 FPS. Degradasi performa yang hanya berkisar 8% ini dinilai sangat wajar dan tidak mengganggu responsivitas operasional (*user experience*). Dengan demikian, *trade-off* berupa kenaikan konsumsi daya ini dapat dibenarkan (*justified*) demi mendapatkan jaminan akurasi keamanan biometrik yang presisi.

3.4 Komparasi dengan Penelitian Terdahulu dan *Novelty* Penelitian

Hasil penelitian ini memvalidasi sekaligus memperbarui lanskap studi biometrik pada perangkat *deep learning*. Secara teoretis, data empiris yang diperoleh mengonfirmasi postulat Dang [11] dan Kishore dkk. [12], yang menyatakan bahwa adopsi arsitektur *Deep learning* kompleks (seperti *ArcFace*) secara inheren menuntut biaya komputasi yang tinggi. Hal ini terbukti secara kuantitatif melalui lonjakan penggunaan RAM dan CPU pada skenario *Hybrid*, yang menegaskan bahwa presisi tinggi memang membutuhkan energi komputasi yang besar untuk proses inferensi matriks.

Dalam konteks komparasi arsitektural, penelitian ini menawarkan pendekatan yang lebih taktis dibandingkan studi terbaru lainnya. Abdullahu dkk. [15] mengusulkan sistem *hybrid* berbasis VGG16 dan SVM untuk IoT. Meskipun efektif, arsitektur VGG16 memiliki jumlah parameter yang sangat masif sehingga cenderung membebani memori perangkat *edge*. Sebaliknya, penelitian ini menggunakan *ArcFace* yang secara spesifik dioptimalkan untuk ekstraksi fitur wajah dengan fungsi *loss angular margin*, menghasilkan vektor fitur yang lebih diskriminatif namun tetap efisien saat dijalankan pada Raspberry Pi 5. Di sisi lain, riset oleh Alfan dkk. [13] dan Ramadini [14] sebelumnya terpaksa bertahan pada metode pengenalan wajah ringan berbasis statistik seperti LBPH akibat kendala spesifikasi perangkat keras generasi lama.

Oleh karena itu, aspek *Novelty* utama dari penelitian ini terletak pada optimasi *pipeline* biometrik modern yang menggantikan pendekatan klasik maupun arsitektur berat umum dengan kombinasi taktis *Haar Cascade* dan *ArcFace*. Selain itu, penelitian ini memberikan validasi empiris bahwa perangkat keras terbaru Raspberry Pi 5 mampu menjalankan algoritma *State-of-the-Art* dengan stabilitas di atas 18 FPS, menjembatani kesenjangan antara akurasi tinggi dan performa waktu nyata yang selama ini menjadi kendala utama.

3.5 Analisis Komparatif: Haar Cascade Standar vs Hybrid

Untuk memberikan gambaran yang tegas mengenai dampak integrasi algoritma *ArcFace*, dilakukan analisis komparatif langsung (*head-to-head*) antara sistem deteksi standar dengan sistem *hybrid*. Rangkuman data perbedaan kinerja kedua sistem tersebut disajikan secara komprehensif dalam Tabel:

Table 3 Matriks Perbedaan Kinerja Haar vs Haar dan *ArcFace*

Parameter Kinerja	Haar Cascade (Standar)	Haar dan *ArcFace* (Hybrid)
Tingkat Keamanan	Rendah (Buta Identitas)	Tinggi (Mengenali Pemilik)
Rata-rata FPS	20.0 FPS	18.3 FPS
Beban CPU	~33% (Beban Ringan)	~53% (Beban Sedang)
Penggunaan RAM	~257 MB	~344 MB
Responsivitas	Sangat Cepat	Cepat (*Real-time*)

Berdasarkan data tersebut, analisis dampak kinerja dapat dipetakan ke dalam tiga dimensi utama. Pertama, dari aspek beban komputasi, penambahan *ArcFace* terbukti memberikan tekanan signifikan pada perangkat, yang ditandai dengan kenaikan penggunaan CPU sebesar 60% relatif terhadap *baseline* (dari 33% menjadi 53%). Lonjakan ini mengonfirmasi secara kuantitatif bahwa algoritma *Deep learning* memang menuntut konsumsi energi yang jauh lebih besar dibandingkan metode konvensional.

Namun, dimensi kedua mengenai stabilitas sistem menunjukkan anomali positif. Meskipun beban komputasi melonjak drastis, degradasi pada laju bingkai (*frame rate*) tercatat sangat minim, yakni hanya sebesar 8% (setara penurunan 1,7 FPS). Fakta ini menjadi bukti empiris bahwa arsitektur Raspberry Pi 5 memiliki toleransi yang sangat tinggi terhadap beban berat, sehingga mampu menjamin pengalaman pengguna tetap mulus meskipun sistem bekerja keras di latar belakang.

Analisis ini bermuara pada justifikasi implementasi sebagai dimensi terakhir. Perbedaan kinerja yang terjadi menunjukkan adanya *trade-off* yang positif dan menguntungkan. Sistem memang mengalami sedikit penurunan dalam efisiensi daya, namun hal tersebut "dibayar lunas" oleh peningkatan masif dalam aspek keamanan dan akurasi identifikasi. Dengan demikian, pengorbanan sumber daya komputasi tersebut dinilai sangat layak untuk diaplikasikan demi mencapai standar keamanan biometrik modern.

3.6 Analisis Faktor Kegagalan

Meskipun sistem mencatatkan stabilitas komputasi yang tinggi, terdapat *gap* keberhasilan akses sebesar 26,3% (5 kegagalan dari 19 percobaan) pada skenario Hybrid. Investigasi mendalam terhadap data *False Negative* ini menunjukkan bahwa faktor determinan kegagalan bukanlah ketidakmampuan perangkat keras, melainkan variasi pencahayaan ekstrem yang bersifat eksternal.

Mengingat sistem *Smartdoor* ditempatkan pada lingkungan semi-terbuka, pengujian pada jam tertentu menghadapi kondisi cahaya latar yang intensitasnya melebihi cahaya depan. Fenomena ini menyebabkan wajah pengguna tertangkap kamera sebagai siluet dengan kontras rendah. Akibatnya, algoritma *ArcFace* kesulitan mengekstraksi detail tekstur wajah yang krusial, menghasilkan vektor *embedding* yang memiliki jarak *Euclidean* terlalu jauh dari data referensi, sehingga akses ditolak. Temuan ini sejalan dengan studi Abidi dkk. [17] yang menyatakan bahwa variasi iluminasi tetap menjadi tantangan fundamental dalam sistem biometrik berbasis visi komputer, terlepas dari seberapa kuat performa komputasi perangkat yang digunakan. Oleh karena itu, *gap* akurasi ini merepresentasikan batasan lingkungan operasional, bukan defisiensi pada arsitektur Raspberry Pi 5 yang diusulkan.

4. Simpulan

Berdasarkan analisis data penelitian ini berhasil membuktikan validitas kapasitas perangkat keras Raspberry Pi 5 yang didukung prosesor Broadcom BCM2712 dalam menangani beban kerja kecerdasan buatan di sisi *edge.* Sistem terbukti mampu mempertahankan stabilitas laju bingkai rata-rata di angka 18,3 FPS meskipun menjalankan operasi matriks kompleks dari algoritma *ArcFace*, sebuah capaian yang mengonfirmasi bahwa perangkat keras generasi terbaru telah mengatasi hambatan latensi pada sistem keamanan waktu nyata (*real-time*). Secara kuantitatif, implementasi metode *Hybrid* ini memang menuntut konsekuensi sumber daya yang signifikan, ditandai dengan lonjakan beban CPU dari 33% menjadi 53% serta peningkatan penggunaan memori (RAM) sebesar 33,7% sebagai "biaya operasional" untuk proses inferensi. Demikian, *trade-off* lonjakan beban tersebut terjustifikasi sepenuhnya oleh superioritas keamanan yang dihasilkan. Metode *Hybrid* mencatatkan tingkat keberhasilan akses (*Success Rate*) sebesar 73,7%, jauh melampaui metode standar (68,4%) yang memiliki keterbatasan fundamental. Dengan demikian, arsitektur *Hybrid* ini merepresentasikan titik keseimbangan terbaik antara efisiensi perangkat keras modern dan standar keamanan biometrik presisi tinggi.

Daftar Referensi

[1] D. Y. Wijaya and A. Yulianto, “Prototype of smartdoor using RFID technology with Internet of Things (IoT),” in *Proc. Conf. Management, Business, Innovation, Education and Social Science (COMBINES)*, vol. 1, no. 1, pp. 196–204, 2021.

[2] L. Qinjun, C. Tianwei, Z. Yan, and W. Yuying, “Facial Recognition Technology : A

Comprehensive Overview," Academic Journal of Computing & Information Science, vol. 6, no. 7, pp. 15–26, 2023, doi: 10.25236/AJCIS.2023.060703.
[3] A. Madan, "Face Recognition using Haar Cascade Classifier," International Journal for Modern Trends in Science and Technology, vol. 7, no. 01, pp. 85–87, 2021.
[4] A. H. Ahmad *et al.*, "Real time face recognition of video surveillance system using haar cascade classifier," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1389–1399, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1389-1399.
[5] P. Mccullagh, "Face detection by using Haar cascade classifier," *Wasit Journal of Computer and Mathematics Science*, vol. 2, no. 1, pp. 1–5, 2023, doi: 10.31185/wjcm.109.
[6] A. A. M. Suradi, I. Djafar, S. Alam, and A. Syam, "Perbandingan metode Haar cascade dan dlib dalam mendeteksi wajah secara realtime," *in Prosiding Seminar Ilmiah Sistem Informasi dan Teknologi Informasi*, Makassar, Indonesia, pp. 94–102, 2023.
[7] S. Saragih, "Implementasi Algoritma Haar Cascade Menggunakan Pengolahan Citra Digital untuk Absensi Deteksi Wajah dan Nama Menggunakan Python," *Jurnal Sosial dan Teknologi (SOSTECH)*, vol. 5, no. 3, pp. 789–798, 2025.
[8] J. H. Sim and A. Yulianto, "Evaluating YOLOv5 and YOLOv8 : Advancements in Human Detection," *Journal of Information Systems and Informatics*, vol. 6, no. 4, pp. 2999–3012, 2024, doi: 10.51519/journalisi.v6i4.944.
[9] A. P. Sari and B. Hendrik, "Analisis komparatif algoritma deep learning untuk pengenalan wajah: CNN, FaceNet, dan ArcFace," *Journal of Education Research*, vol. 6, no. 4, pp. 1029–1036, 2025.
[10] B. W. Nurlita, S. Winarno, A. Nugraha, A. N. I. Muttaqin, Y. Zarifa, P. M. Salsabila, and G. F. Mumtaz, "Comparison of ArcFace and Dlib performance in face recognition with detection using YOLOv8," *Jurnal Inovtek Polbeng - Seri Informatika*, vol. 9, no. 2, pp. 890–903, 2024.
[11] T. V. Dang, "Smart home management system with face recognition based on ArcFace model in deep convolutional neural network," *Journal of Robotics and Control (JRC)*, vol. 3, no. 6, pp. 754–761, 2022, doi: 10.18196/jrc.v3i6.15978.
[12] S. Kishore, P. H. G., S. C. S., and M. K. B., "Evaluation of deep learning methods in face recognition: Datasets, metrics, and results," *International Journal on Science and Technology (IJSAT)*, vol. 16, no. 4, pp. 1–9, 2025.
[13] D. S. Alfan, A. Rochman, M. Firdaus, N. Setiawan, and P. Rosyani, "Penerapan metode Haar-cascade dan LBPH untuk face detection dan recognition," *Jurnal AI dan SPK: Jurnal Artificial Inteligent dan Sistem Penunjang Keputusan*, vol. 2, no. 1, pp. 96–104, 2024.
[14] F. L. Ramadini and E. Haryatmi, "Penggunaan metode Haar cascade classifier dan LBPH untuk pengenalan wajah secara realtime," *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 6, no. 2, pp. 289–296, 2022, doi: 10.30743/infotekjar.v6i2.4714.
[15] E. Abdullahu, H. Wache, and M. Piangerelli, "Secure and decentralized hybrid multi-face recognition for IoT applications," *Sensors*, vol. 25, p. 5880, 2025, doi: 10.3390/s25185880.
[16] Raspberry Pi Ltd, "Raspberry Pi 5 Product Brief," Dec. 2025. [Online]. Available: https://pip-assets.raspberrypi.com/categories/892-raspberry-pi-5/documents/RP-008348-DS-6-raspberry-pi-5-product-brief.pdf. [Accessed: Apr. 13, 2026].
[17] S. M. H. Abidi, S. A. Hassan, S. M. Raza, and M. J. Beliatis, "Advances in face recognition: A comprehensive review of feature extraction and dataset evaluation," *Electronics*, vol. 15, p. 338, 2026, doi: 10.3390/electronics15020338.