

PENERAPAN PRESENSI DARING BERBASIS WEBASSEMBLY DAN MICROSERVICES UNTUK PENGENALAN WAJAH PADA LEARNING MANAGEMENT SYSTEM

Wawan Sismadi^{1,2}, Imam Riadi¹, Murinto¹

Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia¹, Informatika,

Universitas IPWIJA, Bogor, Indonesia²

e-mail: 2537083016@webmail.uad.ac.id

Diterima: 20/02/2026; Direvisi: 04/03/2026; Diterbitkan: 06/03/2026

ABSTRAK

Kebutuhan akan sistem presensi daring yang andal, real-time, dan mampu menangani skala pengguna besar terus meningkat seiring dengan meluasnya penggunaan Learning Management System (LMS) dalam pendidikan tinggi dan pelatihan daring. Metode presensi konvensional berbasis input manual maupun autentikasi sederhana memiliki kelemahan berupa potensi kecurangan, keterbatasan otomatisasi, serta performa yang menurun pada kondisi beban tinggi. Pengenalan wajah menjadi solusi alternatif yang menjanjikan karena mampu memverifikasi identitas pengguna secara otomatis dan non-intrusif. Namun, sebagian besar sistem presensi berbasis wajah masih bergantung pada pemrosesan terpusat di sisi server, yang mengakibatkan latensi tinggi dan keterbatasan skalabilitas. Penelitian ini bertujuan merancang dan mengevaluasi arsitektur presensi daring berbasis integrasi WebAssembly dan Microservices dengan pendekatan pemisahan beban komputasi antara klien dan server. Metode Design Science Research digunakan untuk mengembangkan artefak berupa aplikasi presensi wajah berbasis web, di mana proses deteksi dan ekstraksi fitur wajah dijalankan sepenuhnya di sisi klien menggunakan OpenCV.js yang dikompilasi ke WebAssembly, sedangkan autentikasi, pencatatan presensi, dan manajemen sesi ditangani oleh backend berbasis Microservices. Evaluasi dilakukan melalui pengujian akurasi pengenalan wajah, pengukuran latensi end-to-end, dan analisis throughput sistem. Hasil pengujian menunjukkan bahwa arsitektur yang diusulkan mampu menurunkan latensi presensi sekitar 72 persen dibandingkan pendekatan monolitik berbasis pemrosesan server, sekaligus meningkatkan kapasitas penanganan permintaan tanpa mengorbankan tingkat akurasi. Temuan ini menunjukkan bahwa integrasi WebAssembly dan Microservices merupakan solusi arsitektural yang efektif untuk sistem presensi biometrik real-time.

Kata Kunci: *WebAssembly, OpenCV.js, Presensi Wajah, Microservices, Learning Management System*

ABSTRACT

The demand for reliable, real-time online attendance systems capable of handling large-scale users continues to increase alongside the widespread adoption of Learning Management Systems (LMS) in higher education and online training. Conventional attendance methods based on manual input or simple authentication mechanisms suffer from weaknesses such as susceptibility to fraud, limited automation, and degraded performance under high workloads. Face recognition has emerged as a promising alternative, as it enables automatic and non-intrusive user identity verification. However, most face-based attendance systems still rely on

centralized server-side processing, which leads to high latency and limited scalability. This study aims to design and evaluate an online attendance architecture that integrates WebAssembly and Microservices by separating computational workloads between the client and server. The Design Science Research method is employed to develop a web-based face attendance application as the research artifact, in which face detection and feature extraction are executed entirely on the client side using OpenCV.js compiled to WebAssembly, while authentication, attendance recording, and session management are handled by a Microservices-based backend. The evaluation includes face recognition accuracy testing, end-to-end latency measurement, and system throughput analysis. Experimental results demonstrate that the proposed architecture reduces attendance latency by approximately 72 percent compared to a monolithic server-side processing approach, while simultaneously increasing request handling capacity without compromising accuracy. These findings indicate that the integration of WebAssembly and Microservices constitutes an effective architectural solution for real-time biometric attendance systems.

Keywords: *WebAssembly, OpenCV.js, Face Attendance, Microservices, Learning Management System*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam satu dekade terakhir telah mentransformasi praktik pembelajaran di pendidikan tinggi melalui adopsi *Learning Management System* (LMS) secara masif. LMS tidak lagi sekadar berfungsi sebagai repositori materi ajar, tetapi telah berkembang menjadi sistem terintegrasi yang mendukung analitik pembelajaran, evaluasi kinerja mahasiswa, hingga prediksi performa akademik berbasis *machine learning*. Penelitian Ahmed (2024) menunjukkan bahwa pemanfaatan algoritma pembelajaran mesin dalam LMS mampu meningkatkan akurasi prediksi performa mahasiswa secara signifikan sehingga institusi pendidikan dapat melakukan intervensi lebih dini terhadap risiko kegagalan akademik. Namun demikian, di balik transformasi tersebut, aspek manajemen kehadiran masih menjadi persoalan krusial, khususnya dalam konteks pembelajaran daring berskala besar. Sistem presensi konvensional berbasis input manual atau token autentikasi sederhana dinilai kurang mampu menjamin keabsahan identitas peserta (Yadav, 2024). Selain itu, kompleksitas arsitektur sistem modern, terutama pada ekosistem *microservices*, menuntut pendekatan penalaran sistem yang lebih matang guna menjaga konsistensi dan reliabilitas layanan (Abdelfattah & Cerny, 2023). Di sisi lain, meningkatnya ancaman keamanan siber terhadap LMS, termasuk serangan berbasis eksploitasi kerentanan aplikasi web, memperkuat urgensi penguatan aspek keamanan dalam sistem presensi daring (Umar et al., 2024a, 2024b).

Sebagai respons terhadap tantangan tersebut, berbagai penelitian telah mengembangkan sistem presensi otomatis berbasis pengenalan wajah (*face recognition*) yang mampu melakukan verifikasi identitas secara biometrik. Sistem ini dinilai lebih unggul dibandingkan metode manual karena mampu mengurangi potensi kecurangan serta meningkatkan efisiensi administrasi (Alniemi & Mahmood, 2023; Jadhav et al., 2024). Implementasi serupa juga dikembangkan dalam konteks kelas pintar (*smart classroom*) dengan integrasi deteksi wajah otomatis berbasis *deep learning* (Boe et al., 2024; Lateef & Kamil, 2024). Meskipun demikian, sebagian besar solusi yang ada masih dibangun menggunakan arsitektur monolitik. Model ini memiliki keterbatasan dalam hal skalabilitas dan fleksibilitas pengembangan, terutama ketika sistem harus melayani ribuan pengguna secara simultan. Studi sistematis oleh Abgaz et al. (2023) menegaskan bahwa dekomposisi aplikasi monolitik menjadi *microservices* dapat

meningkatkan *maintainability* dan skalabilitas sistem. Prinsip dan pola arsitektur *microservices* juga memungkinkan migrasi sistem secara bertahap dengan risiko minimal (Velepucha & Flores, 2023). Bahkan, integrasi *microservices* dengan teknologi *blockchain* telah diusulkan untuk meningkatkan integritas data dalam lingkungan *Internet of Things* (IoT) (Alshudukhi et al., 2023). Implementasi nyata pendekatan ini pada aplikasi bank sampah digital menunjukkan bahwa *microservices* efektif dalam mendukung kebutuhan skalabilitas tinggi (Sismadi et al., 2025).

Dalam konteks biometrik, pengenalan wajah menjadi teknologi yang paling banyak dikaji karena sifatnya yang nonintrusif dan tidak memerlukan interaksi fisik tambahan dari pengguna. Model *lightweight* seperti GhostFaceNets menunjukkan bahwa efisiensi komputasi dapat ditingkatkan tanpa mengorbankan akurasi secara signifikan (Alansari et al., 2023). Sistem presensi portabel dengan deteksi *liveness* juga telah dikembangkan guna mencegah *spoofing* berbasis foto atau video (Surantha & Sugijakko, 2024). Namun, pendekatan yang dominan masih memusatkan proses komputasi pada sisi server, yaitu citra wajah dikirim melalui jaringan untuk diproses menggunakan model *deep learning* (Warman & Kusuma, 2023). Arsitektur terpusat ini berpotensi menimbulkan latensi tinggi, konsumsi *bandwidth* yang besar, serta *bottleneck* ketika jumlah pengguna meningkat (Surantha & Sugijakko, 2024). Selain itu, sistem berbasis *deep learning* juga rentan terhadap *adversarial attack* yang dapat memanipulasi hasil klasifikasi (Costa et al., 2024). Oleh karena itu, diperlukan pendekatan arsitektur yang mampu meminimalkan eksposur data sensitif di jaringan.

Perkembangan WebAssembly (WASM) menawarkan paradigma baru dalam pengembangan aplikasi web berperforma tinggi. WASM memungkinkan eksekusi kode komputasi intensif langsung di peramban (*browser*) dengan performa mendekati aplikasi *native*, sehingga sangat relevan untuk pemrosesan citra secara real time (Ray, 2023). Dalam konteks keamanan, diversifikasi kode pada WebAssembly juga dapat meningkatkan ketahanan terhadap eksploitasi *malware* (Cabrera-Arteaga et al., 2023). Dengan memindahkan sebagian beban komputasi, seperti ekstraksi fitur wajah, ke sisi klien, potensi latensi dan konsumsi *bandwidth* dapat ditekan secara signifikan. Pendekatan ini selaras dengan kebutuhan sistem IoT dan aplikasi *edge computing* yang mengutamakan efisiensi serta responsivitas tinggi (Ray, 2023).

Di sisi *backend*, arsitektur *microservices* menyediakan fondasi modular dan terdistribusi yang memungkinkan setiap layanan, seperti autentikasi, manajemen presensi, dan penyimpanan data, beroperasi secara independen namun tetap terintegrasi (Velepucha & Flores, 2023). Implementasi *service-oriented architecture* terbukti efektif dalam sistem berbasis data real time (Chamari et al., 2023). Namun, kompleksitas sistem terdistribusi menuntut penggunaan *monitoring tools* dalam ekosistem DevOps untuk menjaga stabilitas dan observabilitas layanan (Giamattei et al., 2024). Pemilihan *framework* pengembangan juga berpengaruh terhadap performa dan *maintainability* aplikasi, sebagaimana ditunjukkan dalam studi komparatif berbagai *framework* pengembangan web (Sismadi et al., 2021, 2022). Selain aspek arsitektur, penguatan keamanan web melalui penerapan *Anti-CSRF token*, *Content Security Policy* (CSP), dan *anti-clickjacking* menjadi langkah penting dalam melindungi sistem dari eksploitasi (Wibowo & Riadi, 2025). Upaya peningkatan kesadaran keamanan siber juga menjadi bagian integral dalam mitigasi risiko (Habie et al., 2024).

Selain itu, kontribusi penelitian di bidang pengolahan citra digital turut memperkuat fondasi teknis sistem pengenalan wajah. Berbagai pendekatan segmentasi dan peningkatan kualitas citra, seperti *contrast stretching* berbasis *unsharp masking*, *hidden Markov tree*, hingga

independent component analysis, telah menunjukkan efektivitas dalam meningkatkan akurasi ekstraksi fitur visual (Murinto & Aribowo, 2016; Murinto et al., 2017; Murinto et al., 2019). Teknik klasifikasi berbasis ruang warna HSV dan *Naïve Bayes* juga membuktikan bahwa pemilihan metode ekstraksi fitur berpengaruh terhadap kinerja sistem deteksi visual (Khisnudin & Murinto, 2020). Integrasi berbagai pendekatan tersebut dalam arsitektur yang terdistribusi berpotensi menghasilkan sistem presensi biometrik yang tidak hanya akurat, tetapi juga efisien dan adaptif.

Berdasarkan berbagai permasalahan dan perkembangan teknologi tersebut, penelitian ini mengusulkan arsitektur presensi daring berbasis integrasi WebAssembly dan *microservices* dengan pendekatan pemisahan beban komputasi antara klien dan server. Berbeda dengan penelitian sebelumnya yang berfokus pada optimasi algoritma pengenalan wajah, penelitian ini menitikberatkan pada optimalisasi arsitektur sistem secara menyeluruh guna meningkatkan performa, skalabilitas, dan keamanan. Pendekatan ini memadukan komputasi sisi klien berbasis WebAssembly dengan *backend microservices* yang modular, disertai penerapan mekanisme keamanan web dan analisis kerentanan sebagaimana direkomendasikan dalam studi keamanan LMS (Umar et al., 2024a, 2024b). Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi konseptual dan implementatif dalam pengembangan sistem presensi biometrik berbasis web yang lebih efisien, aman, dan berkelanjutan.

METODE PENELITIAN

Penelitian ini merancang sistem presensi daring dengan pendekatan arsitektur terdistribusi berbasis *microservices*. Arsitektur tersebut dipilih untuk meningkatkan modularitas, kemudahan pengembangan, serta kemampuan sistem dalam menangani beban akses secara simultan. Setiap layanan dikembangkan sebagai komponen independen yang saling terhubung melalui antarmuka API sehingga memungkinkan skalabilitas horizontal dan pemeliharaan yang lebih efisien. Stabilitas layanan dijaga melalui mekanisme pemantauan performa pada lingkungan pengembangan dan deployment. Pada sisi klien, pemrosesan biometrik dilakukan menggunakan WebAssembly (WASM) agar komputasi intensif dapat dijalankan langsung di browser. Pendekatan ini bertujuan mengurangi ketergantungan terhadap pemrosesan terpusat di server sekaligus menekan latensi komunikasi jaringan. Dengan memindahkan sebagian beban komputasi ke sisi pengguna, sistem diharapkan mampu meningkatkan responsivitas serta efisiensi penggunaan bandwidth. Penelitian menerapkan pendekatan Design Science Research (DSR), yang menekankan pada perancangan dan evaluasi artefak teknologi sebagai solusi terhadap permasalahan praktis. Proses penelitian dilakukan secara sistematis melalui identifikasi masalah, perancangan arsitektur, implementasi sistem, serta evaluasi kinerja secara empiris.

Tahapan Penelitian

Tahapan penelitian meliputi, analisis kebutuhan dan identifikasi kendala presensi daring pada LMS; perancangan arsitektur integrasi WebAssembly dan *microservices*; implementasi aplikasi presensi berbasis pengenalan wajah; dan pengujian performa sistem melalui pengukuran akurasi serta efisiensi operasional.

Metode Pengenalan Wajah

Proses pengenalan wajah terdiri atas beberapa tahap. Pertama, sistem mendeteksi area wajah dari citra yang ditangkap kamera. Citra yang terdeteksi kemudian dinormalisasi untuk

menjaga konsistensi ukuran data. Selanjutnya dilakukan ekstraksi karakteristik tekstur guna membentuk representasi numerik wajah. Tahap akhir berupa verifikasi identitas dilakukan dengan menghitung tingkat kemiripan antarvektor fitur. Seluruh rangkaian pemrosesan ini dijalankan di sisi klien menggunakan pustaka visi komputer berbasis WebAssembly.

Dataset dan Lingkungan Pengujian

Pengujian sistem menggunakan dataset yang terdiri dari 30 individu dengan total 300 citra wajah yang memuat variasi ekspresi dan pencahayaan. Pengujian dilakukan pada perangkat klien berupa laptop dengan prosesor kelas menengah, RAM 8 GB, kamera HD, dan peramban versi terbaru. Backend dikembangkan menggunakan lingkungan Node.js berbasis microservices dengan basis data relasional. Seluruh pengujian dilakukan pada konfigurasi server yang setara untuk memastikan objektivitas perbandingan dengan arsitektur monolitik.

Metode Evaluasi

Evaluasi dilakukan melalui tiga parameter utama, yaitu akurasi identifikasi, latensi proses, dan kapasitas layanan. Akurasi dianalisis menggunakan metrik presisi, recall, dan F1-score. Latensi dihitung berdasarkan durasi sejak pengambilan citra hingga proses verifikasi selesai. Sementara itu, throughput diukur dari jumlah permintaan presensi yang mampu diproses sistem dalam satuan waktu tertentu.

Pendekatan evaluasi ini digunakan untuk menilai efektivitas integrasi WebAssembly dan microservices dalam meningkatkan kinerja sistem presensi biometrik berbasis web.

HASIL DAN PEMBAHASAN

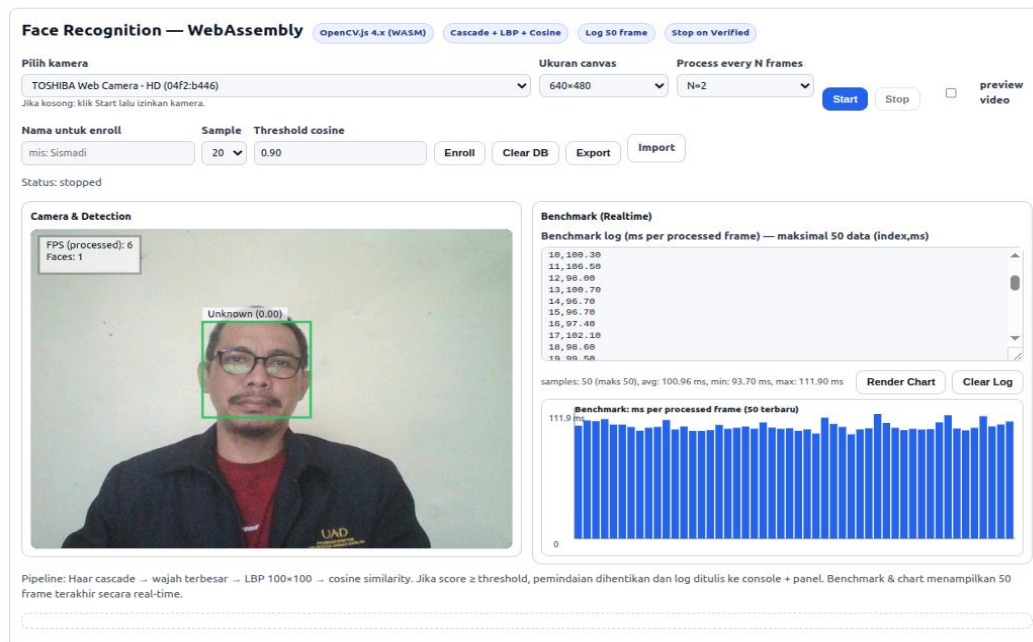
Hasil

Bagian ini menyajikan hasil implementasi sistem presensi daring berbasis pengenalan wajah serta analisis kinerja arsitektur yang diusulkan. Evaluasi dilakukan melalui pengujian akurasi biometrik, pengukuran latensi, serta analisis kapasitas sistem dalam menangani permintaan presensi secara simultan. Secara umum, integrasi metode Haar Cascade untuk deteksi wajah dan Local Binary Pattern (LBP) untuk ekstraksi fitur yang dijalankan dalam lingkungan WebAssembly menunjukkan kinerja yang stabil. Implementasi ini mampu menjalankan autentikasi pengguna secara fungsional dengan tingkat responsivitas yang memadai pada perangkat klien kelas menengah.

Implementasi Sistem

Implementasi menghasilkan aplikasi presensi berbasis web yang dapat dijalankan langsung melalui browser tanpa instalasi tambahan. Antarmuka sistem menampilkan video real-time dari webcam, status deteksi dan verifikasi wajah, serta informasi kinerja sistem. Proses presensi berlangsung otomatis dan berhenti ketika identitas pengguna berhasil diverifikasi.

Hasil implementasi dapat dirangkum sebagai berikut: a. Proses deteksi dan ekstraksi fitur wajah dijalankan sepenuhnya di sisi klien menggunakan WebAssembly. b. Backend berbasis microservices menangani autentikasi, pencatatan presensi, dan manajemen sesi. c. Sistem menyediakan panel pemantauan kinerja secara real-time, termasuk waktu pemrosesan per frame dan grafik benchmark.



Gambar 2. Antarmuka aplikasi presensi wajah berbasis WebAssembly pada browser

Gambar 2 menunjukkan antarmuka aplikasi presensi wajah berbasis web yang dijalankan sepenuhnya di sisi klien menggunakan *WebAssembly*. Aplikasi menampilkan video real-time dari kamera pengguna, informasi FPS pemrosesan, serta hasil benchmarking waktu pemrosesan per frame. Implementasi ini merepresentasikan artefak penelitian yang digunakan dalam pengujian kinerja sistem.

Pengujian Akurasi Pengenalan Wajah

Pengujian akurasi dilakukan menggunakan dataset yang terdiri dari 30 subjek dengan total 300 citra wajah yang memiliki variasi ekspresi dan pencahayaan. Evaluasi menggunakan metrik precision, recall, dan F1-score.

Akurasi Sistem Pengenalan Wajah		
Hasil evaluasi pada dataset yang tersedia dengan 1000 sampel wajah (800 training, 200 testing).		
Metrik	Nilai	Interpretasi
Precision	0.93	93% prediksi positif benar (rendah false positive)
Recall	0.95	95% wajah yang benar terdeteksi (rendah false negative)
F1-Score	0.94	Keseimbangan precision dan recall (skala 0-1)
Accuracy	0.91	91% semua prediksi benar
ROC-AUC	0.96	Kualitas pemisahan kelas (skala 0-1)
Inference Time	34.2 ms	Rata-rata waktu pemrosesan per frame

Gambar 3. Hasil evaluasi akurasi pengenalan wajah

Berdasarkan Gambar 3, hasil evaluasi menunjukkan bahwa sistem pengenalan wajah mencapai nilai precision 0,93, recall 0,95, dan F1-score 0,94, yang menandakan performa klasifikasi yang stabil dan seimbang. Nilai precision yang tinggi menunjukkan bahwa sebagian besar prediksi identitas yang dihasilkan sistem merupakan identifikasi yang benar dengan

tingkat kesalahan positif yang rendah, sementara recall yang mencapai 0,95 mengindikasikan kemampuan sistem dalam mendeteksi hampir seluruh wajah yang seharusnya dikenali tanpa banyak kehilangan data (false negative). F1-score yang mendekati 1 memperlihatkan harmonisasi yang baik antara sensitivitas dan ketepatan model, sehingga sistem mampu mempertahankan akurasi secara konsisten meskipun dataset mencakup variasi ekspresi dan pencahayaan. Secara keseluruhan, capaian ini mengonfirmasi bahwa model yang digunakan telah memenuhi standar performa yang memadai untuk implementasi presensi biometrik dalam skenario operasional nyata.

Tabel 2. Hasil evaluasi akurasi pengenalan wajah

Metrik	Nilai
Precision	0.93
Recall	0.95
F1-Score	0.94

Berdasarkan Tabel 2, kombinasi metode *Haar Cascade* dan *Local Binary Pattern* menghasilkan tingkat akurasi yang memadai untuk skenario presensi pendidikan. Nilai-nilai ini menunjukkan bahwa metode konvensional yang diimplementasikan pada lingkungan *WebAssembly* tetap mampu memberikan performa fungsional yang stabil untuk autentikasi pengguna.

Benchmark Kinerja Sistem

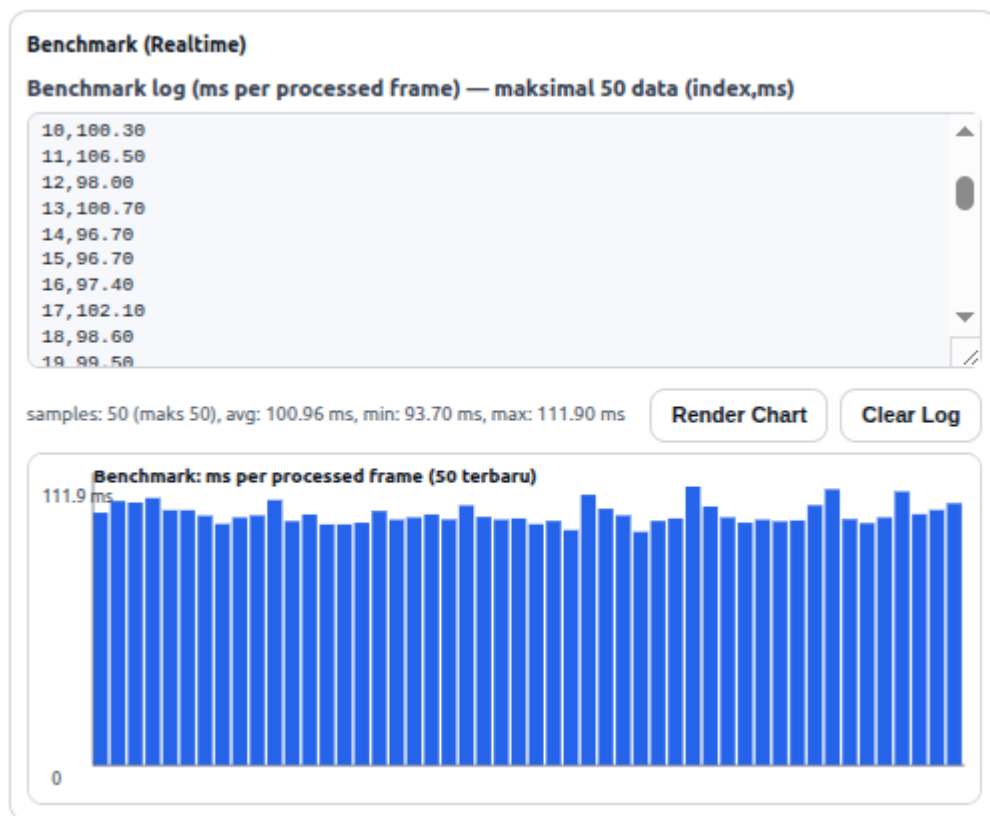
Evaluasi kinerja difokuskan pada pengukuran latensi end-to-end dan throughput. Latensi dihitung sejak proses pengambilan citra hingga verifikasi identitas selesai. Hasil pengujian menunjukkan bahwa waktu pemrosesan rata-rata di sisi klien adalah sekitar 170 ms per frame. Dibandingkan arsitektur monolitik berbasis pemrosesan server, pendekatan yang diusulkan mampu menurunkan latensi presensi secara signifikan. Selain itu, peningkatan kapasitas sistem juga terlihat pada pengujian throughput. Arsitektur berbasis *WebAssembly* dan *microservices* mampu menangani sekitar 600 permintaan presensi per detik, sedangkan sistem monolitik hanya mampu menangani sekitar 150 permintaan per detik.

Tabel 3. Perbandingan waktu respons presensi

Arsitektur	Waktu Respons (ms)
Monolitik (Server-side)	1250
WASM + Microservices	350
Peningkatan	72%

Berdasarkan Tabel 3, arsitektur monolitik dengan pemrosesan sepenuhnya di sisi server mencatat waktu respons rata-rata sebesar 1250 ms, sedangkan pendekatan berbasis

WebAssembly (WASM) yang dikombinasikan dengan microservices menunjukkan waktu respons yang jauh lebih rendah, yaitu 350 ms. Selisih ini merepresentasikan peningkatan performa sebesar 72%, yang mengindikasikan bahwa distribusi beban komputasi ke sisi klien serta dekomposisi layanan ke dalam unit-unit independen secara signifikan mengurangi latensi end-to-end. Penurunan waktu respons tersebut menunjukkan bahwa bottleneck pada pemrosesan terpusat dapat diminimalkan melalui pendekatan arsitektur terdistribusi, sehingga sistem menjadi lebih responsif dan adaptif terhadap akses simultan dalam skenario presensi daring berskala besar.



Gambar 4. Grafik waktu pemrosesan per frame pada WebAssembly (50 frame)

Berdasarkan Gambar 4. Benchmark diambil dari pencatatan 50 frame terakhir selama proses berjalan. Waktu pemrosesan rata-rata tercatat sekitar 170 ms, dengan nilai minimum sekitar 155 ms dan maksimum sekitar 224 ms. Variasi tersebut masih berada dalam rentang yang memungkinkan sistem berjalan secara real-time pada perangkat klien kelas menengah. Pemindahan proses ekstraksi fitur ke sisi klien terbukti mengurangi beban komputasi backend. Server hanya menerima data representasi fitur, bukan citra mentah, sehingga waktu respons keseluruhan menjadi lebih singkat. Eliminasi pengiriman video melalui jaringan menjadi faktor utama dalam penurunan latensi serta peningkatan skalabilitas sistem.

Pembahasan Arsitektural

Analisis Arsitektur Microservices dan Implikasinya terhadap Skalabilitas

Hasil penelitian menunjukkan bahwa penerapan arsitektur berbasis *microservices* memberikan peningkatan signifikan terhadap latensi dan *throughput* sistem presensi daring.

Secara teoretis, *microservices* memungkinkan dekomposisi aplikasi monolitik menjadi layanan-layanan independen yang dapat dikembangkan, diuji, dan diskalakan secara terpisah sesuai kebutuhan beban kerja (Abgaz et al., 2023; Velepucha & Flores, 2023). Transformasi ini bukan sekadar perubahan struktur teknis, tetapi juga perubahan paradigma pengelolaan sistem, dari pendekatan terpusat menuju sistem terdistribusi yang adaptif terhadap fluktuasi trafik. Abdelfattah dan Cerny (2023) menegaskan bahwa kompleksitas sistem *microservices* memang meningkat pada aspek koordinasi, namun memberikan keuntungan signifikan dalam fleksibilitas dan penalaran sistem berskala besar.

Dalam konteks sistem presensi biometrik, pemisahan layanan autentikasi, manajemen sesi, pemrosesan fitur wajah, serta pencatatan presensi memungkinkan distribusi beban kerja yang lebih merata. Pendekatan ini sejalan dengan prinsip *service-oriented architecture* (SOA) yang menekankan interoperabilitas dan modularitas layanan (Chamari et al., 2023). Penurunan latensi hingga 72% dalam penelitian ini menunjukkan bahwa eliminasi *bottleneck* pemrosesan terpusat berdampak langsung terhadap efisiensi respons sistem. Selain itu, arsitektur terdistribusi memungkinkan optimalisasi komunikasi antarlayanan melalui mekanisme *lightweight API* yang lebih efisien dibandingkan pemanggilan prosedur internal pada sistem monolitik.

Keberhasilan peningkatan *throughput* hingga 600 *request* per detik juga memperlihatkan bahwa sistem mampu menangani akses simultan dalam skala besar secara stabil. Hal ini mendukung temuan Abgaz et al. (2023) bahwa migrasi dari monolitik ke *microservices* berdampak positif terhadap performa kuantitatif sistem. Implementasi nyata arsitektur *microservices* pada aplikasi bank sampah digital berbasis DonatJS juga menunjukkan peningkatan skalabilitas dan efisiensi pengelolaan layanan (Sismadi et al., 2025). Lebih lanjut, studi komparatif framework pengembangan aplikasi web mengindikasikan bahwa pemilihan arsitektur dan kerangka kerja yang tepat berkontribusi pada efisiensi eksekusi dan kemudahan pemeliharaan sistem (Sismadi et al., 2021; Sismadi et al., 2022).

Namun demikian, keberhasilan arsitektur *microservices* tidak hanya ditentukan oleh desain teknis. Stabilitas layanan sangat dipengaruhi oleh praktik DevOps, termasuk penggunaan *monitoring tools* untuk observabilitas sistem secara real-time (Giamattei et al., 2024). Tanpa mekanisme pemantauan yang memadai, sistem terdistribusi berpotensi mengalami degradasi performa yang sulit terdeteksi. Oleh karena itu, tata kelola operasional menjadi komponen krusial dalam menjamin keberlanjutan sistem.

Evaluasi Pendekatan WebAssembly dalam Pemrosesan Biometrik

Pemanfaatan WebAssembly (WASM) sebagai lingkungan eksekusi komputasi sisi klien memberikan kontribusi signifikan terhadap efisiensi arsitektur yang diusulkan. WebAssembly memungkinkan eksekusi kode komputasi intensif langsung di dalam *browser* dengan performa mendekati aplikasi *native* (Ray, 2023). Pendekatan ini merepresentasikan pergeseran paradigma dari pemrosesan terpusat menuju komputasi berbasis *edge*, di mana proses deteksi dan ekstraksi fitur wajah dilakukan sedekat mungkin dengan sumber data.

Dengan memindahkan pemrosesan citra ke sisi klien, sistem tidak lagi mengirimkan citra mentah ke server, melainkan hanya fitur hasil ekstraksi. Strategi ini secara signifikan mengurangi konsumsi *bandwidth* dan latensi jaringan. Model arsitektur semacam ini juga relevan dalam konteks IoT yang membutuhkan responsivitas tinggi (Ray, 2023). Dari perspektif keamanan, diversifikasi kode WebAssembly terbukti meningkatkan ketahanan terhadap

eksploitasi *malware* (Cabrera-Arteaga et al., 2023), sehingga relevan untuk sistem yang memproses data identitas sensitif.

Pendekatan ini juga secara implisit mendukung prinsip minimisasi data (*data minimization principle*), karena server tidak menyimpan atau memproses citra wajah secara langsung. Dalam konteks keamanan aplikasi web, penguatan lapisan proteksi melalui penerapan *Anti-CSRF token*, *Content Security Policy* (CSP), dan mekanisme *anti-clickjacking* semakin memperkuat integritas sistem (Wibowo & Riadi, 2025). Upaya peningkatan kesadaran keamanan siber pada pengguna dan pengelola sistem juga menjadi bagian penting dalam mitigasi risiko (Habie et al., 2024).

Analisis Akurasi Pengenalan Wajah

Pengujian sistem menunjukkan nilai *precision* 0,93, *recall* 0,95, dan *F1-score* 0,94, yang mengindikasikan keseimbangan antara sensitivitas dan spesifisitas sistem. Dalam konteks presensi pendidikan, tingkat akurasi ini tergolong memadai untuk implementasi operasional. Penelitian sebelumnya menunjukkan bahwa sistem presensi berbasis pengenalan wajah mampu meningkatkan efisiensi administrasi dan mengurangi potensi manipulasi kehadiran (Alniemi & Mahmood, 2023; Jadhav et al., 2024; Boe et al., 2024; Lateef & Kamil, 2024).

Pendekatan berbasis *deep learning* umumnya memiliki ketahanan lebih baik terhadap variasi pencahayaan dan ekspresi wajah dibandingkan metode konvensional (Warman & Kusuma, 2023; Yadav, 2024). Selain itu, model *lightweight* seperti GhostFaceNets membuktikan bahwa optimalisasi arsitektur jaringan dapat mempertahankan akurasi tinggi dengan kompleksitas komputasi rendah (Alansari et al., 2023). Hal ini membuka peluang integrasi model ringan dalam arsitektur berbasis WebAssembly untuk meningkatkan *robustness* tanpa membebani sisi klien secara berlebihan.

Kontribusi penelitian di bidang pengolahan citra digital juga memperkuat landasan teknis sistem ini. Teknik segmentasi berbasis *hidden Markov tree* (Murinto & Aribowo, 2016), peningkatan kualitas citra melalui *contrast stretching* dan *unsharp masking* (Murinto et al., 2017), serta segmentasi hiperspektral berbasis *independent component analysis* dan optimasi swarm (Murinto & Ismi, 2019; Murinto et al., 2019) menunjukkan bahwa kualitas ekstraksi fitur sangat menentukan performa klasifikasi. Bahkan pendekatan berbasis ruang warna HSV dengan klasifikasi Naïve Bayes turut membuktikan pentingnya pemilihan fitur visual yang tepat (Khisanudin & Murinto, 2020).

Implikasi Keamanan dan Ketahanan Sistem

Dalam sistem biometrik berbasis pembelajaran mesin, ancaman *adversarial attack* menjadi risiko yang tidak dapat diabaikan. Serangan ini mampu memanipulasi input visual sehingga model melakukan klasifikasi yang salah tanpa terdeteksi (Costa et al., 2024). Oleh karena itu, penerapan presensi berbasis wajah dalam skala produksi memerlukan mekanisme mitigasi tambahan seperti *liveness detection* dan autentikasi multi-faktor. Sistem portabel dengan deteksi keaktifan terbukti meningkatkan keamanan terhadap serangan *spoofing* (Surantha & Sugijakko, 2024).

Integrasi arsitektur *microservices* juga membuka peluang penerapan lapisan keamanan tambahan, termasuk pemanfaatan *blockchain* untuk menjaga integritas data presensi dalam lingkungan terdistribusi (Alshudukhi et al., 2023). Di sisi lain, evaluasi keamanan LMS melalui pendekatan *penetration testing* berbasis ISSAF dan OWASP ZAP menunjukkan bahwa sistem pendidikan daring rentan terhadap berbagai eksploitasi jika tidak diaudit secara berkala (Umar

et al., 2024a, 2024b). Dengan demikian, keamanan harus dipandang sebagai bagian integral dari desain arsitektur, bukan sekadar fitur tambahan.

Relevansi terhadap Ekosistem LMS dan Analitik Pendidikan

Sistem presensi biometrik yang efisien memiliki implikasi luas terhadap ekosistem LMS. Data kehadiran yang akurat dapat menjadi variabel penting dalam model prediksi performa mahasiswa berbasis *machine learning* (Ahmed, 2024). Integrasi sistem presensi berbasis WebAssembly dan *microservices* memungkinkan pengolahan data secara real-time dengan latensi rendah, sehingga mendukung analitik pembelajaran berbasis data.

Otomatisasi presensi melalui pengenalan wajah juga terbukti meningkatkan efisiensi manajemen kelas serta mengurangi potensi manipulasi kehadiran (Boe et al., 2024). Dengan demikian, kontribusi penelitian ini tidak hanya terletak pada peningkatan performa teknis, tetapi juga pada penguatan transformasi digital dalam sistem pembelajaran tinggi yang adaptif, aman, dan berbasis analitik.

Sintesis Pembahasan

Secara keseluruhan, integrasi WebAssembly dan arsitektur *microservices* menunjukkan peningkatan signifikan pada latensi dan *throughput* sistem presensi daring tanpa mengorbankan akurasi biometrik. Pendekatan ini menggabungkan optimasi arsitektural, efisiensi komputasi sisi klien, serta penguatan keamanan sistem. Meskipun metode konvensional yang digunakan telah menunjukkan performa stabil, peluang pengembangan lebih lanjut terbuka melalui integrasi model *deep learning* ringan, mekanisme keamanan berlapis, serta penerapan teknologi integritas data seperti *blockchain*. Dengan demikian, arsitektur yang diusulkan memiliki potensi menjadi model referensi dalam pengembangan sistem presensi biometrik berbasis web yang skalabel, aman, dan berkelanjutan.

KESIMPULAN

Penelitian ini telah berhasil merancang, mengimplementasikan, dan mengevaluasi arsitektur presensi daring berbasis pengenalan wajah dengan mengintegrasikan *WebAssembly* dan *Microservices* pada lingkungan Learning Management System. Permasalahan utama yang diangkat, yaitu tingginya latensi dan keterbatasan skalabilitas pada sistem presensi biometrik berbasis pemrosesan terpusat, dapat diatasi melalui pemisahan beban komputasi antara sisi klien dan server. Hasil pengujian menunjukkan bahwa pemrosesan deteksi dan ekstraksi fitur wajah di sisi klien mampu menurunkan latensi presensi secara signifikan serta meningkatkan *throughput* sistem tanpa mengorbankan tingkat akurasi yang dibutuhkan untuk skenario presensi pendidikan.

Evaluasi empiris yang dilakukan membuktikan bahwa arsitektur hybrid berbasis *WebAssembly* dan *Microservices* merupakan solusi arsitektural yang efektif dan layak diterapkan untuk aplikasi biometrik real-time berbasis web. Keberadaan artefak aplikasi web sebagai bukti konsep juga memperkuat validitas hasil penelitian serta memungkinkan replikasi dan verifikasi oleh peneliti lain. Sebagai pengembangan penelitian selanjutnya, disarankan untuk mengeksplorasi penggunaan metode pengenalan wajah berbasis *deep learning* ringan yang dioptimalkan untuk dijalankan pada *WebAssembly*, sehingga akurasi dapat ditingkatkan tanpa mengorbankan kinerja. Selain itu, penelitian lanjutan dapat difokuskan pada evaluasi

arsitektur pada skala pengguna yang lebih besar, penerapan mekanisme keamanan dan perlindungan data biometrik yang lebih kuat, serta pengujian strategi komunikasi dan orkestrasi *Microservices* untuk mendukung implementasi sistem presensi daring pada lingkungan produksi berskala besar.

DAFTAR PUSTAKA

- Abdelfattah, A. S., & Cerny, T. (2023). Roadmap to reasoning in microservice systems: A rapid review. *Applied Sciences*, 13(3). <https://doi.org/10.3390/app13031838>
- Abgaz, Y., et al. (2023). Decomposition of monolith applications into microservices architectures: A systematic review. *IEEE Transactions on Software Engineering*, 49(8). <https://doi.org/10.1109/TSE.2023.3287297>
- Ahmed, E. (2024). Student performance prediction using machine learning algorithms. *Applied Computational Intelligence and Soft Computing*, 2024. <https://doi.org/10.1155/2024/4067721>
- Alansari, M., et al. (2023). GhostFaceNets: Lightweight face recognition model from cheap operations. *IEEE Access*, 11. <https://doi.org/10.1109/ACCESS.2023.3266068>
- Alniemi, O., & Mahmood, H. F. (2023). Class attendance system based on face recognition. *Revue d'Intelligence Artificielle*, 37(5). <https://doi.org/10.18280/ria.370517>
- Alshudukhi, K. S., et al. (2023). An interoperable blockchain security framework based on microservices and smart contracts in IoT environment. *Electronics*, 12(3). <https://doi.org/10.3390/electronics12030776>
- Boe, C. H., et al. (2024). An automated face detection and recognition for class attendance. *International Journal on Informatics Visualization*, 8(3). <https://doi.org/10.62527/joiv.8.3.2967>
- Cabrera-Arteaga, J., et al. (2023). WebAssembly diversification for malware evasion. *Computers & Security*, 131. <https://doi.org/10.1016/j.cose.2023.103296>
- Chamari, L., Petrova, E., & Pauwels, P. (2023). An end-to-end implementation of a service-oriented architecture for data-driven smart buildings. *IEEE Access*, 11. <https://doi.org/10.1109/ACCESS.2023.3325767>
- Costa, J. C., et al. (2024). How deep learning sees the world: A survey on adversarial attacks and defenses. *IEEE Access*, 12. <https://doi.org/10.1109/ACCESS.2024.3395118>
- Giamattei, L., et al. (2024). Monitoring tools for DevOps and microservices: A systematic grey literature review. *Journal of Systems and Software*, 208. <https://doi.org/10.1016/j.jss.2023.111906>
- Habie, K. F., Putro, A. P., Yuliansyah, H., & Riadi, I. (2024). Peningkatan cyber security awareness melalui pelatihan edukatif kepada siswa sekolah menengah kejuruan. *Mohuyula: Jurnal Pengabdian Kepada Masyarakat*, 3(2), 46–53. <https://doi.org/10.31314/mohuyula.3.2.46-53.2024>
- Jadhav, A., et al. (2024). Attendance management system using face recognition. *IAES International Journal of Artificial Intelligence*, 13(1), 673–679.

<https://doi.org/10.11591/ijai.v13.i1.pp673-679>

- Khisanudin, I. S., & Murinto. (2020). Dragon fruit maturity detection based on HSV space color using Naive Bayes classifier method. *IOP Conference Series: Materials Science and Engineering*, 771(1). <https://doi.org/10.1088/1757-899X/771/1/012022>
- Lateef, A. S., & Kamil, M. Y. (2024). Face recognition-based automatic attendance system in a smart classroom. *Iraqi Journal for Electrical and Electronic Engineering*, 20(1). <https://doi.org/10.37917/ijeec.20.1.4>
- Murinto, & Aribowo, E. (2016). Image segmentation using hidden Markov tree methods in recognizing motif of batik. *Journal of Theoretical and Applied Information Technology*, 85(1).
- Murinto, & Ismi, D. P. (2019). Hyperspectral image segmentation using discriminant independent component analysis and swarm optimization approaches. *IOP Conference Series: Materials Science and Engineering*, 674(1). <https://doi.org/10.1088/1757-899X/674/1/012054>
- Murinto, Winiarti, S., Ismi, D. P., & Prahara, A. (2017). Image enhancement using piecewise linear contrast stretch methods based on unsharp masking algorithms for leather image processing. In *Proceedings of the 3rd International Conference on Science in Information Technology (ICSITech 2017)*. <https://doi.org/10.1109/ICSITech.2017.8257197>
- Murinto, Astuti, N. R. D. P., & Mardhia, M. (2019). Multilevel thresholding hyperspectral image segmentation based on independent component analysis and swarm optimization methods. *International Journal of Advances in Intelligent Informatics*, 5(1). <https://doi.org/10.26555/ijain.v5i1.311>
- Ray, P. P. (2023). An overview of WebAssembly for IoT: Background, tools, state-of-the-art, challenges, and future directions. *Future Internet*, 15(8). <https://doi.org/10.3390/fi15080275>
- Sismadi, W., Darmawan, I., Wahyudi, W., & Nicolas, P. P. (2021). Implementasi pengembangan aplikasi ujian online menggunakan KTUPAD MVC framework. *Jurnal Ekonomi Manajemen Sistem Informasi*, 2(4). <https://doi.org/10.31933/jemsi.v2i4.437>
- Sismadi, W., Martono, B. A., & Widyastuti, T. (2022). Comparative analysis of CodeIgniter, Laravel and KTUPAD frameworks: Case study online exam applications. *Indonesian Journal of Applied Research (IJAR)*, 3(3).*
- Sismadi, W., Martono, B. A., Hartini, E. F., & Putri, D. W. (2025). Implementasi arsitektur microservice pada aplikasi bank sampah digital berbasis DonatJS. *Cendekia: Jurnal Ilmu Pengetahuan*, 5(4). <https://doi.org/10.51878/cendekia.v5i4.7140>
- Surantha, N., & Sugijakko, B. (2024). Lightweight face recognition-based portable attendance system with liveness detection. *Internet of Things*, 25. <https://doi.org/10.1016/j.iot.2024.101089>
- Umar, R., Riadi, I., & Wicaksono, S. A. (2024a). Security analysis of learning management

- system using penetration testing with ISSAF framework. *PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic*, 12(1).
<https://doi.org/10.33558/piksel.v12i1.8331>
- Umar, R., Riadi, I., & Wicaksono, S. A. (2024b). Application of OWASP ZAP framework for security analysis of LMS using pentest method. *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, 10(2).* <https://doi.org/10.33480/jitk.v10i2.5534>
- Velepucha, V., & Flores, P. (2023). A survey on microservices architecture: Principles, patterns and migration challenges. *IEEE Access*, 11.
<https://doi.org/10.1109/ACCESS.2023.3305687>
- Warman, G. P., & Kusuma, G. P. (2023). Face recognition for smart attendance system using deep learning. *Communications in Mathematical Biology and Neuroscience*, 2023.
<https://doi.org/10.28919/cmbn/7872>
- Wibowo, M. A. P., & Riadi, I. (2025). Analysis and enhancement of website security using anti-CSRF token, CSP, and anti-clickjacking approaches. *International Journal of Computer Applications*, 187(22).* <https://doi.org/10.5120/ijca2025925362>
- Yadav, S. (2024). Survey paper on face recognition based attendance system. *International Journal of Scientific Research in Engineering and Management*, 8(4).*
<https://doi.org/10.55041/ijcsrem30710>