JOISIE (Journal Of Information Systems And Informatics Engineering)
Vol. 10, No.1, Juni 2026, Hlm 42-52
Received: 26 April 2026 Revised: 26 Juni 2026, Accepted: 29 Juli 2026

p- ISSN: 2503-5304
e- ISSN: 2527-3116

DUAL-LAYER ANTI-SPOOFING UNTUK SISTEM PRESENSI MENGGUNAKAN CONVOLUTIONAL NEURAL NETWORK DAN GEOFENCING HAVERSINE

Yermis Duha[1)], Gusrio Tendra[2)], Wilda Susanti[3)], Wahyu Joni Kurniawan[4)], Nicholas Renaldo[5)]
[1,2]Program Studi Sistem Informasi, Institut Bisnis dan Teknologi Pelita Indonesia, Jl. Srikandi No.1, Pekanbaru, Riau
[2,3,4]Teknik Informatika, Institut Bisnis dan Teknologi Pelita Indonesia, Jl. Srikandi No.1, Pekanbaru, Riau
email: yermias@lecturer.pelitaindonesia.ac.id[1], gusrio.tendra@lecturer.pelitaindonesia.ac.id[2], wilda@lecturer.pelitaindonesia.ac.id[3], wahyu.kurniawan@lecturer.pelitaindonesia.ac.id[4], nicholasrenaldo@lecturer.pelitaindonesia.ac.id[5]

Abstract

Web-based attendance systems face two main vectors of fraud: GPS spoofing and biometric spoofing via photos, video replays, or AI-based deepfakes. Existing solutions generally address only one of these threats, leaving a critical security gap. This research proposes and validates a two-layer security framework that prevents both threats simultaneously through client-side liveness detection and server-side geofencing. Liveness Detection uses a MobileNetV1-based Convolutional Neural Network via the face-api.js library, which runs entirely in the browser. Users must maintain a smiling expression with a probability of ≥0.70 for 1.5 seconds before attendance is recorded. Location authenticity is verified on the server side using the Haversine Formula; submissions exceeding a 50-meter radius are rejected with an HTTP 403 response. The system was developed using the Waterfall methodology with a Flask backend and an SQLite database. Evaluation was conducted through structured security scenario testing that measured the True Positive Rate (TPR), False Acceptance Rate (FAR), and geofencing accuracy under both stable GPS conditions and manipulated coordinates. Out of 40 liveness tests, the system achieved a TPR of 95%, a FAR of 0% against static photo attacks, and 100% geofencing accuracy under stable GPS conditions. This study clearly demonstrates that client-side geofencing can be bypassed via browser-based sensor emulation, a vulnerability that is fully mitigated by server-side validation. The proposed framework provides resilience against presentation and location spoofing attacks without requiring the installation of a native application. These findings need to be validated on a larger sample of participants, given that the dataset is limited to 40 liveness tests and 6 geofencing scenarios. Future research should prioritize resilience against real-time deepfakes and mitigation of GPS degradation indoors.

Keywords: *Anti-Spoofing, Convolutional Neural Network, Dual-Layer Security, Haversine Formula, Liveness Detection*

Abstrak

Sistem absensi berbasis web menghadapi dua vektor penipuan utama yaitu pemalsuan GPS dan pemalsuan biometrik melalui foto, *video replay*, atau *deepfake* berbasis AI. Solusi yang ada umumnya hanya mengatasi satu ancaman, meninggalkan celah keamanan yang kritis. Penelitian ini mengusulkan dan memvalidasi kerangka kerja keamanan dua lapis yang mencegah kedua ancaman secara bersamaan melalui *Liveness Detection* sisi klien dan *geofencing* sisi server. *Liveness Detection* menggunakan *Convolutional Neural Network* berbasis MobileNetV1 melalui pustaka *face-api.js* yang berjalan sepenuhnya di *browser*. Pengguna harus mempertahankan ekspresi senyum dengan probabilitas ≥0,70 selama 1,5 detik sebelum absensi diaktifkan. Otentisitas lokasi diverifikasi di sisi server menggunakan Rumus *Haversine* dengan pengiriman melebihi radius 50 meter ditolak dengan HTTP 403. Sistem dikembangkan menggunakan metodologi *Waterfall* dengan *backend* Flask dan basis data SQLite. Evaluasi dilakukan melalui pengujian skenario keamanan terstruktur yang mengukur *True Positive Rate* (TPR), *False Acceptance Rate* (FAR), dan akurasi *geofencing* pada kondisi GPS stabil maupun koordinat yang dimanipulasi. Dari 40 percobaan *liveness*, sistem menghasilkan TPR 95%, FAR 0% terhadap serangan foto statis, dan akurasi *geofencing* 100% pada kondisi GPS stabil. Penelitian ini membuktikan secara nyata bahwa *geofencing* pada sisi klien dapat

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

dilewati melalui *Sensor Emulation browser* dengan celah yang dieliminasi sepenuhnya oleh validasi sisi server. Kerangka kerja yang diusulkan memberikan ketahanan terhadap serangan presentasi dan penipuan lokasi tanpa instalasi aplikasi *native*. Temuan ini perlu divalidasi pada partisipan yang lebih besar, mengingat dataset terbatas pada 40 percobaan *liveness* dan 6 skenario *geofencing*. Penelitian lanjutan diprioritaskan pada ketahanan terhadap *deepfake real-time* dan mitigasi degradasi GPS dalam ruangan.

Kata Kunci: Anti-Spoofing, Convolutional Neural Network, Dual-Layer Security, Haversine Formula, Liveness Detection

1. PENDAHULUAN

Transformasi digital yang dipercepat oleh era Industri 4.0 dan adopsi sistem kerja hibrida pasca pandemi COVID-19 telah mendorong migrasi masif sistem pencatatan kehadiran dari mekanisme fisik ke platform berbasis *web* dan *mobile* di seluruh sektor (Abdelraheem et al., 2021). Survei terbaru terhadap organisasi di Asia Tenggara menunjukkan bahwa lebih dari 67% perusahaan telah mengimplementasikan atau berencana mengimplementasikan sistem presensi digital pada 2025, seiring ekspansi model kerja terdistribusi yang berkelanjutan (Gunawan & Ikhwan, 2024). Sistem presensi konvensional berbasis sidik jari atau kartu RFID tidak lagi relevan untuk skenario kerja lintas lokasi karena keterbatasan infrastruktur fisik, risiko kontak langsung, serta ketidakmampuan memverifikasi keberadaan karyawan secara spasial (Apriadi & Sutrisna, 2023)

Platform web menawarkan keunggulan aksesibilitas yang signifikan dapat diakses dari berbagai perangkat tanpa instalasi namun keunggulan ini berbanding lurus dengan peningkatan permukaan serangan (*attack surface*) yang harus dikelola. Dua vektor ancaman yang mendominasi kasus kecurangan presensi daring saat ini adalah: (1) manipulasi lokasi (GPS *spoofing*) menggunakan aplikasi pihak ketiga yang mengirimkan koordinat palsu ke sistem, dan (2) serangan presentasi biometrik (*presentation attack*) yang memanfaatkan foto cetak, *video replay*, atau seiring berkembangnya AI generatif wajah *deepfake* sintetis untuk mengelabui sistem verifikasi wajah (Budiarto Hadiprakoso & Buana, 2021; Shinde et al., 2025). Ancaman *deepfake* kini menjadi perhatian kritis dimana laporan industri mencatat peningkatan 245% insiden *deepfake* pada sistem verifikasi identitas antara 2023 dan 2025, dengan serangan *deepfake real-time* yang mampu mensimulasikan ekspresi dinamis mulai mengancam sistem liveness detection berbasis *challenge-response* sederhana (Das et al., 2025).

Tinjauan sistematis terhadap literatur mengungkap kesenjangan solusi yang konsisten. Penelitian yang berfokus pada validasi lokasi seperti (Mutaqin & Nurhayati, 2023) dan (Prasojo & Cahyaningtyas, 2025) berhasil mengimplementasikan Haversine Formula untuk pembatasan radius presensi, namun umumnya dikembangkan sebagai aplikasi native Android. Di sisi lain, penelitian yang menitikberatkan pada pengenalan wajah seperti (Yeovandi et al., 2025) dan (Nurhakim et al., 2025) memerlukan sumber daya komputasi substansial yang tidak optimal untuk lingkungan browser. Sistem serupa yang dibangun dengan *Python-Streamlit* dan *geofencing* dua tahap (Babu et al., 2025) membuktikan bahwa integrasi validasi lokasi-wajah pada platform web adalah pendekatan yang layak, namun belum mengekspos kerentanan *client-side* secara eksplisit. Sebagian besar sistem berbasis web hanya melakukan *face matching* statis tanpa *liveness detection*, menciptakan celah terhadap *presentation attack* (Wibowo & Setiawan, 2024).

Kelemahan kritis yang kerap diabaikan adalah penempatan logika validasi lokasi. Sistem yang mengandalkan validasi sisi klien (*client-side geofencing via JavaScript*) sangat rentan terhadap manipulasi melalui fitur *Sensor Emulation* pada *browser developer tools* atau injeksi skrip eksternal. Teknik ini bahkan dapat dilakukan oleh pengguna non-teknis menggunakan ekstensi *browser* yang tersedia secara bebas (Wibowo & Setiawan, 2024).

Kondisi ini merupakan celah fundamental yang memungkinkan kecurangan bahkan pada sistem yang telah mengimplementasikan *geofencing*. Fakta ini membuktikan bahwa validasi sisi klien hanyalah ilusi keamanan (*security theater*) yang tidak dapat dijadikan andalan dalam sistem presensi yang memiliki implikasi administratif dan finansial. Oleh karena itu, pemindahan seluruh logika validasi ke sisi server merupakan keharusan arsitektural, bukan sekadar pilihan optimasi.

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

Penelitian ini berbeda secara fundamental dari penelitian terdahulu dalam beberapa aspek. Berbeda dengan (Mutaqin & Nurhayati, 2023) dan (Prasojo & Cahyaningtyas, 2025) yang hanya menerapkan Haversine di sisi klien tanpa mekanisme *liveness detection*, penelitian ini mengintegrasikan keduanya secara bersamaan dalam satu platform web ringan. Berbeda pula dengan (Nurhakim et al., 2025) yang menggunakan *deep learning* PAD namun tidak menyertakan validasi lokasi, penelitian ini memberikan perlindungan ganda terhadap dua vektor ancaman sekaligus. Keunikan utama penelitian ini adalah demonstrasi empiris eksplisit terhadap kerentanan arsitektur *client-side validation* yang selama ini diabaikan dalam literatur, serta pembuktian bahwa *server-side enforcement* adalah satu-satunya mitigasi yang efektif terhadap manipulasi koordinat GPS.

Berdasarkan analisis kesenjangan tersebut, penelitian ini mengusulkan, mengimplementasikan, dan memvalidasi secara empiris arsitektur sistem presensi web berlapis keamanan ganda (*dual-layer security*) yang dirancang menutup kedua vektor ancaman secara simultan dalam lingkungan ringan berbasis browser. Kontribusi utama penelitian ini mencakup: (1) integrasi *Liveness Detection* berbasis CNN (arsitektur MobileNetV1) yang berjalan seluruhnya di sisi klien sebagai *Presentation Attack Detection* (PAD) tingkat dasar; (2) implementasi *server-side geofencing* menggunakan Haversine Formula dalam Python sebagai mitigasi terhadap manipulasi koordinat GPS; (3) demonstrasi empiris kerentanan arsitektural *client-side validation* melalui pengujian Sensor Emulation; dan (4) evaluasi komparatif terhadap sistem terdahulu beserta peta jalan pengembangan terhadap ancaman *deepfake* generasi berikutnya.

2. METODE PENELITIAN

Penelitian ini mengadopsi model pengembangan perangkat lunak *Waterfall* yang terdiri dari empat fase berurutan: (1) Analisis Kebutuhan identifikasi vektor ancaman dan spesifikasi fungsional; (2) Desain Sistem perancangan arsitektur *dual-layer*, alur kerja autentikasi, dan skema basis data; (3) Implementasi pengkodean komponen *frontend liveness* dan *backend geofencing*; serta (4) Pengujian dan Validasi eksekusi skenario serangan terstruktur dan analisis metrik keamanan. Model Waterfall dipilih karena ruang lingkup sistem yang telah terdefinisi dengan baik, kebutuhan dokumentasi ketat untuk reprodusibilitas, serta kesesuaiannya dengan penelitian purwarupa berorientasi validasi (Pangihutan Sitanggang et al., 2025).

Model *Waterfall* berkontribusi langsung terhadap kualitas sistem melalui tiga mekanisme. Pertama, fase Analisis Kebutuhan yang dilakukan secara menyeluruh memastikan seluruh vektor ancaman teridentifikasi sebelum implementasi dimulai, mencegah perubahan desain arsitektur di tengah pengembangan yang berpotensi menimbulkan celah keamanan baru. Kedua, pemisahan fase Desain dan Implementasi mendorong pendokumentasian arsitektur *dual-layer* secara eksplisit sebelum pengkodean, sehingga keputusan penempatan logika Haversine di sisi server dapat divalidasi pada level desain. Ketiga, fase Pengujian dan Validasi yang terpisah dan terstruktur memungkinkan evaluasi skenario serangan dilakukan secara sistematis dan terdokumentasi, meningkatkan reprodusibilitas hasil penelitian. Alur kerja sistem secara keseluruhan digambarkan pada Gambar 1.

Gambar 1. Diagram Alir Sistem Presensi Berbasis Web Dual-Layer Security

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

2.1 Arsitektur dan Tumpukan Teknologi

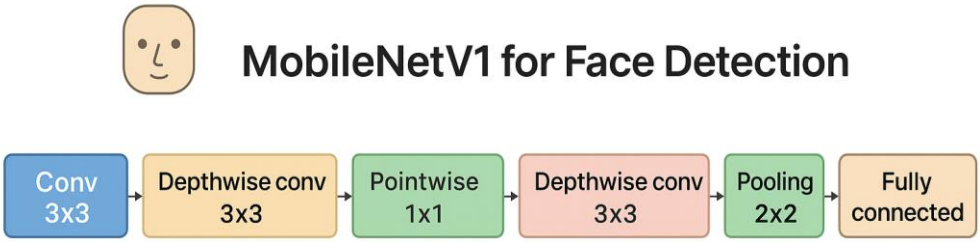
Sistem dibangun menggunakan arsitektur *client-server* dengan pemisahan tanggung jawab yang tegas berdasarkan prinsip *defense-in-depth*. Sisi server (*backend*) menggunakan Python 3.9 dengan framework Flask 2.3 sebagai lapisan aplikasi web. Basis data SQLite dipilih untuk lingkungan purwarupa karena karakteristiknya yang *serverless* dan bebas konfigurasi, untuk skenario produksi skala besar, migrasi ke PostgreSQL atau MySQL direkomendasikan. Sisi klien (*frontend*) menggunakan HTML5 dan Vanilla JavaScript yang mengintegrasikan pustaka *face-api.js* versi 0.22.2. Seluruh pemrosesan citra wajah dilakukan secara lokal di peramban tanpa mengirimkan data biometrik ke server, selaras dengan prinsip data *minimization* dan persyaratan privasi yang semakin ketat di bawah regulasi perlindungan data (Atmawijaya & Radiyah, 2024). Komunikasi antara klien dan server dienkripsi menggunakan TLS 1.3 untuk mencegah intersepsi data koordinat GPS dan snapshot wajah dalam transmisi.

2.2 Algoritma Liveness Detection Berbasis CNN

Liveness Detection adalah komponen krusial dalam sistem autentikasi biometrik *modern* yang bertujuan membedakan antara wajah pengguna asli yang hadir secara fisik dengan Instrumen Serangan Presentasi (*Presentation Attack Instruments* / PAI) berupa foto, video replay, atau topeng (Das et al., 2025; Shinde et al., 2025). Dalam konteks sistem presensi, *liveness* berfungsi sebagai lapisan pertahanan pertama terhadap *proxy attendance* upaya mendaftarkan kehadiran tanpa kehadiran fisik. Lanskap ancaman terus berkembang, sementara serangan 2D (foto, video) dapat diatasi dengan metode berbasis ekspresi, serangan *deepfake real-time* yang menggunakan AI generatif untuk mensimulasikan ekspresi dinamis mulai muncul sebagai vektor ancaman generasi berikutnya yang memerlukan pertahanan berlapis (Kuznetsov & others, 2025).

Dalam penelitian ini, *liveness* diverifikasi melalui tantangan ekspresi dinamis berbasis *active liveness* mewajibkan pengguna menampilkan ekspresi senyum (*happy expression*) di hadapan kamera secara *real-time*. Pendekatan *active liveness* dipilih karena memberikan keseimbangan yang baik antara keamanan dan kemudahan pengguna untuk *deployment browser* tanpa infrastruktur sensor tambahan (*infrared, depth camera*).

Model CNN yang digunakan adalah *Single Shot Multibox Detector* (SSD) dengan *backbone* MobileNetV1, diakses melalui pustaka *face-api.js* versi 0.22.2. MobileNetV1 dipilih karena efisiensinya dalam inferensi *real-time* di CPU *browser* menggunakan *depthwise separable convolutions*, yang menjadikannya lebih ringan secara komputasi dibandingkan arsitektur konvensional seperti VGG atau ResNet (Maulana et al., 2023). Dalam penelitian ini, model dimanfaatkan langsung dari pustaka *face-api.js* yang telah mengemas bobot model terlatih untuk deteksi dan klasifikasi ekspresi wajah secara *real-time*. Arsitektur CNN ditampilkan pada Gambar 2.



Gambar 2. Arsitektur CNN MobileNetV1 untuk Liveness Detection via face-api.js

Pipeline inferensi CNN beroperasi dalam tiga tahap berurutan: (1) *Face Detection* menggunakan *Tiny Face* Detector berbasis CNN ringan untuk mendeteksi *bounding box* wajah pada setiap *frame*; (2) *Facial Landmark Detection* yang mengidentifikasi posisi 68 titik fitur wajah kritis (kontur bibir, sudut mata, hidung, rahang); dan (3) *Expression Classification* yang menganalisis distribusi landmark untuk mengklasifikasikan probabilitas tujuh ekspresi dasar (*neutral, happy, sad, angry, fearful, disgusted, surprised*).

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

Sistem menetapkan ambang batas (*threshold*) probabilitas ekspresi *happy* sebesar 0,70 dan durasi validasi minimal 1,5 detik. Kedua nilai ini ditentukan melalui serangkaian pengujian awal (*pilot testing*) dengan N=10 percobaan pada variasi kondisi pencahayaan dan jarak kamera, untuk menemukan titik keseimbangan antara *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR). *Threshold* sebesar 0,70 dipilih karena nilai yang lebih rendah (misalnya 0,50) meningkatkan risiko *bypassing* oleh foto dengan kontras tinggi, sedangkan nilai yang lebih tinggi (misalnya 0,85) menolak pengguna sah pada kondisi pencahayaan *non-ideal*. Durasi 1,5 detik dipilih untuk mengurangi *false positives* akibat gerakan wajah sesaat tanpa mengorbankan kenyamanan pengguna secara signifikan.

Perlu dicatat bahwa sumber data pelatihan model yang digunakan dalam pustaka *face-api.js* tidak didokumentasikan secara terbuka oleh pengembangnya. Hal ini merupakan keterbatasan dalam menilai generalisasi model terhadap variasi demografis, kondisi pencahayaan ekstrem, atau kelompok usia tertentu. Implikasi dari keterbatasan ini terhadap performa sistem dibahas lebih lanjut dalam bagian keterbatasan penelitian.

2.3 Algoritma Validasi Lokasi Menggunakan Haversine Formula

Haversine Formula adalah persamaan trigonometri bola yang menghitung jarak busur terpendek (*great-circle distance*) antara dua titik koordinat di permukaan bumi (Mutaqin & Nurhayati, 2023; Ode Hazani, 2024). Formula ini dipilih karena memberikan akurasi tinggi untuk jarak pendek yang relevan dengan aplikasi *geofencing*, dengan kesalahan perhitungan di bawah 0,01 meter untuk jarak di bawah 1 km yang jauh melampaui presisi GPS konsumen yang berkisar 3-20 meter (Prasojo & Cahyaningtyas, 2025).

Dalam penelitian ini, *Haversine Formula* diimplementasikan dalam Python di sisi server untuk menghitung jarak antara koordinat yang dikirimkan pengguna dan titik pemeriksaan yang terdaftar. Persamaan matematis Haversine Formula adalah sebagai berikut:

$$a = \sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1) \times \cos(\phi_2) \times \sin^2\left(\frac{\Delta\lambda}{2}\right) \quad (1)$$

$$c = 2 \times \operatorname{atan2}\left(\sqrt{a}, \sqrt{1-a}\right) \quad (2)$$

$$d = R \times c \quad (3)$$

Di mana φ adalah lintang dalam radian, λ adalah bujur dalam radian, R adalah jari-jari bumi rata-rata (6.371 km berdasarkan standar GRS80), dan d adalah jarak hasil perhitungan. Penelitian ini menetapkan *geofence* radius 50 meter berdasarkan dua pertimbangan. Pertama, akurasi GPS konsumen yang umumnya berkisar 3-20 meter (Prasojo & Cahyaningtyas, 2025) memerlukan toleransi minimal dua kali lipat dari *worst-case error* untuk menghindari penolakan pengguna yang secara fisik berada di lokasi yang benar. Kedua, berdasarkan pengujian awal di lingkungan kerja yang menjadi konteks implementasi, radius 50 meter mencakup area fisik yang relevan (gedung dan area parkir terdekat) tanpa memperluas zona presensi ke luar batas properti. Radius yang lebih kecil dari 20 meter berisiko menolak pengguna dengan kondisi GPS tidak stabil di dalam gedung, sedangkan radius di atas 100 meter berpotensi membuka celah bagi presensi dari lokasi terdekat yang tidak sah.

Aspek arsitektural yang paling kritis dari implementasi ini adalah penempatan logika Haversine sepenuhnya di sisi server dalam Python, bukan di sisi klien menggunakan JavaScript. Validasi *client-side*, meskipun dapat mengurangi latensi, dapat dilewati secara *trivial* oleh pengguna yang menggunakan fitur Sensor Emulation pada Chrome DevTools, ekstensi browser pemalsuan lokasi, atau skrip injeksi yang memodifikasi objek navigator *geolocation*. Pemindahan seluruh logika validasi ke server memastikan bahwa meskipun data koordinat yang dikirimkan dimanipulasi, server akan mendeteksi anomali secara mandiri dan menolak permintaan dengan kode status HTTP 403 Forbidden. Ini merupakan implementasi prinsip 'never trust client input' dalam rekayasa keamanan perangkat lunak (Babu et al., 2025).

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

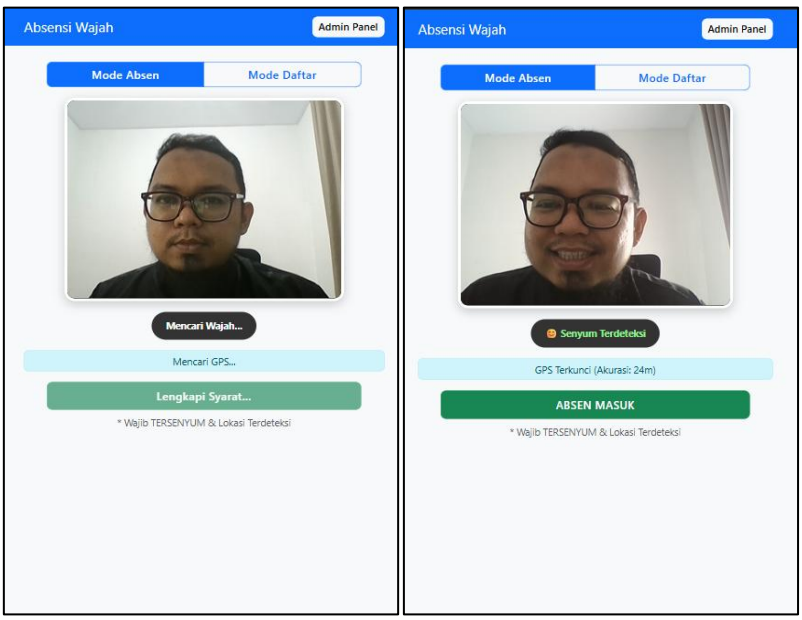
2.4 Alur Kerja dan Protokol Autentikasi Berlapis

Protokol autentikasi berlapis dirancang untuk memastikan bahwa kedua kondisi *liveness* wajah dan keberadaan fisik dalam *geofence* harus terpenuhi secara bersamaan agar presensi diterima. Alur kerja beroperasi dalam tiga fase yaitu Fase I (*Pre-submission Liveness Gate*) dimana CNN memproses setiap frame kamera secara *real-time*. Tombol *submit* tetap nonaktif hingga probabilitas happy ≥0.70 terpenuhi stabil selama 1,5 detik. Fase ini berjalan sepenuhnya di peramban tanpa koneksi jaringan. Fase II (*Simultaneous Data Capture*) dimana begitu *liveness* terkonfirmasi, *snapshot* wajah terenkripsi Base64 dan koordinat GPS diambil secara atomik dalam satu operasi JavaScript untuk meminimalkan jeda temporal antara konfirmasi *liveness* dan pengiriman data. Fase III (*Server-side Dual Validation*) dimana Server Flask menerima *payload* yang berisi *snapshot* dan koordinat, menjalankan Haversine Formula, dan menyimpan *record* presensi hanya jika jarak *geodesik* berada dalam radius 50 meter. Seluruh transmisi diproteksi TLS 1.3.

Desain atomik pada Fase II penting untuk mencegah serangan *time-of-check to time-of-use* (TOCTOU), yaitu skenario di mana pengguna menyelesaikan *liveness challenge* dengan wajah asli, kemudian mengganti koordinat GPS sebelum pengiriman. Dengan pengambilan data simultan dalam satu *event handler* JavaScript, jendela temporal untuk manipulasi tersebut diminimalkan secara signifikan.

3. HASIL DAN PEMBAHASAN

Sistem berhasil diimplementasikan pada lingkungan server lokal menggunakan Python 3.9 dan Flask 2.3. Pengujian klien dilakukan menggunakan tiga perangkat yaitu smartphone Android (Snapdragon 720G, Chrome 124), laptop Windows 11 (Intel Core i5-1135G7, Chrome 124), dan tablet Android (MediaTek Helio G88, Chrome 122). Konsistensi performa di ketiga perangkat memvalidasi keringanan arsitektur MobileNetV1 untuk *deployment* lintas-perangkat. Antarmuka pengguna menampilkan umpan video kamera secara *real-time* dengan *overlay bounding box* wajah dan indikator status ekspresi berwarna yang diperbarui setiap frame dimana merah (tidak ada wajah terdeteksi), kuning (probabilitas senyum di bawah *threshold*), dan hijau (*liveness* terkonfirmasi, presensi dapat disubmit). Tampilan antarmuka saat proses validasi ditunjukkan pada Gambar 3.

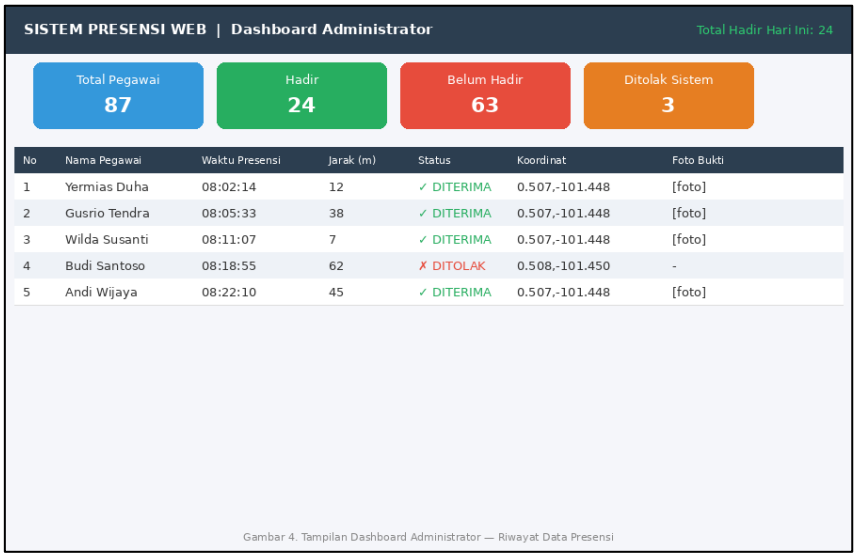


Gambar 3. Antarmuka *Liveness Detection* dan Indikator Status Validasi pada Sisi Pengguna

Dashboard administrator menampilkan data kehadiran dalam tabel terfilter yang memuat waktu presensi, nama pegawai, tautan lokasi Google Maps terverifikasi, dan foto bukti kehadiran

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

(*attendance snapshot*). Dashboard juga mencatat status validasi (*liveness: passed/failed, geofence: passed/failed*) untuk keperluan audit. Tampilan dashboard ditunjukkan pada Gambar 4.



Gambar 4. Tampilan Dashboard Administrator dengan Riwayat Presensi dan Status Validasi

3.1 Hasil Pengujian Liveness Detection

Pengujian *anti-spoofing* biometrik menghasilkan diferensiasi yang sangat jelas antara pengguna asli dan instrumen serangan presentasi. Dari 20 percobaan *spoofing* menggunakan foto statis (10 foto cetak resolusi tinggi 300 dpi, 10 foto digital ditampilkan pada layar sekunder 6 inci dengan kecerahan 500 nit), probabilitas ekspresi *happy* rata-rata hanya 0.12 untuk foto cetak (σ=0.03) dan 0.15 untuk foto digital (σ=0.04) jauh di bawah ambang batas 0.70. Sistem berhasil menolak seluruh 20 percobaan *spoofing* dengan *False Acceptance Rate* (FAR) = 0%. Sebaliknya, dari 20 pengujian oleh pengguna asli dalam berbagai kondisi pencahayaan, 19 berhasil melewati validasi (*True Positive Rate/Sensitivity* = 95%) dengan probabilitas rata-rata 0.92 (σ=0.04). Satu kegagalan terjadi pada kondisi pencahayaan backlit yang ekstrem (sumber cahaya langsung di belakang kepala subjek). Latensi pemrosesan CNN rata-rata 347ms per frame pada smartphone (σ=42ms), dikategorikan responsif untuk interaksi real-time. Rekapitulasi hasil pengujian liveness ditampilkan pada Tabel 1.

Tabel 1. Rekapitulasi Hasil Pengujian Liveness Detection (N=40 percobaan)

Kategori Pengujian	N	P(Happy) Rata-rata	Keputusan Sistem
Pengguna asli - kondisi normal	15	0.93 (σ=0.03)	15 Diterima (TPR=100%)
Pengguna asli - pencahayaan rendah	3	0.82 (σ=0.05)	3 Diterima
Pengguna asli - backlit ekstrem	2	0.61 (σ=0.08)	1 Diterima, 1 Ditolak (FRR=50%)
Foto cetak resolusi tinggi	10	0.12 (σ=0.03)	10 Ditolak (FAR=0%)
Foto digital (layar sekunder)	10	0.15 (σ=0.04)	10 Ditolak (FAR=0%)

Nilai *True Positive Rate* sebesar 95% (19 dari 20 pengguna asli berhasil terverifikasi) dan *False Acceptance Rate* sebesar 0% (0 dari 20 percobaan spoofing berhasil melewati sistem) mengindikasikan kinerja sistem yang baik untuk skenario yang diuji. Menggunakan metode *Wilson*

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

score interval untuk proporsi binomial dengan tingkat kepercayaan 95%, interval kepercayaan untuk TPR adalah [76,4%–99,1%] dan untuk FAR adalah [0%–16,8%]. Rentang interval yang cukup lebar ini mengonfirmasi perlunya validasi pada sampel yang lebih besar untuk memperoleh estimasi performa yang lebih presisi. Hasil ini sejalan dengan temuan (Shinde et al., 2025) yang menunjukkan bahwa model CNN berbasis ekspresi efektif terhadap serangan foto statis 2D, namun (Das et al., 2025) memperingatkan bahwa *deepfake* generasi terbaru yang mampu mensimulasikan ekspresi dinamis dapat melampaui batas kemampuan sistem berbasis *active liveness* sederhana.

3.2 Hasil Pengujian Validasi Geofencing Server-Side

Pengujian validasi lokasi dilakukan dalam tiga kondisi eksperimental yaitu (1) GPS stabil dengan akurasi <20 meter pada lingkungan outdoor terbuka; (2) GPS tidak stabil dengan akurasi >100 meter pada lingkungan semi-tertutup (koridor dalam gedung); dan (3) koordinat dimanipulasi secara artifisial menggunakan *Sensor Emulation Chrome DevTools* untuk mensimulasikan serangan *spoofing* GPS. Temuan paling penting adalah bukti nyata bahwa validasi *client-side* JavaScript sepenuhnya dapat dilewati melalui Sensor Emulation dalam kurang dari 30 detik tanpa keahlian teknis khusus membuktikan urgensi *server-side enforcement*. Setelah pemindahan logika Haversine ke server, serangan ini sepenuhnya terblokir. Untuk kondisi GPS stabil, akurasi keputusan accept/reject mencapai 100%. Pada kondisi GPS tidak stabil (akurasi >100 meter), sistem menolak presensi meskipun pengguna secara fisik berada dalam radius, karena data koordinat yang tidak presisi tidak dapat dijadikan dasar keputusan yang valid perilaku ini merupakan desain yang disengaja untuk mencegah *false acceptance*. Rekapitulasi pengujian ditampilkan pada Tabel 2.

Tabel 2. Rekapitulasi Pengujian Validasi Lokasi *Geofencing Server-Side*

Jarak Fisik (m)	Akurasi GPS	Status Koordinat	Respons Server	Keterangan
10	Tinggi (<20m)	Asli	200 OK – Diterima	Dalam radius, GPS stabil
45	Tinggi (<20m)	Asli	200 OK - Diterima	Batas toleransi geofence
55	Tinggi (<20m)	Asli	403 Forbidden	Di luar radius 50m
10	Rendah (>100m)	Asli	403 Forbidden	GPS tidak stabil - tolak demi keamanan
>200	Tinggi	Dimanipulasi (DevTools)	403 Forbidden	Server-side block - client manipulation gagal
>200	Tinggi	Dimanipulasi (JS injection)	403 Forbidden	Server-side block - injeksi skrip gagal

Perlu ditekankan bahwa pengujian *anti-spoofing* dalam penelitian ini terbatas pada serangan foto statis (*2D print attack* dan *screen replay* foto statis). Ancaman *video replay* dan *deepfake real-time*, meskipun disebutkan dalam pendahuluan sebagai vektor ancaman yang berkembang pesat, belum diuji dalam penelitian ini karena keterbatasan akses terhadap perangkat lunak *deepfake real-time* pada lingkungan pengujian. Klaim FAR = 0% oleh karena itu hanya berlaku untuk skenario serangan foto statis dan tidak dapat digeneralisasi ke seluruh spektrum serangan presentasi. Pengujian terhadap vektor serangan yang lebih canggih ini menjadi prioritas utama penelitian lanjutan.

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

3.3 Analisis Komparatif dan Diskusi

Dibandingkan dengan sistem-sistem terdahulu, kontribusi utama penelitian ini terletak pada sinergi keamanan berlapis dalam satu platform web yang ringan. Tabel 3 merangkum perbandingan fitur dengan penelitian representatif dalam domain ini.

Tabel 3. Perbandingan dengan Penelitian Terkait

Penelitian	Anti-Spoofing Wajah	Validasi Lokasi	Platform	Kelemahan Utama
(Mutaqin & Nurhayati, 2023)	Tidak	*Haversine (client)*	*Android Native*	Tidak ada PAD; *client-side geofencing*
(Wibowo & Setiawan, 2024)	*Face Matching Statis*	*JavaScript*	*Mobile App*	Tanpa *liveness*; *client-side validation*
(Nurhakim et al., 2025)	*Deep Learning PAD*	*Tidak*	*Desktop/Server*	Tidak ada validasi lokasi; infrastruktur berat
(Babu et al., 2025)	*Face Recognition*	*Haversine (server)*	*Web (Streamlit)*	Tidak mengekspos kerentanan *client-side*
Penelitian Ini	*CNN Liveness (PAD)*	*Haversine (server)*	*Web Browser*	Dataset kecil; rentan *deepfake real-time*

Secara kuantitatif, penelitian ini mencapai TPR 95% yang sebanding dengan (Nurhakim et al., 2025) yang melaporkan akurasi *anti-spoofing* di atas 95% namun pada infrastruktur *desktop* yang jauh lebih berat. Keunggulan komparatif penelitian ini terletak bukan semata pada metrik akurasi, melainkan pada kombinasi tiga atribut sekaligus: validasi wajah berbasis *liveness* (bukan sekadar *face matching* statis seperti pada Wibowo & Setiawan, 2024), validasi lokasi di sisi server (berbeda dengan Mutaqin & Nurhayati, 2023 yang menggunakan *client-side*), dan deployment berbasis browser tanpa instalasi aplikasi *native*. Kombinasi ketiga atribut ini belum ditemukan dalam satu sistem terintegrasi pada penelitian-penelitian sebelumnya yang ditinjau.

Temuan paling signifikan adalah demonstrasi secara eksperimental bahwa *client-side geofencing* JavaScript adalah kontrol keamanan yang tidak dapat diandalkan ia memberikan keamanan semu (*security theater*) yang dapat dilewati tanpa keahlian teknis mendalam. Pemindahan logika validasi ke server bukan sekadar optimasi, melainkan keharusan arsitektural yang sejalan dengan prinsip '*never trust client input*' dalam rekayasa keamanan (Saied & Syafii, 2023). Penggunaan CNN di sisi klien untuk *liveness* memiliki implikasi privasi *positif* dimana frame video tidak pernah meninggalkan perangkat pengguna, selaras dengan prinsip data *minimization* yang semakin didorong oleh regulasi perlindungan data global (Atmawijaya & Radiyah, 2024).

Perlu dicatat bahwa pendekatan *active liveness* berbasis *challenge* senyum memiliki batas kemampuan yang semakin relevan di tahun 2025-2026 dimana serangan *deepfake real-time* yang menggunakan model AI generatif untuk mensimulasikan ekspresi wajah dinamis secara meyakinkan kini telah terdokumentasi dalam laporan industri keamanan biometrik (Das et al., 2025; Paravision, 2025). Sistem yang dikembangkan dalam penelitian ini dirancang sebelum proliferasi alat *deepfake* komersial belum diuji terhadap serangan vektor ini. Ini merupakan keterbatasan yang perlu diatasi melalui pengintegrasian teknik *passive liveness detection*, analisis tekstur frekuensi, atau rPPG (*remote photoplethysmography*) pada iterasi berikutnya.

Keterbatasan penelitian ini meliputi: (1) ukuran dataset pengujian yang relatif kecil (N=40 percobaan *liveness*, N=6 skenario *geofencing*) membatasi generalisasi statistik dan memerlukan validasi pada kelompok partisipan yang lebih besar dan beragam; (2) sistem belum diuji terhadap serangan *deepfake real-time* yang mensimulasikan ekspresi dinamis; (3) ketergantungan pada GPS membatasi kegunaan sistem di dalam ruangan atau area dengan sinyal lemah; dan (4) evaluasi

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

performa hanya mencakup tiga jenis perangkat. Penelitian masa depan perlu mengatasi keterbatasan-keterbatasan ini secara sistematis.

4. SIMPULAN

Penelitian ini berhasil merancang, mengimplementasikan, dan memvalidasi sistem presensi berbasis web dengan keamanan berlapis ganda yang secara simultan menangani dua vektor ancaman kritis: *presentation attack* biometrik dan manipulasi lokasi GPS. Integrasi *Liveness Detection* berbasis CNN MobileNetV1 terbukti efektif sebagai mekanisme deteksi serangan presentasi yang ringan di lingkungan *browser*, sementara implementasi *Haversine Formula* di sisi server berhasil mengeliminasi kerentanan inheren pada validasi lokasi *client-side*. Secara keseluruhan, sistem yang diusulkan membuktikan bahwa keamanan berlapis (*defense-in-depth*) dapat diimplementasikan dalam platform web ringan tanpa mengorbankan aksesibilitas.

Kontribusi utama penelitian ini terletak pada (1) demonstrasi empiris bahwa *client-side geofencing* JavaScript adalah kontrol keamanan yang tidak cukup dan dapat dilewati secara *trivial*; (2) validasi pendekatan hybrid yang menggabungkan aksesibilitas web dengan keandalan komputasi server; (3) pembuktian bahwa *liveness detection* berbasis CNN dapat dijalankan secara efisien di peramban tanpa transmisi data biometrik ke server. Hasil ini menegaskan bahwa keamanan berlapis (*defense-in-depth*) merupakan paradigma yang diperlukan untuk sistem dengan implikasi administratif dan finansial.

Meskipun demikian, penelitian ini memiliki beberapa keterbatasan yang perlu diakui secara proporsional. Dataset pengujian yang berjumlah 40 percobaan *liveness* dan 6 skenario *geofencing* membatasi generalisasi statistik hasil penelitian. Klaim efektivitas sistem berlaku terbatas pada skenario yang telah diuji, yaitu serangan foto statis dan manipulasi koordinat melalui *browser emulation*, dan tidak dapat digeneralisasi ke serangan *video replay*, *deepfake real-time*, atau kondisi GPS yang terdegradasi di dalam ruangan. Selain itu, ketidaktersediaan informasi publik mengenai data pelatihan model *face-api.js* membatasi kemampuan untuk menilai generalisasi model terhadap variasi demografis yang lebih luas. Validasi skala besar dengan partisipan yang lebih beragam diperlukan sebelum sistem ini dapat direkomendasikan untuk implementasi produksi.

Untuk penelitian selanjutnya, disarankan (1) mengevaluasi ketahanan model terhadap serangan *deepfake real-time* melalui pengintegrasian *passive liveness detection* atau analisis rPPG; (2) mengeksplorasi validasi lokasi indoor berbasis *WiFi fingerprinting, Bluetooth Low Energy beacon*, atau sensor inersial perangkat sebagai komplemen GPS; (3) mengembangkan *challenge-response* yang lebih variatif dan adaptif terhadap karakteristik serangan; (4) melakukan pengujian skala besar dengan kelompok pengguna yang lebih representatif untuk meningkatkan validitas statistik; dan (5) mengeksplorasi privasi diferensial dan teknik enkripsi homorfik untuk melindungi data presensi pada infrastruktur produksi.

5. DAFTAR PUSTAKA

Abdelraheem, A. A. E., Hussaien, A. M., Mohammed, M. A. A., & Elbokhari, Y. A. E. (2021). The effect of information technology on the quality of accounting information. *Accounting*, *7*(1), 191–196. https://doi.org/https://doi.org/10.5267/j.ac.2020.9.017

Apriadi, P., & Sutrisna, E. (2023). Mobile-Based Employee Absence Application Design Using GPS (Case Study of PT. Trans Retail Indonesia). *JACIS: Journal Automation Computer Information System*, *3*(1), 1–9. https://doi.org/https://doi.org/10.47134/jacis.v3i1.54

Atmawijaya, R., & Radiyah, U. (2024). Perancangan Autentikasi Multi Faktor Dengan Pengenalan Wajah Dan Fido (Fast Identity Online). *INTI Nusa Mandiri*, *19*(1), 46–53. https://doi.org/https://doi.org/10.33480/inti.v19i1.5263

Babu, L. K., Prasad, N. V., Yeswanth, S., & Kumar, E. P. (2025). Smart Attendance System Using Geofencing and Face Recognition. *International Journal of Progressive Research in Engineering Management and Science*, *5*(11), 291–297.

Budiarto Hadiprakoso, R., & Buana, I. K. S. (2021). Deteksi Serangan Spoofing Wajah Menggunakan Convolutional Neural Network. *Jurnal Teknik Informatika Dan Sistem Informasi*, *7*(3), 618–626. https://doi.org/https://doi.org/10.28932/jutisi.v7i3.4001

https://doi.org/10.35145/joisie.v10i1.5906
JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

Das, N., Deb, P., Majumder, S., & Das, D. (2025). *Face-Liveness Detection Using CNN Model*. 343–354. https://doi.org/https://doi.org/10.1007/978-981-96-9932-2_23

Gunawan, A., & Ikhwan, A. (2024). Teacher Presence Application with Geolocation and Self Potrait using Android-based Prototype Method at MTsN Binjai. *Sistemasi: Jurnal Sistem Informasi*, *13*(5), 1773–1782. https://doi.org/https://doi.org/10.32520/stmsi.v13i4.4353

Kuznetsov, A., & others. (2025). Deep Residual Learning for Face Anti-Spoofing: A Mathematical Framework for Optimized Skip Connections. *Technologies*, *13*(9), 413. https://doi.org/https://doi.org/10.3390/technologies13090413

Maulana, I., Khairunisa, N., & Mufidah, R. (2023). Deteksi Bentuk Wajah Menggunakan Convolutional Neural Network (CNN). *Jurnal Mahasiswa Teknik Informatika*, *7*(6), 3348–3355. https://doi.org/https://doi.org/10.36040/jati.v7i6.8171

Mutaqin, H., & Nurhayati. (2023). Perancangan Aplikasi Absensi Menggunakan Metode Haversine Berbasis Android Pada PT. Rangkai Utama Berjaya. *INFORMATIKA*, *11*(2), 112–119. https://doi.org/https://doi.org/10.36987/informatika.v11i2.3799

Nurhakim, B., Rifai, A., Kurnia, D. A., Sudrajat, D., & Supriatna, U. (2025). Smart Attendance Tracking System Employing Deep Learning For Face Anti-Spoofing Protection. *JITK*, *10*(3), 496–505. https://doi.org/https://doi.org/10.33480/jitk.v10i3.5992

Ode Hazani, L. (2024). Implementasi Formula Haversine Pada Sistem Absensi Pegawai Berbasis Web. *Jurnal Teknologi Informasi (JTI)*, *12*(2), 9–17. https://doi.org/https://doi.org/10.58839/jti.v12i2.1468

Pangihutan Sitanggang, J., Sunupurwa Asri, J., & Sutanto, I. (2025). Rancang Bangun Sistem Absensi Berbasis Mobile Dengan Memanfaatkan Pengenalan Wajah. *Teknik Komputer Dan Teknologi Pendidikan (JUSTIKPEN)*, *5*(1), 155–164. https://doi.org/https://doi.org/10.55338/justikpen.v5i1.356

Paravision. (2025). *From Spoofs to Deepfakes: Why Fraud Prevention Needs to Evolve*. Paravision. https://www.paravision.ai/converge/2025/from-spoofs-to-deepfakes-why-fraud-prevention-needs-to-evolve/

Prasojo, G. A., & Cahyaningtyas, C. (2025). Implementasi Algoritma Haversine Formula Dengan Global Positioning System Pada Sistem Absensi Pegawai. *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(2), 598–607. https://doi.org/https://doi.org/10.62712/juktisi.v4i2.469

Saied, M., & Syafii, A. (2023). Perancangan dan Implementasi Sistem Absensi Berbasis Teknologi Terkini. *Jurnal Teknik Indonesia*, *2*(3), 87–92. https://doi.org/https://doi.org/10.58860/jti.v2i3.21

Shinde, S. R., Bongale, A. M., Dharrao, D., Jadhav, D., & Yadav, N. (2025). Enhancing Face Liveness Detection: Novel Deep CNN Architectures for Anti-Spoofing. *Engineering, Technology & Applied Science Research*, *15*(5), 27206–27212. https://doi.org/https://doi.org/10.48084/etasr.12431

Wibowo, B. B., & Setiawan, E. B. (2024). Implementasi Face Recognition Dan Geolocation Pada Sistem Presensi Karyawan Berbasis Mobile Apps. *KOMPUTA: Jurnal Ilmiah Komputer Dan Informatika*, *13*(1), 11. https://doi.org/https://doi.org/10.34010/komputa.v13i1.11149

Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal. *JTIM: Jurnal Teknologi Informasi Dan Multimedia*, *7*(1), 133–148. https://doi.org/https://doi.org/10.35746/jtim.v7i1.653

JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)