

RANCANG BANGUN SISTEM ABSENSI MAHASISWA BERBASIS MOBILE DENGAN INTEGRASI GEOLOCATION DAN FACE RECOGNITION MENGGUNAKAN MOBILEFACENET PADA PROGRAM STUDI D-III TEKNIK INFORMATIKA POLITEKNIK NEGERI PONTIANAK

Yusril Eka Mahendra^{*1}, Nurul Fadillah¹, Karfindo¹

¹Program Studi D-III Teknik Informatika, Jurusan Teknik Elektro, Politeknik Negeri Pontianak, Pontianak, Indonesia

Penulis korespondensi: Yusril Eka Mahendra (yusrilekamahendra@polnep.ac.id)

Presensi mahasiswa pada Program Studi D-III Teknik Informatika Politeknik Negeri Pontianak masih dicatat secara manual sehingga rawan salah catat dan lambat direkap. Penelitian terapan ini merancang dan membangun prototipe presensi berbasis mobile yang memadukan verifikasi wajah MobileFaceNet di perangkat dengan validasi lokasi berbasis geofencing melalui pendekatan prototyping. Prototipe terdiri atas aplikasi Flutter, backend Laravel, dan dashboard web dengan liveness challenge, izin presensi sekali pakai, presensi luring, rekapitulasi kehadiran, serta peringatan dini Surat Peringatan. Seluruh 255 pengujian otomatis backend dan 214 pengujian aplikasi mobile lulus. Evaluasi 1.485 pasangan wajah impostor menghasilkan False Accept Rate 0% pada threshold 0,60, dan uji beban 20-40 pengguna simultan menghasilkan waktu respons persentil ke-95 di bawah 2 detik. Namun, False Reject Rate belum diukur, bukti lokasi dan wajah masih dihitung di perangkat, dan liveness belum diuji terhadap serangan foto, video replay, maupun deepfake, sehingga sistem belum dapat diklaim mencegah titip absen atau pemalsuan lokasi.

Kata Kunci - absensi mahasiswa, face recognition, geofencing, mobile application, MobileFaceNet

I. PENDAHULUAN

Presensi mahasiswa merupakan data operasional strategis dalam pengelolaan akademik perguruan tinggi karena menjadi dasar evaluasi kehadiran, pemantauan kedisiplinan, serta pemberian sanksi akademik berupa Surat Peringatan (SP1, SP2, SP3). Pada Program Studi D-III Teknik Informatika, Jurusan Teknik Elektro, Politeknik Negeri Pontianak, proses presensi masih dilakukan secara konvensional menggunakan lembar kertas pada setiap pertemuan perkuliahan. Dosen mencatat kehadiran secara manual dan admin program

studi melakukan rekapitulasi secara berkala, sehingga proses ini rawan kesalahan pencatatan (human error) serta terlambat dalam mendeteksi mahasiswa dengan tingkat ketidakhadiran tinggi.

Berbagai penelitian telah mengembangkan sistem presensi digital untuk meningkatkan efisiensi dan akurasi pencatatan kehadiran. Isinkaye dkk. mengembangkan sistem presensi berbasis Android yang memanfaatkan deteksi dan pengenalan wajah untuk mengurangi kecurangan absensi [1]. Sunaryono dkk. mengusulkan sistem presensi mobile yang mengombinasikan pengenalan wajah dengan QR Code untuk mempercepat proses absensi [2]. Perkembangan face recognition berbasis deep learning seperti FaceNet [3], ArcFace [4], dan MobileFaceNet [5] terbukti mampu meningkatkan akurasi identifikasi wajah secara real-time bahkan pada perangkat dengan sumber daya terbatas. Penelitian lain juga telah mengombinasikan pengenalan wajah dengan geofencing untuk keperluan presensi [6], [7], namun sebagian besar implementasi tersebut belum mengintegrasikan verifikasi wajah dan validasi lokasi secara simultan dalam satu mekanisme presensi yang juga mendukung monitoring akademik berupa peringatan dini ketidakhadiran.

Berdasarkan uraian tersebut, terdapat gap penelitian berupa belum banyaknya sistem presensi mobile yang mengintegrasikan face recognition berbasis deep learning dan validasi geolocation secara real-time dalam satu platform yang juga mendukung mekanisme peringatan dini akademik. Oleh karena itu, penelitian ini bertujuan merancang dan mengembangkan sistem presensi mahasiswa berbasis mobile yang terintegrasi dengan verifikasi wajah menggunakan MobileFaceNet dan

validasi lokasi berbasis geofencing, guna meningkatkan akurasi pencatatan kehadiran, mempercepat rekapitulasi administrasi, serta membangun mekanisme peringatan dini bagi mahasiswa dengan tingkat ketidakhadiran yang melampaui batas yang ditetapkan.

II. METODE PENELITIAN

Penelitian ini dilaksanakan pada Program Studi D-III Teknik Informatika, Jurusan Teknik Elektro, Politeknik Negeri Pontianak, dengan objek berupa proses presensi mahasiswa pada perkuliahan selama periode Mei–September 2026. Penelitian terapan (applied research) ini menggunakan model pengembangan Research and Development (R&D)/Prototyping [8] agar setiap komponen—aplikasi mobile, backend, dan dashboard—dapat dibangun, diuji, dan diperbaiki secara iteratif hingga diperoleh prototipe yang stabil. Tahapannya meliputi studi literatur dan analisis kebutuhan, perancangan arsitektur, pengembangan perangkat lunak, implementasi dan integrasi modul, serta pengujian, analisis, dan finalisasi.

A. Studi Literatur dan Analisis Kebutuhan

Studi literatur dilakukan terhadap penelitian terdahulu mengenai sistem presensi digital, geolocation dan geofencing, serta face recognition berbasis deep learning seperti FaceNet, ArcFace, dan MobileFaceNet. Analisis kebutuhan dilakukan melalui observasi proses presensi manual dan wawancara dengan pengelola akademik, sehingga diperoleh kebutuhan fungsional berupa autentikasi pengguna, validasi lokasi, verifikasi wajah, dan pencatatan kehadiran, serta kebutuhan non-fungsional berupa keamanan data biometrik dan deteksi dini akumulasi ketidakhadiran sebagai dasar early warning akademik.

B. Perancangan Arsitektur, Basis Data, dan Antarmuka

Arsitektur sistem dirancang dengan pendekatan mobile–

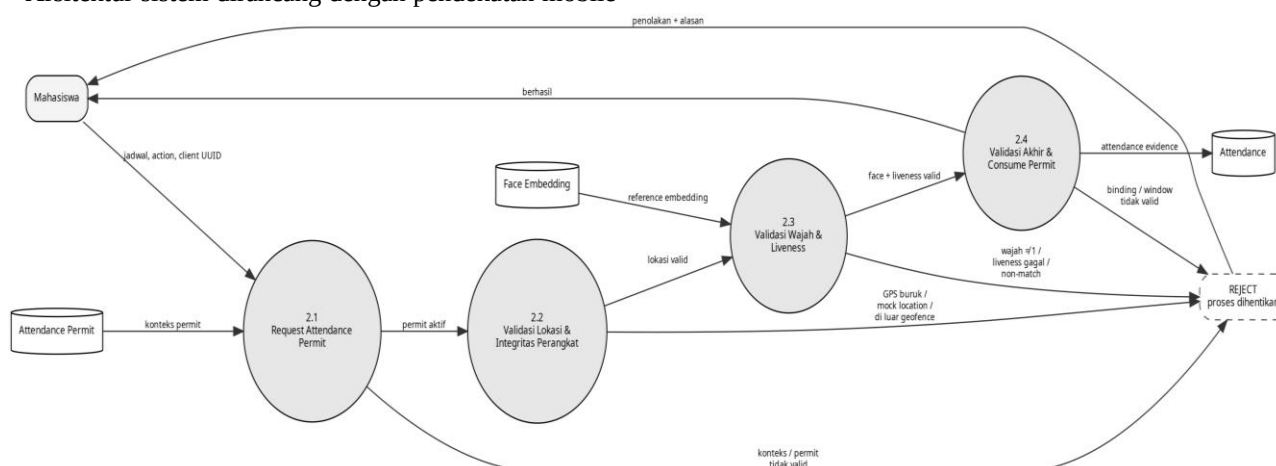
backend–dashboard. Aplikasi mobile menangani autentikasi, lokasi, kamera, preprocessing dan verifikasi wajah, liveness, serta pengiriman evidence; backend menangani autentikasi, aturan bisnis, penerbitan attendance permit, validasi konteks akademik, dan pencatatan transaksi; sedangkan dashboard digunakan dosen dan admin untuk pengelolaan data dan monitoring. Alur data dan struktur basis data dirancang sebagai berikut.

1. Diagram Konteks dan DFD

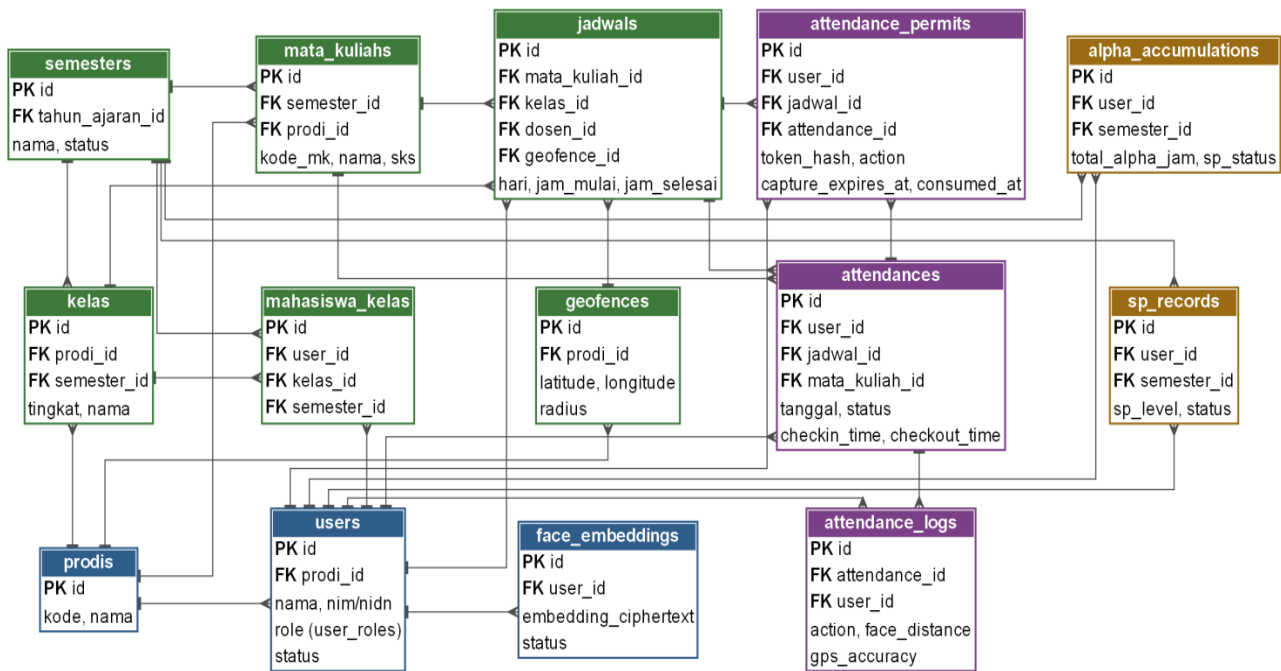
Diagram konteks menggambarkan sistem sebagai satu proses tunggal yang berinteraksi dengan Mahasiswa serta Dosen/Admin, dan DFD Level 0 memecahnya menjadi autentikasi dan akses akademik, validasi absensi, verifikasi biometrik, serta pengelolaan attendance dan early warning. Pada DFD Level 1 (Gambar 1), attendance permit diterbitkan setelah identitas, keanggotaan kelas, jadwal, periode akademik, dan waktu absensi dinyatakan sesuai; selanjutnya lokasi diperiksa, biometrik dan liveness divalidasi, lalu evidence dikirim untuk validasi akhir dan permit dikonsumsi. DFD Level 2 merinci proses tersebut hingga akuisisi GPS, pemeriksaan mock location, perhitungan geofence, liveness challenge, ekstraksi embedding MobileFaceNet, dan pencocokan jarak terhadap threshold.

2. Entity Relationship Diagram (ERD)

ERD pada Gambar 2 memvisualisasikan entitas inti basis data beserta relasinya. Pengguna terhubung dengan program studi, peran, embedding wajah terenkripsi, dan keanggotaan kelas per semester; jadwal menghubungkan mata kuliah, kelas, dosen, dan geofence; sedangkan attendance_permits berfungsi sebagai pre-authorization yang dikonsumsi satu kali ketika transaksi attendance dicatat. Data attendance menjadi dasar akumulasi alpha dan catatan Surat Peringatan (SP).



Gambar 1. DFD Level 1 proses validasi absensi: permit diterbitkan server, dilanjutkan validasi lokasi, validasi wajah dan liveness, serta validasi akhir sebelum permit dikonsumsi. Setiap proses dapat menolak transaksi.



Gambar 2. Entity Relationship Diagram basis data inti sesuai skema terbaru, mencakup data pengguna, akademik (termasuk kelas per semester), biometrik, attendance permit, transaksi kehadiran, dan early warning SP. Warna header menandai kelompok entitas.

C. Pengembangan Backend API, Dashboard, dan Aplikasi Mobile

Backend dibangun sebagai REST API yang menjadi pusat aturan bisnis dan sumber kebenaran (single source of truth) seluruh transaksi presensi [8]. Dashboard web dikembangkan untuk pengelolaan pengguna, jadwal, geofence, dan pemantauan rekapitulasi oleh admin dan dosen, sedangkan aplikasi mobile menjadi antarmuka mahasiswa untuk enrollment wajah, autentikasi, serta check-in dan check-out.

D. Implementasi dan Integrasi

Pada tahap ini dilakukan implementasi modul akuisisi geolocation dengan memanfaatkan layanan GPS perangkat untuk menentukan posisi mahasiswa saat melakukan presensi [9]. Validitas lokasi dianalisis dengan menghitung jarak antara koordinat perangkat dan pusat geofence menggunakan rumus Haversine, sejalan dengan mekanisme geofencing berbasis titik koordinat dan radius yang lazim diterapkan pada platform Android [9]:

$$a = \sin^2\left(\frac{\Delta\varphi}{2}\right) + \cos\varphi_1 \cos\varphi_2 \sin^2\left(\frac{\Delta\lambda}{2}\right), \quad (1)$$

$$d = 2R \arcsin(\sqrt{a}), \quad (2)$$

dengan d adalah jarak antara perangkat dan pusat geofence (m), R adalah jari-jari bumi (6.371 km), φ_1 dan λ_1 adalah lintang dan bujur perangkat, φ_2 dan λ_2 adalah lintang dan bujur pusat geofence, a adalah besaran antara Haversine, sedangkan $\Delta\varphi = \varphi_2 - \varphi_1$ dan $\Delta\lambda = \lambda_2 - \lambda_1$ dinyatakan dalam radian.

Lokasi dinyatakan valid apabila jarak d tidak melebihi radius geofence dan kualitas akurasi GPS memenuhi batas yang ditentukan. Selanjutnya, dilakukan implementasi modul face detection dan ekstraksi face embedding menggunakan model MobileFaceNet secara on-device. Verifikasi wajah dilakukan secara one-to-one: citra wajah dideteksi menggunakan Google ML Kit, dipotong, diubah ukurannya menjadi 112×112 piksel, dinormalisasi, kemudian diproses menggunakan MobileFaceNet melalui

TensorFlow Lite untuk menghasilkan embedding berdimensi 192 [5], [10]. Kecocokan identitas dihitung menggunakan jarak Euclidean antara embedding hasil ekstraksi (e) dan embedding referensi (t):

$$d(e, t) = \sqrt{\sum_{i=1}^n (e_i - t_i)^2}, \quad (3)$$

dengan e_i dan t_i adalah elemen ke- i dari embedding hasil ekstraksi dan embedding referensi, serta $n = 192$ adalah dimensi embedding.

Nilai jarak dibandingkan dengan threshold θ ; apabila $d \leq \theta$ maka wajah diklasifikasikan match, dan sebaliknya non-match. Seluruh modul tersebut—geolocation, geofencing, face detection, dan face verification—selanjutnya diintegrasikan ke dalam satu alur presensi terpadu yang dilindungi oleh mekanisme attendance permit bersifat one-time, bound, dan expiring, sehingga setiap transaksi presensi hanya dapat dilakukan setelah seluruh syarat akademik dan validasi teknis terpenuhi.

E. Pengujian, Analisis, dan Finalisasi

Pengujian dilakukan dalam tiga bagian. Pertama, pengujian fungsional menggunakan black box testing dan automated testing pada backend dan aplikasi mobile [8].

Kedua, verifikasi wajah dievaluasi dengan False Accept Rate (FAR) dan False Reject Rate (FRR) [11], [12]. FAR(θ) adalah persentase pasangan impostor yang jaraknya menurut (3) tidak melebihi θ , dihitung di server dari seluruh pasangan lintas pengguna embedding enrollment yang telah disetujui, sedangkan FRR memerlukan percobaan genuine berulang dari frame verifikasi langsung. Pengujian liveness diperlakukan terpisah dari FAR/FRR sesuai prinsip presentation attack detection [13].

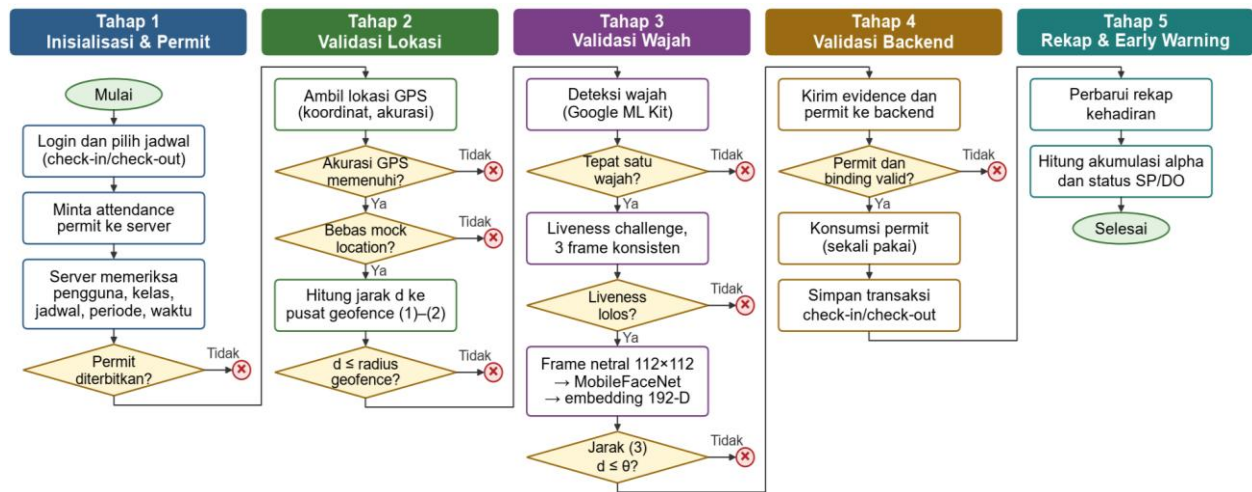
Ketiga, uji beban dilakukan pada server produksi dengan 20, 30, dan 40 pengguna virtual simultan (39 akun mahasiswa) selama 45 detik per level terhadap endpoint baca dashboard, jadwal hari ini, dan riwayat presensi, dengan metrik waktu respons persentil ke-95 (p95) dan persentase respons gagal.

III. HASIL DAN PEMBAHASAN

A. Implementasi Alur Proses Absensi

Alur operasional sistem, yang merupakan implementasi rancangan DFD Level 1 dan Level 2, ditunjukkan pada Gambar 3. Mahasiswa melakukan autentikasi dan

memilih jadwal, meminta attendance permit, lalu menjalani validasi lokasi, deteksi wajah, liveness challenge, dan verifikasi wajah sebelum evidence dikirim untuk divalidasi dan dicatat; setiap titik keputusan dapat menghentikan proses.



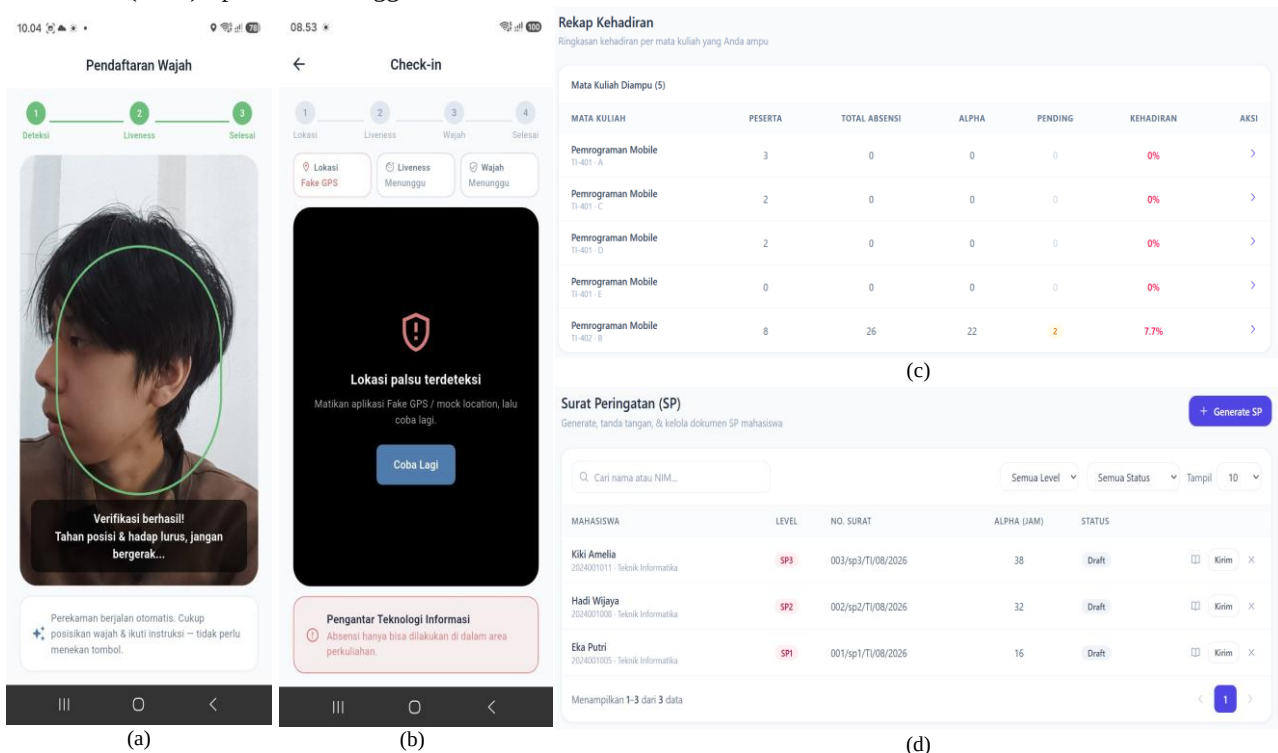
Gambar 3. Alur proses absensi dalam lima tahap, mulai dari penerbitan attendance permit hingga pembaruan early warning. Setiap titik keputusan yang tidak terpenuhi (tanda ×) menolak transaksi sehingga kehadiran tidak dicatat.

B. Implementasi Liveness Challenge dan Mekanisme Penolakan

Pada sisi liveness, implementasi menggunakan lima challenge, yaitu tersenyum, menoleh ke kiri, menoleh ke kanan, berkedip, dan mengangguk. Sistem mengawali challenge dari neutral state dan menetapkan keberhasilan setelah respons terdeteksi konsisten pada tiga frame berturut-turut. Tampilan implementasi liveness challenge pada aplikasi mobile ditunjukkan pada Gambar 4(a). Prototipe ini tidak diklaim sebagai Presentation Attack Detection (PAD) penuh, sehingga klaim keamanan

terhadap foto, video replay, atau deepfake tetap memerlukan pengujian tersendiri [13].

Mekanisme penolakan juga diterapkan pada integritas lokasi. Ketika terdeteksi indikasi mock location, aplikasi menampilkan indikator manipulasi lokasi dan menghentikan validasi sebagaimana ditunjukkan pada Gambar 4(b). Koordinat, face distance, dan status liveness pada prototipe merupakan client-attested evidence; attendance permit mengurangi risiko replay dan salah binding, tetapi belum menghilangkan residual trust terhadap client.



Gambar 4. Implementasi antarmuka: (a) liveness challenge yang menuntut respons wajah konsisten pada tiga frame berturut-turut; (b) penolakan transaksi akibat indikasi mock location; (c) dashboard rekapitulasi kehadiran per mata kuliah dan kelas; (d) monitoring early warning dan Surat Peringatan berdasarkan akumulasi jam alpha (ditampilkan dengan data uji).

C. Rekapitulasi dan Early Warning

Attendance yang berhasil dicatat digunakan untuk membentuk rekap berdasarkan mahasiswa, mata kuliah, jadwal, dan periode. Dashboard admin pada Gambar 4(c) menyediakan informasi kehadiran secara terstruktur sehingga riwayat transaksi tidak perlu direkap manual dari setiap check-in dan check-out.

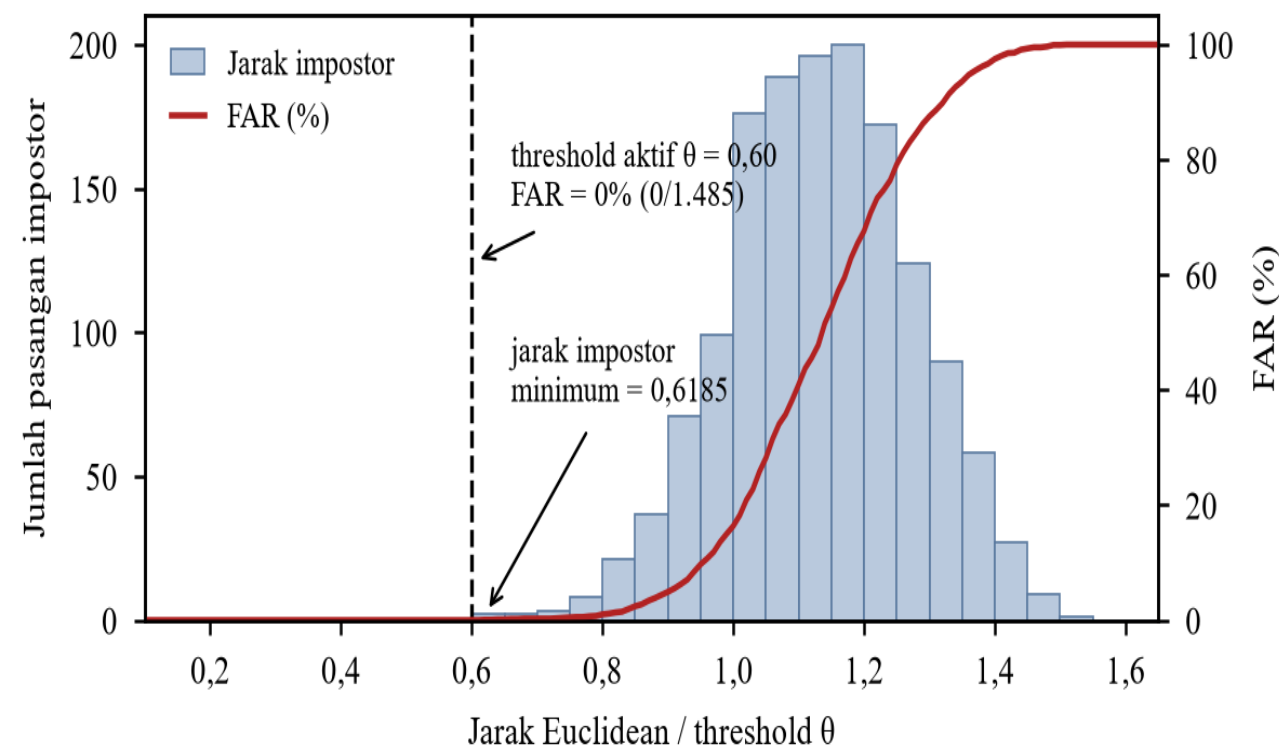
Sistem juga menghitung akumulasi ketidakhadiran sebagai dasar early warning dengan ambang konfigurasi SP1 sebesar 16 jam, SP2 32 jam, SP3 38 jam, dan Drop Out (DO) 46 jam. Gambar 4(d) menunjukkan fasilitas monitoring yang menyajikan akumulasi ketidakhadiran serta status peringatan.

D. Hasil Pengujian

Hasil pengujian terdiri atas pengujian fungsional, evaluasi FAR, dan uji beban. Status implementasi dan hasil pengujian fungsional ditunjukkan pada Tabel 1.

Tabel 1. Status implementasi komponen dan hasil pengujian fungsional

No	Komponen	Status	Keterangan
1	Verifikasi wajah on-device	Selesai	MobileFaceNet TFLite, embedding 192-D, jarak Euclidean + θ
2	Liveness challenge	Prototipe	Lima challenge; belum diuji sebagai PAD
3	Integritas lokasi	Parsial	Akurasi GPS, mock location, geofence; client-attested



Gambar 5. Distribusi jarak Euclidean 1.485 pasangan impostor (histogram) dan kurva FAR terhadap threshold θ . Pada $\theta = 0,60$ tidak ada pasangan impostor yang diterima, tetapi jarak impostor minimum (0,6185) hanya sedikit di atas θ .

Hasil uji beban pada Tabel 2 menunjukkan p95 seluruh endpoint di bawah 2 detik pada ketiga level, tertinggi 1.119 ms (dashboard, 40 pengguna). Seluruh respons gagal berupa HTTP 429 dari rate limiter (60 permintaan per menit per pengguna) karena beban uji melampaui batas tersebut, tanpa galat server pada log aplikasi. Uji dijalankan dari dalam server tanpa latensi jaringan, hanya pada endpoint baca, dan p95 mencakup respons 429.

4	Attendance permit	Selesai	One-time, bound, dan expiring
5	Presensi daring dan luring	Selesai	REST API; antrean Hive terenkripsi
6	Rekapitulasi dan early warning SP	Selesai	Dashboard; ambang SP konfiguratif
7	Enkripsi biometrik	Selesai	AES-256-GCM
8	Pengujian backend	Lulus	255 test / 936 assertion
9	Pengujian aplikasi mobile	Lulus	214 test; static analysis tanpa isu

Tabel 1 menunjukkan bahwa seluruh komponen inti telah terimplementasi dan seluruh pengujian otomatis lulus. Pengujian ini membuktikan kebenaran fungsi perangkat lunak, tetapi tidak mengukur kinerja verifikasi wajah maupun ketahanan terhadap presentation attack.

Evaluasi FAR menggunakan embedding enrollment 55 mahasiswa (1.485 pasangan impostor) dengan jarak 0,6185–1,5083 (rata-rata 1,1332), sebagaimana ditunjukkan pada Gambar 5. Pada $\theta = 0,60$ tidak ada impostor yang diterima (FAR 0%; 0 dari 1.485), sedangkan pada $\theta = 0,65, 0,80$, dan 1,00 FAR menjadi 0,13%, 1,01%, dan 16,36%. Hasil ini membandingkan template enrollment satu sama lain sehingga belum merepresentasikan verifikasi langsung dari frame kamera.

Tabel 2. Hasil uji beban pada server produksi (45 detik per level)

Metrik	20	30	40
	pengguna	pengguna	pengguna
p95 dashboard (ms)	611	907	1.119
p95 jadwal hari ini (ms)	305	701	796
p95 riwayat presensi (ms)	193	696	604
Jumlah permintaan	720	990	1.248
Respons HTTP 429 (%)	33,2	37,2	37,8

Uji coba lapangan terbatas dilakukan oleh kelas Pengantar Teknologi Informasi (27 mahasiswa) pada 22 dan 23 September 2026. Sebanyak 16 check-in tercatat dari 11 model ponsel Android dan seluruhnya lolos liveness, dengan jarak wajah genuine 0,3468–0,5966 (rata-rata 0,4894); 3 check-out juga terverifikasi wajah, sedangkan 13 lainnya ditutup otomatis oleh sistem pada akhir jadwal. Karena aplikasi hanya mengirim percobaan yang lolos verifikasi di perangkat, FRR belum dapat dihitung.

Selama uji coba, perkuliahan dialihkan ke daring akibat bencana alam sehingga radius geofence sementara diperbesar menjadi 500 km; sistem tetap mencatat jarak setiap check-in ke pusat geofence (6 check-in 7,5–13,9 m dan 10 check-in 1,2–7,7 km), sedangkan penolakan di luar radius dibuktikan melalui pengujian otomatis aplikasi mobile.

E. Pembahasan

Integrasi geolocation, biometrik, liveness, dan attendance permit membuat penerimaan transaksi lebih terstruktur dibandingkan sistem dengan satu faktor validasi, sedangkan MobileFaceNet on-device mengurangi ketergantungan pada server [5] dan jarak Euclidean konsisten dengan pendekatan FaceNet [3]. Data FAR dan uji coba lapangan menunjukkan $\theta = 0,60$ berada di antara jarak genuine maksimum (0,5966) dan jarak impostor minimum (0,6185), sehingga perubahan kecil θ langsung berdampak pada FAR atau FRR; penetapannya perlu didasarkan pada kurva FAR–FRR dan EER dari data genuine lapangan [11], [12]. Dari sisi kinerja, p95 di bawah 2 detik pada 40 pengguna simultan menunjukkan backend mampu melayani permintaan baca pada skala satu kelas.

Dari sisi validasi lokasi, sistem membawa metadata akurasi GPS, usia lokasi, dan indikator mock location (Gambar 4(b)), dan radius geofence dapat diatur per lokasi sesuai kebutuhan operasional, misalnya saat perkuliahan daring. Karena evidence masih berasal dari sisi client, sistem ini diposisikan sebagai validasi terintegrasi dengan mitigasi risiko, bukan jaminan anti-fraud absolut.

Pada aspek akademik, data attendance diolah menjadi rekap (Gambar 4(c)) dan akumulasi alpha untuk early warning SP (Gambar 4(d)), sehingga sistem berfungsi sebagai instrumen monitoring akademik, bukan sekadar alat presensi.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, diperoleh tiga kesimpulan berikut:

1. Prototipe presensi mahasiswa berbasis mobile yang memadukan verifikasi wajah MobileFaceNet on-device dan validasi lokasi berbasis geofencing berhasil dibangun melalui tahapan R&D/Prototyping, mencakup alur dari penerbitan attendance permit hingga rekapitulasi kehadiran dan peringatan dini SP.
2. Seluruh pengujian fungsional otomatis berhasil dilalui, evaluasi 1.485 pasangan impostor menghasilkan FAR 0% pada $\theta = 0,60$, uji beban

20–40 pengguna simultan menghasilkan p95 di bawah 2 detik, dan uji coba lapangan mencatat 16 check-in dari 11 model ponsel. Hasil tersebut membuktikan kebenaran fungsi dan kinerja dasar sistem, tetapi belum mengukur FRR, validasi lokasi di lapangan, maupun akurasi pencatatan kehadiran; peningkatan akurasi dan efisiensi dibandingkan presensi berbasis kertas belum dapat disimpulkan karena data perbandingan belum dikumpulkan.

3. Attendance permit memastikan setiap transaksi presensi telah diotorisasi server serta menolak penggunaan ulang dan salah binding. Namun, koordinat lokasi, jarak wajah, dan hasil liveness masih merupakan bukti yang dihitung di perangkat (client-attested) dan liveness belum diuji terhadap presentation attack, sehingga sistem belum dapat diklaim mencegah titip absen atau pemalsuan lokasi, dan keputusan SP/DO tetap memerlukan verifikasi administratif.

B. Saran

Saran untuk penelitian selanjutnya adalah sebagai berikut:

1. Mengumpulkan data genuine berulang dari frame verifikasi langsung di lapangan untuk menghitung FRR dan EER, mengulang evaluasi FAR pada kondisi yang sama, dan mengevaluasi validasi lokasi dengan radius geofence operasional, sebagai dasar penentuan threshold dan parameter validasi yang optimal.
2. Melakukan uji presentation attack detection yang terukur menggunakan foto cetak, tampilan layar, dan video replay, terpisah dari evaluasi FAR/FRR.
3. Membandingkan sistem dengan presensi berbasis kertas pada kelas yang sama, meliputi waktu presensi, akurasi pencatatan, jumlah kesalahan rekap, dan kecepatan penyediaan data, serta mengevaluasi usability menggunakan System Usability Scale (SUS) [14].
4. Memindahkan keputusan verifikasi wajah dan liveness ke verifikator sisi server berbasis artefak capture yang terikat challenge, disertai platform attestation, agar bukti presensi tidak sepenuhnya bergantung pada klaim perangkat.

DAFTAR PUSTAKA

- [1] F. O. Isinkaye, J. Soyemi, and O. I. Arowosegbe, "An Android-based face recognition system for class attendance and malpractice control," *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 1, pp. 79–83, 2020.
- [2] D. Sunaryono, J. Siswanto, and R. Anggoro, "An android based course attendance system using face recognition," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 3, pp. 304–312, 2021, doi: 10.1016/j.jksuci.2019.01.006.
- [3] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, 2015, pp. 815–823.
- [4] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, Long Beach, CA, 2019, pp. 4690–4699.
- [5] S. Chen, Y. Liu, X. Gao, and Z. Han, "MobileFaceNets: Efficient CNNs for accurate real-time face verification on mobile devices," *arXiv*, Apr. 2018, [Online]. Available: <https://arxiv.org/abs/1804.07573>

- [6] J. R. Fernandez, H. Mamarungkas, S. Vinson, and K. Atuel, "Facial and geofencing-based attendance tracking system for deployed personnel," *Mindanao J. Sci. Technol.*, vol. 23, no. 2, pp. 133–148, 2025, doi: 10.61310/mjst.v23i2.2478.
- [7] P. D. Lanjewar, S. S. Joshi, D. B. Patil, H. S. Patil, and V. D. Patil, "Automated attendance management system using face recognition and GPS localization," *Int. J. Innov. Eng. Sci.*, vol. 10, no. 6, pp. 17–22, 2025, doi: 10.46335/IJIES.2025.10.6.4.
- [8] R. S. Pressman and B. R. Maxim, *Software Engineering: A Practitioner's Approach*, 9th ed. New York: McGraw-Hill, 2020.
- [9] Android Developers, "Create and monitor geofences," 2026. [Online]. Available: <https://developer.android.com/develop/sensors-and-location/location/geofencing>
- [10] Google for Developers, "Face detection – ML Kit," 2024. [Online]. Available: <https://developers.google.com/ml-kit/vision/face-detection>
- [11] P. Grother and M. Ngan, "Face recognition vendor test (FRVT): Performance of face identification algorithms," Gaithersburg, MD: National Institute of Standards and Technology, 2014. doi: 10.6028/NIST.IR.8009.
- [12] P. Grother, M. Ngan, and K. Hanaoka, "Face recognition vendor test (FRVT) part 2: Identification," Gaithersburg, MD: National Institute of Standards and Technology, 2019. doi: 10.6028/NIST.IR.8271.
- [13] ISO/IEC, "Information Technology – Biometric Presentation Attack Detection – Part 3: Testing and Reporting (ISO/IEC 30107-3:2023)," 2023.
- [14] J. Brooke, "SUS: A 'quick and dirty' usability scale," in *Usability Evaluation in Industry*, P. W. Jordan, B. Thomas, B. A. Weerdmeester, and I. L. McClelland, Eds., London: Taylor & Francis, 1996, pp. 189–194.