



Implementation Anti-Fraud Security on Smart Campus Attendance System Using Face Recognition Liveness Detection and Anti-Fake GPS Geofencing

Azral Satrani ¹, Tanwir ¹, Dading Oktaviadi Resminanta ¹, Muhammad Maulana ¹, Kartarina Agustina ¹, Gede Yogi Pratama ¹

¹. Program Studi Ilmu Komputer, Universitas Bumigora, Indonesia.

* Korespondensi: azral@universitasbumigora.ac.id

Sitasi: A. Satrani, T. Tanwir, D. O. Resminanta, M. Maulana, K. Agustina, and G. Y. Pratama, "Implementation Anti-Fraud Security on Smart Campus Attendance System Using Face Recognition Liveness Detection and Anti-Fake GPS Geofencing", *Jurnal Teknologi Informasi Dan Multimedia*, vol. 8, no. 3, hlm. xx-yy, 2026.

<https://doi.org/10.35746/jtim.v8i3.1057>

Diterima: 06-06-2026

Direvisi: 16-07-2026

Disetujui: 31-07-2026



Copyright: © 2026 oleh para penulis. Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License. (<https://creativecommons.org/licenses/by-sa/4.0/>).

Abstract. In the digital era, the fingerprint-based attendance system used by University of Bumigora where considered ineffective and inefficient due to hygiene issues, physical vulnerability, the risk of forgery, and slow processing speed during peak hours. In addition, as the digital attendance system develops, new challenges arise in the form of biometric data manipulation through presentation attacks (photos/videos/masks) and location manipulation using fake GPS applications. This dual vulnerability is a critical issue that can damage data integrity and the governance of educational institutions. To address these issues, this study proposes the design and development of a Smart Campus attendance system that integrates two anti-fraud security mechanisms, namely Face Recognition *liveness* detection and Anti-Fake GPS *Geofencing*. *Liveness* Detection technology functions to detect real-life signs to distinguish real faces from fake representations, while Anti-Fake GPS validates the signal consistency and physicality of users within a predetermined campus geographic radius (geofence). This system was developed using Agile methods to ensure adaptive and structured development. From a technological perspective, this system integrates the Vue JS framework in the user interface (UI) due to its robust performance, and the Laravel framework in the backend due to its advantages in *Model-View-Controller* (MVC) architecture, security, and high scalability. Through this approach, the study aims to evaluate the effectiveness of a layered anti-fraud mechanism in preventing fraud and measure improvements in administrative efficiency compared to conventional fingerprint systems.

Keywords: Digital Presence, Liveness Detection, Anti-Fake GPS, Geofencing, Vue JS, Laravel, Agile.

Abstrak. Di era digital, sistem presensi berbasis *fingerprint* yang digunakan Universitas Bumigora dinilai kurang efektif dan efisien karena masalah higienitas, kerentanan fisik, risiko pemalsuan, serta rendahnya kecepatan proses pada jam sibuk. Selain itu, seiring berkembangnya sistem presensi digital, muncul tantangan baru berupa manipulasi data biometrik melalui *presentation attack* (foto/video/topeng) dan manipulasi lokasi menggunakan aplikasi *fake GPS*. Kerentanan ganda ini menjadi masalah kritis yang dapat merusak integritas data dan tata kelola institusi pendidikan. Untuk mengatasi masalah tersebut, penelitian ini mengusulkan rancangan dan pengembangan sistem presensi *Smart Campus* yang mengintegrasikan dua mekanisme keamanan anti-kecurangan (*anti-fraud security*), yaitu *Face Recognition Liveness Detection* dan *Anti-Fake GPS Geofencing*. Teknologi *Liveness Detection* berfungsi mendeteksi tanda kehidupan nyata untuk membedakan wajah asli dari

representasi palsu, sementara *Anti-Fake GPS* memvalidasi konsistensi sinyal dan fisik pengguna dalam radius geografis (*geofence*) kampus yang telah ditentukan. Sistem ini dikembangkan menggunakan metode *Agile* untuk memastikan pengembangan yang adaptif dan terstruktur. Dari sisi teknologi, sistem ini mengintegrasikan *framework* Vue JS pada antarmuka pengguna (UI) karena performanya yang tangguh, serta *framework* Laravel pada *backend* karena keunggulannya dalam arsitektur *Model-View-Controller* (MVC), keamanan, dan skalabilitas yang tinggi. Melalui pendekatan ini, penelitian bertujuan mengevaluasi efektivitas mekanisme *anti-fraud* berlapis dalam mencegah kecurangan serta mengukur peningkatan efisiensi administrasi dibandingkan dengan sistem *fingerprint* konvensional.

Kata Kunci: Presensi Digital, *Liveness Detection*, *Anti-Fake GPS*, *Geofencing*, Vue JS, Laravel, *Agile*.

1. Pendahuluan

Perkembangan dunia komputer beberapa tahun terakhir maju dengan pesat, baik pada perangkat keras (*hardware*) maupun pada perangkat lunak (*software*). Dari media cetak hingga elektronik menjadikan kebutuhan masyarakat terhadap suatu informasi menjadi sangat besar [1] *satu*. Seiring dengan semakin maju dan canggih teknologi, dirasakan semakin pentingnya *hardware* dan *software* sebagai sarana penunjang untuk memenuhi kebutuhan dalam melakukan atau membantu dalam menyelesaikan pekerjaan yang senantiasa dilakukan dalam kegiatan sehari-hari di dunia kerja, terutama yang berkaitan dengan pengambilan data dan pengolahan data [2] [3]. Sistem presensi menjadi komponen vital untuk manajemen sumber daya manusia diberbagai institusi, seperti sekolah, perkantoran, maupun pabrik yang berfungsi untuk memantau kedisiplinan dan penggajian [3]. Teknologi sidik jari (*fingerprint*) telah lama menjadi pilihan, karena keamanannya, namun kini efektivitas nya mulai diragukan. Sistem presensi yang berbasis sidik jari, seringkali dibangun pada *platform* yang *hardcoded* (tidak mengizinkan komunikasi dengan sistem atau piranti lain) sehingga menyulitkan ketika harus diintegrasikan dengan sistem utama [4] *empat*[4]. ketergantungan pada platform *hardcoded* sering kali menghambat integrasi sistem tersebut dengan infrastruktur data utama di instansi terkait [5] *lima*.

Sistem presensi dosen dan staf pada Institusi Universitas Bumigora meggunakan *tools Fingerprint* (sidik jari). Presensi menggunakan sidik jari memang membantu dalam administrasi sumber daya manusia, dimana dari sistem, dapat mengetahui jam masuk, pulang, telat, pulang cepat, dan lembur. Dengan *fingerprint*, Universitas Bumigora masih memiliki beberapa kelemahan seperti sulitnya pengidentifikasian jari jika kondisi jari terkelupas, berminyak dan celah untuk melakukan manipulasi sidik jari antar pengguna hal ini juga diutarakan pada penelitian sebelumnya [6], [7] sehingga menimbulkan masalah baru, menjadikan *Fingerprint* tidak efektif dan efisien dari segi proses pengambilan data dan pengolahan data. Permasalahan ini sejalan dengan hasil penelitian sebelumnya yang menunjukkan penggunaan presensi *fingerprint* kurang fleksibilitas dan tidak lebih baik dalam hal higienitas dibandingkan dengan *face recognition* [8], [9].

Selain itu, dengan meluasnya penggunaan sistem presensi digital, metode untuk memanipulasinya turut berkembang. Dua bentuk kecurangan yang paling umum terjadi adalah *Spoofing* pada data *biometrik* dan manipulasi lokasi geografis [10], [11]. Pada sistem pengenalan wajah, serangan *presentation attack* seperti penggunaan foto, video rekaman, atau topeng dapat dengan mudah mengelabui kamera untuk mengonfirmasi kehadiran seseorang yang sebenarnya tidak hadir secara fisik [12]. Sementara itu, pada sistem yang berbasis lokasi, mahasiswa atau staf dapat menggunakan *fake GPS* atau *GPS spoofing app* untuk mengubah sinyal lokasi perangkat mereka, seolah-olah mereka berada di area kampus padahal berada di tempat lain.

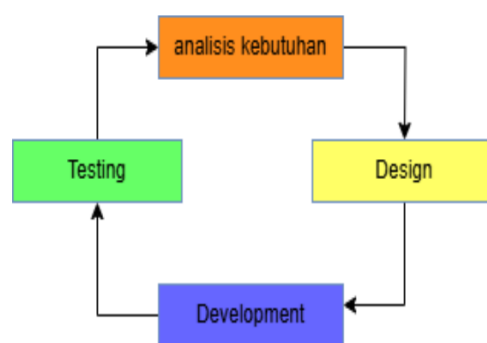
Kerentanan ganda ini menjadi masalah kritis, terutama pada institusi pendidikan yang menjadikan tingkat kehadiran sebagai salah satu komponen penilaian atau syarat administratif. Presensi yang tidak akurat tidak hanya merugikan secara akademik tetapi juga merusak integritas data dan tata kelola kampus. Oleh karena itu, diperlukan sebuah pendekatan keamanan yang proaktif dan komprehensif, yang tidak hanya berfokus pada kemudahan akses tetapi juga pada ketahanan terhadap serangan [13].

Penelitian ini mengusulkan implementasi sistem presensi *Smart Campus* yang mengintegrasikan dua mekanisme anti-kecurangan (*anti-fraud security*), yaitu *Liveness Detection* pada pengenalan wajah dan *Anti-Fake GPS Geofencing* [14]. *Liveness detection* bekerja dengan mendeteksi tanda-tanda kehidupan nyata (seperti gerakan kelopak mata, kedipan, atau perubahan tekstur kulit) untuk membedakan wajah asli dari representasi palsu. Sementara itu, anti-fake GPS menggunakan validasi multi-sumber dan analisis konsistensi sinyal untuk memastikan bahwa lokasi perangkat tidak dimanipulasi sebelum mengizinkan proses presensi dalam batasan geografis (*geofence*) [15].

Penelitian ini merancang dan mengembangkan sistem presensi menggunakan Face Recognition *Liveness Detection* dan terintegrasi dengan *Anti-Fake GPS Geofencing* yang bertujuan untuk memvalidasi fisik pengguna dalam radius serta mendeteksi alat manipulasi lokasi menggunakan metode pengembangan system, dengan menggunakan SDLC (*Software Development Life Cycle*) model *Agile*. Melalui pendekatan *Agile*, penelitian ini mengevaluasi efektivitas mekanisme *anti-fraud* berlapis dalam mencegah kecurangan serta mengukur peningkatan efisiensi administrasi dibanding sistem *fingerprint* konvensional.

2. Metode Penelitian

Dalam sistem presensi ini penulis mengembangkan sistem informasi dengan metode pengembangan perangkat lunak *Agile*. *Agile* adalah pendekatan pengembangan perangkat lunak yang menekankan fleksibilitas, kerja tim, dan pengiriman produk yang cepat dan iteratif. Metode ini berbeda dari model pengembangan tradisional yang lebih linear dan berbasis tahapan seperti *waterfall* [16] yang ditampilkan pada gambar 1.



Gambar 1. Tahapan metode *Agile*

Gambar 1 menunjukkan bahwa fase penelitian dilakukan dalam 4 tahapan sebagai berikut:

2.1. Analisis Kebutuhan

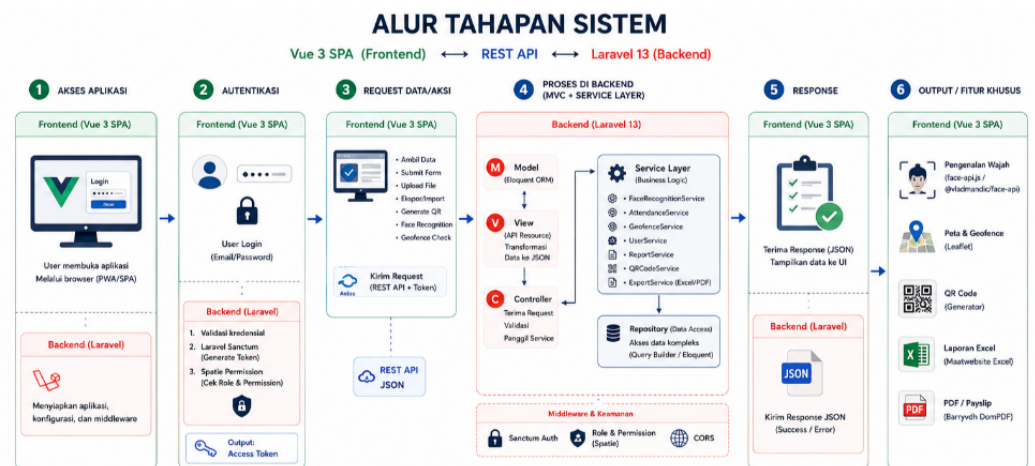
Tujuan dari tahap ini melakukan pengumpulan data dengan melakukan observasi langsung terkait proses presensi di Universitas Bumigora dan melakukan dokumentasi melalui penelusuran dan analisis dokumen dengan bekerja sama staf PUSTIK terkait alur presensi setiap karyawan dan laporan presensi serta kebutuhan perangkat keras dan kebutuhan perangkat lunak yang digunakan untuk sistem presensi ditampilkan pada tabel 1.

Tabel 1. Detail perangkat yang digunakan untuk pengembangan sistem presensi

Jenis	Nama Alat	Fungsi penting
Perangkat keras	Laptop (Intel core i5/8GB RAM)	Media perancangan, coding, dan pengujian
	Node Js	Node Js memungkinkan kode javascript berjalan di server, luar browser.
	Vue Js 3	Kerangka untuk membangun antarmuka pengguna
	Geolocation API	Ambil Latitude, Longitude, & Accuracy Flag
Perangkat Lunak	Laravel v.13 (PHP)	Kerangka kerja pengembangan Backend
	Basis Data : MySQLv.8.0	Manajemen basis data (<i>Database</i>)
	Web Server : Apache (via Laragon)	Server local development untuk menjalankan aplikasi
	Face-API.js	Untuk pengenalan wajah
	Leaflet	Peta (Geofence)
	Maatwebsite Excel, Barryvdh DomPDF	Ekspor/import Excel dan format PDF

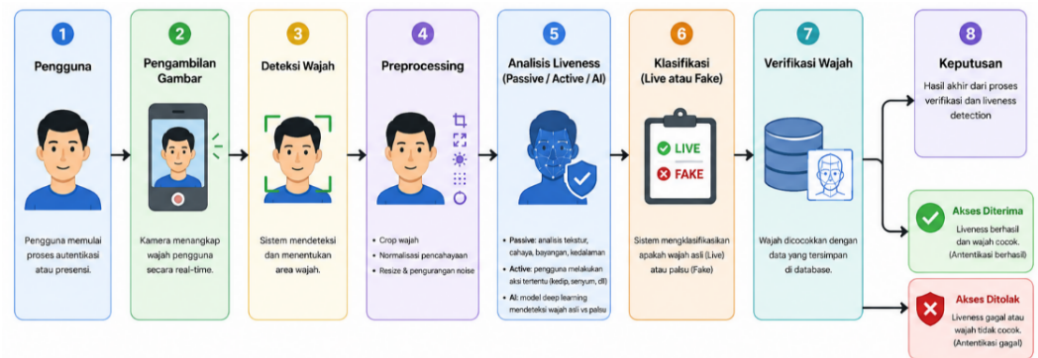
2.2. Perancangan (Design)

Pada tahapan desain berkaitan dengan merancang arsitektur sistem, desain database, antarmuka pengguna (UI/UX), dan alur proses aplikasi setiap proses aplikasi. Alur tahapan sistem dapat dilihat pada gambar 2.

**Gambar 2.** Alur tahap sistem

2.3. Liveness detection

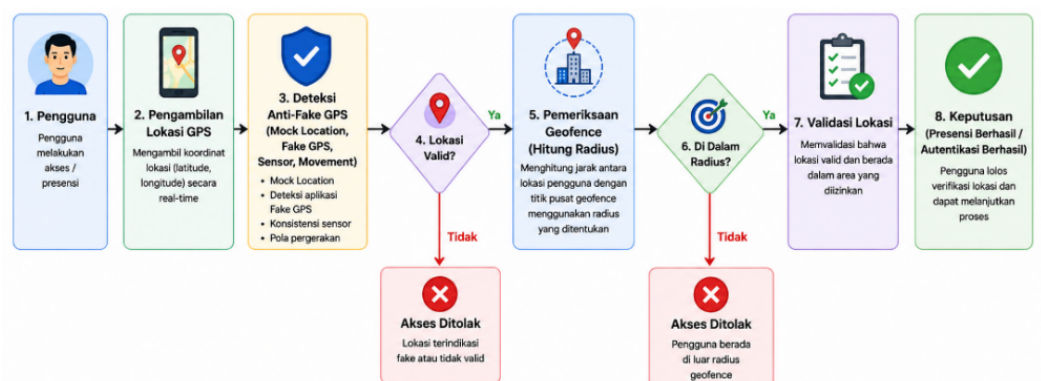
Liveness Detection merupakan mekanisme keamanan biometrik yang memastikan bahwa wajah yang digunakan dalam proses autentikasi benar-benar berasal dari manusia yang hadir secara langsung, sehingga mampu mencegah berbagai serangan *spoofing* seperti penggunaan foto, video, layar perangkat, maupun topeng. Secara umum, metode ini melalui tujuh tahapan utama, yaitu akuisisi gambar, deteksi wajah, pra-pemrosesan, analisis liveness, klasifikasi, verifikasi identitas, dan pengambilan keputusan. Dengan menggabungkan teknik pengolahan citra dan kecerdasan buatan, *liveness detection* mampu meningkatkan keandalan sistem presensi, e-KYC, maupun kontrol akses karena hanya mengizinkan autentikasi ketika identitas pengguna dan keaslian wajah telah tervalidasi [17]. Tahapan proses liveness detection dapat dilihat pada gambar 3.



Gambar 3. Tahapan proses Liveness Detection

2.3.1. Anti fake GPS Geofencing

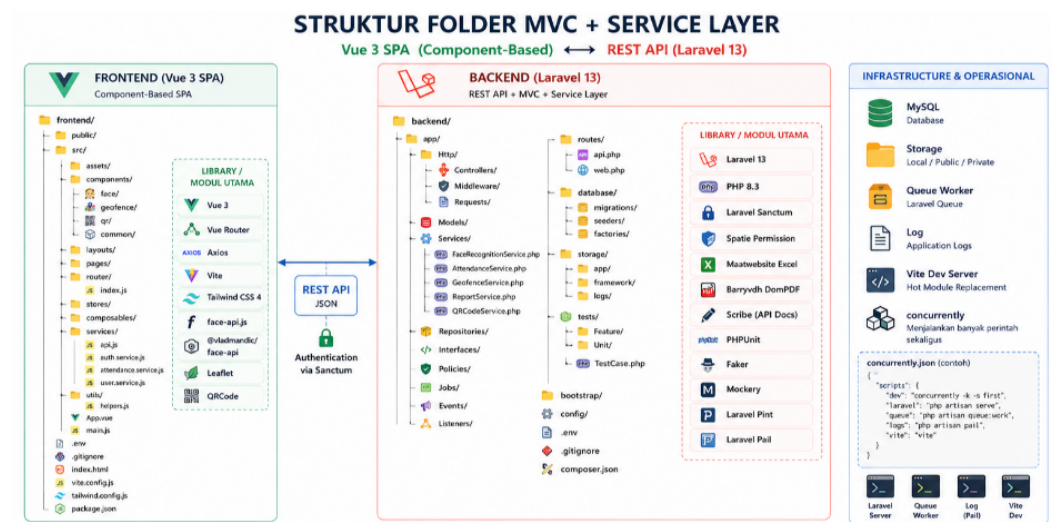
Metode Anti-Fake GPS Geofencing mengintegrasikan deteksi pemalsuan lokasi dengan pembatasan area berbasis *geofence* untuk memastikan bahwa pengguna benar-benar berada di lokasi yang sah. Tahapannya meliputi akuisisi lokasi GPS, validasi keaslian lokasi (mock location, deteksi aplikasi *Fake GPS*, konsistensi sensor, dan analisis pola pergerakan), pemeriksaan *geofence* berdasarkan radius lokasi, validasi hasil, dan pengambilan keputusan. Pendekatan ini mampu meningkatkan keamanan sistem presensi maupun kontrol akses dengan mencegah manipulasi lokasi sekaligus memastikan pengguna berada dalam area yang telah ditentukan [18]. Tahapan proses anti fake GPS *geofencing* dapat dilihat pada gambar 4.



Gambar 4. Tahapan proses Anti Fake GPS Geofencing

2.3.2. Development

Pada tahap *development*, pengembang (*developer*) mulai melakukan pengkodean (*coding*) untuk mengimplementasikan algoritma pengenalan wajah, membangun mekanisme *liveness detection*, dan memprogram fitur *geofencing* yang mampu mendeteksi manipulasi lokasi GPS. Struktur folder pada tahapan *development* untuk pengkodean menggunakan struktur MVC (*Model, View, Controller*) dapat dilihat pada gambar 3.



Gambar 5. Struktur MVC

2.4. Testing

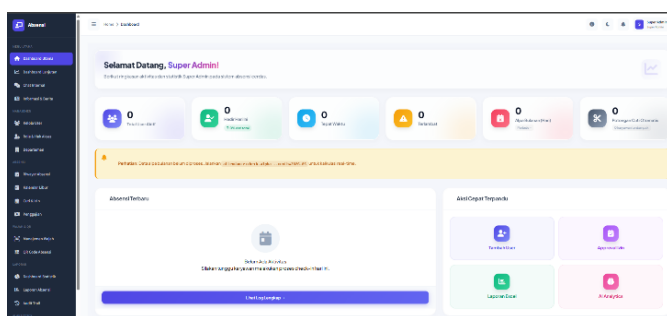
Penggabungan sistem pendeteksi penipuan ke dalam platform yang sudah ada dikenal sebagai integrasi modul anti-fraud. Modul ini memungkinkan platform untuk memantau transaksi secara real-time dan menemukan pola mencurigakan seperti transaksi tidak wajar, identitas palsu, atau klaim fiktif.

Metode *Black-Box Testing* digunakan untuk menguji setiap fitur yang telah dikembangkan. Pengujian ini memvalidasi kesesuaian input dan *output* sistem terhadap spesifikasi kebutuhan tanpa melakukan peninjauan ke dalam struktur kode internal dan pengujian setiap pengguna dalam melakukan presensi, untuk meminimalisir *error* fungsional sebelum sistem diterapkan.

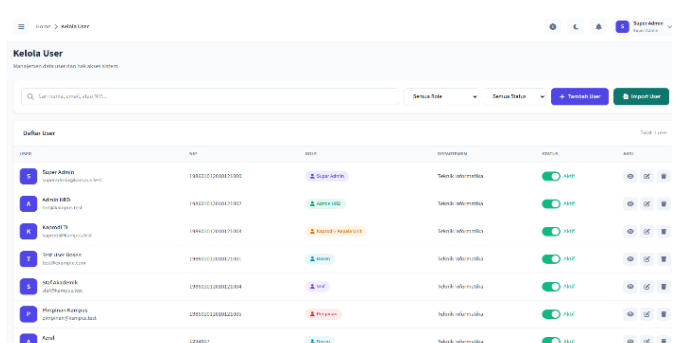
3. Hasil dan Pembahasan

3.1. Hasil Penelitian

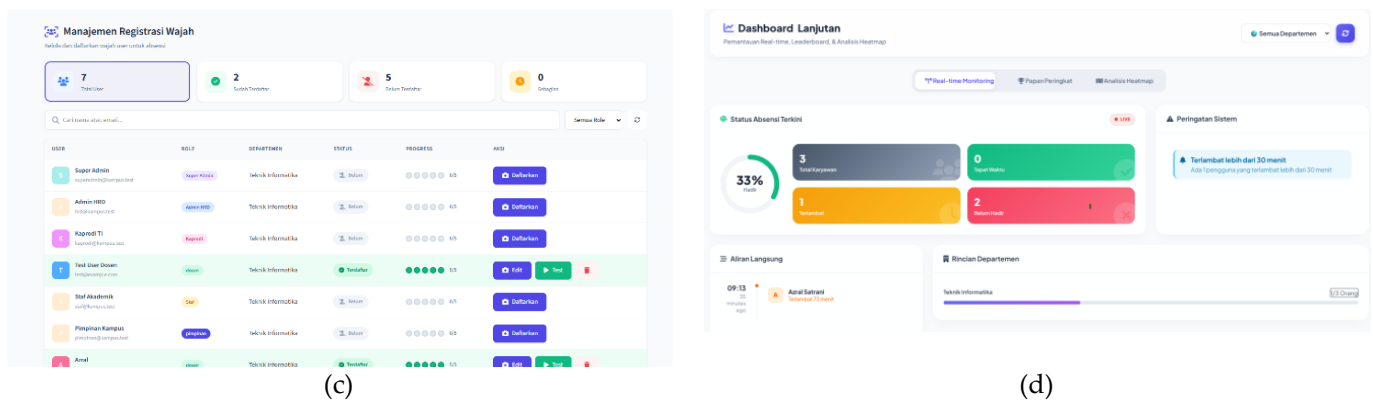
Sistem memiliki 2 jenis pengguna, Pengguna pertama untuk super admin dan pengguna, memiliki hak akses yang dapat melakukan CRUD (*Create, Read, Update, Delete*) untuk menambah, mengubah, dan menghapus pengguna serta membuat laporan presensi. Hasil tampilan pada halaman super admin dapat dilihat pada gambar.



(a)



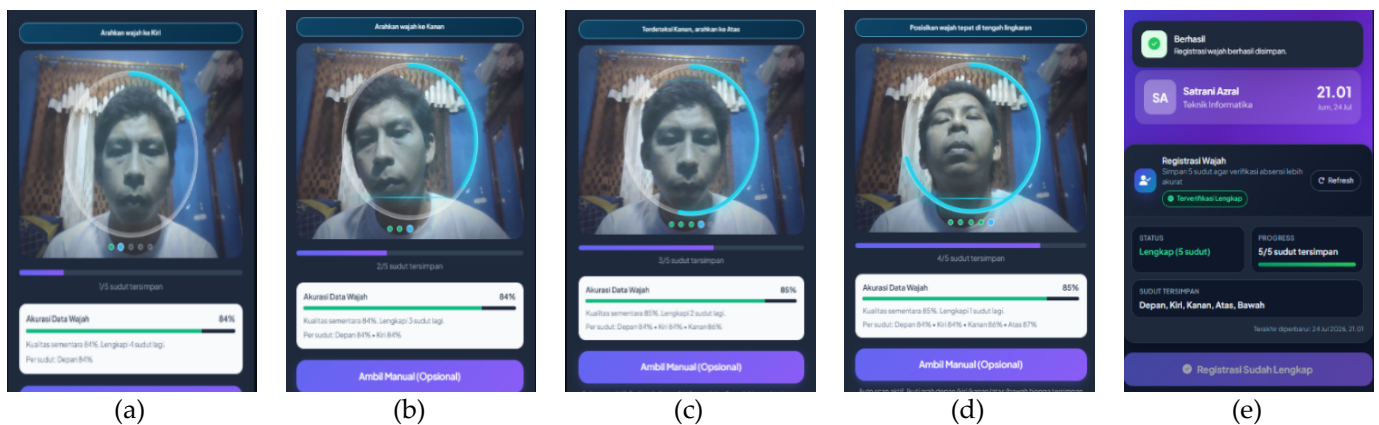
(b)



Gambar 6. Halaman dashboard super admin

Pada gambar 6 terlihat tampilan aplikasi autentikasi user: (a) laman dashboard super admin, (b) halaman penambahan untuk akun pengguna baru, (c) laman manajemen registrasi wajah, (d) laman untuk dashboard lanjutan monitoring status absensi terkini.

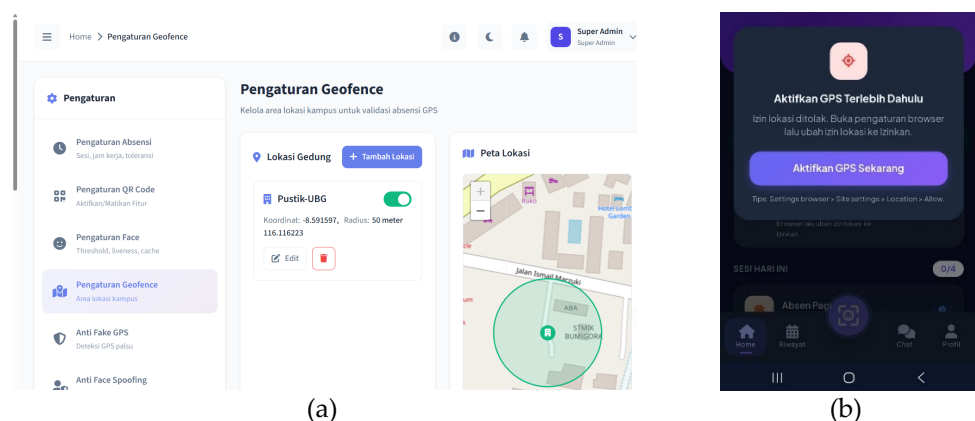
Pengguna kedua ditujukan untuk karyawan divisi sumber daya manusia (SDM) dan dosen untuk melakukan registrasi untuk penggunaan aplikasi, presensi harian berdasarkan lokasi dan wajah yang ditampilkan pada gambar 7.



Gambar 7. Halaman proses registrasi wajah dari 5 sudut

Pada gambar 5 menampilkan halaman: (a) registrasi wajah untuk dari sudut kiri, (b) halaman registrasi wajah dari sudut kanan (c) registrasi wajah dari sudut atas (d) registrasi wajah dari sudut bawah (e) halaman berhasil registrasi wajah dari 5 sudut.

Pengaturan mekanisme *geofence* dan pada lokasi kampus oleh super admin dan notifikasi aktivasi untuk pengguna saat akan melakukan presensi pada aplikasi yang dapat dilihat pada gambar 8.



Gambar 8. Pengaturan mekanisme geofence dan notifikasi aktivasi untuk pengguna

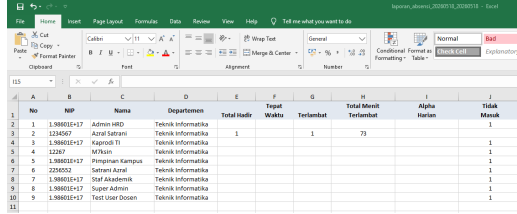
Gambar 8 menampilkan halaman: (a) Pengaturan *Geofence* GPS koordinat dan radius aplikasi (b) halaman peringatan yang meminta pengguna untuk mengaktifkan layanan GPS (*Location Services*).

3.2. Hasil Ekspor Laporan

Fitur reporting yang terbukti lebih cepat dibandingkan dengan cara konvensional, dapat merekap dengan format file excel atau PDF. Memberikan efisiensi lebih baik untuk rekapitulasi presensi dan melihat kinerja dan karyawan dapat dilihat pada gambar 9.



(a)



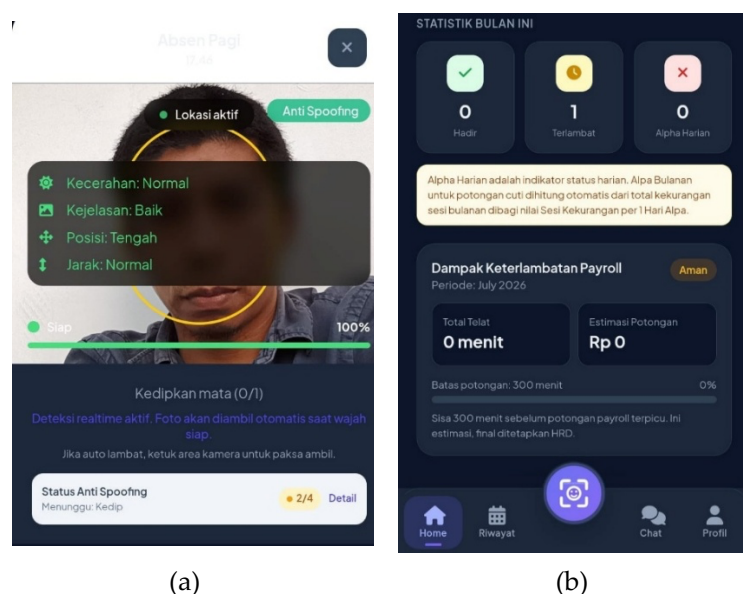
(b)

Gambar 9. Hasil Ekspor Laporan

Pada Gambar 9 Menampilkan halaman: (a) hasil ekspor laporan presensi dengan format PDF (b) hasil ekspor laporan presensi dengan format excel.

3.3. Testing Presensi

Hasil percobaan yang dilakukan jika gambar sesuai dengan dan terdeteksi aplikasi akan menampilkan informasi terkait kecerahan, kejelasan gambar, posisi dan jarak, serta akurasi dan memberikan informasi statistik staf atau dosen dan informasi dampak keterlambatan yang dapat dilihat pada gambar 10.

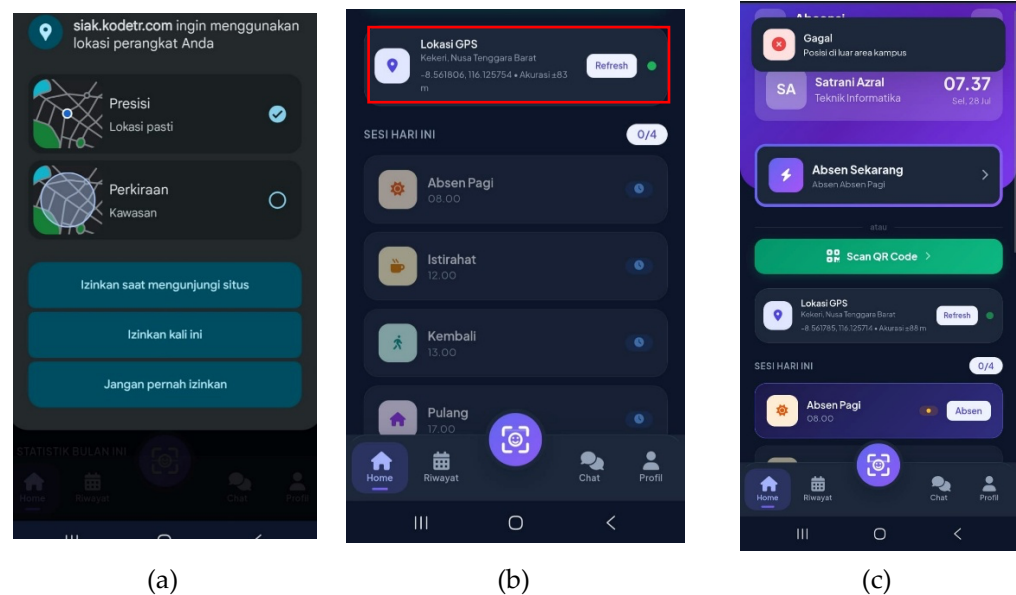


Gambar 10. Testing presensi

Gambar 7 menampilkan halaman (a): menampilkan informasi testing presensi dan menampilkan informasi pengambilan gambar serta instruksi untuk melakukan pengambilan gambar dan lokasi aktif (b): laman informasi statistik dampak keterlambatan payroll berupa total keterlambatan serta estimasi pemotongan gaji.

3.4. Pengujian Anti Fake GPS

Hasil pengujian anti fake GPS saat aplikasi digunakan diluar area kampus akan menampilkan penggunaan lokasi perangkat, informasi lokasi perangkat saat ini dan sistem tidak bisa digunakan untuk presensi seperti pada gambar 11.



Gambar 11. Pengujian Anti Fake GPS

Gambar 11 menampilkan halaman (a): sistem meminta izin untuk menggunakan lokasi perangkat agar dapat mengetahui posisi pengguna secara akurat (b): menampilkan informasi lokasi pengguna serta daftar sesi presensi, (c): notifikasi pesan pengguna berada diluar area kampus, sehingga presensi belum dapat dilakukan.

3.5. Testing (Black-Box Testing)

Eksperimen fungsionalitas menggunakan pendekatan Black-Box Testing dilakukan untuk memastikan bahwa input dan output sesuai dengan spesifikasi yang diminta. Tabel 2 berikut menyajikan informasi tentang hasil pengujian untuk sepuluh skenario utama, yang mencakup dari pembuatan akun baru hingga pembuatan laporan.

Tabel 2. Pengujian Black-Box

No	Rencana Eksperimen	Deskripsi eksperimen	Hasil	Penjelasan
1	Pendaftaran akun	Pembuatan pengguna baru	Sesuai	Berhasil
2	Registrasi wajah	Pendaftaran wajah pengguna dari 5 sudut berbeda	Sesuai	Berhasil
3	Autentikasi login	Login pengguna dengan dengan kredensial	Sesuai	Berhasil
4	Cek radius lokasi	Melakukan pengecekan lokasi area untuk presensi	Sesuai	Berhasil
5	Monitoring presensi	Pemantauan pengguna secara realtime	Sesuai	Berhasil
6	Presensi dengan wajah dan GPS	Pengguna melakukan presensi dengan wajah dan GPS	Sesuai	Berhasil
7	Manajemen user	Pengelolaan pengguna seperti mengatur hak akses, menambah dan menghapus pengguna.	Sesuai	Berhasil
8	Manajemen presensi	Mengelola riwayat presensi, kalender, libur dan cuti	Sesuai	Berhasil

No	Rencana Eksperimen	Deskripsi eksperimen	Hasil	Penjelasan
9	Manajemen wajah dan GPS	Melakukan perubahan pada sudut pengambilan wajah dan posisi pengguna	Sesuai	Berhasil
10	Pembuatan Laporan	Pembuatan dan percetakan laporan berupa file Excel dan PDF	Sesuai	Berhasil

4. Kesimpulan dan Saran

Berdasarkan hasil penelitian menunjukkan bahwa digitalisasi sistem presensi yang menerapkan pengenalan wajah dan GPS dapat melakukan proses presensi dengan lebih efisien dan efektif dibandingkan presensi dengan fingerprint atau presensi manual dengan kertas absen dan pulpen. Hasil ini sesuai dengan penelitian sebelumnya yang menemukan bahwa presensi menggunakan wajah dan menerapkan arsitektur MVC dalam kerangka kerja Laravel dan metode Agile menambah fleksibilitas dalam pembuatan sistem informasi absensi kampus [19].

Studi ini memberikan kontribusi faktual yang lebih spesifik daripada penelitian sebelumnya yang hanya berfokus pada presensi pengenalan wajah. Keunggulan utama penelitian ini adalah bukti kuantitatif tentang efisiensi dan keefektifan waktu proses. Dibandingkan dengan sistem presensi fingerprint, digitalisasi proses presensi memberikan dampak yang jauh lebih cepat, akurat dan transparan. Dengan peningkatan efisiensi yang signifikan, digitalisasi proses presensi berdampak pada operasional yang lebih cepat, akurat dan fleksibel dibandingkan dengan menggunakan fingerprint dan presensi manual [20].

Meskipun capaian sistem presensi secara fungsional efektif dan efisien, sistem masih memiliki keterbatasan. Sebagai langkah pengembangan untuk penelitian selanjutnya dapat menambahkan fitur barcode berbasis aplikasi sebagai metode verifikasi sekunder. Kehadiran fitur ini dapat berfungsi sebagai sistem cadangan (backup) guna menjaga kelancaran proses presensi apabila terjadi kendala teknis pada pemindaian wajah akibat intensitas cahaya yang buruk atau gangguan akurasi pada sinyal GPS. Penambahan fitur ini bertujuan untuk mempercepat proses antrian presensi saat terjadi masalah.

Referensi

- [1] R. D. Lestari, "Perlindungan Hukum bagi Pasien dalam Telemedicine," *Jurnal Cakrawala Informasi*, vol. 1, no. 2, pp. 51–65, Dec. 2021, <https://doi.org/10.54066/jci.v1i2.150>.
- [2] M. E. Arjunda Hepa Laurentius, "Desain dan Implementasi Sistem Informasi Presensi Website untuk Meningkatkan Efisiensi Manajemen," *MNEMONIC*, vol. 8, pp. 271–279, 2025, <https://doi.org/10.36040/mnemonic.v8i2.14397>.
- [3] A. K. Saputro, A. Ubaidillah, H. A. Diputra, D. T. Laksono, A. F. Ibadillah, and A. Z. Nur, "Liveness Detection-Based Home Door Security System for Anti-Spoofing Using Intel RealSense F455 Camera and LBPH," *Jambura Journal of Electrical and Electronics Engineering*, vol. 8, no. 1, pp. 062–071, Jan. 2026, <https://doi.org/10.37905/jjee.v8i1.34918>.
- [4] Miftakhurrokhmat, R. A. Rajagede, and R. Rahmadi, "Classroom Attendance Based on Smiling Face Patterns and Nearby Wifi with Deep Learning," *Jurnal RESTI*, vol. 5, no. 1, pp. 31–38, Feb. 2021, <https://doi.org/10.29207/resti.v5i1.2575>.
- [5] T. Budiarto and B. Hartono, "Perancangan Sistem Presensi Karyawan Menggunakan Scan Sidik Jari pada MTs Fatahillah Karangawen Demak," *Jurnal Cakrawala Informasi*, vol. 3, no. 1, pp. 28–41, Jun. 2023, <https://doi.org/10.54066/jci.v3i1.279>.
- [6] J. R. K. Putra, "Sistem Absensi Mahasiswa Menggunakan Finger Print U Are U 4500 Pada Stmik Amik Riau," *JSR : Jaringan Sistem Informasi Robotik*, vol. 2, no. 1, pp. 75–80, 2018, <https://doi.org/10.58486/jsr.v2i1.28>.
- [7] Moh. W. Septyanto, H. Sofyan, H. Jayadianti, O. S. Simanjuntak, and D. B. Prasetyo, "Aplikasi Presensi Pengenalan Wajah Dengan Menggunakan Algoritma Haar Cascade Classifier," *Telematika*, vol. 16, no. 2, p. 87, Jan. 2020, <https://doi.org/10.31315/telematika.v16i2.3182>.
- [8] F. Adiputra and F. Umam, "Presensi Wireless Otomatis menggunakan Face Recognition," *Rekayasa*, vol. 15, no. 3, pp. 386–397, Dec. 2022, <https://doi.org/10.21107/rekayasa.v15i3.19762>.

- [9] I. P. E. D. Nugraha and G. Sukadarmika, "Sistem Presensi Otomatis Menggunakan Pengenalan Wajah Berbasis Deep Learning dan Real-Time Database," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 10, no. 4, pp. 958–966, Sep. 2025, <https://doi.org/10.30591/jpit.v10i4.8792>.
- [10] W. Liu and P. Papadimitratos, *Coordinated Position Falsification Attacks and Countermeasures for Location-Based Services*. 2025. <https://doi.org/10.48550/arXiv.2510.27346>.
- [11] R. Ramachandra and C. Busch, "Presentation Attack Detection Methods for Face Recognition Systems," *ACM Comput. Surv.*, vol. 50, no. 1, pp. 1–37, Jan. 2018, <https://doi.org/10.1145/3038924>.
- [12] M. Salim, "Design and Creation of Web-Based Online Attendance Systems in Higher Education Institutions," *Journal of Dinda Data Science, Information Technology, and Data Analytics*, vol. 3, no. 1, pp. 1–5, 2023, <https://doi.org/10.20895/dinda.v3i1.771>.
- [13] E. N. F. Dewi, G. N. Tarempa, A. N. Rachman, and A. Febriansyah, "Sistem Presensi Perkuliahan Mahasiswa Berbasis Face Recognition dengan Metode Liveness Detection," *Indonesian Journal Computer Science*, vol. 4, no. 2, pp. 118–126, Oct. 2025, <https://doi.org/10.31294/ijcs.v4i2.9876>.
- [14] D. F. Putri, and D. Widhiantoro, "Implementasi Metode Geofencing Untuk Sistem Pelacak Lokasi : Studi Literatur Sistematis". *SNIV: Seminar Nasional Inovasi Vokasi*, vol. 4, no. 1, pp. 785–791, 2025, <https://prosiding.pnj.ac.id/index.php/sniv/article/view/3966>
- [15] N. Purnomo, R. M. Dinata, M. Marhaeni, and K. Atmadja, "Penilaian Kuantitatif Kedisiplinan Asisten Laboratorium Fstt Istn Menggunakan Sistem Absensi Berbasis Geofencing Dan GPS," *Journal of Information System, Applied, Management, Accounting and Research*, vol. 10, no. 1, p. 358, Feb. 2026, <https://doi.org/10.52362/jisamar.v10i1.2320>.
- [16] A. N. Yusril, I. Larasati, and P. Al Zukri, "Systematic Literature Review Analisis Metode Agile dalam Pengembangan Aplikasi Mobile," 2021. Accessed: Jun. 10, 2026. <https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/view/1237/376>
- [17] A. Kumar, P. Shruthi, P. Vinay, M. Nithin, M. Abhishek, and P. Sriteja, "Liveness Detection Authentication," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. 4, pp. 1778–1781, Apr. 2024, <https://doi.org/10.22214/ijraset.2024.60165>.
- [18] S. Susafa'ati and S. Supriyadi, "Sistem Absensi Dan Pemantauan Kegiatan Marketing Menggunakan Geofence Lock GPS," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 10, no. 1, pp. 1602–1607, Jan. 2026, <https://doi.org/10.36040/jati.v10i1.16773>.
- [19] N. Fatjriah, D. Nur Sholihaningtias, J. Raya Tengah No, K. Gedong, P. Rebo, and J. Timur, "Sistem Informasi Penjualan Hijab Pada Hayya Hijab Menggunakan Metode Agile Software Development," *Profitabilitas: Jurnal Sistem Informasi Akuntansi*, vol. 3, pp. 29–34, 2023, <https://doi.org/10.31294/profitabilitas.v3i1.2197>.
- [20] N. Lediwara *et al.*, "Pengembangan Sistem Presensi Digital Berbasis Face Recognition dan Geolocation untuk Meningkatkan Efisiensi Kehadiran Pegawai," *Jurnal Algoritma*, vol. 22, no. 2, pp. 277–286, Nov. 2025, <https://doi.org/10.33364/algoritma/v.22-2.2518>.