

BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan yang pesat pada teknologi informasi di era Revolusi Industri 4.0 telah mengubah paradigma manajemen administrasi di berbagai institusi, termasuk perguruan tinggi, menjadi lebih terintegrasi dan otomatis. Hal ini menegaskan bahwa kehadiran teknologi informasi membawa dampak positif yang nyata, mengingat berbagai sektor, termasuk perguruan tinggi, kini mulai memperlihatkan transformasi dan kemajuan yang sangat signifikan (Ridwan, 2024).

Salah satu aspek administratif yang krusial dalam transformasi teknologi informasi adalah sistem presensi (Febrianti et al., 2023). Namun, dalam praktiknya, banyak institusi masih menghadapi tantangan untuk mendigitalisasi sistem pencatatan kehadiran secara menyeluruh. Kendala terkait tingginya biaya implementasi dan pemeliharaan sering kali menjadi hambatan utama dalam mengadopsi teknologi presensi yang lebih canggih (Jannah et al., 2023). Akibatnya, tidak sedikit instansi yang terpaksa mempertahankan sistem pencatatan kehadiran secara manual berbasis dokumen fisik (*hardcopy*). Sistem absensi manual ini memiliki berbagai keterbatasan administratif. Prosedur verifikasi yang mengharuskan persetujuan atau tanda tangan staf dinilai tidak efisien dan berpotensi mengganggu produktivitas pegawai. Selain itu, akurasi pencatatan waktu kehadiran sulit dipastikan secara presisi. Kerentanan media kertas terhadap kerusakan fisik, seperti sobek atau terkena cairan, juga menjadi kendala serius karena proses penggantian dokumen tersebut akan menyulitkan personel dan menghambat alur kerja di instansi terkait (Sophiana & Jaya, 2022).

Lebih jauh lagi, urgensi untuk beralih ke sistem digital juga didorong oleh temuan mengenai celah keamanan pada perangkat keras biometrik konvensional yang ada. Observasi menunjukkan bahwa mesin absensi yang mengandalkan sensor fisik pun masih memiliki kerentanan terhadap serangan spoofing sederhana, seperti penggunaan media kertas bergambar wajah. Upaya digitalisasi sistem absensi sebenarnya telah banyak dikembangkan dengan berbagai teknologi, namun setiap metode memiliki keterbatasan fungsional yang memengaruhi keandalannya. Penggunaan kartu RFID (Radio Frequency Identification) masih menyimpan

kelemahan mendasar berupa risiko manipulasi data, ketidakteraturan pencatatan, serta potensi pemalsuan kehadiran yang tinggi (Rikki & Sinaga, 2025). Di sisi lain, teknologi sidik jari (*fingerprint*) menghadapi tantangan terkait biaya implementasi yang relatif mahal, risiko penguncian akses informasi jika terjadi kegagalan sistem, serta kendala teknis di mana tidak semua subjek dapat melakukan pemindaian jari secara efektif (Decaprio et al., 2023). Selain itu, meskipun metode kode QR menawarkan kecepatan dan kemudahan, faktor keamanan serta integritas data tetap menjadi isu kritis yang harus diperhatikan secara serius dalam lingkungan akademik (Hamdani et al., 2024). Terakhir, sistem pengenalan wajah konvensional tanpa dukungan fitur *anti-spoofing* terbukti rentan terhadap upaya penipuan menggunakan media foto atau video palsu, sehingga diperlukan integrasi teknik *liveness detection* dan analisis tekstur untuk membedakan serta menangkal tindakan kecurangan tersebut (Supriatna et al., 2024).

Guna mengatasi kerentanan sistem terhadap serangan spoofing tersebut baik pada sistem manual maupun celah pada perangkat keras konvensional penelitian ini mengusulkan solusi *low-cost high security* melalui integrasi algoritma YOLO11n sebagai modul utama deteksi wajah sekaligus mekanisme *liveness detection*. Penggunaan arsitektur YOLO versi terbaru ini terbukti mampu melakukan deteksi wajah secara *real-time* dengan tingkat akurasi yang tetap terjaga meskipun dalam kondisi pencahayaan yang bervariasi (Dewi et al., 2025). Namun demikian, hasil evaluasi menunjukkan bahwa sistem masih memiliki keterbatasan pada kondisi input yang tidak ideal. Hal ini terbukti dari adanya potensi kesalahan klasifikasi sesaat, di mana model dapat gagal mengenali wajah asli pada pose tertentu atau keliru mengklasifikasikan manipulasi visual statis, seperti media cetak, sebagai wajah asli (Tanujaya et al., 2026).

Untuk menutup celah tersebut, penelitian ini menerapkan lapis verifikasi kedua berupa mekanisme *active liveness (challenge-response)* memanfaatkan MediaPipe Face Landmarker. Modul ini bertugas mendeteksi arah pergerakan kepala (melalui *facial transformation matrix*) dan ekspresi wajah (seperti tersenyum) guna memastikan bahwa wajah yang dipindai berasal dari pengguna yang berinteraksi langsung secara langsung (hidup), bukan dari rekaman (Jie et al., 2023). Selanjutnya, untuk proses identifikasi yang lebih presisi, sistem

mengintegrasikan pustaka InsightFace yang berfungsi mengekstraksi fitur wajah menjadi representasi vektor numerik atau *face embeddings* yang unik bagi setiap individu. Pustaka ini telah teruji efektif dalam mendukung sistem presensi otomatis karena kemampuannya mengenali karakteristik wajah secara akurat dan efisien di lingkungan pendidikan (Setiawan et al., 2025). Untuk menentukan validitas identitas, peneliti menerapkan algoritma *Cosine Similarity* yang bekerja dengan mengukur tingkat kemiripan atau kedekatan sudut antara vektor wajah yang diambil saat absensi dengan data referensi yang tersimpan dalam basis data. Integrasi algoritma ini memberikan solusi yang lebih ringan dan mudah dalam melakukan perbandingan citra wajah digital untuk aplikasi presensi (Sirait & Siddik, 2025).

Sebagai studi kasus untuk menguji keandalan sistem yang diusulkan, implementasi penelitian ini akan diterapkan di Universitas Mercu Buana. Instansi pendidikan ini menghadapi dua kendala utama terkait manajemen kehadiran, yaitu belum adanya digitalisasi sistem absensi khusus bagi peserta magang dan pekerja lepas (*freelance*), serta perangkat mesin absensi *real-time* untuk karyawan tetap yang saat ini masih memiliki celah keamanan karena rentan terhadap pemalsuan (*spoofing*) menggunakan media cetak atau gambar wajah. Oleh karena itu, implementasi sistem presensi berbasis *face recognition* yang dilengkapi dengan kombinasi fitur *passive* dan *active liveness detection* ini diharapkan dapat memberikan solusi pengamanan yang tangguh sekaligus menyelesaikan masalah administrasi manual tersebut. Signifikansi penelitian ini terletak pada kemampuannya menawarkan alternatif biometrik berbasis perangkat lunak (*software-based*) yang mampu menutup celah keamanan serangan media cetak maupun video tanpa memerlukan investasi perangkat keras tambahan yang mahal. Penelitian ini akan mengevaluasi kinerja sistem melalui pengukuran metrik akurasi, presisi, dan *recall* untuk memastikan tingkat keberhasilan identifikasi mencapai standar optimal. Hasil akhir dari penelitian ini diharapkan dapat mewujudkan sistem kehadiran yang lebih modern, transparan, dan ke depannya dapat direplikasi oleh instansi lain dengan tantangan serupa.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengimplementasikan kombinasi *InsightFace* untuk ekstraksi fitur dan algoritma *Cosine Similarity* untuk pencocokan wajah pada sistem presensi mahasiswa magang?
2. Bagaimana efektivitas algoritma YOLO11n dalam mendeteksi *passive liveness* (keaslian wajah) untuk mencegah upaya manipulasi presensi melalui serangan *spoofing* statis (foto/kertas)?
3. Bagaimana mekanisme *active liveness* (*challenge-response*) dapat diimplementasikan sebagai lapisan verifikasi tambahan untuk menutup celah serangan yang lolos dari deteksi *passive* YOLO11n, khususnya serangan *replay* video atau layar dinamis?
4. Bagaimana merancang arsitektur API berbasis Flask untuk mengintegrasikan model *Deep Learning* dan basis data PostgreSQL dengan sistem informasi presensi berbasis web?
5. Seberapa besar tingkat keberhasilan sistem dalam mengenali identitas dan mendeteksi keaslian wajah?

Dengan merumuskan masalah-masalah tersebut, penelitian ini diharapkan dapat memberikan arah yang jelas dalam membangun sistem presensi mahasiswa magang yang otomatis, aman dari kecurangan, serta efisien secara infrastruktur.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, penelitian ini dilakukan untuk mencapai tujuan yang menjadi dasar pelaksanaan penelitian. Adapun tujuan penelitian ini adalah sebagai berikut:

1. Membangun modul pengenalan wajah biometrik yang akurat untuk sistem presensi mahasiswa magang di Universitas Mercu Buana.

2. Menerapkan fitur *passive liveness detection* menggunakan algoritma YOLO11n guna meningkatkan keamanan awal sistem.
3. Mengimplementasikan *active liveness* berbasis MediaPipe Face Landmarker (deteksi arah kepala via *facial transformation matrix* dan deteksi senyum) sebagai lapisan verifikasi kedua untuk membedakan interaksi pengguna asli dengan serangan *spoofing*.
4. Mengembangkan layanan Flask API yang terintegrasi dengan PostgreSQL sebagai jembatan komunikasi data yang *real-time* antara model kecerdasan buatan dan aplikasi web.
5. Mengevaluasi kinerja sistem secara menyeluruh, yang meliputi evaluasi model AI menggunakan *Confusion Matrix*, *User Acceptance Testing* (UAT), pengujian fungsionalitas sistem (Black Box) dari berbagai skenario serangan, serta pengujian integrasi dan performa latensi.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dari hasil penelitian ini terbagi menjadi dua aspek utama, yaitu manfaat teoritis dan manfaat praktis, dengan penjabaran sebagai berikut:

1. Manfaat Teoritis
 - a. Kontribusi Akademik: Memberikan kontribusi pada perkembangan literatur di bidang visi komputer (*computer vision*) dan kecerdasan buatan, khususnya mengenai efektivitas integrasi algoritma YOLO11n untuk deteksi *passive liveness*, MediaPipe untuk *active liveness*, dan pustaka InsightFace untuk ekstraksi fitur wajah secara *real-time*.
 - b. Referensi Inovasi Keamanan: Menjadi rujukan ilmiah bagi penelitian selanjutnya yang berfokus pada pengembangan sistem pengamanan biometrik berbasis perangkat lunak (*software-based*) sebagai alternatif solusi *low-cost high-security* untuk menangkal ancaman spoofing tanpa perangkat keras tambahan.

2. Manfaat Praktis

a. Bagi Institusi:

- Efisiensi Administratif: Menyediakan sistem digitalisasi presensi otomatis yang menghilangkan ketergantungan pada dokumen fisik (kertas), sehingga mengurangi beban kerja staf dalam melakukan verifikasi manual dan meminimalisir kesalahan pencatatan (human error).
- Peningkatan Keamanan: Memberikan solusi presensi yang tangguh terhadap manipulasi kehadiran menggunakan media statis (foto/kertas) maupun layar digital, menutupi celah keamanan yang selama ini ada pada perangkat mesin biometrik konvensional.

b. Bagi Pengguna:

- Memberikan kemudahan, kecepatan, dan transparansi dalam melakukan pencatatan kehadiran sehari-hari hanya melalui antarmuka kamera perangkat (seperti *handphone* atau laptop).
- Menghilangkan risiko administratif akibat kerusakan dokumen fisik (seperti hilang, basah, atau sobek) yang berpotensi menghambat alur kerja dan evaluasi kinerja peserta magang.

c. Bagi Peneliti:

- Meningkatkan pengalaman dan pemahaman praktis dalam membangun arsitektur sistem cerdas terintegrasi, mulai dari pelatihan model *deep learning*, perancangan Microframework (Flask API), hingga pengelolaan basis data relasional (PostgreSQL) pada lingkungan pengembangan web.

1.5 Batasan Masalah

Agar penelitian ini lebih terarah dan fokus pada tujuan yang ingin dicapai, penulis menetapkan batasan masalah sebagai berikut:

1. Subjek Penelitian: Sistem dikhususkan untuk pencatatan kehadiran mahasiswa magang dan *freelance* di lingkungan Universitas Mercu Buana, bukan untuk karyawan tetap.
2. *Dataset*: Data latih dan uji untuk *passive liveness detection (YOLO11n)* difokuskan pada dua kelas utama, yaitu *Real* (Wajah Asli) dan *Fake* (Serangan Spoofing).
3. Jenis Serangan *Spoofing*: Deteksi *liveness* dibatasi pada penanganan serangan presentasi (*Presentation Attack*) berupa foto cetak (kertas), foto digital di layar ponsel (*screen attack*), dan *video replay*.
4. Mekanisme *Active Liveness*: Verifikasi *active liveness* menggunakan MediaPipe dibatasi pada empat arah pergerakan kepala (atas, bawah, kiri, kanan) serta deteksi senyuman. Proses ini dijalankan sepenuhnya pada sisi klien (*client-side*) di peramban menggunakan kombinasi WASM/GPU *delegate*, dan bukan merupakan verifikasi di sisi peladen (*server-side*).
5. Perangkat Keras: Sistem dirancang untuk beroperasi menggunakan perangkat kamera depan *handphone*, tanpa memerlukan sensor tambahan seperti inframerah atau depth camera.
6. Pengujian sistem: Pengujian dilakukan menggunakan beberapa metode, yaitu Blackbox testing untuk memastikan fungsionalitas sistem berjalan sesuai yang diharapkan, pengujian kecepatan latensi dan ketepatan integrasi data, serta *User Acceptance Testing (UAT)* untuk mengukur kesesuaian sistem dengan kebutuhan pengguna.