BAB I
PENDAHULUAN

Bab pendahuluan ini membahas mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan yang digunakan dalam dokumen skripsi ini.

1.1 Latar Belakang

Teknologi biometrik berbasis pengenalan wajah (*face recognition*) telah berkembang pesat dalam satu dekade terakhir dan menjadi salah satu standar autentikasi digital yang banyak diadopsi pada sistem keamanan modern. Kemampuan sistem pengenalan wajah dalam melakukan verifikasi wajah secara cepat, non-intrusif, dan berbasis karakteristik unik individu mendorong implementasinya pada berbagai sektor, termasuk kontrol akses dan sistem presensi. Namun, peningkatan adopsi tersebut juga diiringi oleh munculnya berbagai ancaman keamanan, khususnya serangan presentasi (*presentation attack*) yang memanfaatkan representasi wajah tiruan untuk mengecoh sistem autentikasi. Ramachandra & Busch (2018) menjelaskan bahwa sistem pengenalan wajah konvensional memiliki kerentanan inheren terhadap serangan *spoofing* akibat kemudahan dalam mereproduksi citra wajah target melalui media cetak maupun layar digital. Kondisi ini menunjukkan bahwa peningkatan akurasi pengenalan wajah saja tidak cukup untuk menjamin keamanan sistem biometrik secara menyeluruh.

Serangan terhadap sistem pengenalan wajah umumnya dilakukan melalui *print attack* dan *replay attack*, yaitu penggunaan foto cetak atau tampilan ulang video wajah target untuk memperoleh akses tidak sah. Aydin dkk. (2023) menjelaskan bahwa sistem pengenalan wajah konvensional yang hanya melakukan pencocokan fitur identitas tidak mampu membedakan wajah asli dengan representasi tiruannya tanpa mekanisme deteksi tambahan. Kerentanan ini menjadi semakin signifikan pada sistem autentikasi berbasis aplikasi web atau perangkat bergerak yang beroperasi tanpa pengawasan langsung, karena sistem hanya menerima *input* citra atau video dari sisi klien tanpa verifikasi fisik terhadap keberadaan subjek nyata. Variasi media *spoof* seperti foto cetak, tampilan layar digital, dan masker tiga dimensi juga menunjukkan bahwa pola tekstur dan karakteristik visual wajah tiruan dapat menyerupai wajah asli dalam kondisi tertentu. Kondisi tersebut menegaskan bahwa modul

*liveness detect*ion diperlukan sebagai mekanisme mitigasi untuk memastikan bahwa *input* yang diproses berasal dari individu hidup (*live subject*), sehingga risiko *False Acceptance Rate* (FAR) akibat serangan *spoofing* dapat ditekan.

Implementasi sistem autentikasi wajah pada lingkungan berbasis web atau *cloud* umumnya menggunakan arsitektur *client–cloud*, di mana proses akuisisi citra dilakukan pada sisi klien dan proses inferensi model dijalankan pada server. Arsitektur ini memungkinkan sentralisasi model dan pengelolaan pembaruan sistem secara terpusat, namun menimbulkan tantangan baru terkait latensi inferensi dan beban komputasi. Li dkk. (2019) menjelaskan bahwa pemrosesan citra berbasis *deep learning* pada lingkungan *cloud* memerlukan alokasi sumber daya komputasi yang memadai agar waktu respons tetap berada dalam batas toleransi aplikasi *real-time*. Proses ekstraksi fitur, klasifikasi, serta pengiriman data melalui jaringan dapat menambah waktu tunda (*network delay*) yang berdampak pada pengalaman pengguna. Tantangan tersebut menjadi semakin kompleks ketika sistem mengintegrasikan modul *liveness detection* dan verifikasi wajah secara bersamaan, karena kedua modul memerlukan komputasi intensif berbasis *convolutional neural network*. Kondisi ini menunjukkan bahwa perancangan sistem biometrik harus mempertimbangkan ketahanan terhadap serangan *spoofing*, efisiensi komputasi, serta optimasi latensi agar sistem tetap responsif dalam skenario penggunaan nyata.

Permasalahan keamanan sistem biometrik juga relevan pada implementasi presensi karyawan di PT Sidorejo Makmur Sejahtera. Sistem presensi yang digunakan saat ini masih berbasis unggah foto *selfie* sehingga proses verifikasi wajah harus dilakukan secara manual oleh administrator untuk memastikan kesesuaian wajah dengan identitas karyawan. Mekanisme tersebut membuka peluang terjadinya manipulasi kehadiran, termasuk praktik *proxy attendance*, di mana seseorang melakukan presensi menggunakan identitas karyawan lain. Selain berpotensi menurunkan integritas data kehadiran, proses pemeriksaan manual juga meningkatkan beban administratif karena setiap bukti presensi harus diperiksa satu per satu. Kondisi ini menunjukkan perlunya sistem presensi berbasis biometrik yang mampu melakukan verifikasi wajah secara otomatis serta dilengkapi mekanisme *liveness detection* untuk memastikan bahwa proses autentikasi dilakukan oleh individu yang sah dan benar-benar hadir secara fisik.

Penelitian pada bidang biometrik wajah menunjukkan kecenderungan pengembangan yang terpisah antara modul verifikasi wajah dan *liveness detection*. Studi verifikasi wajah umumnya berfokus pada optimasi model embedding dan metrik kemiripan untuk meningkatkan akurasi pencocokan identitas, seperti penggunaan FaceNet dan ArcFace dalam berbagai skenario kontrol akses (Firmansyah dkk., 2023; Juwanda dkk., 2024). Di sisi lain, penelitian *liveness dete*ction lebih banyak menitikberatkan pada klasifikasi citra untuk membedakan wajah asli dan wajah tiruan menggunakan pendekatan berbasis CNN atau model *lightweight* (Alya dkk., 2023; Smiley & Sam, 2025). Meskipun masing-masing pendekatan menunjukkan peningkatan performa pada domainnya, integrasi verifikasi wajah dan *liveness detection* dalam satu *pipeline* autentikasi terpadu masih relatif terbatas. Selain itu, evaluasi pada sebagian besar penelitian tersebut berfokus pada metrik klasifikasi seperti *accuracy* atau *error rate* tanpa membahas secara eksplisit keseimbangan antara tingkat akurasi deteksi dan latensi inferensi yang menjadi faktor penting dalam implementasi sistem *real-time* berbasis *cloud*. Kajian mengenai pengujian sistem biometrik terintegrasi pada arsitektur *serverless* juga belum banyak dilaporkan dalam literatur. Kondisi tersebut menunjukkan adanya celah penelitian dalam pengembangan sistem autentikasi presensi yang menggabungkan keamanan, efisiensi komputasi, dan kesiapan *deployment* dalam satu kerangka sistem yang komprehensif.

Penelitian mengenai sistem presensi biometrik berbasis *cloud* ini mengusulkan pendekatan integratif yang menggabungkan modul *liveness detection* dan verifikasi wajah dalam satu alur autentikasi terpadu. Modul *liveness detection* memanfaatkan arsitektur *one-stage object detection* YOLOv8 yang memungkinkan deteksi wajah sekaligus klasifikasi kondisi *live*, *spoof screen*, dan *spoof print* dalam satu proses inferensi. Pendekatan ini dipilih untuk mendukung kebutuhan pemrosesan *real-time* serta efisiensi komputasi, karena arsitektur *one-stage* melakukan prediksi *bounding box* dan probabilitas kelas dalam satu kali evaluasi jaringan sehingga mengurangi *overhead* komputasi dibandingkan pendekatan dua tahap (*two-stage detector*) yang memisahkan proses proposal region dan klasifikasi (Chen dkk., 2021). Modul verifikasi wajah menggunakan model embedding berbasis *deep learning*, yaitu ArcFace, FaceNet512, dan VGG-Face, yang dievaluasi secara komparatif untuk menentukan model dengan performa paling optimal dalam konteks dataset penelitian. Integrasi kedua modul tersebut dirancang pada arsitektur *serverless* menggunakan Google Cloud Run guna mendukung skalabilitas dan efisiensi pengelolaan sumber daya komputasi.

Evaluasi sistem dilakukan berdasarkan metrik klasifikasi serta melalui analisis keseimbangan antara tingkat keamanan dan latensi inferensi untuk memastikan sistem tetap tahan terhadap *spoofing* tanpa mengorbankan efisiensi komputasi pada lingkungan operasional nyata. Pendekatan ini diharapkan memberikan kontribusi dalam pengembangan sistem presensi biometrik yang aman, responsif, dan siap diimplementasikan pada arsitektur layanan modern.

1.2 Rumusan Masalah

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

1. Bagaimana performa model YOLOv8 sebagai metode *liveness detection* dalam mendeteksi wajah asli, *spoof print*, dan *spoof screen* pada sistem presensi biometrik?
2. Bagaimana performa komparatif model verifikasi wajah berbasis embedding, yaitu ArcFace, FaceNet512, dan VGG-Face, dalam proses verifikasi wajah menggunakan metrik evaluasi seperti *Accuracy*, *Balanced Accuracy*, FAR, FRR, EER, dan ROC-AUC?
3. Bagaimana pengaruh penerapan arsitektur *serverless* terhadap latensi inferensi dan efisiensi komputasi pada sistem presensi biometrik berbasis *deep learning* yang mengintegrasikan modul *liveness detection* dan verifikasi wajah?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari pelaksanaan penelitian ini adalah:

1. Menghasilkan analisis performa model YOLOv8 sebagai metode *liveness detection* dalam mendeteksi kategori wajah asli, *spoof print*, dan *spoof screen* pada sistem presensi biometrik.
2. Menghasilkan perbandingan performa model verifikasi wajah berbasis embedding, yaitu ArcFace, FaceNet512, dan VGG-Face, berdasarkan metrik evaluasi *Accuracy*, *Balanced Accuracy*, FAR, FRR, EER, dan ROC-AUC.
3. Menghasilkan analisis pengaruh penerapan arsitektur *serverless* terhadap latensi inferensi dan efisiensi komputasi pada sistem presensi biometrik berbasis *deep learning* yang mengintegrasikan modul *liveness detection* dan verifikasi wajah.

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dan manfaat nyata sebagai berikut:

1. Manfaat Teoritis
    a. Memberikan bukti empiris mengenai integrasi model *deep learning* berbasis *computer vision* dalam arsitektur *serverless* serta implikasinya terhadap latensi inferensi dan efisiensi komputasi pada sistem biometrik.
    b. Menyediakan kajian komparatif mengenai penskalaan arsitektur deteksi dan model embedding wajah untuk menganalisis keseimbangan antara performa keamanan dan kecepatan inferensi pada sistem autentikasi terpadu.
    c. Memperkaya literatur evaluasi biometrik wajah pada konteks dataset lokal melalui penggunaan metrik keamanan dan diskriminatif yang komprehensif, sehingga memberikan perspektif evaluasi yang lebih menyeluruh dibandingkan pelaporan akurasi tunggal.
2. Manfaat Praktis
    a. Memberikan rekomendasi teknis kepada PT Sidorejo Makmur Sejahtera dalam pengembangan sistem presensi biometrik berbasis web yang mempertimbangkan keamanan, stabilitas latensi, dan efisiensi biaya operasional *cloud*.
    b. Menyediakan kerangka sistem presensi biometrik yang terintegrasi dan lebih tahan terhadap risiko *spoofing* pada skenario tanpa pengawasan langsung.

1.5 Ruang Lingkup

Penelitian ini menetapkan ruang lingkup pembahasan agar fokus dan tidak menyimpang dari tujuan utama sebagai berikut:

1. Objek penelitian difokuskan pada perancangan arsitektur sistem presensi untuk PT Sidorejo Makmur Sejahtera. Pengambilan data pelatihan dan pengujian dilakukan melalui skenario simulasi dengan partisipan sukarela sebagai *proof-of-concept* guna menjaga privasi data karyawan.
2. Sistem diimplementasikan berbasis web dengan arsitektur terpisah, di mana *frontend* berjalan pada *hosting* konvensional dan layanan kecerdasan buatan dijalankan pada Google Cloud Run (*serverless*).

3. Analisis *liveness detection* dibatasi pada arsitektur YOLOv8 dengan perbandingan varian *Nano*, *Small*, dan *Medium* untuk mengevaluasi performa deteksi serta implikasinya terhadap latensi inferensi pada lingkungan *serverless*.
4. Proses verifikasi wajah menggunakan model ArcFace sebagai model utama, dengan validasi performa melalui perbandingan terhadap FaceNet512 dan VGG-Face berdasarkan metrik keamanan dan diskriminatif.
5. Pengujian latensi difokuskan pada evaluasi waktu inferensi dalam kondisi *cold start* dan *warm start* untuk menganalisis dampak arsitektur *serverless* terhadap efisiensi komputasi.
6. Sistem dibatasi pada penanganan serangan presentasi 2D berupa *print attack* dan *replay attack*, serta menggunakan mekanisme pengambilan citra berbasis *snapshot* melalui HTTP/REST API tanpa pemrosesan video berkelanjutan.

1.6 Sistematika Penulisan

Laporan tugas akhir ini disusun dalam lima bab dengan sistematika pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang permasalahan terkait integrasi sistem biometrik wajah pada arsitektur web modern, rumusan masalah yang berfokus pada perancangan sistem terdistribusi berbasis *serverless* serta evaluasi komparatif model *deep learning*, tujuan dan manfaat penelitian, ruang lingkup yang membatasi kajian pada skenario simulasi lingkungan, serta sistematika penulisan laporan. Pembahasan dalam bab ini menjadi landasan konseptual untuk menjelaskan urgensi penelitian dalam konteks keamanan, efisiensi komputasi, dan implementasi sistem presensi berbasis biometrik wajah.

BAB II LANDASAN TEORI

Bab ini memaparkan kerangka teoritis yang menjadi fondasi penelitian, meliputi konsep *Computer Vision*, arsitektur *Deep Learning* (CNN), teknologi *Cloud Computing* (*Serverless*/Google Cloud Run), serta tinjauan mendalam mengenai algoritma YOLOv8 dan ArcFace beserta model pembandingnya (FaceNet512 dan VGG-Face). Bab ini juga menjelaskan metrik evaluasi kinerja yang digunakan dalam penelitian, meliputi *Confusion Matrix*, *Mean*

Average Precision (mAP), *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), *Balanced Accuracy*, *Equal Error Rate* (EER), serta analisis *Receiver Operating Characteristic* (ROC) dan *Area Under Curve* (AUC).

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan prosedur eksperimen secara sistematis. Pembahasan mencakup skenario pengumpulan *custom dataset* wajah di lingkungan simulasi, tahapan pelatihan (*training*) komparatif untuk tiga varian model YOLOv8 (*Nano, Small, Medium*), konfigurasi *hyperparameter*, perancangan arsitektur sistem terdistribusi, serta prosedur pengujian integrasi sistem berbasis API (*Integration Testing*) pada infrastruktur Cloud Run.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil empiris penelitian yang meliputi analisis komparatif performa *liveness detection* menggunakan tiga varian model YOLOv8 *(Nano, Small, Medium*), dilanjutkan dengan evaluasi kinerja verifikasi wajah melalui *benchmarking* ArcFace terhadap FaceNet512 dan VGG-Face menggunakan metrik FAR, FRR, *Balanced Accuracy*, EER, dan ROC-AUC. Setelah analisis performa model selesai, dibahas karakteristik latensi dan stabilitas sistem pada infrastruktur Google Cloud Run, termasuk fenomena *cold start* dan *warm start*, sebagai evaluasi aspek implementasi operasional sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini menarik kesimpulan akhir berdasarkan data hasil analisis untuk menjawab rumusan masalah mengenai konfigurasi model dan arsitektur infrastruktur yang paling optimal dari segi keamanan dan efisiensi biaya. Bab ini juga memberikan saran teknis strategis, seperti mitigasi dampak *cold start* dan pengembangan fitur penilaian kualitas citra (*quality assessment*), untuk pengembangan sistem selanjutnya agar lebih adaptif terhadap kebutuhan industri.