BAB I
PENDAHULUAN

1.1. Latar Belakang

Era transformasi digital, yang dipercepat oleh kemajuan pesat dalam Kecerdasan Artifisial (AI), telah secara fundamental mengubah cara interaksi manusia dengan lingkungan fisik dan digital. Dalam berbagai skenario operasional, mulai dari pencatatan kehadiran di institusi pendidikan dan korporat, personalisasi layanan di sektor ritel, hingga peningkatan protokol keamanan di area vital, kebutuhan akan metode verifikasi identitas yang cepat, akurat, dan tanpa gesekan (*frictionless*) menjadi semakin krusial. Metode verifikasi tradisional, baik yang bersifat manual maupun yang mengandalkan kredensial fisik seperti kartu akses, atau kredensial digital seperti kata sandi dan PIN, seringkali terbukti tidak efisien. Sistem ini tidak hanya rentan terhadap kesalahan manusia, tetapi juga membuka celah keamanan yang signifikan melalui kehilangan, pencurian, atau penggandaan kredensial [1]. Sebagai respons terhadap tantangan ini, teknologi biometrik, khususnya pengenalan wajah, muncul sebagai solusi unggul karena sifatnya yang non-intrusif dan menawarkan tingkat keamanan serta kenyamanan yang jauh lebih tinggi. Tren adopsi ini tercermin dalam proyeksi pertumbuhan pasar biometrik global yang akan mencapai ratusan miliar dolar pada akhir dekade ini, menurut penelitian dari Grand View Research (2022) menyatakan bahwa akan ada peningkatan kebutuhan terhadap teknologi verifikasi wajah di tahun 2023-2030 dengan menandakan adanya permintaan masif dari berbagai sektor industri akan solusi verifikasi identitas yang inovatif dan efisien [2].

Secara teoretis, konvergensi antara *Internet of Things* (IoT) dan Kecerdasan Artifisial (AI) telah melahirkan konsep *Artificial Intelligence of Things* (AIoT) [3]. AIoT bukan hanya tentang menghubungkan perangkat ke internet, melainkan tentang menciptakan sebuah ekosistem kecerdasan terdistribusi. Dalam ekosistem ini, perangkat di lapangan (dikenal sebagai perangkat *edge*) dapat melakukan pemrosesan data awal secara mandiri sebelum berkomunikasi dengan sistem *cloud* untuk analisis yang lebih mendalam [4]. Dalam konteks verifikasi identitas, teknologi pengenalan wajah (*face recognition*) berbasis *deep learning* telah

menjadi standar emas. Model *deep learning* modern, seperti yang dibangun di atas arsitektur *Convolutional Neural Network* (CNN), mampu mempelajari fitur-fitur wajah yang sangat kompleks dan diskriminatif, sehingga dapat mengenali individu dengan akurasi sangat tinggi bahkan di bawah berbagai kondisi dunia nyata yang menantang, seperti perubahan pencahayaan, ekspresi wajah, pose, dan adanya oklusi parsial (misalnya, penggunaan kacamata) [5].

Namun, implementasi model *deep learning* yang canggih ini pada perangkat IoT menghadapi dilema teknis yang signifikan, misalnya model pengenalan wajah modern seperti VGG-Face atau Facenet memiliki ukuran yang besar (seringkali ratusan *megabyte*) dan memerlukan jutaan operasi *floating-point* per detik (FLOPS) untuk melakukan satu kali inferensi. Menjalankan beban komputasi seberat ini secara langsung pada perangkat *edge* berdaya rendah seperti mikrokontroler (misalnya, ESP32-S3) hampir tidak mungkin dilakukan karena keterbatasan memori (RAM dan Flash) serta kecepatan prosesor. Di sisi lain, pendekatan naif dengan mengirimkan seluruh aliran video (*video stream*) dari perangkat IoT ke *server* untuk diproses akan membebani jaringan secara masif, meningkatkan latensi secara drastis, dan sangat boros daya, yang bertentangan dengan prinsip efisiensi yang menjadi inti dari IoT [6]. Latensi yang tinggi akan merusak pengalaman pengguna dalam aplikasi *real-time* seperti absensi atau akses pintu.

Kondisi ini menciptakan sebuah masalah fundamental dalam desain sistem AIoT yang efisien: bagaimana cara memanfaatkan kekuatan dan akurasi model AI di *server* tanpa membebani perangkat *edge* dan jaringan secara berlebihan? [7] Untuk menjawab permasalahan ini, penelitian ini mengusulkan sebuah sistem verifikasi wajah yang dibangun di atas arsitektur *hybrid* (*hybrid architecture*). Dalam arsitektur ini, beban kerja didistribusikan secara cerdas berdasarkan kapabilitas komputasi setiap komponen. Perangkat *edge* (ESP32-S3) hanya dibebani tugas ringan yaitu mendeteksi keberadaan wajah (*face detection*) dalam gambar menggunakan model yang telah dioptimalkan untuk mikrokontroler. Perangkat *edge* bertindak sebagai "filter cerdas"; setelah wajah terdeteksi, hanya data gambar wajah yang relevan yang diekstraksi dan dikirim ke *server*. Selanjutnya, *server*, yang memiliki sumber daya komputasi yang jauh lebih besar,

akan melakukan tugas berat yaitu pengenalan wajah (*face recognition*) menggunakan *framework* DeepFace untuk memverifikasi identitas.

Meskipun *framework* DeepFace menyediakan akses mudah ke berbagai model *pre-trained* yang kuat [8], pemilihan model yang tepat untuk arsitektur *hybrid* ini menimbulkan celah penelitian (*research gap*) yang krusial. Setiap model (VGG-Face, Facenet, SFace, ArcFace, dan lainnya) memiliki karakteristik dan *trade-off* yang berbeda. Model seperti VGG-Face mungkin menawarkan akurasi tinggi, namun dengan kecepatan inferensi yang lambat. Sebaliknya, model yang lebih modern seperti SFace mungkin dirancang lebih ringan dan cepat, namun bisa jadi akurasinya sedikit menurun pada kondisi tertentu [9]. Hingga saat ini, belum banyak penelitian yang secara spesifik melakukan analisis kinerja komparatif untuk menentukan model mana yang memberikan keseimbangan (*trade-off*) terbaik antara akurasi verifikasi dan kecepatan respons total dalam konteks arsitektur *edge-server* berbasis mikrokontroler. Pemilihan model yang tidak tepat dapat menyebabkan latensi tinggi di sisi *server*, yang pada akhirnya akan mengurangi efektivitas dan pengalaman pengguna dari sistem secara keseluruhan.

Oleh karena itu, penelitian ini memiliki tujuan ganda. Pertama, merancang dan membangun sebuah prototipe fungsional dari platform verifikasi wajah berbasis AIoT yang efisien dan terukur. Kedua, melakukan analisis kinerja komparatif yang mendalam terhadap berbagai model yang tersedia di DeepFace untuk memberikan panduan berbasis data empiris. Hasil dari penelitian ini diharapkan dapat menghasilkan sebuah prototipe platform verifikasi yang andal, serta memberikan rekomendasi teknis bagi para pengembang dalam memilih model yang paling optimal untuk aplikasi serupa di masa depan, baik itu untuk sistem absensi, kontrol akses, maupun sistem monitoring keamanan lainnya.

1.2. Rumusan Masalah

Berdasarkan latar belakang dan judul penelitian, maka permasalahan yang akan dijawab dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana merancang dan membangun sebuah prototipe sistem verifikasi wajah berbasis AIoT dengan arsitektur *hybrid*, yang mengimplementasikan

deteksi wajah pada perangkat *edge* (ESP32-S3 WROOM CAM) dan rekognisi wajah di sisi *server* menggunakan *framework* DeepFace?

2. Bagaimana perbandingan kinerja berbagai model pengenalan wajah pada *framework* DeepFace dari segi akurasi dan kecepatan, serta model mana yang paling optimal untuk prototipe sistem verifikasi wajah ini?

1.3. Tujuan Penelitian

Selaras dengan rumusan masalah di atas, tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menghasilkan sebuah prototipe fungsional dari sistem verifikasi wajah berbasis AIoT yang menerapkan arsitektur *hybrid* dengan deteksi wajah pada ESP32-S3 WROOM CAM dan rekognisi di sisi *server*.
2. Melakukan analisis dan perbandingan kinerja (*benchmark*) terhadap berbagai model yang ada di dalam *framework* DeepFace dan memberikan rekomendasi model yang paling optimal berdasarkan hasil *benchmark*.

1.4. Manfaat Penelitan

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoretis maupun praktis.

1.4.1 Manfaat Teoretis

1. Memberikan kontribusi pada studi tentang arsitektur AIoT, khususnya pada implementasi model pemrosesan *hybrid* (*edge-server*) untuk tugas-tugas identifikasi biometrik seperti pengenalan wajah.
2. Menyediakan data hasil benchmark yang empiris mengenai perbandingan kinerja dari berbagai model *deep learning* pada *framework* DeepFace dalam skenario implementasi yang spesifik.

1.4.2 Manfaat Praktis

1. Menghasilkan sebuah prototipe yang dapat menjadi dasar atau cetak biru (*blueprint*) bagi pengembang untuk membangun aplikasi dunia nyata yang lebih kompleks, seperti sistem absensi otomatis, kontrol akses ruangan, atau sistem monitoring keamanan.

2. Memberikan panduan praktis bagi para pengembang IoT dalam memilih model *face recognition* yang paling sesuai dengan kebutuhan sistem mereka, dengan mempertimbangkan *trade-off* antara akurasi dan kecepatan.

1.5. Batasan Masalah

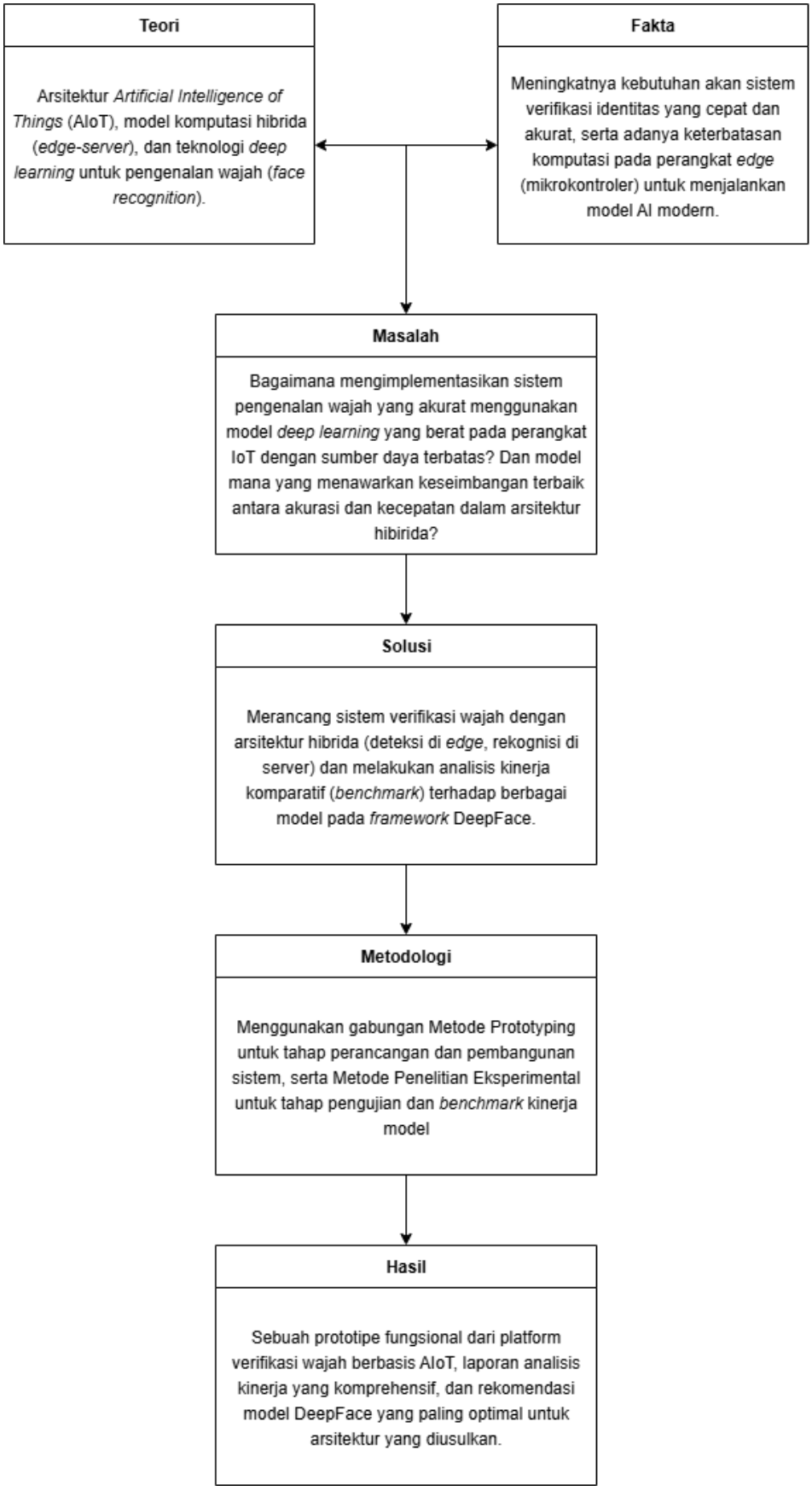
Untuk menjaga agar penelitian ini tetap fokus dan terarah, maka ditetapkan beberapa batasan masalah sebagai berikut:

1. Penelitian ini berfokus pada implementasi dan analisis kinerja arsitektur *hybrid* (deteksi di *edge*, rekognisi di *server*), dan tidak melakukan perbandingan dengan arsitektur lain seperti pemrosesan penuh di *edge* atau penuh di *server*.
2. Perangkat keras di sisi *edge* terbatas pada penggunaan modul ESP32-S3 WROOM CAM, kamera OV2640, dan *buzzer* sebagai aktuator umpan balik, tanpa menggunakan aktuator fisik seperti motor servo atau kunci *solenoid*.
3. Deteksi wajah di sisi *edge* menggunakan *library* yang tersedia dalam ekosistem ESP-IDF, sedangkan rekognisi wajah di sisi *server* terbatas pada model-model *pre-trained* yang ada di dalam *framework* DeepFace tanpa melakukan pelatihan ulang model dari awal.
4. Sistem yang dibangun merupakan prototipe fungsional untuk membuktikan kelayakan konsep dan mengukur kinerja teknis, sehingga belum mencakup fitur tingkat produksi seperti manajemen pengguna yang kompleks atau skalabilitas untuk ribuan perangkat.
5. Aspek keamanan siber tingkat lanjut seperti enkripsi *end-to-end* atau mekanisme pertahanan terhadap serangan *spoofing* (misalnya, *liveness detection*) tidak dibahas secara mendalam.
6. Pengujian kinerja sistem dilakukan dalam lingkungan yang terkontrol (terutama kondisi pencahayaan dan konektivitas jaringan) untuk memastikan validitas hasil perbandingan antar model.

1.6. Kerangka Pemikiran

Kerangka pemikiran ini disusun untuk memberikan alur berpikir yang sistematis dan logis dalam penelitian ini, mulai dari landasan teoretis hingga hasil

akhir yang diharapkan. Alur ini berfungsi sebagai peta jalan yang menghubungkan setiap tahapan penelitian secara koheren.



Gambar 1.1 Kerangka Pemikiran

1.7. Sistematika Penulisan

Sistematika penulisan dalam tugas akhir ini terdiri dari 6 bab dengan rincian sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan konteks penelitian, mencakup latar belakang masalah, perumusan masalah, tujuan yang ingin dicapai, manfaat, serta batasan-batasan untuk menjaga fokus penelitian.

BAB II KAJIAN LITERATUR

Bab ini berisi tinjauan *library* terhadap penelitian terdahulu yang relevan serta landasan teori yang mendasari penelitian, mencakup konsep AIoT, arsitektur *hybrid*, dan teknologi spesifik yang digunakan seperti ESP32-S3 WROOM Cam dan *framework* DeepFace.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan kerangka kerja penelitian secara rinci. Metode yang digunakan adalah gabungan antara Prototyping untuk tahap perancangan dan pembangunan sistem, serta metode Penelitian Eksperimental untuk tahap pengujian dan analisis kinerja komparatif model.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi prototipe sistem serta data hasil pengujian *benchmark* terhadap berbagai model. Setiap hasil akan dibahas dan dianalisis secara mendalam untuk menjawab rumusan masalah.

BAB V PENUTUP

Bab ini berisi kesimpulan dari keseluruhan hasil penelitian dan analisis, serta menyajikan saran untuk pengembangan atau penelitian lebih lanjut di masa mendatang.

DAFTAR *LIBRARY*