SISTEM PENGENALAN WAJAH UNTUK AKSES KONTROL BANGUNAN CERDAS

Proposal Tugas Akhir

Oleh

Axelius Davin
18222016

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

November 2025

LEMBAR PENGESAHAN

PERANCANGAN SISTEM INFORMASI AKADEMIK BERBASIS WEB

Proposal Tugas Akhir

Oleh

Axelius Davin
18222016

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Proposal Tugas Akhir ini telah disetujui dan disahkan
di Bandung, pada tanggal 11 November 2025

Pembimbing

Dr. Fadhil Hidayat, S.Kom., M.T.

NIP. 198609252012121002

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

BAB I

PENDAHULUAN

I.1 Latar Belakang

Di era digital saat ini, pengembangan bangunan cerdas (smart building) menjadi sebuah kebutuhan fundamental untuk mencapai tingkat keamanan dan efisiensi operasional yang tinggi. Salah satu aspek krusial dalam operasional bangunan cerdas adalah sistem kontrol akses. Namun, seiring dengan kemajuan teknologi, metode kontrol akses konvensional seperti kunci fisik dan kartu akses mulai menunjukkan kelemahan yang signifikan. Metode ini sangat rentan terhadap berbagai risiko, seperti kehilangan, pencurian, atau duplikasi yang tidak sah. Celah keamanan ini dapat secara langsung membahayakan aset berharga dan penghuni di dalam bangunan.

Konteks permasalahan ini menjadi sangat relevan dengan kondisi di Gedung ITB Innovation Park (IIP). Sebagai bangunan yang tergolong baru dan menjadi pusat inovasi, Gedung IIP menyimpan berbagai aset bernilai tinggi. Akan tetapi, saat ini gedung tersebut belum memiliki sistem kontrol akses modern yang terimplementasi secara optimal. Ketiadaan sistem yang aman ini menciptakan kerentanan keamanan yang nyata dan mendesak untuk segera diatasi. Situasi ini memberikan kesempatan strategis untuk mengimplementasikan solusi teknologi modern sebagai studi kasus nyata yang solutif dan dapat menjadi percontohan.

Kebutuhan akan sistem yang lebih cerdas dan aman ini tidak hanya bersifat lokal, tetapi juga sejalan dengan arah kebijakan nasional. Pemerintah, melalui Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR), secara aktif mendorong implementasi Bangunan Gedung Cerdas (BGC) untuk mendukung konsep Kota Cerdas (Smart City), terutama dalam pembangunan Ibu Kota Nusantara (IKN). Keseriusan ini terkonfirmasi di tahun 2024 dengan dikeluarkannya beberapa regulasi turunan, seperti Surat Edaran Menteri PUPR Nomor 22/SE/M/2024 tentang Pedoman Penilaian Kinerja Bangunan Gedung Cerdas dan Keputusan Menteri PUPR Nomor

1982/KPTS/M/2024 tentang Pembentukan Tim Ahli Bangunan Gedung Cerdas Pusat. Adanya kerangka regulasi ini memperkuat urgensi bagi fasilitas-fasilitas penting seperti IIP untuk segera mengadopsi standar teknologi yang lebih tinggi.

Untuk mengatasi permasalahan kontrol akses, berbagai solusi telah ada dan dapat diterapkan. Solusi konvensional yang umum digunakan adalah kunci fisik dan kartu akses. Meskipun biaya implementasinya relatif rendah, solusi ini memiliki tingkat keamanan yang terbatas karena risiko duplikasi dan kehilangan seperti yang telah disebutkan. Di sisi lain, telah berkembang berbagai solusi modern berbasis teknologi biometrik, seperti pemindai sidik jari, pemindai iris mata, dan pengenalan wajah.

Dari berbagai alternatif modern tersebut, teknologi pengenalan wajah (face recognition), sebagai salah satu inovasi dalam bidang computer vision, menawarkan keunggulan kompetitif. Solusi ini bersifat non-kontak (contactless), lebih higienis, dan memberikan kemudahan bagi pengguna karena tidak memerlukan perangkat fisik tambahan. Dengan tingkat akurasi yang semakin andal, pengenalan wajah menjadi pilihan yang paling sesuai untuk diterapkan di lingkungan modern seperti Gedung IIP.

Berdasarkan analisis tersebut, solusi yang diusulkan adalah pengembangan ”Sistem Pengenalan Wajah untuk Akses Kontrol Bangunan Cerdas”. Sistem ini akan diwujudkan dalam bentuk prototipe fungsional yang mengintegrasikan perangkat keras Internet of Things (IoT), seperti kamera untuk akuisisi citra wajah dan kunci elektronik (electronic lock) sebagai aktuator pintu.

Lebih lanjut, sistem yang diusulkan ini memiliki potensi skalabilitas yang tinggi dan dapat diperluas dengan berbagai fitur tambahan untuk meningkatkan fungsionalitasnya, antara lain:

1. Sistem Absensi Otomatis: Mengintegrasikan fungsi pencatatan kehadiran secara otomatis ketika pegawai atau anggota terdaftar memasuki area gedung.
2. Deteksi Pengunjung Tidak Dikenal: Menambahkan fitur keamanan untuk mengidentifikasi, mencatat, dan memberikan notifikasi jika ada wajah yang tidak terdaftar dalam sistem mencoba mengakses.
3. Dashboard Analisis Data: Membangun modul visualisasi data untuk memantau dan menganalisis pola penggunaan akses, seperti jam sibuk dan frekuensi keluar-masuk. Data ini dapat dimanfaatkan oleh manajemen untuk pengambilan keputusan berbasis data demi efisiensi operasional dan peningkatan keamanan.

I.2 Rumusan Masalah

Masalah utama yang akan diselesaikan dalam tugas akhir ini adalah belum adanya sistem kontrol akses yang terintegrasi, modern, dan aman di gedung ITB Innovation Park (IIP). Penggunaan metode akses konvensional seperti kunci fisik atau kartu akses memiliki kelemahan mendasar yang rentan terhadap risiko kehilangan, pencurian, dan duplikasi. Selain tidak efisien dalam pengelolaan, sistem ini tidak lagi memadai untuk melindungi aset-aset bernilai tinggi di dalamnya.

Dalam menjawab permasalahan tersebut, akan dikembangkan sebuah prototipe sistem kontrol akses berbasis pengenalan wajah. Adapun rumusan masalah spesifik yang akan dibahas adalah sebagai berikut:

1. Bagaimana merancang arsitektur sistem kontrol akses berbasis Internet of Things (IoT) yang mengintegrasikan kamera sebagai sensor dan kunci elektronik sebagai aktuator?
2. Bagaimana mengimplementasikan algoritma pengenalan wajah pada perangkat keras untuk dapat melakukan otentikasi pengguna secara akurat dan real-time?
3. Bagaimana performa sistem yang dibangun dalam hal kecepatan, akurasi, dan keandalan dalam memberikan atau menolak hak akses pada skenario penggunaan yang disimulasikan?

I.3 Tujuan

Tujuan utama dari tugas akhir ini adalah merancang, membangun, dan mengevaluasi sebuah prototipe fungsional ”Sistem Pengenalan Wajah untuk Akses Kontrol Bangunan Cerdas” yang dapat diimplementasikan di lingkungan ITB Innovation Park (IIP).

Secara lebih detail, tujuan yang ingin dicapai adalah sebagai berikut:

1. Menghasilkan rancangan arsitektur sistem berbasis Internet of Things (IoT) yang mampu mengintegrasikan perangkat keras berupa kamera, unit pemrosesan, dan kunci elektronik secara efektif.
2. Mengimplementasikan algoritma pengenalan wajah yang dapat melakukan proses otentikasi pengguna secara akurat dan real-time pada perangkat yang telah dirancang.
3. Menganalisis dan mengukur kinerja prototipe sistem untuk memastikan fungsionalitasnya sesuai dengan kebutuhan, sehingga dapat menyelesaikan perso-

alan keamanan yang telah dijabarkan pada rumusan masalah.

Tugas akhir ini dianggap berhasil apabila tujuan yang telah ditetapkan tercapai, yang akan diukur melalui kriteria-kriteria berikut:

1. Terbangunnya sebuah prototipe sistem kontrol akses yang dapat berfungsi secara end-to-end, mulai dari pengambilan citra wajah oleh kamera hingga aktuator (kunci elektronik) berhasil membuka akses.
2. Sistem mampu melakukan otentikasi wajah pengguna yang terdaftar dengan tingkat akurasi di atas 95% pada kondisi pengujian yang terkontrol (misalnya, pencahayaan dan posisi wajah yang ideal).
3. Waktu yang dibutuhkan sistem untuk menyelesaikan satu siklus proses otentikasi, mulai dari deteksi wajah hingga pengiriman perintah ke kunci elektronik. kurang dari 3 detik.
4. Sistem mampu secara konsisten membedakan antara pengguna terdaftar (memberikan akses) dan pengguna tidak terdaftar (menolak akses).

I.4 Batasan Masalah

Berikut merupakan beberapa batasan yang ditetapkan untuk memfokuskan ruang lingkup pengerjaan dan memastikan hasil dari tugas akhir ini relevan dengan tujuan yang telah ditetapkan:

1. Tugas akhir ini dikerjakan secara berkelompok yang terdiri dari 3 orang mahasiswa, yaitu Axelius Davin (NIM 18222016), Muhammad Rifa (NIM 18222004), dan Natanael Steven (NIM 18222054).

I.5 Metodologi

Tahapan yang akan dilalui selama pelaksanaan tugas akhir ini terdiri dari empat bagian, yaitu:

1. Perumusan Masalah dan Studi Kebutuhan
   Tahap awal pengerjaan adalah perumusan masalah dan studi kebutuhan, yang dimulai dengan observasi awal terhadap kondisi gedung ITB Innovation Park (IIP) yang belum memiliki sistem kontrol akses optimal. Fakta dari observasi ini kemudian divalidasi melalui diskusi informal dengan pihak terkait untuk mengonfirmasi urgensi masalah dan memahami persyaratan dasar sistem yang dibutuhkan. Berdasarkan temuan tersebut, dirumuskanlah pokok permasalahan utama mengenai kerentanan sistem akses konvensional, yang menjadi fondasi bagi penulisan Latar Belakang dan Rumusan Masalah.
2. Studi Literatur

Selanjutnya, dilakukan studi literatur untuk membangun landasan teori dan tinjauan teknologi yang relevan. Tahap ini dimulai dengan mengidentifikasi kebutuhan informasi yang mencakup konsep dasar seperti Computer Vision dan arsitektur Internet of Things (IoT), tinjauan state-of-the-art dari penelitian sejenis, serta informasi pendukung berupa dokumentasi teknis. Pencarian literatur dilakukan secara strategis pada portal publikasi ilmiah menggunakan kombinasi kata kunci spesifik seperti ”face recognition access control” dan ”IoT smart building security”. Seluruh literatur yang terkumpul kemudian dikelompokkan dan ditapis berdasarkan relevansi serta kebaruannya untuk memastikan solusi yang dirancang didasarkan pada pengetahuan yang solid dan mutakhir.

3. Perancangan dan Pengembangan Sistem

   Setelah landasan teori terbentuk, pengerjaan dilanjutkan dengan tahap perancangan dan pengembangan sistem. Tahap ini diawali dengan perancangan arsitektur sistem secara menyeluruh, baik dari sisi perangkat keras maupun perangkat lunak. Kemudian, dilakukan pengembangan perangkat keras yang meliputi perakitan komponen IoT seperti Single-Board Computer (Raspberry Pi), kamera, dan kunci elektronik. Secara paralel, perangkat lunak dikembangkan dengan mengimplementasikan kode program untuk modul akuisisi citra, algoritma pengenalan wajah, dan logika kontrol. Puncak dari tahap ini adalah proses integrasi untuk menggabungkan modul perangkat keras dan perangkat lunak menjadi satu kesatuan prototipe yang fungsional.

4. Pengujian dan Evaluasi Sistem

   Tahap terakhir dari metodologi ini adalah pengujian dan evaluasi sistem. Proses ini dimulai dengan merancang skenario pengujian yang sistematis berdasarkan kriteria keberhasilan yang telah ditetapkan, seperti akurasi, kecepatan, dan keandalan. Selanjutnya, prototipe diuji coba sesuai skenario tersebut menggunakan dataset wajah pengguna terdaftar dan tidak terdaftar. Data yang diperoleh dari hasil pengujian kemudian dianalisis secara kuantitatif untuk mengevaluasi performa sistem. Evaluasi ini bertujuan untuk memvalidasi apakah solusi yang dibangun berhasil menjawab rumusan masalah dan mencapai tujuan tugas akhir, serta mengidentifikasi potensi perbaikan di masa depan.

BAB II

STUDI LITERATUR

II.0.1 Penggunaan Kata ”masing-masing” dan ”setiap”

Kata “masing-masing” digunakan di belakang kata yang diterangkan, misalnya ”Setiap proses menggunakan algoritma masing-masing”. Kata “tiap-tiap” atau “setiap” ditempatkan di depan kata yang diterangkan, misalnya ”Setiap proses menggunakan algoritma tertentu”.

II.1 Survei Pengenalan Wajah Berbasis Deep Learning

Sebuah survei mengenai pengenalan wajah berbasis deep learning yang menyajikan gambaran umum tentang perkembangan di bidang ini. Studi membahas berbagai arsitektur jaringan saraf tiruan, fungsi loss, dan strategi pelatihan yang digunakan untuk meningkatkan akurasi dan ketahanan sistem pengenalan wajah. Fungsi loss mempunyai peran yang vital dalam melatih model agar bisa membedakan identitas yang berbeda. Pembahasan di studi ini mencakup evolusi dari fungsi loss tradisional hingga fungsi loss berbasis margin yang meningkatkan jarak antar kelas dan penurunan jarak intra kelas.

II.2 AdaFace : Quality Adaptive Margin for Face Recognition

Penelitian ini berfokus pada penyelesaian masalah variabilitas kualitas gambar. Konsep utama dari AdaFace adalah tidak semua gambar memberikan kontribusi belajar yang sama. Contohnya adalah gambar yang berkualitas tinggi merupakan contoh yang “mudah”, sementara gamabr yang berkualitas rendah adalah contoh yang “sulit”. Metode pelatihan konvensional memperlakukan semua gambar ini secara setara, membuat model sulit belajar dari gambar berkualitas rendah. Kualitas setiap gambar dalam data training diestimasi secara langsung. Tanpa menggunakan model yang terpisah, AdaFace menggunakan norma dari feature norm yang dihasilkan dari

model itu sendiri sebagai proksi untuk kualitas gambar. Gambar yang berkualitas tinggi cenderung menghasilkan fitur dengan norma yang lebih besar. Dengan estimasi kualitas, AdaFace menyesuaikan margin pada fungsi loss. Untuk gambar berkualitas tinggi, margin yang lebih besar diterapkan agar model bekerja lebih keras dan menghasilkan fitur yang lebih diskriminatif. Sebaliknya, untuk gambar berkualitas rendah, margin yang lebih kecil dilakukan. Hal ini mencegah terpengaruh oleh noise dan artefak pada gambar tetapi tetap bisa mempelajari fitur identitas dasarnya.

II.3 Android Mobile Security and File Protection Using Face Recognition

Penelitian ini mengubah fokus dari pengembangan algoritma menjadi implementasi praktik pada platform Android. Studi ini mendemonstrasikan kelayakan dan tantangan dalam menerapkan teknologi pengenalan wajah untuk tujuan keamanan. Untuk dapat berjalan secara efisien di perangkat seluler, model CNN yang digunakan harus dioptimalkan. Arsitektur yang dirancang khusus untuk perangkat edge, seperti MobileNet atau SqueezeNet, yang menyeimbangkan akurasi dengan kecepatan komputasi dan penggunaan memori yang rendah.

II.4 Efficient Face Recognition System for Operating in Unconstrained Environments

Penelitian ini berasal dari masalah bahwa banyak sistem pengenalan wajah yang sudah akurat, tetapi belum efisien atau tidak stabil jika dalam kondisi linkungan yang tidak terkendali. Sebaliknya, sistem yang ringan dan cepat sering kali tidak mampu mempertahankan akurasi tinggi. Berdasarkan ini, penelitian dilakukan agar sistem pengenalan wajah tetap akurat meskipun dijalankan di linkungan tidak terkendali. Deteksi wajah berbasis deep learning seperti You Only Look Once yang cepat dan efisien, ekstraksi fitur wajah berbasis embedding seperti FaceNet, yang bisa merepresentasikan wajah kedalam vektor numerik dengan jarak Euclidean. Penelitian juga menggunakan algoritma klasifikasi tradisional seperti SVM, KNN, dan Random Forest untuk menggantikan layer softmax pada jaringan FaceNet.

II.5 Face Recognition Using Facial Features

Dalam penelitian ini, masalah yang diangkat adalah metode pengenalan wajah masih bersifat “black box” dan kurang menjelaskan fitur wajah yang memengaruhi hasil pengenalan. Selain itu, sebagian metode deep learning memerlukan data dan daya komputasi yang besar, sementara metode berbasis geometri dan struktural untuk

fitur wajah masih jarang dikaji dengan pendekatan modern. Penelitian ini mencoba menyelesaikan masalah untuk bagaimana menggunakan fitur waja utama untuk pengenalan yang ringan dan akurat. Penelitian mendasarkan penelitian pada teori ekstraksi fitur geometris dan landmark wajah, di mana posisi dan jarak antar fitur wajah menjadi representasi identitas seseorang. Metode ini menggunakan algoritma seperti Active Shape Model (ASM) atau Active Appearance Model (AAM) untuk mendeteksi landmark dan Local Binary Pattern (LBP) atau Histogram of Oriented Gradients (HOG) untuk mengekstrak tekstur. Konsep ini menggabungkan pendekatan analisis bentuk dan tekstur sebagai tekstur pengenalan.

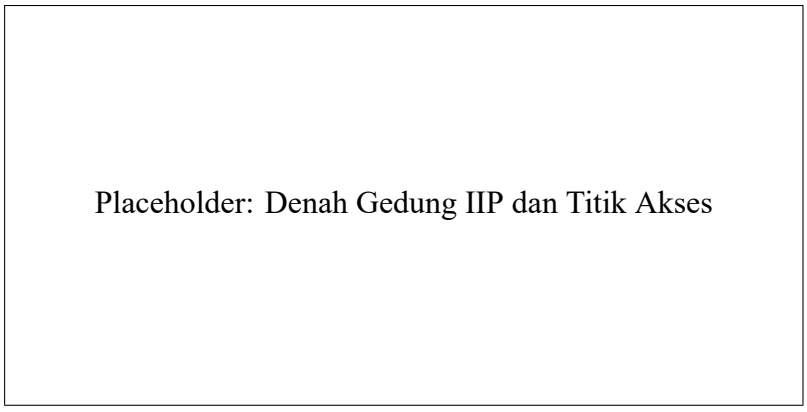
BAB III

ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Model konseptual sistem kontrol akses yang ada saat ini di Gedung ITB Innovation Park (IIP) masih mengandalkan, atau setidaknya mempertimbangkan, metode konvensional. Komponen utamanya adalah kunci fisik dan kartu akses. Ketiadaan sistem modern yang terimplementasi secara optimal ini menimbulkan beberapa masalah fundamental.

Analisis kondisi saat ini didasarkan pada observasi lapangan serta analisis dokumen yang relevan. Dari observasi, teridentifikasi bahwa titik-titik akses utama belum dilengkapi sistem keamanan terotomatisasi. Analisis dokumen mencakup tinjauan terhadap Standar Operasional Prosedur (SOP) keamanan gedung dan denah arsitektur untuk memetakan alur pergerakan manusia serta posisi strategis untuk penempatan sistem kontrol. Gambar III.1 menunjukkan denah Gedung IIP dan titik-titik akses yang menjadi fokus dalam penelitian ini.



Gambar III.1 Denah Gedung IIP dan Titik Akses Kritis

Masalah utama dari sistem konvensional ini adalah tingkat keamanannya yang terba-

tas. Metode kunci fisik dan kartu akses sangat rentan terhadap risiko umum seperti kehilangan, pencurian, atau duplikasi yang tidak sah. Mengingat Gedung IIP berfungsi sebagai pusat inovasi yang menyimpan berbagai aset bernilai tinggi, celah keamanan ini menciptakan sebuah kerentanan keamanan yang nyata dan mendesak untuk segera diatasi. Sistem yang ada saat ini (atau ketiadaan sistem yang memadai) dinilai tidak lagi efisien dalam pengelolaan dan tidak mampu melindungi aset di dalamnya secara optimal.

III.2 Analisis Kebutuhan

Proses analisis kebutuhan sistem dilakukan untuk mendefinisikan apa yang harus dilakukan oleh sistem guna menyelesaikan masalah yang ada. Metode pengumpulan kebutuhan yang digunakan adalah:

1. Wawancara Semi-Terstruktur: Dilakukan dengan pemangku kepentingan, yaitu perwakilan dari Manajemen/Pengelola Gedung IIP untuk memahami kebutuhan dari sisi keamanan dan operasional, serta wawancara dengan beberapa Penghuni Gedung (staf/peneliti) untuk memahami kebutuhan dari sisi pengguna akhir.
2. Observasi Langsung: Mengamati secara langsung proses keluar-masuk gedung pada jam-jam sibuk untuk mengidentifikasi potensi masalah alur dan kebutuhan non-fungsional seperti kecepatan akses.

Hasil dari kedua metode ini digunakan untuk merumuskan masalah pengguna serta kebutuhan fungsional dan non-fungsional.

III.2.1 Identifikasi Masalah Pengguna

Berdasarkan analisis kondisi saat ini dan metode pengumpulan kebutuhan, terdapat dua kelompok pengguna utama dengan masalah yang spesifik:

1. Penghuni Gedung (Pegawai, Anggota Terdaftar, Staf)
   (a) Mengalami kesulitan dengan metode akses konvensional yang merepotkan (harus membawa kartu/kunci) dan tidak higienis (harus menyentuh perangkat bersama).
   (b) Membutuhkan sistem yang memberikan ”kemudahan bagi pengguna”.
   (c) Memiliki risiko keamanan pribadi jika kunci atau kartu akses mereka hilang atau diduplikasi.
2. Manajemen/Pengelola Gedung IIP
   (a) Menghadapi masalah utama berupa kerentanan keamanan terhadap aset bernilai tinggi.

(b) Kesulitan mengelola dan melacak hak akses secara efisien menggunakan metode konvensional.
(c) Kekurangan data operasional mengenai pola keluar-masuk, yang dapat digunakan untuk efisiensi.

III.2.2 Kebutuhan Fungsional

Berdasarkan rumusan masalah dan tujuan, kebutuhan fungsional (KF) untuk prototipe yang diusulkan adalah sebagai berikut:

1. KF-1: Sistem harus dapat mengakuisisi citra wajah pengguna secara real-time melalui sensor kamera.
2. KF-2: Sistem harus dapat melakukan proses otentikasi (verifikasi) dengan membandingkan citra wajah yang ditangkap dengan basis data pengguna yang terdaftar.
3. KF-3: Sistem harus dapat memberikan perintah untuk membuka aktuator (kunci elektronik) jika otentikasi pengguna berhasil (memberikan hak akses).
4. KF-4: Sistem harus dapat menolak akses (tidak mengirim perintah ke kunci elektronik) jika otentikasi gagal atau wajah tidak terdaftar.

III.2.3 Kebutuhan Nonfungsional

Kebutuhan nonfungsional (KNF) didefinisikan secara spesifik dalam kriteria keberhasilan tugas akhir ini:

1. KNF-1 (Kecepatan): Waktu yang dibutuhkan sistem untuk menyelesaikan satu siklus proses otentikasi—mulai dari deteksi wajah hingga pengiriman perintah ke kunci elektronik—harus kurang dari 3 detik.
2. KNF-2 (Akurasi): Sistem harus mampu melakukan otentikasi wajah pengguna yang terdaftar dengan tingkat akurasi di atas 95% pada kondisi pengujian yang terkontrol.
3. KNF-3 (Keandalan): Sistem harus mampu secara konsisten membedakan antara pengguna terdaftar (memberikan akses) dan pengguna tidak terdaftar (menolak akses).

III.3 Analisis Pemilihan Solusi

III.3.1 Alternatif Solusi

Berdasarkan penelusuran literatur dan studi kasus pada sistem kontrol akses modern, diidentifikasi tiga alternatif solusi utama yang relevan untuk dibandingkan:

III.3.1.1 Solusi Konvensional (Kartu Akses/RFID)

1. Konsep Dasar: Menggunakan kartu berbasis *Radio-Frequency Identification* (RFID) yang di-tap pada sebuah pembaca (reader) untuk memverifikasi hak akses.
2. Kelebihan: Biaya implementasi per unit relatif rendah, teknologi matang, dan kecepatan otentikasi sangat cepat (kurang dari 1 detik).
3. Keterbatasan: Keamanan terbatas (kartu dapat hilang, dicuri, atau diduplikasi), merepotkan pengguna (harus selalu membawa kartu), dan biaya operasional untuk penggantian kartu yang hilang.

III.3.1.2 Solusi Biometrik (Sidik Jari)

1. Konsep Dasar: Menggunakan pemindai untuk merekam pola unik sidik jari pengguna dan mencocokkannya dengan basis data.
2. Kelebihan: Tingkat keamanan tinggi (sulit dipalsukan), tidak memerlukan perangkat tambahan yang harus dibawa pengguna.
3. Keterbatasan: Memerlukan kontak fisik (tidak higienis, menjadi masalah terutama pasca-pandemi), rentan gagal baca jika jari kotor atau basah, dan dapat menimbulkan antrian karena proses *scan* yang individual.

III.3.1.3 Solusi Biometrik (Pengenalan Wajah)

1. Konsep Dasar: Menggunakan kamera untuk menangkap fitur wajah pengguna, kemudian algoritma *computer vision* memverifikasi identitas pengguna tersebut.
2. Kelebihan: Bersifat *non-kontak* (higienis dan nyaman), keamanan tinggi, dan tidak memerlukan perangkat tambahan. Proses bisa berjalan pasif tanpa interaksi eksplisit dari pengguna.
3. Keterbatasan: Biaya implementasi awal bisa lebih tinggi (memerlukan kamera dan unit pemrosesan yang mumpuni), akurasi dapat dipengaruhi oleh kondisi pencahayaan ekstrem, penggunaan masker, atau perubahan penampilan drastis.

III.3.2 Analisis Penentuan Solusi

Untuk memilih solusi terbaik secara sistematis dan objektif, digunakan metode *Weighted Scoring Model* (WSM). Kriteria penilaian dan bobotnya ditentukan berdasarkan prioritas kebutuhan yang diidentifikasi pada bagian Analisis Kebutuhan. Kriteria

utama meliputi Keamanan (Bobot: 40%), Kemudahan Pengguna/Higienitas (Bobot: 30%), Kecepatan Akses (Bobot: 20%), dan Biaya Implementasi Awal (Bobot: 10%).

Setiap alternatif solusi diberi skor 1 (Sangat Buruk) hingga 5 (Sangat Baik) untuk setiap kriteria.

Tabel III.1 Analisis Penentuan Solusi Menggunakan Weighted Scoring Model

Kriteria Penilaian	**Bobot**	**Kartu Akses (RFID)**	**Sidik Jari**	**Pengenalan Wajah**
Keamanan	40%	Skor: 2 (1.0)	Skor: 4 (1.6)	Skor: 4 (1.6)
Kemudahan/Higienitas	30%	Skor: 3 (0.9)	Skor: 2 (0.6)	Skor: 5 (1.5)
Kecepatan Akses	20%	Skor: 5 (1.0)	Skor: 3 (0.6)	Skor: 4 (0.8)
Biaya Implementasi	10%	Skor: 5 (0.5)	Skor: 4 (0.4)	Skor: 3 (0.3)
Total Skor	**100%**	**3.4**	**3.2**	**4.2**

Berdasarkan hasil pada Tabel III.1, Solusi Pengenalan Wajah memperoleh total skor tertinggi (4.2). Meskipun sedikit lebih mahal dalam implementasi awal (Skor: 3), keunggulannya yang signifikan pada kriteria Kemudahan Pengguna/Higienitas (Skor: 5) dan Keamanan (Skor: 4) menjadikannya pilihan yang paling sesuai untuk diterapkan di lingkungan modern seperti Gedung IIP, sejalan dengan penyelesaian masalah utama yang telah diidentifikasi.

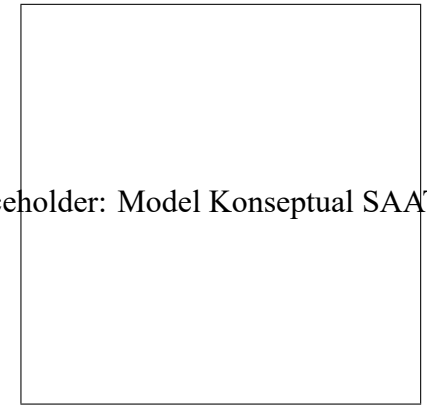
BAB IV

DESAIN KONSEP SOLUSI

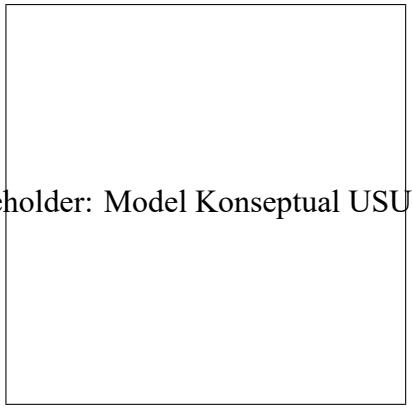
Bab ini berisi penjelasan detail tentang desain dan arsitektur sistem yang diusulkan untuk menjawab rumusan masalah yang telah dijabarkan pada Bab I. Penjelasan diberikan secara sistematis, dimulai dari tahapan perancangan yang dilakukan, hingga hasil akhir desain sistem yang akan dibangun.

IV.1 Model Konseptual Solusi (Before vs After)

Bagian ini mengilustrasikan perbedaan konseptual antara sistem kontrol akses saat ini (seperti yang dianalisis pada Bab III) dengan sistem yang diusulkan. Ilustrasi sistem sebelum (Gambar IV.1a) menunjukkan sistem konvensional, sedangkan ilustrasi sistem sesudah (Gambar IV.1b) menunjukkan desain konsep solusi yang diusulkan.



(a) Sistem Saat Ini (Konvensional)



(b) Sistem Usulan (Pengenalan Wajah)

Gambar IV.1 Perbandingan Model Konseptual Sistem (Before vs After)

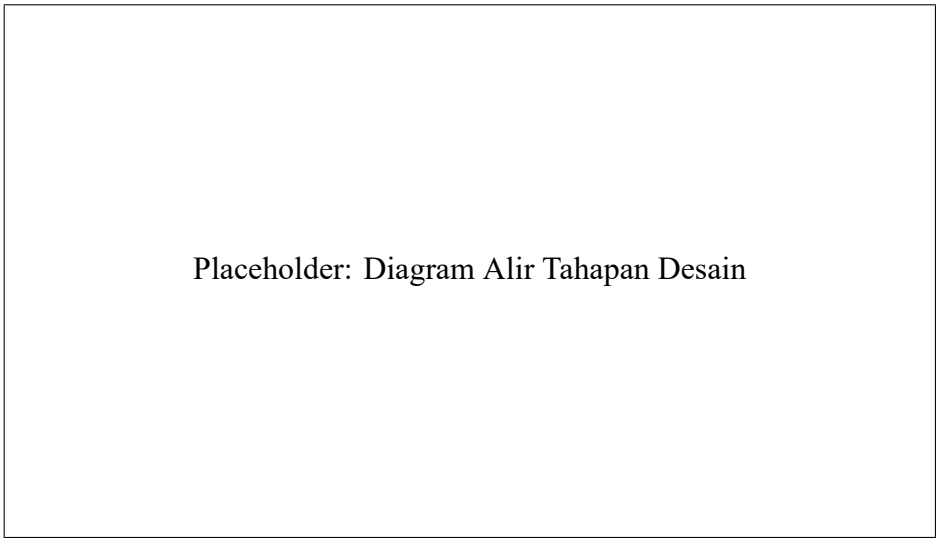
Perbedaan utama antara kedua model tersebut adalah:

1. **Sistem Saat Ini (Before):** Belum ada sistem sebelumnya
2. **Sistem Usulan (After):** Gambar IV.1b menunjukkan sistem yang diusulkan berbasis otentikasi biometrik (*inherence* atau ”apa diri Anda”). Alur kerja menjadi terotomatisasi penuh, *contactless* (tanpa sentuh), dan terintegrasi, yang secara fundamental meningkatkan keamanan dan efisiensi operasional.

IV.2 Tahapan Desain

Proses perancangan sistem dilakukan melalui beberapa tahapan yang logis dan sistematis untuk memastikan bahwa hasil desain selaras dengan kebutuhan fungsional dan nonfungsional yang telah diidentifikasi pada Bab III. Tahapan ini tidak didasarkan pada preferensi pribadi, melainkan pada pendekatan rekayasa sistem yang umum digunakan untuk pengembangan prototipe berbasis *Internet of Things* (IoT) dan kecerdasan buatan.

Gambar IV.2 menyajikan diagram alir (flowchart) dari langkah-langkah perancangan yang dilakukan.



Gambar IV.2 Diagram Alir Tahapan Perancangan Sistem

Penjelasan detail untuk setiap tahapan dalam diagram alir tersebut adalah sebagai berikut:

IV.2.1 Perancangan Arsitektur Sistem

Tahapan pertama adalah merancang arsitektur sistem secara *high-level*. Tahap ini berfokus pada penentuan komponen-komponen utama sistem, yaitu perangkat keras (*hardware*), perangkat lunak (*software*), dan basis data (*database*). Tujuannya adalah untuk mendefinisikan bagaimana ketiga komponen utama tersebut saling berinteraksi untuk membentuk satu solusi yang terintegrasi dan dapat menjawab rumusan masalah pertama (RM-1).

IV.2.2 Perancangan Perangkat Keras

Setelah arsitektur *high-level* ditentukan, tahapan dilanjutkan dengan perancangan perangkat keras. Berdasarkan kebutuhan fungsional (KF-1, KF-3) dan nonfungsional (KNF-1), dilakukan pemilihan komponen spesifik untuk akuisisi citra, pemrosesan data, dan aktuator kontrol akses. Tahap ini mencakup perancangan skematik dan diagram koneksi antar komponen, seperti hubungan antara unit pemrosesan (misalnya *Single-Board Computer*), kamera, dan kunci elektronik.

IV.2.3 Perancangan Perangkat Lunak dan Algoritma

Tahap ini merupakan inti dari sistem dan berfokus untuk menjawab rumusan masalah kedua (RM-2). Perancangan perangkat lunak dibagi lagi menjadi beberapa sub-tahapan:

1. Perancangan Alur Akuisisi Citra: Menentukan bagaimana sistem akan menangkap video *stream* dari kamera dan mengambil *frame* untuk diproses.
2. Pemilihan dan Desain Algoritma: Memilih model atau algoritma yang tepat untuk deteksi wajah (*face detection*) dan pengenalan wajah (*face recognition*).
3. Perancangan Logika Kontrol: Merancang alur logika *if-then-else* yang akan mengambil keputusan (memberi atau menolak akses) berdasarkan hasil dari algoritma pengenalan wajah.

IV.2.4 Perancangan Basis Data

Tahapan terakhir adalah merancang struktur penyimpanan data. Untuk memenuhi kebutuhan fungsional KF-2, sistem memerlukan basis data untuk menyimpan informasi pengguna terdaftar. Tahap ini menentukan bagaimana data pengguna (misalnya ID, nama) dan data biometrik mereka (misalnya *feature embeddings* dari wajah) akan disimpan, diindeks, dan diakses oleh perangkat lunak untuk proses pencocokan.

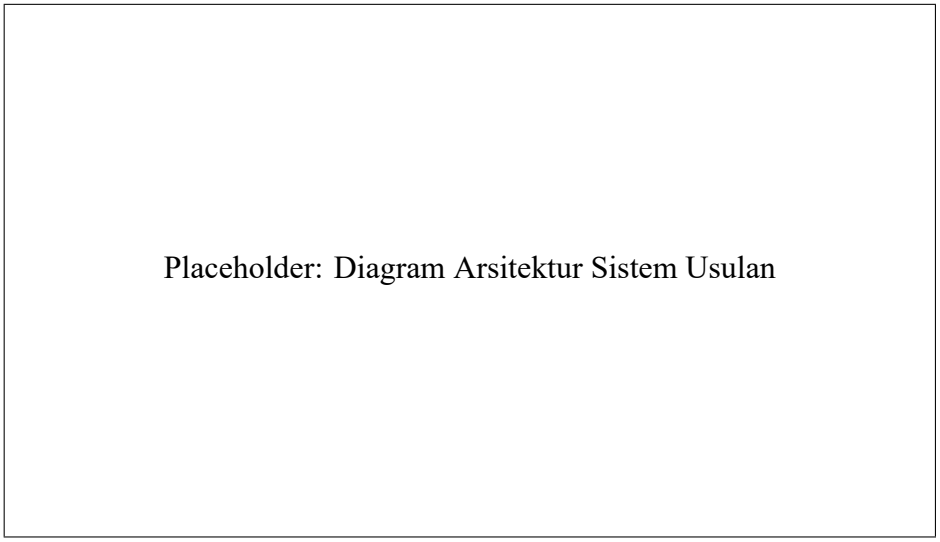
IV.3 Hasil Desain

Hasil akhir dari seluruh tahapan perancangan di atas adalah arsitektur sistem usulan yang akan diimplementasikan.

IV.3.1 Arsitektur Sistem Usulan

Arsitektur sistem yang diusulkan dirancang sebagai sistem *edge computing*, di mana seluruh proses komputasi (deteksi dan pengenalan) terjadi secara lokal di perangkat yang terpasang di titik akses. Hal ini dipilih untuk memenuhi kebutuhan nonfungsional KNF-1 (Kecepatan) dengan mengurangi latensi jaringan.

Gambar IV.3 mengilustrasikan arsitektur sistem usulan secara detail.



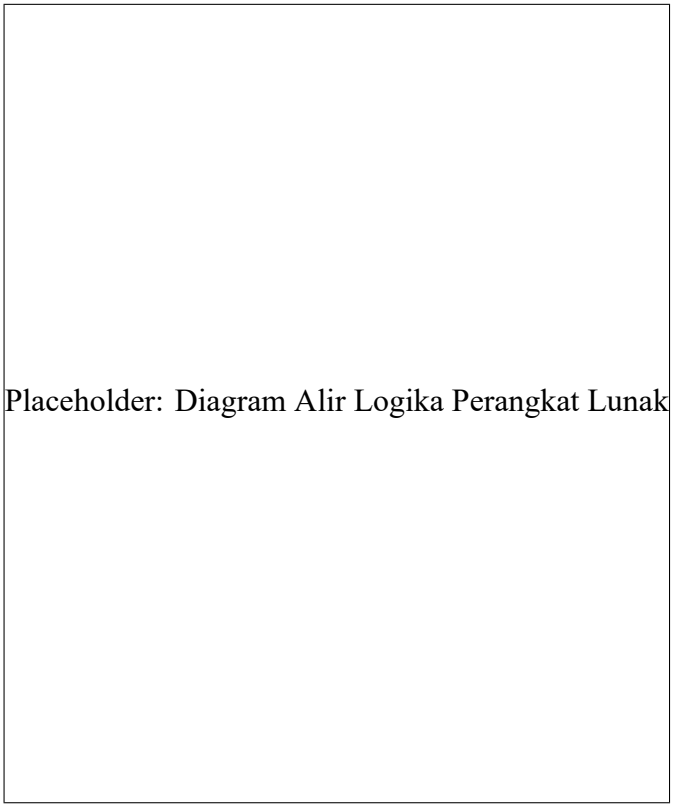
Gambar IV.3 Diagram Arsitektur Sistem Kontrol Akses

Alur kerja sistem berdasarkan arsitektur tersebut adalah sebagai berikut:

1. Pengguna berdiri di depan perangkat.
2. Kamera (Sensor) menangkap video *stream* secara terus-menerus dan mengirimkannya ke Unit Pemrosesan.
3. Unit Pemrosesan (misal: Raspberry Pi) menjalankan Modul Perangkat Lunak.
4. Perangkat lunak pertama-tama mendeteksi adanya wajah dalam *stream* (KF-1).
5. Jika wajah terdeteksi, algoritma pengenalan wajah mengekstraksi fitur biometrik dari wajah tersebut.
6. Fitur ini kemudian dicocokkan dengan Basis Data Wajah Terdaftar yang tersimpan di dalam perangkat (KF-2).
7. Logika Kontrol mengambil keputusan:
   (a) Jika fitur cocok (terdaftar), sinyal ”BUKA” dikirim ke Aktuator (KF-3).
   (b) Jika fitur tidak cocok (tidak terdaftar), sinyal ”TOLAK” dikirim (atau tidak ada sinyal) (KF-4).
8. Kunci Elektronik (Aktuator) membuka atau tetap mengunci pintu.

IV.3.2 Desain Alur Logika Perangkat Lunak

Untuk menjawab RM-2 secara lebih rinci, alur logika perangkat lunak yang akan diimplementasikan dirancang seperti pada Gambar IV.4. Desain ini memastikan bahwa sumber daya pemrosesan hanya digunakan saat diperlukan (yaitu, saat wajah terdeteksi).



Gambar IV.4 Diagram Alir Logika Proses Otentikasi

BAB V

RENCANA SELANJUTNYA

Bab ini merincikan rencana dan jadwal pengerjaan selanjutnya untuk mengimplementasikan dan mengevaluasi solusi yang telah dirancang pada Bab IV. Rencana ini disajikan dalam bentuk linimasa (timeline) pengerjaan, yang kemudian dirincikan lebih lanjut ke dalam rencana implementasi, desain pengujian, dan analisis risiko.

V.1 Linimasa Pengerjaan

Pengerjaan Tugas Akhir direncanakan berlangsung selama 14 bulan, dimulai dari September 2025 (tahap studi awal dan proposal) hingga Oktober 2026. Implementasi sistem akan dimulai pada Januari 2026. Linimasa pengerjaan disajikan dalam bentuk Gantt chart pada Tabel V.1.

Tabel V.1 Gantt Chart Rencana Pengerjaan Tugas Akhir

Tahapan Kegiatan	Sep-Okt '25	Nov-Des '25	Jan-Mar '26	Apr-Jun '26	Jul-Sep '26	Okt '26
1. Perencanaan dan Persiapan						
Penyusunan Proposal (Studi Awal)						
Studi Lanjut dan Persiapan Perangkat						
2. Implementasi dan Pengembangan						
Pengembangan Perangkat Keras						
Pengembangan Perangkat Lunak						
Integrasi Sistem						
3. Pengujian dan Evaluasi						
Pengujian dan Analisis Hasil						
4. Penulisan dan Finalisasi						
Penulisan Laporan (Bab 1-5)						
Penulisan Bab 6 dan Finalisasi						

V.2 Rencana Implementasi

Tabel V.2 merincikan rencana implementasi prototipe, mencakup perangkat keras, perangkat lunak, lingkungan, dan estimasi biaya yang diperlukan.

Tabel V.2 Rencana Implementasi Prototipe

Komponen / Aspek	Deskripsi dan Spesifikasi
Perangkat Keras	
Unit Pemrosesan	Raspberry Pi 4 Model B (4GB RAM) - Dipilih karena keseimbangan antara performa untuk *edge computing* dan ketersediaan *port* GPIO.
Sensor (Kamera)	Raspberry Pi Camera Module v2 - Untuk akuisisi citra wajah.
Aktuator (Kunci)	Solenoid Door Lock 12V, dikontrol melalui 5V Relay Module.
Pendukung	Power Supply 5V 3A (untuk Pi), Power Supply 12V 1A (untuk kunci), *breadboard*, dan kabel *jumper*.
Perangkat Lunak	
Sistem Operasi	Raspberry Pi OS (sebelumnya Raspbian) - Berbasis Debian.
Bahasa	Python 3.
Pustaka Utama	OpenCV (untuk akuisisi dan pemrosesan gambar), Dlib (untuk deteksi *landmark* dan pengenalan wajah), RPi.GPIO (untuk kontrol aktuator).
Lingkungan	
Lokasi	Prototipe akan diuji pada simulasi pintu masuk di Laboratorium X, Gedung IIP.
Konfigurasi	Perangkat akan dipasang setinggi rata-rata wajah orang berdiri (sekitar 160-170 cm) dengan kondisi pencahayaan dalam ruangan yang terkontrol.
Estimasi Biaya	
Raspberry Pi 4	Rp 1.000.000
Pi Camera Module	Rp 400.000
Solenoid Lock + Relay	Rp 150.000
Komponen Pendukung	Rp 200.000
Total Estimasi	**Rp 1.750.000**

V.3 Desain Pengujian dan Evaluasi

Pengujian dan evaluasi akan dilakukan untuk memverifikasi kebutuhan fungsional (KF) dan memvalidasi kebutuhan nonfungsional (KNF). Metode pengujian dirangkum pada Tabel V.3.

Tabel V.3 Desain Pengujian dan Evaluasi Sistem

Kriteria (dari Bab III)	**Metode Verifikasi / Validasi**	**Parameter Keberhasilan**
Verifikasi Fungsional		
KF-1 s.d. KF-4	**Pengujian Fungsional (Black-box)** Skenario: 1. Uji pengguna terdaftar. 2. Uji pengguna tidak terdaftar.	1. Skenario 1: Kunci harus terbuka (KF-1, KF-2, KF-3 terpenuhi). 2. Skenario 2: Kunci harus tetap tertutup (KF-4 terpenuhi).
Validasi Nonfungsional		
KNF-1 (Kecepatan)	**Pengujian Waktu Respon** Mengukur waktu (dengan *stopwatch* atau *logging* internal) dari saat wajah terdeteksi penuh oleh kamera hingga sinyal dikirim ke aktuator.	Waktu rata-rata dari 20 kali percobaan harus **kurang dari 3 detik**.
KNF-2 (Akurasi)	**Pengujian Akurasi** Membuat *dataset* uji (10 pengguna terdaftar, 5 pengguna tidak terdaftar). Setiap pengguna diuji 5 kali dalam kondisi pencahayaan ideal.	Akurasi $= \frac{\text{TP}+\text{TN}}{\text{Total Percobaan}}$ Akurasi harus **di atas 95%**.
KNF-3 (Keandalan)	**Pengujian Konsistensi** Menggunakan 1 pengguna terdaftar dan 1 pengguna tidak terdaftar, diuji secara bergantian sebanyak 20 kali.	Sistem harus secara konsisten (100%) memberi akses kepada pengguna terdaftar dan menolak pengguna tidak terdaftar.

V.4 Analisis Risiko dan Mitigasi

Analisis risiko dilakukan untuk mengidentifikasi potensi masalah selama implementasi dan pengujian, beserta tindakan mitigasi yang disiapkan (Tabel V.4).

Tabel V.4 Analisis Risiko dan Mitigasi Proyek

No.	Risiko	Dampak	Tindakan Mitigasi
1.	**Risiko Teknis:** Akurasi pengenalan wajah rendah (di bawah 95%).	Gagal memenuhi KNF-2. Pengguna terdaftar ditolak.	1. Melakukan *data augmentation* pada *dataset* latih. 2. Memastikan pencahayaan di area pengujian cukup dan merata.
2.	**Risiko Teknis:** Waktu respon lambat (lebih dari 3 detik).	Gagal memenuhi KNF-1. Menyebabkan antrian di pintu.	1. Optimasi kode (misalnya, mengurangi resolusi *frame* yang diproses). 2. Menyesuaikan *threshold* algoritma untuk kecepatan.
3.	**Risiko Operasional:** Kegagalan fungsi akibat variasi pencahayaan ekstrem (misal: terlalu gelap atau *backlight*).	Akurasi menurun drastis pada jam-jam tertentu.	1. Menambahkan sumber pencahayaan eksternal (misal: LED) pada prototipe. 2. Mengumpulkan data latih tambahan pada kondisi pencahayaan tersebut.
4.	**Risiko Proyek:** Kerusakan komponen perangkat keras (misal: Raspberry Pi atau kamera).	Keterlambatan pengerjaan.	1. Mengalokasikan dana darurat (telah termasuk dalam ”Komponen Pendukung”) untuk pembelian ulang.