

**PENGEMBANGAN SISTEM KONTROL AKSES
BERBASIS PENGENALAN WAJAH UNTUK
MANAJEMEN TAMU PADA BANGUNAN
CERDAS**

Proposal Tugas Akhir

Oleh

**Natanael Steven Simangunsong
18222054**



**PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
5 Desember 2025**

LEMBAR PENGESAHAN

PENGEMBANGAN SISTEM KONTROL AKSES BERBASIS PENGENALAN WAJAH UNTUK MANAJEMEN TAMU PADA BANGUNAN CERDAS

Proposal Tugas Akhir

Oleh

**Natanael Steven Simangunsong
18222054**

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 5 Desember 2025

Pembimbing

Dr. Fadhil Hidayat, S.Kom., M.T.
NIP. 198609252012121002

DAFTAR ISI

DAFTAR GAMBAR	iv
DAFTAR TABEL	v
DAFTAR KODE	vi
I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Rumusan Masalah	3
I.3 Tujuan	3
I.4 Batasan Masalah	4
I.5 Metodologi	4
II STUDI LITERATUR	6
II.1 Tinjauan Regulasi Bangunan Gedung Cerdas	6
II.2 Kontrol Akses	7
II.3 Gerbang sebagai Kontrol Akses	7
II.4 Pengenalan Wajah	8
II.4.1 Parameter Evaluasi Kinerja Biometrik	9
II.5 Keamanan Data dan Privasi	9
II.6 Metodologi Design Thinking	10
III ANALISIS MASALAH	11
III.1 Analisis Kondisi Saat Ini	11
III.1.1 Alur Masuk Tamu Saat Ini	11
III.1.2 Kondisi Lobi Saat Ini	12
III.2 Analisis Kebutuhan	12
III.2.1 Identifikasi Masalah Pengguna	13
III.2.2 Kebutuhan Fungsional	13
III.2.3 Kebutuhan Nonfungsional	14
III.3 Analisis Pemilihan Solusi	15
III.3.1 Alternatif Solusi	15
III.3.2 Analisis Penentuan Solusi	17
III.3.2.1 KF-1: Kontrol Akses	17
III.3.2.2 KF-2: Deteksi Wajah	19
III.3.2.3 KF-3: Pengenalan Wajah	20

III.3.2.4	KF-4: Manajemen Pendaftaran	22
III.3.2.5	KF-5: Integrasi Sistem	24
III.3.2.6	KF-6: Keselamatan/safety	25
IV DESAIN KONSEP SOLUSI	26
IV.1	Diagram Konseptual	26
IV.2	Penjelasan Desain	29
IV.2.1	Spesifikasi Perangkat Keras	29
IV.2.2	Diagram Komponen	30
IV.2.3	Logika Autentikasi	31
IV.2.4	Alur Pendaftaran pada Sistem Kontrol Akses	32
V RENCANA SELANJUTNYA	34
V.1	Rencana Implementasi	34
V.1.1	Lini masa Penggerjaan	34
V.1.2	Implementasi Prototipe	36
V.2	Rencana Pengujian dan Evaluasi	37
V.3	Analisis Risiko dan Mitigasi	39
LAMPIRAN A - TRANSKRIP WAWANCARA I	43
LAMPIRAN B - TRANSKRIP WAWANCARA II	45
LAMPIRAN C - DOKUMENTASI KEGIATAN	47
LAMPIRAN D PERHITUNGAN ESTIMASI KEBUTUHAN PENYIMPANAN DATA	48
LAMPIRAN E PERHITUNGAN KAPASITAS DAN JUMLAH GERBANG	50

DAFTAR GAMBAR

II.1	Contoh penerapan desain pada pintu akses (<i>turnstile</i>)	8
III.1	Kondisi lapangan dari lobi Gedung IIP	12
IV.1	Alur kontrol akses sebelum penerapan sistem gerbang	26
IV.2	Alur kontrol akses sesudah penerapan sistem gerbang untuk karyawan gedung	27
IV.3	Alur kontrol akses sesudah penerapan sistem gerbang untuk tamu gedung	27
IV.4	Alur kontrol akses sesudah penerapan sistem gerbang saat kondisi darurat	28
IV.5	Denah lobi sebelum pemasangan sistem gerbang	28
IV.6	Denah lobi setelah pemasangan sistem gerbang	29
IV.7	Dimensi dari <i>swing barrier</i>	30
IV.8	Diagram komponen dari rancangan sistem	31
IV.9	Logika autentikasi dari rancangan sistem	32
IV.10	Alur pendaftaran pada sistem kontrol akses	33
1	Dokumentasi Proses Wawancara dengan Pengelola Gedung dan Pihak DKST	47

DAFTAR TABEL

III.1	Kebutuhan fungsional sistem	14
III.2	Kebutuhan Nonfungsional Sistem	15
III.3	Kriteria Evaluasi Kontrol Akses Fisik	18
III.4	Analisis Penentuan Solusi Perangkat Gerbang Menggunakan Weighted Scoring Model	19
III.5	Kriteria Evaluasi Pendekripsi Wajah	19
III.6	Analisis Penentuan Solusi Model Pendekripsi Wajah Menggunakan Weighted Scoring Model	20
III.7	Kriteria Evaluasi Untuk Solusi Pengenalan Wajah	21
III.8	Analisis Penentuan Solusi Model Pengenalan Wajah Menggunakan Weighted Scoring Model	22
III.9	Kriteria Evaluasi Proses Pendaftaran Mandiri	23
III.10	Analisis Penentuan Solusi Pendaftaran Mandiri Menggunakan Weighted Scoring Model	23
III.11	Kriteria evaluasi Metode Integrasi Data	24
III.12	Analisis Penentuan Solusi Integrasi Sistem Menggunakan Weighted Scoring Model	24
III.13	Kriteria Evaluasi Mekanisme Keselamatan	25
III.14	Analisis Penentuan Mekanisme Keselamatan Menggunakan Weighted Scoring Model	25
V.1	Gantt chart rencana pelaksanaan tugas akhir	34
V.2	Rencana implementasi prototipe	36
V.2	Rencana implementasi prototipe (lanjutan)	37
V.3	Desain pengujian dan evaluasi sistem	37
V.4	Analisis risiko dan mitigasi proyek	40
5	Transkrip Wawancara dengan Pengelola Gedung (10 November 2025)	43
5	Transkrip Wawancara dengan Pengelola Gedung (lanjutan)	44
6	Transkrip Diskusi Teknis dan Bisnis (21 November 2025)	45
6	Transkrip Diskusi Teknis dan Bisnis (lanjutan)	46

DAFTAR KODE

BAB I

PENDAHULUAN

I.1 Latar Belakang

Pengelolaan keamanan pada bangunan cerdas merupakan aspek yang penting untuk memastikan aktivitas di dalam gedung berlangsung dengan aman, tertib, dan efisien. Sistem kontrol digunakan akses oleh karyawan sebagai pengguna tetap gedung dan bagi tamu atau pengunjung yang memiliki tujuan dan durasi kunjungan yang beragam. Sistem kontrol akses yang baik harus mampu mengidentifikasi pengguna gedung secara tepat, mencatat aktivitas keluar-masuk secara otomatis, serta mengelola akses antar-area di dalam gedung dengan aman.

Science Techno Park (STP) Gedebage, yang juga dikenal sebagai ITB Innovation Park (IIP) Bandung Technopolis, merupakan fasilitas yang dibangun untuk mendukung inovasi serta komersialisasi berbagai produk teknologi milik Institut Teknologi Bandung (ITB). Saat ini, proses kontrol akses bagi tamu pada gedung ITB Innovation Park (IIP) masih dilakukan secara manual oleh petugas keamanan. Tamu yang datang akan diminta memberikan informasi mengenai tujuan kunjungan dan kemudian diarahkan untuk masuk ke gedung. Proses ini memiliki beberapa kelemahan. Pertama, pencatatan identitas dan aktivitas kunjungan masih bersifat manual dan tidak terdokumentasi secara otomatis. Kedua, keputusan pemberian akses bergantung pada penilaian petugas sehingga rawan subjektivitas. Ketiga, sistem akses tamu saat ini belum terintegrasi dengan sistem manajemen gedung secara menyeluruh. Kondisi ini belum memenuhi kriteria bangunan cerdas yang mengutamakan sistem kontrol akses yang otomatis dan terintegrasi.

Kebutuhan akan kontrol akses sebagai salah satu elemen utama bangunan cerdas telah tertuang dalam regulasi pemerintah. Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 10 Tahun 2023 menetapkan bahwa kontrol akses merupakan salah satu komponen wajib dalam konsep Bangunan Gedung Cerdas (BGC).

Selain itu, Surat Edaran Menteri Pekerjaan Umum Nomor 22/SE/M/2024 tentang Pedoman Penilaian Kinerja Bangunan Gedung Cerdas Tahap Pemanfaatan dan Periksaan Kinerja Bangunan Gedung Cerdas Tahap Pembongkaran menyebutkan bahwa keandalan sistem kontrol akses menjadi salah satu parameter kinerja yang wajib dipenuhi dalam evaluasi bangunan cerdas. Regulasi tersebut menekankan bahwa sistem kontrol akses harus mampu memberikan pencatatan dan pengelolaan data pergerakan orang di dalam gedung secara aman dan terintegrasi dengan sistem manajemen gedung lainnya.

Berbagai institusi dan organisasi telah menerapkan solusi teknologi kontrol akses menggunakan RFID, QR code, hingga pengenalan wajah (*face recognition*). Namun, metode berbasis kartu akses memiliki risiko kartu bisa hilang, tertukar, atau dipinjamkan, yang mengurangi keamanan akses. Sistem sidik jari, meskipun memakai biometrik, tetap memerlukan kontak fisik sehingga kurang higienis dan kurang nyaman, terutama pada area publik atau gedung dengan banyak kunjungan. Teknologi pengenalan wajah menawarkan keunggulan berupa otomatisasi, peningkatan keamanan, pengurangan interaksi fisik, dan kecepatan verifikasi pengguna. Namun dalam konteks tamu, penerapan pengenalan wajah memiliki pertimbangan tambahan seperti aspek privasi dan risiko penggunaan data biometrik. Hal ini selaras dengan prinsip perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi di Indonesia, yang mengatur bahwa pengumpulan dan pemrosesan data biometrik membutuhkan persetujuan dari pemilik data. Oleh karena itu, sistem kontrol akses pada bangunan cerdas perlu menyediakan alternatif metode autentikasi bagi tamu yang tidak bersedia atau tidak memungkinkan untuk memberikan data biometriknya.

Untuk menjawab kebutuhan tersebut, diperlukan sistem kontrol akses tamu yang fleksibel dan dapat mengakomodasi dua metode autentikasi, yaitu pengenalan wajah dan peminjaman kartu akses RFID melalui proses verifikasi identitas di resepsionis. Dengan pendekatan ini, proses kontrol akses tamu dapat dilakukan secara lebih aman, otomatis, terdokumentasi dengan baik, serta tetap menghormati pilihan dan privasi tamu. Pengembangan sistem ini diharapkan dapat meningkatkan keamanan dan efisiensi operasional gedung, sekaligus selaras dengan regulasi mengenai standar bangunan gedung cerdas.

I.2 Rumusan Masalah

Saat ini, proses kontrol akses bagi tamu yang memasuki Gedung ITB Innovation Park belum dilakukan secara otomatis dan belum terintegrasi dengan sistem manajemen gedung. Pencatatan identitas dan aktivitas kunjungan masih dilakukan secara manual oleh petugas keamanan atau resepsionis sehingga berpotensi menimbulkan ketidakteraturan pencatatan, risiko keamanan, dan ketidakefisienan dalam pengelolaan arus tamu. Proses pemberian akses masih bertumpu pada subjektivitas petugas dan belum memenuhi standar sistem kontrol akses pada bangunan cerdas.

Jika masalah tersebut tidak diatasi, maka risiko keamanan, ketidakteraturan alur kunjungan, serta ketidakpatuhan terhadap standar bangunan cerdas akan tetap terjadi. Selain itu, proses verifikasi tamu yang tidak otomatis dapat menyebabkan antrean, ketidakefisienan waktu, serta kurangnya dokumentasi aktivitas kunjungan sebagai bagian dari pengelolaan bangunan cerdas.

Oleh karena itu, diperlukan sistem kontrol akses yang mampu melakukan identifikasi dan pencatatan tamu secara otomatis serta tetap memperhatikan aspek keamanan dan perlindungan data pribadi. Masalah tersebut dapat dirumuskan sebagai berikut:

1. Bagaimana merancang sistem kontrol akses berbasis pengenalan wajah untuk manajemen tamu pada Gedung ITB Innovation Park?
2. Bagaimana mengembangkan mekanisme pendaftaran mandiri berbasis web dan sinkronisasi data wajah untuk mendukung alur masuk tamu?

I.3 Tujuan

Tujuan dari tugas akhir ini adalah mengembangkan sistem kontrol akses berbasis pengenalan wajah untuk mendukung pengelolaan tamu pada gedung IIP. Sistem ini diharapkan dapat meningkatkan keamanan dan efisiensi pengelolaan kunjungan tamu serta menyediakan opsi autentikasi yang sesuai dengan kebutuhan operasional gedung.

Secara khusus, tujuan tugas akhir ini adalah:

1. Mengembangkan sistem kontrol akses tamu yang mampu melakukan identifikasi dan pencatatan kunjungan secara otomatis pada bangunan cerdas.
2. Mengembangkan sistem pendaftaran mandiri yang memungkinkan tamu untuk mendaftarkan data identitas dan wajahnya sebelum melakukan kunjungan.

Tugas akhir ini dinyatakan berhasil apabila memenuhi kriteria berikut:

1. Sistem mampu melakukan proses autentikasi wajah tamu dan memberikan sinyal buka ke gerbang dengan waktu respons yang cepat untuk meminimalisir antrian.
2. Sistem pendaftaran mandiri dapat diakses dengan mudah oleh tamu dan mampu menyimpan data identitas serta wajah secara aman.
3. Sistem mampu secara konsisten membedakan antara tamu yang terdaftar dan yang tidak terdaftar.

I.4 Batasan Masalah

Untuk menjaga ruang lingkup pembahasan dan memastikan solusi yang dikembangkan tetap fokus serta dapat dicapai dalam rentang waktu penggeraan tugas akhir, maka diperlukan batasan-batasan masalah sebagai berikut:

1. Tugas akhir ini dikerjakan secara berkelompok yang terdiri dari 3 orang mahasiswa, yaitu Axelius Davin dengan NIM 18222016, Muhammad Rifa Ansyari dengan NIM 18222004, dan Natanael Steven dengan NIM 18222054. Penulis dalam hal ini berfokus pada pengembangan sistem kontrol akses untuk manajemen tamu.
2. Sistem yang dikembangkan hanya mencakup satu unit gerbang sesuai ketersementaraan sumber daya, namun dirancang dan dikembangkan sebagai representasi dari keseluruhan sistem.
3. Sistem akan dikembangkan menggunakan basis data independen yang tidak terintegrasi langsung dengan data yang dimiliki gedung.

I.5 Metodologi

Metodologi yang digunakan dalam tugas akhir ini mengacu pada pendekatan *design thinking*. *Design thinking* merupakan metode pengembangan sistem yang bersifat iteratif, berpusat pada pengguna (*human-centered*), serta menekankan proses kolaborasi dengan pihak yang terlibat. Pendekatan ini membantu menghasilkan solusi yang relevan dengan kebutuhan operasional gedung dan perilaku pengguna dalam proses kontrol akses tamu. *Design thinking* terdiri atas lima tahapan utama, yaitu *Empathize, Define, Ideate, Prototype, dan Test*.

1. *Empathize*

Tahap ini bertujuan memahami kebutuhan pengguna dan permasalahan yang terjadi pada proses kontrol akses tamu. Informasi dikumpulkan melalui observasi langsung ke gedung IIP, wawancara, dan interaksi langsung dengan pengguna sistem seperti pengelola harian gedung. Data yang diperoleh men-

jadi dasar untuk merumuskan kasus nyata di lapangan.

2. *Define*

Pada tahap ini, temuan dari proses *empathize* dianalisis untuk mengidentifikasi kendala utama dan karakteristik pengguna. Data yang diperoleh diolah untuk membangun *problem statement* yang spesifik dan terukur sebagai dasar dalam merancang sistem kontrol akses tamu yang akan dikembangkan.

3. *Ideate*

Tahap ini berfokus pada eksplorasi ide-ide solusi berdasarkan masalah yang telah didefinisikan. Pengembang dapat menggunakan teknik seperti *brain-storming*, *sketching*, atau simulasi alur sistem untuk menghasilkan berbagai alternatif solusi dalam pengelolaan akses tamu.

4. *Prototype*

Tahap ini bertujuan mewujudkan ide menjadi bentuk nyata menggunakan komponen perangkat keras maupun perangkat lunak. Prototipe dirancang untuk mengevaluasi solusi yang diusulkan dan melihat bagaimana sistem kontrol akses bekerja dalam skenario operasional. Tujuan utama bukan menghasilkan produk final, tetapi sebagai sarana evaluasi awal dan eksplorasi desain.

5. *Test*

Tahap ini dilakukan untuk mengevaluasi prototipe melalui uji coba, pengamatan, serta penerimaan umpan balik dari pengguna sistem. Hasil evaluasi kemudian digunakan untuk menyempurnakan solusi, merumuskan ulang kebutuhan, atau memperbaiki desain sistem agar lebih sesuai dengan kondisi operasional gedung.

Selain itu, metode penelusuran literatur juga digunakan dalam pengembangan sistem ini, yang mencakup:

1. Literatur ilmiah seperti buku dan artikel untuk mempelajari konsep dasar kontrol akses.
2. Regulasi pemerintah terkait Bangunan Gedung Cerdas, kontrol akses, serta perlindungan data pribadi.
3. Jurnal ilmiah dalam lima tahun terakhir untuk mengidentifikasi solusi dan celah penelitian yang relevan dengan sistem kontrol akses tamu.

Dokumentasi data yang digunakan meliputi foto, data kunjungan, serta catatan hasil observasi dan wawancara.

BAB II

STUDI LITERATUR

II.1 Tinjauan Regulasi Bangunan Gedung Cerdas

Penerapan sistem kontrol akses pada bangunan cerdas di Indonesia tidak dapat dilepaskan dari kerangka regulasi yang telah ditetapkan pemerintah. Regulasi tersebut berfungsi sebagai pedoman agar setiap sistem yang dibangun mampu mendukung keamanan, efisiensi, serta keberlanjutan operasional gedung. Salah satu regulasi utama yang menjadi dasar adalah Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 10 Tahun 2023. Dalam peraturan ini, bangunan gedung cerdas definisikan sebagai bangunan yang memanfaatkan sistem pengelolaan terpadu yang mampu merespons kebutuhan pengguna dan lingkungan secara otomatis (Kementerian Pekerjaan Umum dan Perumahan Rakyat 2023). Definisi tersebut menegaskan pentingnya integrasi teknologi dalam menunjang fungsi bangunan modern.

Ketentuan mengenai bagaimana kinerja sebuah bangunan cerdas dinilai dijelaskan lebih detail pada Surat Edaran Menteri PUPR Nomor 22/SE/M/2024. Dalam pedoman ini, sistem kontrol akses termasuk dalam unsur yang dievaluasi sebagai bagian dari parameter kemampuan sistem. Penilaian yang dilakukan tidak hanya berfokus pada fungsi dasar pembatasan akses, tetapi juga mencakup kemampuan sistem untuk memberikan pemantauan status perangkat secara langsung, pencegahan akses ganda ke area tertentu (fitur *antipassback*), pengaturan hak akses yang dapat disesuaikan menurut lokasi serta waktu, serta keandalan dalam menghadapi kondisi darurat. (Kementerian Pekerjaan Umum dan Perumahan Rakyat 2024).

Dengan adanya standar tersebut, setiap sistem kontrol akses pada bangunan cerdas perlu dirancang agar mampu memenuhi berbagai kebutuhan operasional gedung, termasuk akurasi identifikasi pengguna, integrasi dengan infrastruktur keselamatan, dan kemampuan melakukan pengelolaan akses yang terstruktur. Kepatuhan terhadap regulasi ini menjadi dasar penting dalam pengembangan sistem kontrol akses

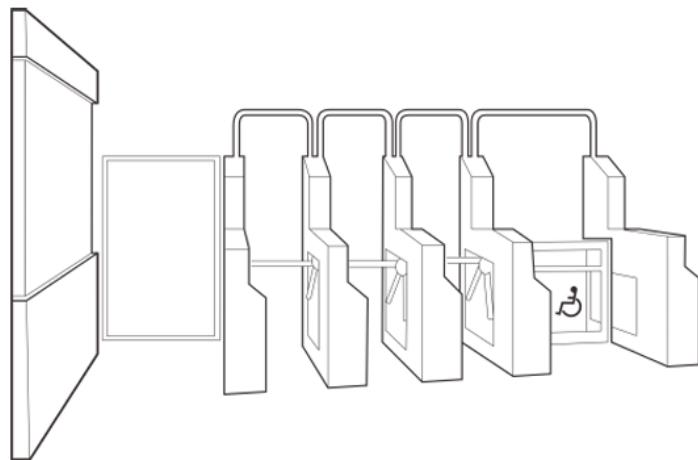
yang aman, adaptif, dan sesuai dengan praktik terbaik bangunan cerdas.

II.2 Kontrol Akses

Sistem kontrol akses merupakan rangkaian mekanisme teknis dan kebijakan yang dirancang untuk mengatur hak masuk ke suatu area, sehingga hanya individu yang berwenang dapat memasuki area tersebut. Sistem ini biasanya melibatkan kredensial (misalnya kartu, token, biometrik), perangkat pembaca, aktuator pintu/gerbang, serta perangkat lunak manajemen identitas dan otorisasi. Dengan demikian, kontrol akses tidak hanya berfungsi sebagai pintu fisik, tetapi juga sebagai sistem audit yang merekam aktivitas masuk-keluar, memelihara catatan akses, dan mendukung keamanan serta manajemen operasional bangunan. Dalam literatur terbaru, sistem ini digambarkan sebagai bagian dari manajemen identitas dan akses (Identity and Access Management - IAM) yang menjadi fondasi keamanan dalam lingkungan IoT dan bangunan cerdas. (Wang, Ragothaman, dan Rimal 2023)

II.3 Gerbang sebagai Kontrol Akses

Gerbang sebagai elemen kontrol akses fisik harus memenuhi standar keselamatan dan kenyamanan pengguna sesuai ketentuan bangunan gedung. Regulasi nasional menekankan bahwa pintu atau portal yang digunakan pada area dengan pergerakan manusia dalam jumlah besar harus dapat terbuka mengikuti arah evakuasi, agar alur keluar lebih aman dan tidak menimbulkan hambatan. Kementerian Pekerjaan Umum dan Perumahan Rakyat (2017) menetapkan bahwa *turnstile* atau pintu akses wajib memiliki lebar bukaan efektif minimal 60 cm, sedangkan akses untuk pengguna disabilitas harus memiliki lebar minimal 80 cm. Ketentuan tersebut menjadi acuan penting dalam menentukan spesifikasi dan dimensi gerbang yang akan digunakan dalam sistem kontrol akses berbasis otomasi. Gambar II.1 menunjukkan contoh implementasi desain pintu akses tersebut sebagaimana tercantum pada lampiran Peraturan Menteri PUPR 14/PRT/M/2017.



Gambar II.1 Contoh penerapan desain pada pintu akses (*turnstile*)

II.4 Pengenalan Wajah

Pengenalan wajah merupakan salah satu teknologi dalam bidang visi komputer yang berfungsi untuk mengidentifikasi atau memverifikasi identitas seseorang berdasarkan citra atau rekaman video. Pada dasarnya, teknologi ini memecahkan persoalan pengenalan pola visual, di mana sistem harus mampu mengenali wajah sebagai objek tiga dimensi yang ditangkap dalam bentuk gambar dua dimensi, meskipun terdapat variasi pencahayaan, sudut pandang, maupun ekspresi wajah. Li, Jain, dan Deng (2024) menjelaskan bahwa sebuah sistem pengenalan wajah umumnya terdiri dari empat komponen utama: *face detection*, *alignment*, *feature extraction*, dan *matching*. Proses lokalisasi dan normalisasi wajah melalui dua tahapan awal tersebut menjadi prasyarat sebelum fitur wajah dapat diekstraksi dan dibandingkan dalam proses pengenalan.

Penggunaan teknologi pengenalan wajah sebagai metode autentikasi biometrik semakin meluas di berbagai sektor, mulai dari pertahanan dan keamanan, layanan finansial, hingga aplikasi sehari-hari seperti kontrol akses pada perangkat dan bangunan. Tren adopsi biometrik ini juga tercermin dalam laporan HID Global yang dikutip oleh Jadhav (2024), yang menunjukkan peningkatan penggunaan biometrik untuk kontrol akses dari 30 persen menjadi 39 persen dalam dua tahun terakhir. Temuan ini mengindikasikan bahwa pengenalan wajah semakin diandalkan sebagai solusi autentikasi yang cepat, praktis, dan aman bagi berbagai kebutuhan operasional.

II.4.1 Parameter Evaluasi Kinerja Biometrik

Untuk menilai tingkat keandalan sistem pengenalan wajah, standar internasional ISO/IEC 19795-1 menetapkan sejumlah metrik utama yang digunakan dalam proses pengujian (International Organization for Standardization 2021).

1. *Accuracy*, yaitu perbandingan antara jumlah prediksi yang benar dengan total keseluruhan percobaan.
2. *False Acceptance Rate (FAR)*, yaitu tingkat kesalahan ketika sistem justru menerima atau mengenali individu yang tidak dikenal atau tidak terdaftar sebagai pengguna sah. Dalam sistem keamanan gedung, nilai FAR harus dijaga se rendah mungkin.
3. *False Rejection Rate (FRR)*, yaitu tingkat kesalahan ketika sistem menolak pengguna yang sebenarnya terdaftar dan memiliki izin akses. FRR yang tinggi dapat mengurangi kenyamanan pengguna.
4. Waktu Respons atau *Latency*, yaitu waktu yang dibutuhkan sistem mulai dari saat wajah terdeteksi oleh kamera hingga perintah kontrol dikirim ke aktuator.

II.5 Keamanan Data dan Privasi

Pengelolaan data biometrik, termasuk data wajah, membutuhkan standar perlindungan yang tinggi karena sifatnya yang sensitif dan tidak dapat diganti apabila bocor atau disalahgunakan. Dalam kerangka regulasi nasional, seluruh kegiatan yang melibatkan pengumpulan, penyimpanan, maupun pemrosesan data pribadi wajib mengikuti ketentuan yang tercantum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Salah satu prinsip penting yang diatur dalam Pasal 20 UU PDP adalah kewajiban memperoleh persetujuan eksplisit dari pemilik data sebelum data tersebut diproses. Ketentuan ini memastikan bahwa penggunaan data biometrik dilakukan secara transparan dan berdasarkan persetujuan sadar dari subjek data.

Selain UU PDP, aspek keamanan data biometrik juga berkaitan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU Informasi dan Transaksi Elektronik (UU ITE). UU ITE mengatur kewajiban penyelenggara sistem elektronik untuk menerapkan langkah-langkah keamanan siber yang memadai, termasuk perlindungan terhadap akses ilegal, manipulasi data, serta kebocoran informasi. Pasal 30 dan Pasal 32 UU ITE menegaskan bahwa akses tanpa izin, perusakan, atau penyalahgunaan informasi elektronik merupakan pelanggaran hukum yang dapat dikenakan sanksi pidana. Dengan demikian, sistem kontrol akses berbasis biometrik

wajib memastikan keamanan penyimpanan data, integritas sistem elektronik, serta pencegahan akses tidak sah sebagai bagian dari kepatuhan regulasi nasional.

II.6 Metodologi Design Thinking

Pendekatan pengembangan sistem pada penelitian ini menggunakan metodologi *Design Thinking*, yaitu kerangka kerja iteratif yang berfokus pada pemahaman mendalam terhadap pengguna sebagai dasar pengembangan solusi. Plattner (2010) menyatakan bahwa proses ini dimulai dari tahap *Empathize*, yaitu pengumpulan wawasan mengenai perilaku, kebutuhan, dan tantangan pengguna melalui observasi maupun interaksi langsung. Selanjutnya, tahap *Define* digunakan untuk menyusun dan merumuskan inti permasalahan berdasarkan temuan yang telah terkumpul. Pada tahap *Ideate*, berbagai kemungkinan solusi dieksplorasi dan dikembangkan melalui teknik kreatif seperti *brainstorming* atau pemetaan ide. Tahap berikutnya adalah *Prototype*, yaitu pembuatan representasi awal dari solusi agar dapat diuji dan divalidasi secara cepat. Terakhir, tahap *Test* dilakukan untuk mengumpulkan umpan balik pengguna, yang kemudian menjadi dasar untuk penyempurnaan solusi secara berulang (Plattner 2010).

BAB III

ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Tahap ini bertujuan untuk memahami kondisi aktual terkait alur kedatangan tamu di Gedung ITB Innovation Park serta kendala yang muncul dalam proses operasionalnya. Berdasarkan hasil observasi lapangan dan wawancara dengan petugas keamanan dan resepsionis, dapat disimpulkan bahwa sistem kontrol akses untuk tamu saat ini masih sepenuhnya manual dan belum terintegrasi dengan sistem manajemen gedung.

III.1.1 Alur Masuk Tamu Saat Ini

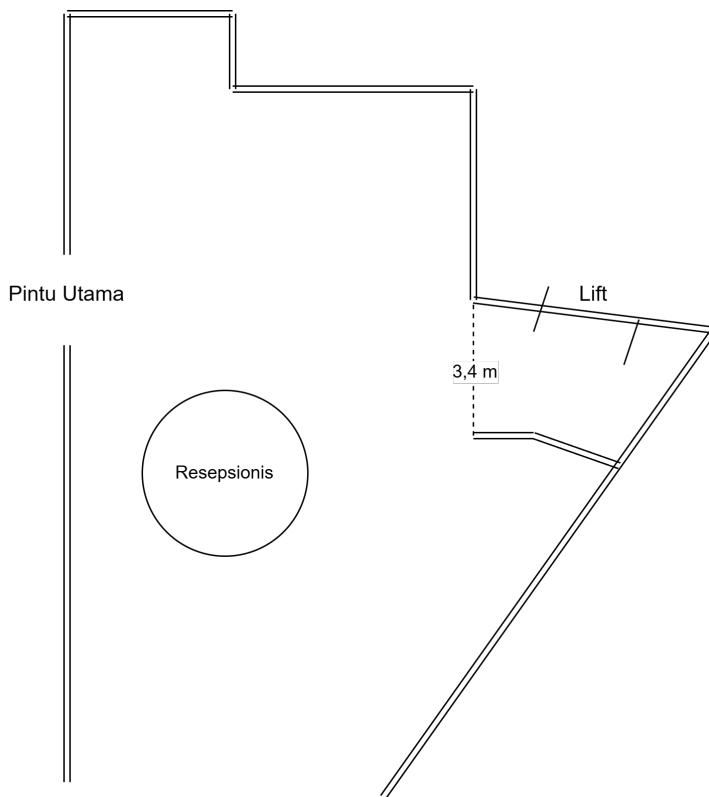
Proses penerimaan tamu saat ini mengandalkan interaksi langsung dengan petugas resepsionis atau petugas keamanan. Alur yang berlangsung di lapangan adalah sebagai berikut:

1. Tamu memasuki lobi dan langsung berinteraksi dengan petugas keamanan. Petugas menanyakan keperluan tamu, identitas, serta pihak yang ingin ditemui. Proses verifikasi dilakukan secara verbal tanpa pencocokan dokumen atau identitas digital apa pun
2. Tidak ada sistem registrasi atau pencatatan tamu yang terpusat. Petugas keamanan hanya melakukan konfirmasi secara manual kepada tenant atau staf terkait melalui pesan singkat atau panggilan telepon untuk memastikan bahwa tamu tersebut memang memiliki janji atau terdapat kebutuhan kunjungan.
3. Tamu diperbolehkan melanjutkan ke area lift tanpa mekanisme autentikasi tambahan. Seluruh tamu dapat mengakses area lift setelah mendapatkan persetujuan verbal dari petugas keamanan.
4. Tidak ada pencatatan waktu masuk dan keluar. Aktivitas tamu tidak terdokumentasi, sehingga tidak ada data historis yang dapat digunakan untuk kebutuhan audit keamanan, monitoring, atau analisis operasional.

Alur ini menunjukkan bahwa seluruh proses penerimaan tamu sangat bergantung pada komunikasi informal dan pengawasan manual oleh resepsionis. Ketergantungan pada proses manual ini menimbulkan sejumlah risiko, antara lain keterbatasan akurasi verifikasi identitas, potensi akses tanpa izin saat petugas lengah, serta tidak tersedianya data kunjungan untuk evaluasi keamanan gedung.

III.1.2 Kondisi Lobi Saat Ini

Hasil peninjauan area lobi menunjukkan bahwa gedung belum dilengkapi dengan perangkat pendukung sistem kontrol akses apa pun. Akses menuju lift terbuka secara langsung dari area lobi, hanya diawasi oleh petugas keamanan. Tidak adanya sistem kontrol akses mengakibatkan seluruh proses penyaringan tamu harus dilakukan secara manual dan tidak memiliki *backup* apabila petugas tidak berada di tempat. Gambar III.1 menunjukkan gambaran dari lobi Gedung ITB Innovation Park saat ini.



Gambar III.1 Kondisi lapangan dari lobi Gedung IIP

III.2 Analisis Kebutuhan

Tahap ini bertujuan untuk mengidentifikasi kebutuhan yang harus dipenuhi dalam pengembangan sistem kontrol akses di Gedung ITB Innovation Park. Analisis di-

lakukan dengan memperhatikan kondisi operasional saat ini, pola interaksi antara tamu dan petugas, serta kebutuhan pengelola gedung terhadap keamanan dan efisiensi. Hasil analisis kebutuhan ini menjadi dasar dalam menentukan fitur, komponen, dan alur sistem yang akan dikembangkan.

III.2.1 Identifikasi Masalah Pengguna

Berdasarkan hasil observasi di lobi Gedung ITB Innovation Park, proses pengaturan tamu yang berkunjung menunjukkan sejumlah permasalahan yang memengaruhi efisiensi dan keamanan operasional. Tamu yang datang belum memiliki alur registrasi yang jelas dan terstruktur, sehingga verifikasi identitas sangat bergantung pada percakapan langsung dengan resepsionis. Kondisi ini menyebabkan alur masuk yang tidak konsisten dan rentan menimbulkan antrean pada jam sibuk. Selain itu, ketiadaan sistem pencatatan kunjungan membuat aktivitas tamu tidak terdokumentasi, sehingga menyulitkan pengelola gedung dalam melakukan penelusuran dan audit keamanan. Pengguna gedung, baik resepsionis maupun pengelola, juga tidak memiliki alat bantu untuk mengontrol area mana saja yang boleh diakses tamu maupun jangka waktu kunjungannya. Permasalahan tersebut menunjukkan perlunya sistem yang dapat mengatur proses kunjungan tamu secara lebih tertib, aman, dan terdigitalisasi.

III.2.2 Kebutuhan Fungsional

Kebutuhan fungsional merupakan fitur atau fungsi utama yang harus dimiliki oleh sistem agar dapat memenuhi kebutuhan pengguna dan menyelesaikan permasalahan yang telah diidentifikasi pada subbab sebelumnya. Rincian kebutuhan nonfungsional disajikan pada tabel III.1.

Tabel III.1 Kebutuhan fungsional sistem

Nama Kebutuhan	Penjelasan
KF-1: Kontrol Akses	Sistem harus mampu mengendalikan mekanisme pembatasan fisik (<i>barrier</i>) untuk memblokir atau mengizinkan jalur akses berdasarkan hasil autentikasi.
KF-2: Deteksi Wajah	Sistem harus dapat mendeteksi apakah terdapat wajah manusia di depan input kamera yang dimiliki sistem.
KF-3: Pengenalan Wajah	Sistem harus mampu membandingkan fitur unik subjek yang hadir dengan basis data terdaftar untuk melakukan verifikasi identitas.
KF-4: Manajemen Pendaftaran	Sistem harus memiliki antarmuka yang terpusat untuk mengelola registrasi, hak akses, dan visualisasi catatan atau riwayat aktivitas pengguna.
KF-5: Integrasi Sistem	Sistem harus mampu menerima dan mengirimkan informasi (data log, status akses, sinyal peringatan) dengan sistem informasi eksternal yang terhubung.
KF-6: Keselamatan/ <i>safety</i>	Sistem wajib memiliki mekanisme keselamatan saat terjadi kondisi darurat.

III.2.3 Kebutuhan Nonfungsional

Kebutuhan nonfungsional menentukan batasan kualitas yang harus dipenuhi sistem, seperti target akurasi, kapasitas basis data, waktu respons, keamanan data, serta keandalan operasi. Rincian kebutuhan nonfungsional ditampilkan pada tabel III.2.

Tabel III.2 Kebutuhan Nonfungsional Sistem

Nama Kebutuhan	Penjelasan
KNF-01: Akurasi	Sistem dapat mengetahui dan memberikan akses kepada pengguna dengan akurasi 90%
KNF-02: Kapasitas	Sistem harus dapat menjalankan fungsi kontrol akses dengan baik untuk kapasitas 1200 pengguna.
KNF-03: Waktu Respon	Sistem harus dapat memberikan keputusan tentang kontrol akses dalam waktu tiga detik.
KNF-04: Keamanan	Sistem harus dapat memastikan keamanan data tersimpan sehingga hanya dapat diakses oleh pemilik data ataupun orang yang berwenang.
KNF-05: Keandalan	Sistem harus dapat beroperasi secara penuh selama 24 jam selama hari kerja (Senin s.d Jumat).

III.3 Analisis Pemilihan Solusi

Setelah kebutuhan sistem ditetapkan, tahap berikutnya adalah mengevaluasi berbagai pilihan solusi yang dapat memenuhi kebutuhan tersebut. Setiap alternatif akan dianalisis dan dibandingkan melalui pendekatan *trade-off* untuk menentukan opsi yang paling sesuai dengan tujuan pengembangan sistem.

III.3.1 Alternatif Solusi

Berikut merupakan rangkuman alternatif solusi yang dapat digunakan untuk memenuhi masing-masing kebutuhan fungsional dari sistem.

1. KF-1 Kontrol Akses
 - a. *Swing Barrier*, yaitu tipe gerbang yang membuka dan menutup ke arah dalam atau luar.
 - b. *Flap Barrier*, yaitu tipe gerbang yang membuka dan menutup dengan menggeser penghalang ke arah samping.
 - c. *Tripod Gate*, yaitu tipe gerbang dengan 3 batang besi yang dapat berputar searah saat kunci terbuka.
2. KF-2 Deteksi Wajah
 - a. RetinaFace, merupakan detektor wajah satu tahap dengan akurasi tinggi yang mampu mendeteksi wajah dalam berbagai kondisi pose dan pencahayaan. Model ini memanfaatkan landmark detection untuk meningkatkan stabilitas proses alignment pada tahap selanjutnya.

- b. YOLO-face adalah pendekatan deteksi wajah berbasis arsitektur YOLO yang berorientasi pada kecepatan dan kemampuan real-time. Metode ini memperlakukan wajah sebagai objek yang dideteksi melalui bounding box secara langsung, sehingga cocok untuk implementasi sistem kontrol akses yang memerlukan respons cepat. Model YOLO-based face detector telah banyak digunakan dalam sistem deteksi wajah pada perangkat edge dan aplikasi absensi otomatis.
 - c. Blazeface adalah detektor wajah yang dirancang untuk efisiensi tinggi pada perangkat mobile dengan sumber daya terbatas. Dengan ukuran model yang kecil dan latensi sangat rendah, BlazeFace dapat digunakan untuk prototipe sistem atau perangkat kontrol akses dengan komputasi ringan tanpa mengorbankan performa secara signifikan.
3. KF-03 Pengenalan Wajah

Alternatif Solusi untuk pengenalan wajah adalah kombinasi dari alternatif solusi untuk *Feature Extraction* dan *Matching Feature Extraction*:

- a. ResNet-50, yaitu arsitektur CNN dengan 50 layer yang menggunakan mekanisme residual learning, menjadi backbone umum untuk pengenalan wajah karena mampu mengekstraksi fitur wajah yang kuat dan stabil.
- b. MobileFaceNet, yaitu model CNN ringan yang cocok digunakan pada perangkat kecil, tetapi masih cukup baik dalam menangkap ciri penting dari wajah.

Loss Function:

- a. ArcFace, metode pelatihan yang membedakan wajah dengan ‘menjauhkan’ jarak antar wajah yang berbeda dan ‘mendekatkan’ wajah dari orang yang sama.
- b. MagFace, metode pelatihan yang tidak hanya membuat model mengenali wajah, tapi juga bisa menilai kualitas foto wajah, sehingga hasil pengenalannya lebih stabil.

4. KF-4 Manajemen Pendaftaran

- a. Aplikasi Web, menggunakan website yang dapat diakses melalui browser untuk pendaftaran.
- b. Aplikasi Desktop, menggunakan aplikasi berbasis desktop untuk perangkat PC resepsionis.
- c. Aplikasi Mobile, menggunakan aplikasi berbasis mobile untuk ponsel pengguna.

5. KF-5 Integrasi Sistem

- a. Integrasi berbasis API, memungkinkan sistem saling bertukar data secara

- ra langsung melalui HTTP *request* dan *response*.
- b. Integrasi berbasis *Message Queue*, mengirim dan memproses pesan secara asinkron melalui antrian.
 - c. Integrasi berbasis *Webhook*, mengirimkan notifikasi otomatis ke sistem lain setiap adanya peristiwa (*event*) tertentu.
6. KF-6 Keselamatan/*safety*
- a. Gerbang *fail-safe*, yaitu gerbang yang memiliki kondisi terbuka saat tidak mendapatkan aliran listrik.
 - b. Tombol Darurat, yaitu tombol yang dapat membuka gerbang tanpa autentikasi.
 - c. Gerbang *fail-safe* + Tombol Darurat, yaitu penggabungan solusi yang memungkinkan gerbang terbuka saat listrik padam atau tombol ditekan.

III.3.2 Analisis Penentuan Solusi

Untuk menentukan pemilihan solusi terbaik, dilakukan analisis kuantitatif untuk memilih solusi terbaik. Analisis kuantitatif dilakukan dengan metode *Weighted Scoring Model* (WSM) untuk membandingkan setiap alternatif solusi. Berikut merupakan analisis WSM dari setiap alternatif solusi setiap kebutuhan.

III.3.2.1 KF-1: Kontrol Akses

Berikut merupakan kriteria penilaian dari fungsionalitas kontrol akses.

Tabel III.3 Kriteria Evaluasi Kontrol Akses Fisik

Kriteria	Bobot (%)	Alasan
Keamanan Fisik	35%	Berdasarkan ISO/IEC 21964:2021, pengamanan fisik harus mencegah akses tidak sah dan meminimalkan risiko pelanggaran keamanan, sehingga menjadi aspek terpenting dalam evaluasi sistem kontrol akses.
Kecepatan Melalui Gerbang (Throughput)	25%	Tingkat throughput berpengaruh langsung pada kelancaran arus pengguna. Sistem kontrol akses perlu mempertahankan flow rate yang tinggi untuk menghindari penuh-pukan dan meningkatkan efisiensi operasional bangunan.
Kenyamanan dan Aksesibilitas	15%	Peraturan Menteri PUPR No. 14/PER-T/M/2017 menekankan pentingnya kemudahan penggunaan, termasuk aksesibilitas bagi penyandang disabilitas, sehingga gerbang harus aman namun tetap nyaman.
Efisiensi Energi dan Perawatan	15%	perangkat fisik yang hemat energi dan mudah dipelihara dapat mengurangi total biaya kepemilikan (total cost of ownership) pada sistem gedung.
Keandalan Operasional	10%	Perangkat kontrol akses harus dapat beroperasi stabil dalam kondisi normal maupun darurat, serta mendukung keamanan evakuasi.

Berdasarkan kriteria tersebut, berikut merupakan *Weighted Scoring Model* dari setiap alternatif solusi.

Tabel III.4 Analisis Penentuan Solusi Perangkat Gerbang Menggunakan Weighted Scoring Model

Kriteria Penilaian	Bobot	Swing Barrier	Flap Barrier	Tripod
Keamanan Fisik	35%	4 (1.40)	3 (1.05)	2 (0.70)
Kecepatan Melalui Gerbang (Throughput)	25%	4 (1.00)	5 (1.25)	3 (0.75)
Kenyamanan & Aksesibilitas	15%	5 (0.75)	3 (0.45)	2 (0.30)
Efisiensi Energi & Perawatan	15%	3 (0.45)	4 (0.60)	4 (0.60)
Keandalan Operasional	10%	4 (0.40)	3 (0.30)	3 (0.30)
Total Skor	100%	4.00	3.65	2.65

Analisis menunjukkan bahwa *swing barrier* merupakan solusi terbaik yang menawarkan keseimbangan antara keamanan, kecepatan, dan aksesibilitas yang baik dibandingkan dengan alternatif solusi lainnya.

III.3.2.2 KF-2: Deteksi Wajah

Berikut merupakan kriteria penilaian dari fungsionalitas deteksi wajah.

Tabel III.5 Kriteria Evaluasi Pendekripsi Wajah

Kriteria	Bobot(%)	Alasan
Akurasi Deteksi	40%	Pada sistem kontrol akses, akurasi deteksi wajah sangat penting karena kesalahan deteksi (<i>missed detection</i> atau <i>false detection</i>) dapat menghambat proses autentikasi.
Kecepatan (<i>Latency</i> / FPS)	25%	Sistem gerbang membutuhkan respons <i>real-time</i> agar tidak terjadi antrean.
Efisiensi Perangkat (Resource Usage)	15%	Model deteksi yang efisien dapat berjalan pada edge device tanpa memerlukan perangkat keras mahal.
Robustness Kondisi Lapangan	10%	Detektor harus tahan terhadap variasi pose, pencahayaan, dan occlusion.
Kompleksitas Implementasi	10%	Kompleksitas memengaruhi waktu integrasi dan risiko bug. Model dengan arsitektur sederhana lebih mudah di-deploy pada sistem pintu otomatis tanpa modifikasi pipeline besar.

Berdasarkan kriteria tersebut, berikut merupakan *Weighted Scoring Model* dari setiap alternatif solusi.

Tabel III.6 Analisis Penentuan Solusi Model Pendeteksi Wajah Menggunakan Weighted Scoring Model

Kriteria Penilaian	Bobot	RetinaFace	YOLO-Face	BlazeFace
Akurasi	40%	5 (2.00)	4 (1.60)	3 (1.20)
Kecepatan	25%	3 (0.75)	5 (1.25)	5 (1.25)
Efisiensi HW	15%	2 (0.30)	4 (0.60)	5 (0.75)
Robustness	10%	5 (0.50)	4 (0.40)	3 (0.30)
Kompleksitas	10%	3 (0.30)	4 (0.40)	5 (0.50)
Total Skor	100%	3.85	4.25	4.00

Analisis menunjukkan bahwa YOLO-Face terpilih karena menawarkan performa paling seimbang untuk implementasi di Raspberry Pi.

III.3.2.3 KF-3: Pengenalan Wajah

Berikut merupakan kriteria penilaian dari fungsionalitas pengenalan wajah.

Tabel III.7 Kriteria Evaluasi Untuk Solusi Pengenalan Wajah

Kriteria	Bobot (%)	Alasan
Akurasi	40%	ISO/IEC 19795-1:2021 menyatakan bahwa akurasi merupakan aspek utama untuk penilaian sistem biometrik, serta memastikan keamanan pada sistem akses kontrol.
Kecepatan	20%	Li, Jain, dan Deng (2024) dalam bukunya membahas bahwa kecepatan sistem melakukan pengenalan penting untuk menghindari antrean.
Efisiensi perangkat keras	15%	Efisiensi perangkat keras dapat menekan biaya yang diperlukan untuk pengembangan sistem.
Skalabilitas dan Pemeliharaan (<i>maintainability</i>)	15%	Pressman dan Maxim (2014) membahas tentang kualitas perangkat lunak dapat diukur dengan berbagai kriteria, diantaranya adalah skalabilitas dan pemeliharaan. Skalabilitas dan pemeliharaan yang baik dapat menekan biaya operasional sistem.
Kompleksitas implementasi	10%	Kompleksitas yang rendah mempercepat pengembangan sistem dan menghindari risiko bug.

Berdasarkan kriteria tersebut, berikut merupakan *Weighted Scoring Model* dari setiap alternatif solusi berikut :

1. Solusi 1: ResNet-50 + ArcFace
2. Solusi 2: ResNet-50 + MagFace
3. Solusi 3: MobileFaceNet + ArcFace
4. Solusi 4: MobileFaceNet + MagFace

Tabel III.8 Analisis Penentuan Solusi Model Pengenalan Wajah Menggunakan Weighted Scoring Model

Kriteria Penilaian	Bobot	Solusi 1	Solusi 2	Solusi 3	Solusi 4
Akurasi	40%	4 (1.60)	5 (2.00)	3 (1.20)	4 (1.60)
Kecepatan	20%	3 (0.60)	3 (0.60)	5 (1.00)	5 (1.00)
Efisiensi Perangkat Keras	15%	3 (0.45)	3 (0.45)	5 (0.75)	5 (0.75)
Skalabilitas dan Maintainability	15%	4 (0.60)	4 (0.60)	4 (0.60)	4 (0.60)
Kompleksitas Implementasi	10%	3 (0.30)	2 (0.20)	4 (0.40)	3 (0.30)
Total Skor	100%	3.55	3.85	3.95	4.25

Berdasarkan analisis, terlihat bahwa solusi terbaik adalah MobileFaceNet + MagFace, dimana kombinasi ini menawarkan solusi pengenalan wajah yang ringan secara komputasi namun tetap tangguh terhadap citra gambar yang bervariatif, sehingga sangat cocok digunakan pada perangkat terbatas seperti kontroler Raspberry Pi. MobileFaceNet memberikan keunggulan sebagai model yang sangat efisien dengan jumlah parameter yang rendah, memungkinkan inferensi cepat dan akurasi yang memadai. Sementara itu, MagFace merupakan *loss function* yang peka terhadap kualitas citra gambar, sehingga sistem dapat mengurangi kesalahan pada saat mendekripsi dalam pencahayaan rendah, pose yang bervariasi, atau gangguan (*noise*).

III.3.2.4 KF-4: Manajemen Pendaftaran

Berikut merupakan kriteria penilaian dari fungsionalitas pengenalan wajah.

Tabel III.9 Kriteria Evaluasi Proses Pendaftaran Mandiri

Kriteria	Bobot(%)	Alasan
Efisiensi Waktu	35%	Proses pendaftaran yang cepat mengurangi usaha dan waktu pengguna, sesuai dengan heuristic <i>Efficiency of Use / Flexibility and Efficiency</i> (Nielsen 1994).
Kemudahan Penggunaan	30%	Antarmuka yang intuitif dan rendah beban kognitif memungkinkan pengguna menyelesaikan pendaftaran tanpa kebingungan, sejalan dengan heuristics <i>Match between system and the real world</i> dan <i>Recognition rather than recall</i> (Nielsen 1994).
Kompatibilitas Perangkat	20%	Sistem harus konsisten dan berjalan pada berbagai perangkat agar akses lebih luas, sesuai dengan heuristik <i>Consistency and Standards</i> (Nielsen 1994).
Persepsi Privasi	15%	Pengguna merasa aman ketika data pribadi tidak disalahgunakan, sesuai dengan prinsip keamanan dalam <i>usability</i> (Nielsen 1994).

Berdasarkan kriteria tersebut, berikut merupakan *Weighted Scoring Model* dari setiap alternatif solusi.

Tabel III.10 Analisis Penentuan Solusi Pendaftaran Mandiri Menggunakan Weighted Scoring Model

Kriteria Penilaian	Bobot	Web	Mobile	Desktop
Efisiensi Waktu	35%	4 (1.40)	5 (1.75)	3 (1.05)
Kemudahan Penggunaan	30%	4 (1.20)	4 (1.20)	3 (0.90)
Kompatibilitas Perangkat	20%	5 (1.00)	3 (0.60)	4 (0.80)
Persepsi Privasi	15%	5 (0.75)	3 (0.45)	4 (0.60)
Total Skor	100%	4.35	4.00	3.35

Berdasarkan analisis, terlihat bahwa Aplikasi *web* menawarkan efisiensi waktu, kemudahan, kompatibilitas, dan privasi yang lebih baik dibandingkan dengan *mobile*

dan *dekstop*.

III.3.2.5 KF-5: Integrasi Sistem

Berikut merupakan kriteria penilaian dari fungsionalitas integrasi sistem.

Tabel III.11 Kriteria evaluasi Metode Integrasi Data

Kriteria	Bobot(%)	Alasan
Standarisasi	40%	Metode integrasi data yang memiliki tingkat standarisasi tinggi umumnya didukung oleh dokumentasi lengkap dan ekosistem pustaka pemrograman yang matang, sehingga memudahkan implementasi dan interoperabilitas antarsistem.
Kemudahan Debug	30%	Kemudahan dalam melakukan pelacakan dan penanganan kesalahan (<i>debugging</i>) penting untuk mempercepat proses pengembangan dan mengurangi risiko kegagalan integrasi saat sistem berjalan.
Real-time	30%	Kemampuan sinkronisasi data secara real-time memastikan informasi antar sistem selalu mutakhir, sehingga mendukung proses operasional yang memerlukan respons cepat dan konsistensi data.

Berdasarkan kriteria tersebut, berikut merupakan *Weighted Scoring Model* dari setiap alternatif solusi.

Tabel III.12 Analisis Penentuan Solusi Integrasi Sistem Menggunakan Weighted Scoring Model

Kriteria Penilaian	Bobot	REST API	Webhook	Manual
Standarisasi	40%	5 (2.0)	4 (1.6)	1 (0.4)
Kemudahan Debug	30%	5 (1.5)	3 (0.9)	2 (0.6)
Real-time	30%	3 (0.9)	5 (1.5)	1 (0.3)
Total Skor	100%	4.4	4.0	1.3

Analisis penilaian menunjukkan bahwa REST API merupakan solusi terbaik diban-

dingkan alternatif solusi lainnya, dimana REST API lebih unggul dalam standarisasi kemudahan dalam melakukan *debugging*.

III.3.2.6 KF-6: Keselamatan/safety

Berikut merupakan kriteria penilaian dari fungsionalitas integrasi sistem.

Tabel III.13 Kriteria Evaluasi Mekanisme Keselamatan

Kriteria	Bobot(%)	Alasan
Keandalan	50%	Sistem keselamatan harus tetap berfungsi dalam kondisi kritis seperti kebakaran atau pemadaman listrik untuk menjamin proses evakuasi berjalan tanpa hambatan.
Kepatuhan	30%	Pemenuhan standar keselamatan bangunan dan evakuasi menjadi syarat utama agar mekanisme keselamatan sesuai regulasi yang berlaku.
Kecepatan Respon	20%	Respons cepat dalam membuka kunci setelah sinyal darurat diterima memastikan tidak ada keterlambatan pada proses evakuasi.

Berdasarkan kriteria tersebut, berikut merupakan *Weighted Scoring Model* dari setiap alternatif solusi.

Tabel III.14 Analisis Penentuan Mekanisme Keselamatan Menggunakan Weighted Scoring Model

Kriteria Penilaian	Bobot	Otomatis (Fail-Safe)	Manual	Kombinasi
Keandalan	50%	4	3	5
Kepatuhan	30%	5	2	5
Kecepatan Respon	20%	5	2	5
Total Skor	100%	4.5	2.5	5.0

Solusi kombinasi, yaitu gabungan dengan solusi otomatis(*fail-safe*) dan tombol darurat merupakan solusi terbaik pada sistem. Solusi ini memastikan aspek keselamatan yang mumpuni dengan keandalan, kepatuhan dan kecepatan respon yang tinggi.

BAB IV

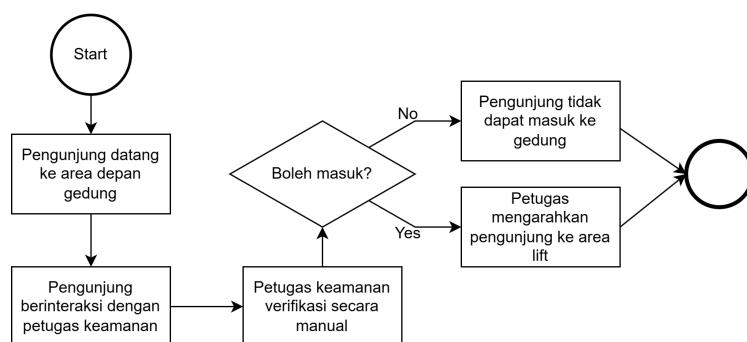
DESAIN KONSEP SOLUSI

Tujuan dari bab desain konsep solusi adalah menjelaskan model konseptual dan uraian desain yang telah dipilih pada bab sebelumnya terkait penerapan sistem pengenalan wajah untuk kontrol akses di lobi ITB Innovation Park.

IV.1 Diagram Konseptual

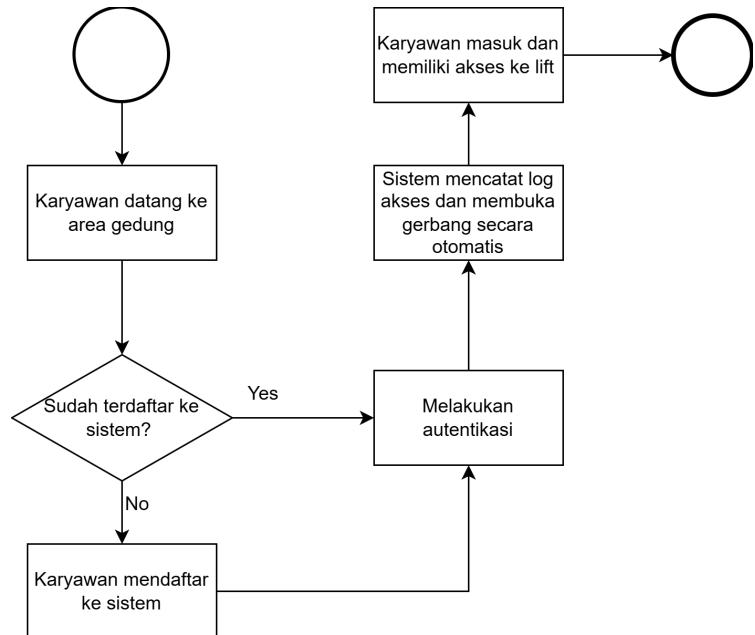
Pada tahap ini dijelaskan gambaran konseptual mengenai perubahan alur kontrol akses yang terjadi setelah sistem baru diimplementasikan. Model konseptual ini bertujuan menunjukkan bagaimana proses operasional di lobi Gedung ITB Innovation Park (IIP) akan berubah dibandingkan dengan mekanisme sebelumnya. Penyajian diagram dilakukan untuk memudahkan pembaca memahami perbedaan aliran proses before and after pemasangan gerbang otomatis berbasis pengenalan wajah serta metode autentifikasi alternatif.

Sebelum sistem dikembangkan, seluruh proses verifikasi identitas pengunjung, baik karyawan maupun tamu masih sepenuhnya dilakukan oleh petugas keamanan secara manual. Gambar IV.1 menampilkan alur kontrol akses lama, mulai dari kedatangan pengguna hingga diperbolehkan memasuki area lift.

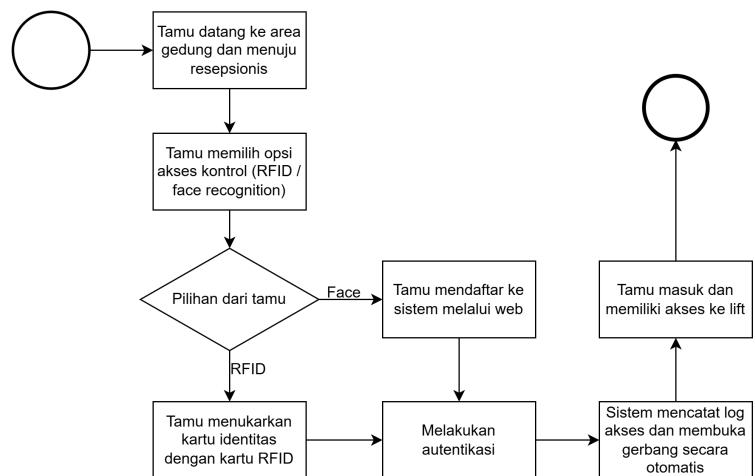


Gambar IV.1 Alur kontrol akses sebelum penerapan sistem gerbang

Setelah sistem dirancang dan dipilih pada bab sebelumnya, alur kontrol akses diperbarui menjadi lebih terstruktur dan otomatis. Untuk karyawan, proses autentikasi akan dilakukan menggunakan *face recognition* sebagai metode utama. Alur tersebut ditampilkan pada Gambar IV.2. Sementara itu, tamu memiliki dua pilihan autentikasi, yaitu menggunakan pengenalan wajah atau kartu RFID hasil verifikasi identitas di resepsionis. Ilustrasi alur ini ditampilkan pada Gambar IV.3.



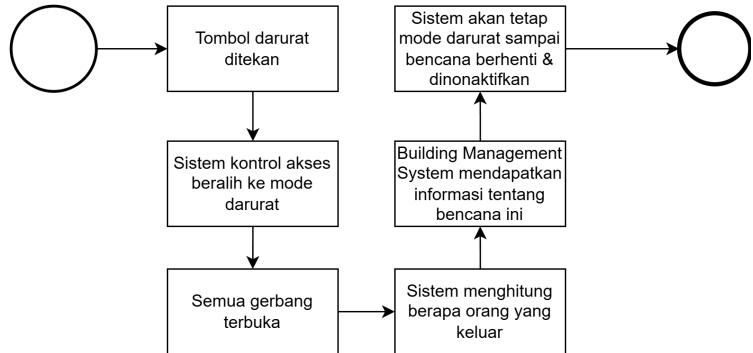
Gambar IV.2 Alur kontrol akses sesudah penerapan sistem gerbang untuk karyawan gedung



Gambar IV.3 Alur kontrol akses sesudah penerapan sistem gerbang untuk tamu gedung

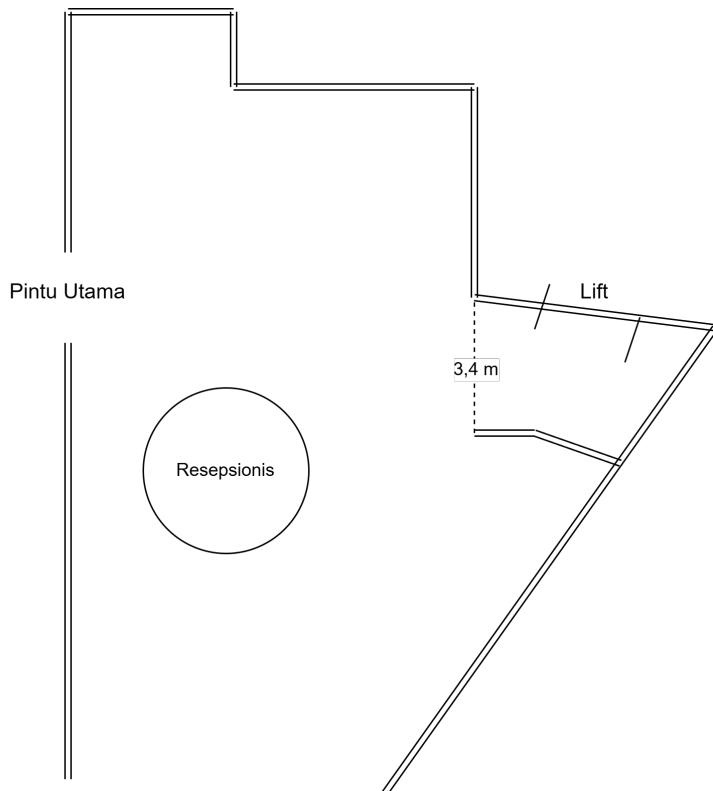
Selain kedua alur tersebut, sistem juga dirancang untuk berfungsi secara aman pada

kondisi darurat, misalnya saat terjadi kebakaran atau pemadaman listrik. Dalam skenario tersebut, gerbang akan masuk ke mode *fail-safe* dan terbuka otomatis. Alur untuk kontrol akses saat kondisi darurat, ditampilkan pada Gambar IV.4.

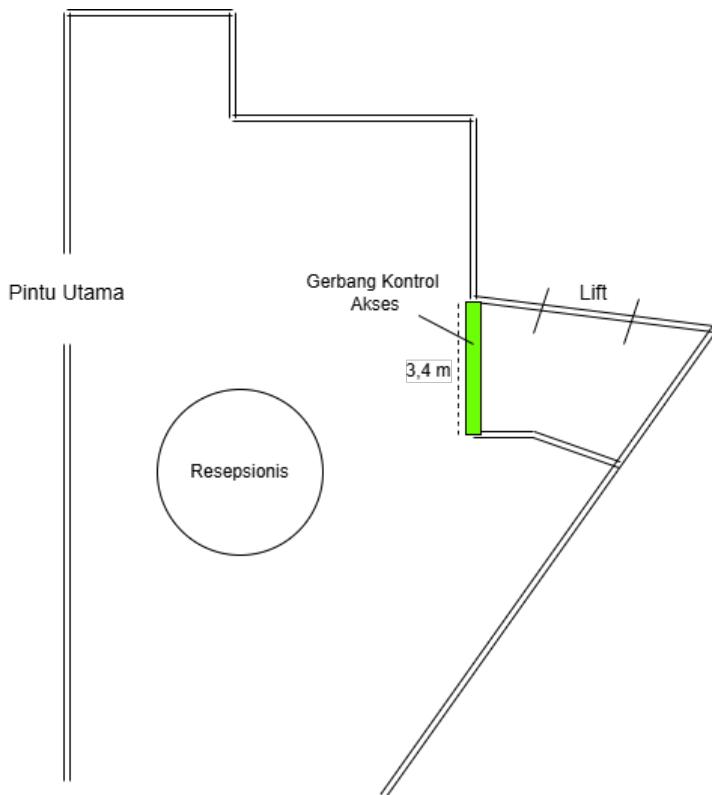


Gambar IV.4 Alur kontrol akses sesudah penerapan sistem gerbang saat kondisi darurat

Selain menggambarkan perubahan alur proses, model konseptual juga mencakup visualisasi tata letak lobi gedung sebelum dan sesudah pemasangan gerbang. Denah awal ditampilkan pada Gambar IV.5, sedangkan penempatan gerbang baru, yang terdiri dari tiga gerbang ditampilkan pada Gambar IV.6.



Gambar IV.5 Denah lobi sebelum pemasangan sistem gerbang



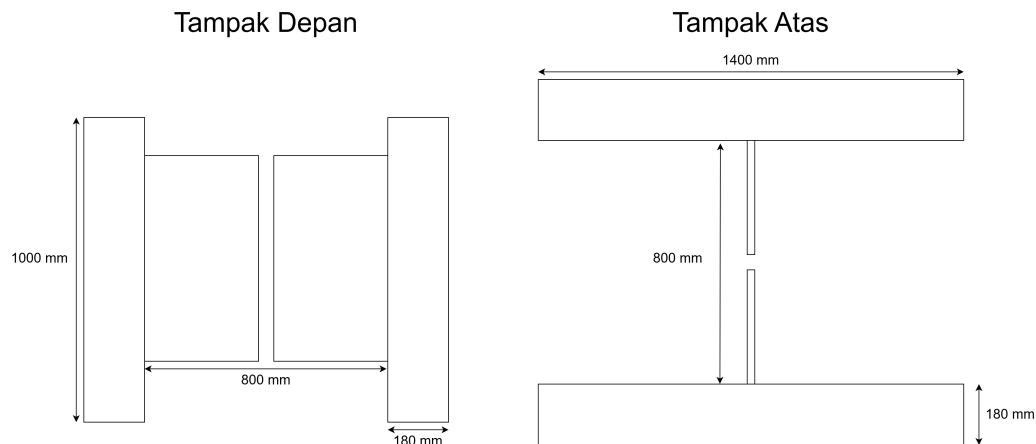
Gambar IV.6 Denah lobi setelah pemasangan sistem gerbang

IV.2 Penjelasan Desain

Bagian ini akan menjelaskan secara ringkas bagaimana rancangan sistem kontrol akses akan diimplementasikan. Penjelasan desain ini meliputi keterhubungan antar-komponen, penjelasan tentang komponen yang dipilih secara ringkas, logika proses autentikasi serta logika proses pendaftaran.

IV.2.1 Spesifikasi Perangkat Keras

Gerbang bertipe *swing barrier* dipilih untuk mendukung aksesibilitas yang luas, sesuai dengan standar keselamatan (Simarmata, Gunawan, dan Sari 2021). Dalam implementasinya, Sistem dirancang akan memiliki tiga gerbang normal pada satu sisi dan satu gerbang disabilitas untuk sisi lainnya, dengan gerbang disabilitas akan memiliki jalur minimal yang lebih lebar (80 cm) dibandingkan dengan gerbang normal (60 cm). Gambar IV.7 menunjukkan dimensi dari gerbang yang akan digunakan.



Gambar IV.7 Dimensi dari *swing barrier*.

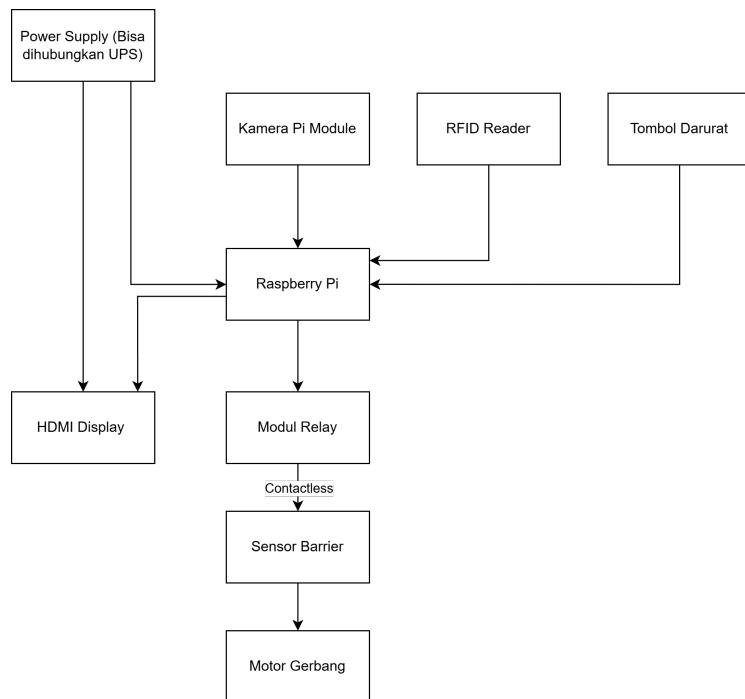
Gerbang yang akan digunakan kemudian akan terhubung langsung dengan sistem pengenalan wajah dan RFID. Berdasarkan analisis kebutuhan pada Bab III, spesifikasi perangkat keras yang dipilih meliputi:

1. **Unit Pemrosesan:** Raspberry Pi 4 Model B (4GB) dipilih karena kemampuan *edge computing* yang memadai untuk menjalankan algoritma *Deep Learning* (Raspberry Pi Foundation 2023).
2. **Visual:** Raspberry Pi Camera Module v3 dengan fitur HDR untuk mengatasi kondisi pencahayaan lobi.
3. **Antarmuka:** Layar LCD 5 inci HDMI untuk menampilkan status akses kepada pengguna.
4. **Autentikasi Sekunder:** Modul RFID *Reader* sebagai opsi akses cadangan.
5. **Kontrol Akses:** Modul Relay 5V untuk memicu pembukaan gerbang melalui mekanisme kontak kering (*dry contact*) (Kainz dkk. 2019).

Mekanisme fisik gerbang menggunakan *Swing Barrier* untuk mendukung aksesibilitas yang luas, sesuai dengan standar keselamatan (Simarmata, Gunawan, dan Sari 2021).

IV.2.2 Diagram Komponen

Rancangan sistem kontrol akses ini akan terdiri dari beberapa komponen yang saling terhubung. Gambar IV.8 Menunjukkan diagram komponen dari sistem.



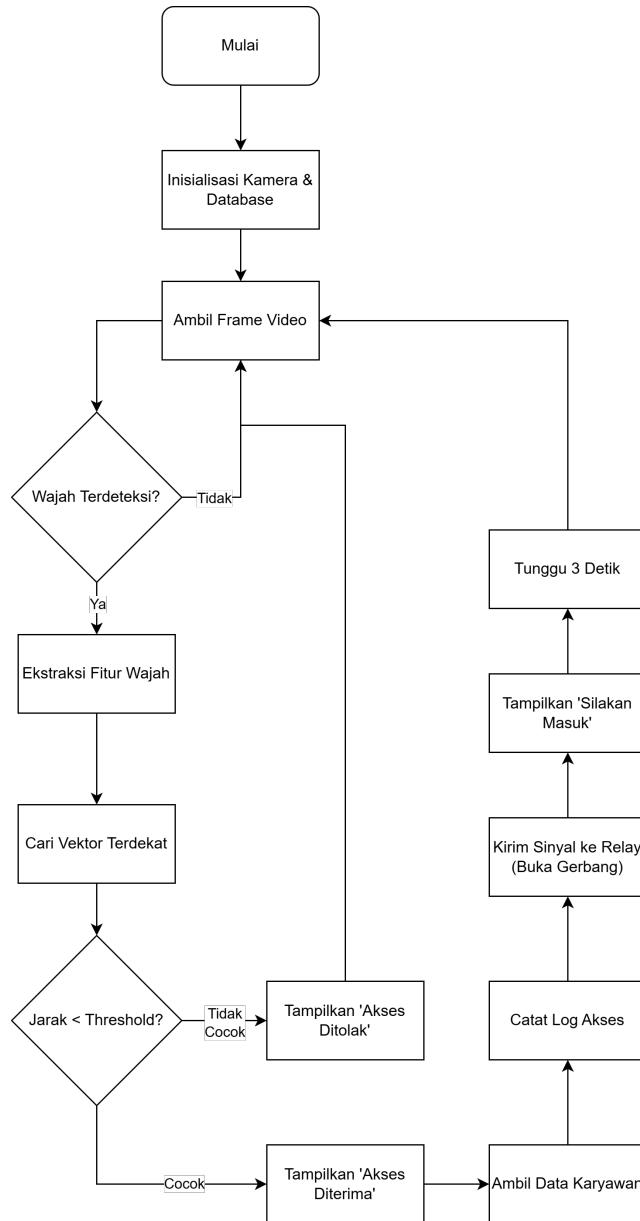
Gambar IV.8 Diagram komponen dari rancangan sistem

Berdasarkan gambar, terlihat bahwa sistem kontrol akses dengan gerbang otomatis terdiri dari komponen yang ada pada pemilihan solusi yaitu gerbang, sistem pengenalan wajah (kamera, kontroler, *display*), sistem RFID (RFID Reader, Kontroler), Tombol darurat, serta komponen-komponen seperti sumber listrik untuk memastikan sistem bekerja sesuai dengan kebutuhan.

IV.2.3 Logika Autentikasi

Logika autentikasi menjelaskan proses pengenalan pengguna yang dilakukan oleh sistem pengenalan wajah. Gambar IV.9 adalah alur proses dari proses pengenalan wajah untuk autentikasi pengguna.

Setiap beberapa waktu, sistem akan mengambil *frame* video melalui kamera, jika mendeteksi adanya wajah pada frame, sistem kemudian akan melakukan proses ekstrasi dari fitur wajah menjadi sebuah vektor. hasil ini kemudian dibandingkan dengan data tersimpan untuk mencari vektor terdekat. Jika tidak ditemukan, sistem akan menunjukkan bahwa akses masuk ditolak.



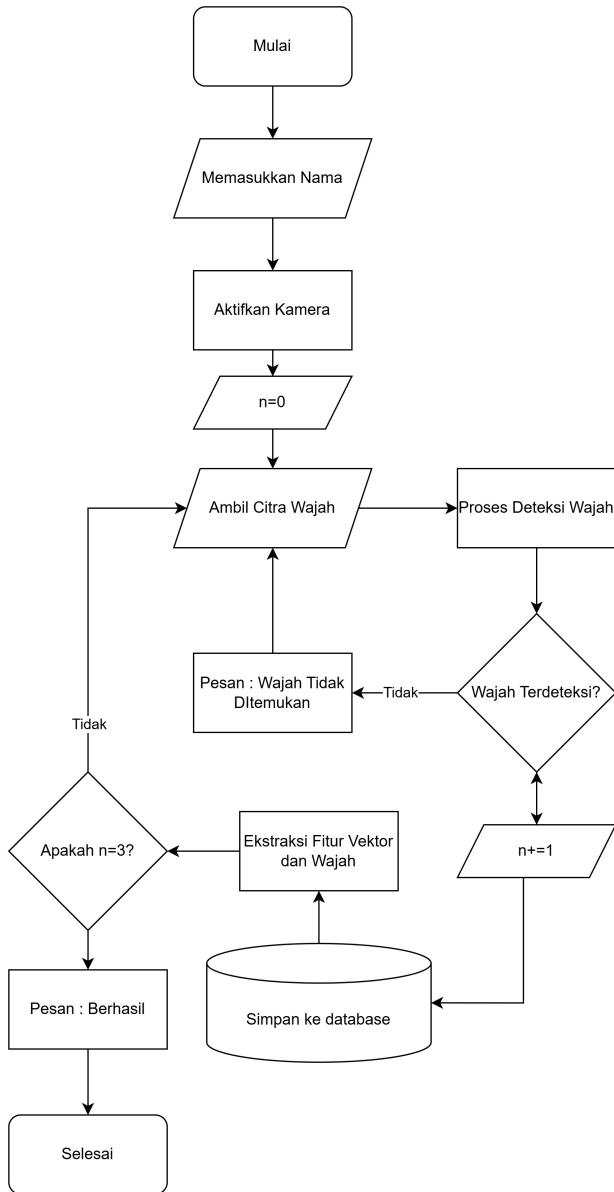
Gambar IV.9 Logika autentikasi dari rancangan sistem

Jika menemukan jarak vektor yang dibawah *threshold*, sistem akan menampilkan akses diterima. Setelah itu, sistem akan mengambil data pengguna yang dikenali tersebut, lalu mencatat log akses dan membuka gerbang. Sistem kemudian akan menunggu beberapa saat sebelum akhirnya kembali mengambil *frame* video untuk mendeteksi pengguna berikutnya.

IV.2.4 Alur Pendaftaran pada Sistem Kontrol Akses

Sistem pendaftaran digunakan oleh pengguna untuk mendaftarkan wajah mereka, sehingga pengguna dapat dikenali dan diberikan akses masuk. Berikut merupakan

alur pendaftaran dari sistem kontrol akses yang akan dikembangkan.



Gambar IV.10 Alur pendaftaran pada sistem kontrol akses

Pendaftaran dimulai dengan memasukkan data pengguna berupa nama, kemudian sistem akan meminta akses kamera pada perangkat. Setelah pengguna mengambil citra gambar, sistem kemudian akan melakukan proses deteksi wajah, dan jika terdeteksi, wajah akan disimpan ke database. Proses ini berlangsung sebanyak tiga kali untuk meningkatkan akurasi pengenalan wajah.

BAB V

RENCANA SELANJUTNYA

Bab ini menjelaskan langkah implementasi sistem yang akan dilakukan kedepannya. Rencana ini dijabarkan dalam bentuk linimasa pekerjaan, yang kemudian dilanjutkan dengan rencana implementasi, desain pengujian, serta analisis risiko.

V.1 Rencana Implementasi

V.1.1 Linimasa Pengerjaan

Pengerjaan tugas akhir direncanakan berlangsung selama 14 bulan, dimulai dari September 2025 untuk tahap studi awal dan proposal hingga Desember 2026. Implementasi sistem fisik akan dimulai pada Januari 2026. Linimasa pengerjaan disajikan dalam bentuk bagan Gantt 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						

Rencana linimasa pengerjaan untuk implementasi dan pengembangan sistem untuk tugas akhir ini adalah sebagai berikut:

1. Persiapan dan Perakitan Perangkat Keras

Tahap awal berfokus pada penyiapan fisik sistem agar siap dipasang pada gerbang.

- a. Perakitan Unit Pemrosesan: Menyiapkan unit mikrokontroler (Raspberry Pi) dan menghubungkannya dengan modul pendukung seperti kamera dan layar antarmuka.
- b. Instalasi Modul Kontrol: Merangkai modul relay elektronik yang berfungsi sebagai jembatan penghubung antara sinyal digital dari sistem dengan kunci fisik pada gerbang.
- c. Pemasangan Fisik: Menempatkan seluruh komponen elektronik ke dalam *casing* pelindung dan memasangnya pada tiang gerbang dengan posisi sudut pandang kamera yang optimal untuk menangkap wajah pengguna.

2. Pengembangan Logika Perangkat Lunak

Pada tahap ini, logika kecerdasan buatan dan kontrol sistem dibangun.

- a. Implementasi Algoritma: Menanamkan algoritma deteksi dan pengenalan wajah ke dalam unit pemrosesan agar mampu mengidentifikasi pengguna secara real-time.
- b. Pemrograman Logika Kontrol: Membuat program pengendali yang bertugas mengirimkan sinyal pembukaan gerbang hanya jika hasil verifikasi wajah dinyatakan valid (cocok dengan basis data).
- c. Mekanisme Sinkronisasi: Mengembangkan skrip otomatis untuk memastikan perangkat gerbang selalu memiliki data karyawan terbaru yang tersinkronisasi dari server pusat.

3. Pengembangan Sistem Pendaftaran (Web)

Tahap ini bertujuan menyediakan antarmuka bagi pengguna untuk mendaf-tarkan diri.

- a. Pembuatan Portal Web: Membangun aplikasi berbasis web yang mudah diakses oleh karyawan melalui perangkat pribadi (laptop/ponsel).
- b. Sistem Validasi Otomatis: Mengimplementasikan fitur cerdas pada web yang mampu menolak foto buram atau gelap secara otomatis saat pendaftaran, guna menjamin kualitas data dalam sistem.

4. Integrasi dan Kalibrasi Sistem

Tahap akhir adalah menyatukan perangkat lunak dan perangkat keras dalam satu lingkungan kerja.

- a. Pengujian Integrasi: Menghubungkan sistem wajah dengan mekanisme gerbang fisik untuk memastikan perintah "buka kunci" dari perangkat

- lunak benar-benar menggerakkan lengan gerbang.
- Kalibrasi Lapangan: Melakukan penyesuaian sensitivitas kamera dan ambang batas (*threshold*) algoritma berdasarkan kondisi pencahayaan di lokasi pemasangan untuk meminimalkan kesalahan deteksi.

V.1.2 Implementasi Prototipe

Lingkup implementasi pada tahap ini difokuskan pada satu gerbang akses dengan kemampuan dua arah, yaitu masuk dan keluar. Oleh karena itu, dibutuhkan total dua set perangkat pengenalan wajah. Tabel V.2 merincikan kebutuhan perangkat keras dan estimasi biaya untuk implementasi tersebut.

Tabel V.2 Rencana implementasi prototipe

Komponen atau Aspek	Deskripsi dan Spesifikasi
<i>Perangkat Keras (x2 Set)</i>	
Unit Pemrosesan	2 unit Raspberry Pi 4 Model B (4GB RAM). Dipilih karena keseimbangan antara performa untuk <i>edge computing</i> dan ketersediaan <i>port GPIO</i> .
Sensor Kamera	2 unit Raspberry Pi Camera Module v3. Digunakan untuk akuisisi citra wajah dengan fitur HDR.
Layar Display	2 unit LCD 5 inch HDMI. Untuk antarmuka visual pengguna.
Aktuator Kunci	Solenoid Door Lock 12V yang dikontrol melalui 5V Relay Module (Simulasi).
Pendukung	Power Supply 5V 3A, Fan Cooling, SSD Eksternal 128GB, dan kabel <i>jumper</i> .
<i>Perangkat Lunak</i>	
Sistem Operasi	Raspberry Pi OS berbasis Debian.
Bahasa	Python 3.
Pustaka Utama	OpenCV, Dlib, RPi.GPIO.
<i>Lingkungan</i>	
Lokasi	Prototipe akan diuji pada simulasi pintu masuk di Laboratorium X, Gedung IIP.
Konfigurasi	Perangkat akan dipasang pada ketinggian rata-rata wajah orang berdiri, yaitu sekitar 160 cm sampai 170 cm.
<i>Estimasi Biaya</i>	

Tabel V.2 Rencana implementasi prototipe (lanjutan)

Komponen atau Aspek	Deskripsi dan Spesifikasi
Perangkat Keras Utama	Rp 5.000.000 (untuk 2 unit sistem wajah)
Komponen Pendukung	Rp 500.000
<i>Total Estimasi</i>	Rp 5.500.000

V.2 Rencana Pengujian dan Evaluasi

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

Tabel V.3 Desain pengujian dan evaluasi sistem

Kriteria	Metode Verifikasi atau Validasi	Parameter Keberhasilan
<i>Verifikasi Fungsional</i>		
KF-1 (Kontrol Akses)	Melakukan simulasi autentikasi berhasil dan gagal pada karyawan dan tamu untuk memeriksa apakah gerbang merespons sesuai sinyal yang diberikan.	Gerbang selalu terbuka ketika autentikasi valid dan tetap tertutup ketika autentikasi tidak valid, dengan tingkat keberhasilan 100% selama pengujian.
KF-2 (Pendeteksi Wajah)	Menguji sistem dengan 5 pengguna dan 5 objek bukan wajah untuk memastikan deteksi keberadaan wajah sebelum proses pengenalan dilakukan.	Sistem mendeteksi seluruh wajah pengguna yang muncul di kamera, dan tidak memberikan deteksi ketika objek bukan wajah manusia.
KF-3 (Pengenalan Wajah)	Uji 5 pengguna yang belum terdaftar dan 5 orang yang sudah terdaftar untuk menggunakan sistem pengenalan wajah.	Sistem dapat dengan benar mengenali seluruh pengguna yang terdaftar dan dapat dengan benar tidak mengenali seluruh pengguna yang tidak terdaftar.

Tabel V.3 Desain pengujian dan evaluasi sistem (lanjutan)

Kriteria	Metode Verifikasi atau Validasi	Parameter Keberhasilan
KF-4 (Pendaftaran)	Uji pengguna menggunakan aplikasi untuk mendaftarkan wajah mereka.	Pengguna berhasil mendaftarkan wajahnya ke sistem tanpa arahan.
KF-5 (API)	Pengujian <i>endpoint API</i> menggunakan Postman.	API mengembalikan respon kode 200 OK dan format JSON yang valid.
KF-6 (Safety)	Simulasi pemutusan daya listrik dan penekanan tombol darurat.	Kunci gerbang terlepas (mode bebas dorong) secara instan.
Validasi Nonfungsional		
KNF-1 (Akurasi)	Pengujian dilakukan dengan 20 sampel pengguna (10 terdaftar dan 10 tidak terdaftar) untuk menghitung jumlah prediksi benar (true positive + true negative) dan prediksi salah (false positive + false negative).	Tingkat akurasi $\geq 90\%$, dihitung dari total prediksi benar dibandingkan seluruh percobaan.
KNF-2 (Kapasitas Sistem)	Pengujian beban dilakukan dengan mensimulasikan proses pendaftaran dan penyimpanan data hingga mencapai 1200 pengguna, serta melakukan uji akses bergantian oleh beberapa pengguna.	Sistem mampu beroperasi normal pada jumlah 1200 pengguna tanpa error penyimpanan dan seluruh pengguna tetap dapat dilayani.
KNF-3 (Waktu Respon)	Pengujian dengan menghitung waktu dari pengguna menampilkan wajah sampai gerbang dibuka.	Waktu sampai gerbang terbuka kurang dari tiga detik.

Tabel V.3 Desain pengujian dan evaluasi sistem (lanjutan)

Kriteria	Metode Verifikasi atau Validasi	Parameter Keberhasilan
KNF-4 (Keamanan)	<ul style="list-style-type: none"> a. Pengujian enkripsi data wajah b. Pengujian akses kontrol database c. Pengujian integritas data d. Pengujian Audit dan Logging 	<ul style="list-style-type: none"> a. Semua file template dan foto harus terenkripsi. b. Pengguna tidak sah tidak bisa melihat, mengubah, atau menghapus data wajah. c. Sistem menolak autentikasi jika data wajah rusak atau dimanipulasi. d. Semua log akses tercatat dan tidak bisa diubah.
KNF-5 (Keandalan)	Uji operasional (<i>stress test</i>) selama sehari.	Tidak terjadi <i>crash</i> , <i>overheat</i> , atau kegagalan fungsi selama pengujian.

V.3 Analisis Risiko dan Mitigasi

Analisis risiko dilakukan untuk mengidentifikasi potensi masalah selama implementasi dan pengujian, beserta tindakan mitigasi yang disiapkan sebagaimana tercantum pada 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 90%.	Gagal memenuhi KNF-1. Pengguna terdaftar ditolak.	1. Melakukan <i>data augmentation</i> . 2. Menggunakan lampu tambahan (<i>fill light</i>).
2.	Risiko Teknis: Waktu respon lambat lebih dari 3 detik.	Gagal memenuhi KNF-3. Menyebabkan antrian.	1. Optimasi kode. 2. Menggunakan algoritma pencarian vektor cepat (Annoy).
3.	Risiko Keamanan: <i>Spoofing attack</i> menggunakan foto HP.	Akses ilegal.	1. Implementasi deteksi kedipan mata. 2. Pengawasan oleh sekuriti (mitigasi prosedural).
4.	Risiko Pengembangan: Jadwal aktual tidak sesuai dengan estimasi yang ditetapkan	Keterlambatan Waktu Penyelesaian	1. Prioritisasi Fitur 2. Penjadwalan Ulang yang lebih realistik.

DAFTAR PUSTAKA

- International Organization for Standardization. 2021. *ISO/IEC 19795-1:2021 Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*. Geneva, Switzerland. <https://www.iso.org/standard/73515.html>.
- Jadhav, Abhishek. 2024. *2 in 5 Businesses Now Use Biometrics for Physical Access Control: HID*. <https://www.biometricupdate.com/202407/2-in-5-businesses-now-use-biometrics-for-physical-access-control-hid>. Diakses pada 30 November 2025.
- Kainz, Ondrej, Jan Drozd, Miroslav Michalko, dan Frantisek Jakab. 2019. “Raspberry Pi-Based Access Control Using Face Recognition”. Dalam *Proceedings of the International Conference on Engineering and Information Technology*. https://www.researchgate.net/publication/338598684_RASPBERRY_PI-BASED_ACCESS_CONTROL_USING_FACE_RECOGNITION.
- Kementerian Pekerjaan Umum dan Perumahan Rakyat. 2017. *Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 14/PRT/M/2017 Tahun 2017 tentang Persyaratan Kemudahan Bangunan Gedung*. <https://peraturan.bpk.go.id/Details/104477/permendagri-no-14pmtm2017-tahun-2017>. Diakses pada 01 Desember 2025.
- . 2023. *Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 10 Tahun 2023 tentang Bangunan Gedung Cerdas*. Peraturan Menteri. Jakarta.
- . 2024. *Surat Edaran Menteri PUPR Nomor 22/SE/M/2024 tentang Pedoman Penilaian Kinerja Bangunan Gedung Cerdas*. Surat Edaran Menteri. Jakarta.
- Li, Stan Z., Anil K. Jain, dan Jiankang Deng, penyunting. 2024. *Handbook of Face Recognition*. 3rd edisi. Springer Cham. ISBN: 978-3-031-43567-6. <https://doi.org/10.1007/978-3-031-43567-6>.

- Nielsen, Jakob. 1994. *Usability Engineering*. San Francisco: Morgan Kaufmann.
- Plattner, Hasso. 2010. *An Introduction to Design Thinking Process Guide*. <https://web.stanford.edu/~mshanks/MichaelShanks/files/509554.pdf>. Diakses pada 3 Desember 2025.
- Pressman, Roger S., dan Bruce R. Maxim. 2014. *Software Engineering: A Practitioner's Approach*. 8th edisi. New York: McGraw-Hill.
- Raspberry Pi Foundation. 2023. “Raspberry Pi 4 Model B Specifications”. Diakses pada November 24, 2025. <https://www.raspberrypi.org/products/raspberry-pi-4-model-b/>.
- Simarmata, S. D., I. Gunawan, dan I. P. Sari. 2021. “Sistem Kendali Pintu Gerbang Otomatis Menggunakan Koneksi Wireless Module Wifi Berbasis Mikrokontroler Arduino Uno”. *Jurnal Pendidikan dan Teknologi Indonesia (JPTI)* 1 (7): 297–308. <https://jpti.journals.id/index.php/jpti/article/view/67>.
- Wang, Y., K. Ragothaman, dan B. Rimal. 2023. “Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions”. Diakses pada 1 Desember 2025, *Sensors* 23 (4): 1805. <https://doi.org/10.3390/s23041805>.

LAMPIRAN A

TRANSKRIP WAWANCARA I

Tabel 5 Transkrip Wawancara dengan Pengelola Gedung (10 November 2025)

No	Pertanyaan / Topik	Jawaban Narasumber
1	Bagaimana sistem kontrol akses saat ini?	Kontrol masih standar menggunakan CCTV. Rencananya dalam bulan ini akan dilakukan pendekatan untuk pemasangan <i>barrier</i> atau <i>access door</i> .
2	Bagaimana alur masuk pengunjung dan karyawan saat ini?	Saat ini masih manual. Pengunjung melapor di lobi sebelum menuju lantai tujuan. Rencananya akses kontrol akan dipasang di lobi, area B1, akses lift, dan setiap pintu ruangan.
3	Apa saja yang dicek oleh petugas keamanan?	Petugas mencatat tujuan lantai dan orang yang dituju secara manual. Ke depannya direncanakan menggunakan <i>face recognition</i> , sidik jari, dan RFID.
4	Apakah ada rencana spesifik untuk jenis gerbang?	Ya, direncanakan menggunakan <i>swing barrier</i> . Akses masuk-keluar akan menggunakan pengenalan wajah (prioritas untuk karyawan) dan kartu akses/RFID (untuk tamu).
5	Bagaimana spesifikasi kinerja gerbang yang diharapkan?	Akurasi pembacaan wajah diharapkan maksimal di angka 90%. Kecepatan input (<i>speed</i>) juga harus diatur agar tidak menghambat alur.
6	Berapa jumlah gerbang yang akan dipasang?	Dengan lebar area 3,4 meter, direncanakan dipasang 3 unit <i>barrier</i> (3 jalur masuk dan 3 jalur keluar) untuk menutup celah agar orang tidak bisa menyelinap.

Tabel 5 Transkrip Wawancara dengan Pengelola Gedung (lanjutan)

No	Pertanyaan / Topik	Jawaban Narasumber
7	Apakah sistem absensi akan diintegrasikan?	Absensi diserahkan ke masing-masing <i>tenant</i> /perusahaan di setiap lantai. Pengelola gedung hanya fokus pada akses masuk utama.
8	Berapa estimasi kapasitas pengguna gedung?	Kapasitas maksimal gedung diperkirakan mencapai 1.200 orang.
9	Bagaimana prosedur penerimaan tamu saat ini (SOP)?	Tamu melapor ke sekuriti di B1 atau resepsionis di lobi. Petugas akan menghubungi PIC di lantai tujuan untuk konfirmasi izin masuk.
10	Bagaimana rencana SOP se-telah sistem otomatis terpasang?	Tamu menukar KTP dengan kartu akses (RFID) di resepsionis untuk membuka gerbang dan akses lift. Karyawan wajib menggunakan wajah (<i>face recognition</i>). Sekuriti akan menggunakan sidik jari untuk akses mereka.
11	Bagaimana mekanisme keselamatan saat bencana (kebakaran/gempa)?	Gedung sudah memiliki <i>Master Control Fire Alarm</i> (MCFA). Jika terjadi bencana, sistem gerbang (<i>barrier</i>) harus tersetting untuk terbuka otomatis (<i>fail-safe</i>) agar tidak menghalangi evakuasi.

LAMPIRAN B

TRANSKRIP WAWANCARA II

Tabel 6 Transkrip Diskusi Teknis dan Bisnis (21 November 2025)

No	Pertanyaan / Topik	Jawaban Narasumber
1	Status pemilihan vendor?	Sudah ada 5 vendor yang disurvei untuk tender. Mahasiswa diminta membuat surat pengajuan pemasangan untuk ditembuskan ke pimpinan DKST.
2	Penjelasan kebutuhan teknis (<i>Requirement</i>).	Sistem wajib mendukung TCP/IP, POE (<i>Power Over Ethernet</i>), serta standar W26/W34 dan RS485 untuk kompatibilitas RFID (13,56 MHz). Sistem juga harus mampu sinkronisasi data pegawai dari HRIS ITB melalui API-/SDK.
3	Klarifikasi model bisnis dan kepemilikan.	Perlu dipastikan status alat setelah implementasi: apakah menjadi aset gedung, sistem sewa, atau bentuk kerja sama vendor. Disarankan mengajukan konsep jual-beli dengan harga di bawah vendor pasar.
4	Konfirmasi metode akses untuk pengguna.	Tamu menggunakan RFID (tukar identitas). Karyawan menggunakan <i>Face Recognition</i> . Perlu dibuat SOP pendukungnya.
5	Umpaman balik terkait komponen gerbang.	Jenis gerbang bebas (<i>swing</i> atau <i>flap</i>), yang penting akurasi kamera tinggi (80-90%).
6	Klarifikasi lingkup pengerjaan mahasiswa.	Mahasiswa (Davin dkk.) akan mencari vendor untuk unit gerbang fisik, namun pengembangan sistem perangkat lunak dan integrasinya menjadi ruang lingkup Tugas Akhir.

Tabel 6 Transkrip Diskusi Teknis dan Bisnis (lanjutan)

No	Pertanyaan / Topik	Jawaban Narasumber
7	Bagaimana dengan akses VIP?	Disediakan satu jalur manual atau jalur khusus yang tidak memerlukan pendaftaran rumit.
8	Estimasi harga vendor pasar.	Kisaran harga vendor saat ini adalah Rp125-140 juta untuk 3 unit gerbang (<i>exclude PPN</i>).

LAMPIRAN C

DOKUMENTASI KEGIATAN

Lampiran ini memuat dokumentasi visual dari kegiatan pengambilan data dan wawancara yang telah dilakukan bersama narasumber terkait di Gedung ITB Innovation Park.



Gambar 1 Dokumentasi Proses Wawancara dengan Pengelola Gedung dan Pihak DKST

LAMPIRAN D

PERHITUNGAN ESTIMASI KEBUTUHAN PENYIMPANAN DATA

D.1 Opsi Media Penyimpanan

Berdasarkan analisis kebutuhan sistem, terdapat beberapa opsi media penyimpanan yang dievaluasi untuk menyimpan data citra wajah dan basis data pengguna:

1. Penyimpanan Fisik (*Local Storage*):

- SSD Eksternal
- HDD Eksternal
- Micro SD (Khusus untuk perangkat Edge/Raspberry Pi)

2. Penyimpanan Awan (*Cloud Storage*):

- Google Cloud Platform (GCP)
- Amazon Web Services (AWS) S3
- Supabase Storage

D.2 Estimasi Kapasitas Penyimpanan Citra (Server/Cloud)

Perhitungan ini digunakan untuk mengestimasi kebutuhan ruang penyimpanan bagi data mentah (*raw images*) yang digunakan untuk proses pendaftaran dan validasi visual.

Parameter:

- Total Kapasitas Pekerja: 1.200 orang
- Asumsi Pengunjung Mingguan: 200 orang
- Total Basis Pengguna (N): $1.200 + 200 = 1.400$ orang
- Jumlah Sampel Foto per Orang: 3 foto
- Ukuran Maksimum per Foto: 400 KB
- Retensi Foto Pengunjung: 7 hari (Siklus mingguan)

Kalkulasi Total:

$$\begin{aligned} \text{Total Storage} &= N \times \text{Jml Foto} \times \text{Ukuran} \\ &= 1.400 \text{ orang} \times 3 \text{ foto} \times 400 \text{ KB} \\ &= 1.680.000 \text{ KB} \\ &\approx \mathbf{1,68 \text{ GB}} \end{aligned}$$

D.3 Estimasi Penyimpanan Vektor Wajah (*Edge Device*)

Pada perangkat *edge* (Raspberry Pi), sistem tidak menyimpan foto asli melainkan hanya menyimpan representasi matematis (vektor) dari wajah untuk mempercepat proses pencocokan dan menghemat ruang.

Parameter:

- Ukuran Vektor Fitur (Embeddings): 512 Byte s.d. 2 KB (tergantung model)
- Total Pengguna: 1.400 orang

Kalkulasi:

$$\text{Min Storage} = 1.400 \times 3 \times 512 \text{ Byte} = 2.150.400 \text{ Byte} \approx \mathbf{2,15 \text{ MB}}$$

$$\text{Max Storage} = 1.400 \times 3 \times 2 \text{ KB} = 8.400 \text{ KB} \approx \mathbf{8,4 \text{ MB}}$$

LAMPIRAN E

PERHITUNGAN KAPASITAS DAN JUMLAH GERBANG

Perhitungan ini bertujuan untuk menentukan jumlah minimum unit *turnstile* (gerbang) yang diperlukan untuk mencegah penumpukan antrean pada jam sibuk (*peak hour*).

E.1 Parameter Studi

- **Total Populasi Gedung:** 1.200 orang.
- **Pola Kedatangan:** Berdasarkan studi, 60% karyawan tiba dalam jendela waktu 30 menit sebelum jam kerja.
- **Waktu Layanan (Service Time):** 3 detik per orang (waktu rata-rata deteksi wajah hingga gerbang terbuka).

E.2 Analisis Beban Puncak (*Peak Load*)

Volume kedatangan pada jam sibuk dihitung sebagai berikut:

$$\begin{aligned} Volume_{peak} &= 60\% \times 1.200 \text{ orang} \\ &= 720 \text{ orang} \end{aligned}$$

Asumsi kedatangan tersebar merata (*uniform distribution*) selama 30 menit, maka laju kedatangan (*Arrival Rate*) adalah:

$$\begin{aligned} Arrival Rate(\lambda) &= \frac{720 \text{ orang}}{30 \text{ menit}} \\ &= 24 \text{ orang/menit} \end{aligned}$$

E.3 Kapasitas Pelayanan (*Throughput*)

Kapasitas maksimal satu unit gerbang (*Service Rate*) dalam satu menit:

$$\begin{aligned} \text{Service Rate}(\mu) &= \frac{60 \text{ detik}}{3 \text{ detik/orang}} \\ &= \mathbf{20 \text{ orang/menit}} \end{aligned}$$

E.4 Penentuan Jumlah Unit

Rasio kebutuhan gerbang dihitung dengan membagi laju kedatangan dengan kapasitas pelayanan:

$$\begin{aligned} N_{gerbang} &= \frac{\text{Arrival Rate}(\lambda)}{\text{Service Rate}(\mu)} \\ &= \frac{24}{20} \\ &= \mathbf{1,2 \text{ Unit}} \end{aligned}$$

E.5 Kesimpulan

Secara teoritis, dibutuhkan **1,2 gerbang**. Karena jumlah gerbang harus bilangan bulat dan nilai > 1 mengindikasikan bahwa 1 gerbang tidak akan sanggup menampung antrean (akan terjadi *bottleneck*), maka kebutuhan minimum adalah **2 unit**.

Untuk memastikan keandalan sistem (*reliability*) dan mengantisipasi kerusakan alat, disarankan menggunakan konfigurasi **3 unit gerbang** (Redundansi N+1).