

**Pengembangan Sistem Deteksi Aktivitas
Mencurigakan Menggunakan Kamera Pengawas
Berbasis Machine Learning Pada Building
Management System**

Proposal Tugas Akhir

Oleh

**Chairul Nur Wahid
18222132**



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

LEMBAR PENGESAHAN

Pengembangan Sistem Deteksi Aktivitas Mencurigakan Menggunakan Kamera Pengawas Berbasis Machine Learning Pada Building Management System

Proposal Tugas Akhir

Oleh

Chairul Nur Wahid

18222132

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	2
I.3 Tujuan	3
I.4 Batasan Masalah	3
I.5 Metodologi	4
II STUDI LITERATUR	6
II.1 <i>Building Management System (BMS)</i>	6
II.2 Sistem Keamanan Berbasis CCTV	7
II.3 <i>Computer Vision</i>	7
II.3.1 <i>Object Detection</i>	7
II.3.2 <i>Object Tracking</i>	8
II.3.3 <i>Pose Estimation</i>	8
II.4 Aktivitas Mencurigakan	8
II.5 Metrik Evaluasi	9
II.5.1 <i>Confusion Matrix</i>	9
II.5.2 <i>Precision</i>	9
II.5.3 <i>Recall</i>	9
II.5.4 <i>F1-score</i>	10
II.5.5 <i>mean Average Precision (mAP)</i>	10
II.6 Penelitian Terkait	10
II.6.1 <i>Real-Time Building Management System Visual Anomaly Detection</i> .	10
II.6.2 <i>A Framework for the Video Surveillance Suspicious Activity Detection</i>	10
II.6.3 <i>Suspicious Activity Detection Using Convolution Neural Network</i> . .	11
III ANALISIS MASALAH	12
III.1 Analisis Kondisi Saat Ini	12
III.2 Analisis Kebutuhan	14
III.2.1 Identifikasi Masalah Pengguna	14

III.2.2 Kebutuhan Fungsional	15
III.2.3 Kebutuhan Nonfungsional	16
III.3 Analisis Pemilihan Solusi	18
III.3.1 Alternatif Solusi	18
III.3.2 Analisis Penentuan Solusi	19
IV DESAIN KONSEP SOLUSI	21
IV.1 Arsitektur Konsep Solusi	21
IV.2 Pembuatan dan Penggunaan Model	22
IV.2.1 Alur Pembuatan	22
IV.2.2 Penggunaan Model	23
IV.3 Perbandingan	24
V RENCANA SELANJUTNYA	26
V.1 Rencana Implementasi	26
V.1.1 Lini Masa	26
V.1.2 Alat dan Bahan	27
V.2 Desain Pengujian dan Evaluasi	27
V.3 Analisis Risiko dan Mitigasi	28

DAFTAR GAMBAR

III.1	Proses Bisnis Sistem Pengawasan Saat Ini (As-Is)	13
IV.1	Arsitektur Konsep Solusi	21
IV.2	Alur Pembuatan Sistem	23
IV.3	Proses Bisnis Sistem Pengawasan yang Diusulkan (To-Be)	24

DAFTAR TABEL

III.1 Kebutuhan Fungsional	15
III.1 Kebutuhan Fungsional	16
III.2 Kebutuhan Nonfungsional	17
III.3 Alternatif Solusi	18
III.4 Weighted Scoring Matrix	19
V.1 Lini Masa Rencana Implementasi	26
V.2 Alat dan Bahan	27
V.3 Metrik Evaluasi	27
V.3 Metrik Evaluasi	28

DAFTAR KODE

BAB I

PENDAHULUAN

I.1 Latar Belakang

Building Management System (BMS) merupakan sistem terpadu yang berfungsi memantau dan mengendalikan berbagai subsistem gedung, seperti kelistrikan, ventilasi, pencahayaan, hingga keamanan, dengan tujuan meningkatkan efisiensi operasional dan kualitas layanan gedung. Melalui BMS, data dari beragam perangkat dan sensor dikumpulkan dalam satu platform sehingga pengelola gedung dapat memantau kondisi secara real-time, mengambil keputusan berbasis data, dan melakukan tindakan korektif dengan lebih cepat.

Secara regulasi, Permen PUPR No. 10 Tahun 2023 tentang Bangunan Gedung Cerdas mendorong pengelola gedung untuk mengimplementasikan sistem manajemen yang terintegrasi, adaptif, dan memanfaatkan teknologi digital untuk mendukung operasi, termasuk aspek pemantauan dan keamanan. Regulasi tersebut menegaskan bahwa bangunan gedung cerdas diharapkan mengintegrasikan berbagai subsistem, menyediakan pemantauan terpusat, serta memungkinkan respons yang lebih cepat dan terukur terhadap kondisi lingkungan gedung.

Salah satu aspek penting pada sistem tersebut adalah aspek keamanan karena di dalam gedung terdapat jumlah orang yang tinggi serta menyimpan aset bernilai, sehingga kejadian seperti kehilangan barang, akses tidak sah, atau gangguan aktivitas dapat menimbulkan kerugian material maupun mengganggu operasional. Sistem keamanan sendiri tidak hanya terdiri dari CCTV, tetapi juga mencakup access control, prosedur patroli, alarm, dan sistem keselamatan lain. Namun, CCTV menjadi salah satu komponen yang paling kaya informasi karena merekam perilaku dan pergerakan di area gedung.

Komponen CCTV umumnya hanya merekam dan menampilkan video ke ruang ken-

dali dengan petugas keamanan harus mengamati beberapa tampilan dalam waktu lama untuk mendeteksi kejadian penting. Pendekatan ini memiliki keterbatasan karena kapasitas perhatian manusia terbatas, terlebih ketika jumlah kamera bertambah dan durasi pemantauan panjang, sehingga aktivitas yang berpotensi merugikan dapat terlewat atau terlambat disadari. Keterbatasan tersebut menimbulkan kebutuhan akan sistem yang dapat membantu mengidentifikasi aktivitas tertentu secara otomatis dan memberikan peringatan ke petugas sehingga proses pengawasan menjadi lebih konsisten.

Perkembangan teknologi computer vision dan machine learning membuka peluang untuk menjadikan kamera pengawas sebagai sensor cerdas yang mampu menganalisis video untuk mendeteksi pola perilaku yang berpotensi menimbulkan kerugian. Melalui integrasi modul ini ke dalam BMS mengubah informasi dari CCTV dari sekadar rekaman visual menjadi sesuatu yang dapat mendeteksi aktivitas mencurigakan secara otomatis.

Kebutuhan akan modul tersebut muncul di lingkungan ITB Innovation Park, yang saat ini aspek keamanannya masih lemah, masih sepenuhnya bergantung pada petugas keamanan serta CCTV biasa. Kondisi ini menjadi semakin krusial mengingat gedung tersebut berada di kawasan yang dikelilingi area ramai seperti masjid, mall, dan stadion sepak bola, sehingga mobilitas orang dari luar relatif tinggi. Oleh karena itu, diperlukan suatu Building Management System yang dapat mengintegrasikan hasil analisis aktivitas mencurigakan dan mendukung terhadap proses pengawasan keamanan secara efisien.

I.2 Rumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang muncul adalah belum adanya sistem yang dapat membantu proses pengawasan dengan melakukan analisis otomatis terhadap aktivitas yang terekam CCTV. Saat ini, pengawasan masih sepenuhnya mengandalkan petugas keamanan yang harus memantau dalam waktu lama, sementara jumlah kamera yang diawasi cukup banyak. Kondisi ini membuat beberapa aktivitas yang berpotensi mencurigakan dapat terlewatkan. Untuk mengatasi permasalahan tersebut, dirumuskan beberapa pertanyaan penelitian sebagai berikut:

1. Bagaimana merancang sistem deteksi aktivitas mencurigakan berbasis computer vision yang mampu menganalisis video secara otomatis?
2. Bagaimana mendefinisikan pola perilaku yang dapat dikategorikan sebagai aktivitas mencurigakan?

3. Bagaimana merancang dashboard yang dapat menampilkan hasil analisis dan memberikan peringatan yang membantu petugas keamanan dalam proses pemantauan?
4. Bagaimana mengevaluasi performa dan efektivitas sistem yang dikembangkan ketika diterapkan?

I.3 Tujuan

Tujuan dari penelitian ini adalah merancang dan mengembangkan sebuah sistem yang dapat membantu proses pengawasan keamanan gedung melalui analisis video otomatis. Secara khusus, penelitian ini bertujuan untuk:

1. Mengembangkan sistem deteksi aktivitas mencurigakan berbasis computer vision yang mampu melakukan analisis video secara otomatis sebagai pendukung pemantauan CCTV.
2. Menyusun definisi dan model pola perilaku yang dianggap mencurigakan
3. Merancang dashboard yang menampilkan hasil analitik dan memberikan peringatan sederhana yang dapat membantu petugas keamanan dalam memantau kondisi area secara lebih efisien
4. Melakukan evaluasi terhadap performa dan efektivitas sistem melalui pengujian pada kondisi nyata untuk melihat tingkat keandalan, keterbatasan, serta manfaat sistem dalam membantu proses pengawasan

I.4 Batasan Masalah

Adapun beberapa batasan masalah yang diambil untuk memfokuskan ruang lingkup penelitian dalam pengerjaan tugas akhir ini meliputi:

1. Penelitian hanya berfokus pada area koridor lantai 9 ITB Innovation Park
2. Sistem hanya memanfaatkan delapan kamera CCTV existing yang sudah terpasang pada lantai 9, tanpa melakukan pemasangan kamera tambahan
3. Deteksi aktivitas mencurigakan dibatasi pada pola perilaku yang telah ditentukan. Penelitian tidak mencakup identifikasi wajah, identifikasi individu, maupun analisis biometrik
4. Model yang dikembangkan hanya menganalisis perilaku berdasarkan informasi visual, tanpa menggabungkan data dari sensor lain
5. Sistem yang dibangun berfungsi sebagai alat bantu untuk mendukung tugas pengawasan, sehingga tidak menggantikan peran dari petugas keamanan

I.5 Metodologi

Tugas akhir ini menggunakan pendekatan Design Thinking sebagai metodologi pengembangan sistem. Pendekatan ini dipilih karena memungkinkan untuk menemukan solusi terbaik sesuai kebutuhan pengguna. Dalam pekerjaan ini, Design Thinking direncanakan dilakukan dalam minimal dua iterasi agar sistem yang dikembangkan dapat dievaluasi dan diperbaiki

1. Empathize

Tahap ini dilakukan untuk memahami kebutuhan dan kondisi lapangan melalui observasi pada area lantai 9 ITB Innovation Park dengan observasi langsung terhadap tata letak koridor, posisi kamera CCTV. Selain itu juga dilakukan wawancara dengan penghuni, petugas keamanan. Serta building management untuk mengetahui operasional gedung secara menyeluruh.

2. Define

Dari informasi didapat pada tahap sebelumnya, dilakukan penentuan masalah yang perlu diselesaikan. Selanjutnya dilakukan identifikasi kebutuhan fungsional dan non-fungsional berdasarkan temuan sebelumnya. Dari kebutuhan-kebutuhan tersebut dapat diidentifikasi spesifikasi sistem yang akan digunakan sebagai acuan dalam merancang dan mengevaluasi solusi.

3. Ideate

Tahap ini berfokus pada eksplorasi pengembangan berbagai ide solusi yang dapat menjawab masalah dan memenuhi kebutuhan yang telah ditetapkan sebelumnya. Setelah ide terkumpul, dilakukan pemilihan solusi terbaik menggunakan beberapa pertimbangan seperti kelayakan teknis, kesesuaian dengan requirement, ketersediaan infrastruktur, dan efektivitas. Hasil pada tahap ini adalah konsep solusi untuk diwujudkan.

4. Prototype

Pada tahap ini, konsep solusi diimplementasikan dalam bentuk prototipe awal. Prototipe dibuat dengan fokus pada fungsi inti agar dapat didemonstrasikan, namun tetap sederhana dan tidak mencakup seluruh fitur akhir. Komponen yang dikembangkan meliputi model deteksi aktivitas mencurigakan, alur pemrosesan video, serta tampilan dasar untuk memvisualisasikan hasil deteksi. Tujuan dari prototipe adalah menyediakan gambaran konkret mengenai cara kerja sistem.

5. Evaluate

Pada tahap ini dilakukan demonstrasi pada prototipe yang telah dikembangkan sebelumnya. Dari prototipe tersebut dilakukan evaluasi untuk menilai apakah sistem bekerja sesuai spesifikasi, apakah deteksi perilaku berjalan dengan

baik, dan apakah informasi yang dihasilkan bermanfaat bagi proses pemantauan. Jika ditemukan kekurangan, ketidaksesuaian, atau kebutuhan baru, proses kembali ke tahap Empathize untuk memulai iterasi berikutnya hingga sistem mencapai bentuk yang lebih sesuai dengan kebutuhan.

BAB II

STUDI LITERATUR

II.1 *Building Management System (BMS)*

Building Management System (BMS) merupakan sistem terpusat yang mengintegrasikan pemantauan dan pengendalian berbagai subsistem gedung seperti HVAC, pencahayaan, energi, dan keamanan dalam satu *platform* untuk meningkatkan kenyamanan penghuni sekaligus efisiensi energi dan biaya operasional (Hussain dkk. 2025).

Secara arsitektural, BMS umumnya dibangun dalam tiga lapisan, yaitu *low layer* yang terdiri atas perangkat seperti *sensor*, aktuator, dan kontroler. Kemudian ada *middle layer* yang berisi pengolah data dari perangkat *low layer* seperti *Supervisory Control and Data Acquisition (SCADA)* atau *Direct Digital Control (DDC)*. Terakhir adalah *top layer* yang berisi tampilan penyajian *dashboard*, analitik, dan pelaporan, yang diolah dari *middle layer* (Domingues dkk. 2016).

BMS sering diposisikan sebagai pondasi bangunan cerdas (*smart building*), karena integrasi teknologi informasi, *sensor*, dan otomasi yang memungkinkan gedung beroperasi secara efisien berdasarkan data *real-time*, sekaligus mengelola kinerja energi, kenyamanan, keamanan, dan keselamatan dalam satu kerangka manajemen terintegrasi (Eini dkk. 2022).

Di Indonesia, Bangunan Gedung Cerdas diatur dalam Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 10 Tahun 2023 yang menekankan bahwa bangunan cerdas harus memanfaatkan teknologi otomasi, sensor, dan sistem manajemen terintegrasi untuk mencapai efisiensi energi, keselamatan, kenyamanan, dan keberlanjutan. Regulasi tersebut menempatkan BMS sebagai komponen wajib dalam arsitektur bangunan cerdas karena fungsinya tersebut. Permen ini juga menegaskan bahwa BGC harus memiliki sistem manajemen keamanan dan kesela-

matan yang terhubung dengan platform pengelolaan gedung, sehingga memastikan kemampuan monitoring, respons, dan pengelolaan risiko yang lebih baik.

II.2 Sistem Keamanan Berbasis CCTV

Sistem kamera pengawas atau *closed-circuit television* (CCTV) merupakan bagian penting dari sistem keamanan dan keselamatan Bangunan Gedung. Sistem ini berfungsi merekam dan memantau aktivitas pada area-area tertentu melalui kamera yang dipasang secara strategis. Dengan pemantauan yang berlangsung terus-menerus, CCTV memungkinkan petugas keamanan untuk mengidentifikasi aktivitas mencurigakan dan mengambil tindakan secara cepat.

Menurut ketentuan paparan teknis Permen PUPR Nomor 10 Tahun 2023, sistem kamera pengawas terdiri atas tujuh komponen utama, yaitu kamera, stasiun pemantauan, perekam video, jaringan kabel atau *router*, perangkat penyimpanan rekaman, catu daya utama dan cadangan, serta sistem manajemen video. Kamera yang digunakan dapat berupa kamera IP atau kamera analog, dengan beragam bentuk seperti *bullet*, *dome*, dan *pan-tilt-zoom* (PTZ) yang dipilih sesuai kebutuhan pemantauan di area gedung.

Dalam konteks Bangunan Gedung Cerdas, CCTV bekerja secara terintegrasi dengan sistem keamanan lainnya seperti sistem kontrol akses dan sistem alarm. Integrasi ini menghasilkan mekanisme pengawasan yang lebih komprehensif dan responsif.

II.3 Computer Vision

Computer vision merupakan cabang dari kecerdasan buatan yang berfokus pada bagaimana mesin dapat memahami data visual sehingga mampu mengekstrak informasi untuk pengambilan keputusan (Szeliski 2022). Bidang ini memiliki banyak aplikasinya seperti *object detection*, *object tracking*, *pose estimation*, dan masih banyak lagi.

II.3.1 Object Detection

Object detection merupakan metode untuk mengenali sekaligus menemukan keberadaan suatu objek pada video dan gambar digital (Kumar 2024). Menurut Aslam (2020) terdapat dua tipe *object detector*, yaitu *two-stage detector* dan *one-stage detector*.

Pada *two-stage detector*, seperti *Faster R-CNN*, proses deteksi dilakukan dalam dua

tahap, yaitu menghasilkan kandidat *region proposal*, kemudian mengklasifikasikan dan menyempurnakan *bounding box* pada tiap *region* tersebut. Pendekatan ini biasanya memberikan akurasi tinggi, tetapi memiliki kecepatan inferensi yang lebih lambat karena prosesnya yang bertingkat.

Sedangkan *one-stage detector*, seperti *Single Shot MultiBox Detector* (SSD) dan YOLO memproses seluruh gambar secara langsung tanpa tahap terpisah, sehingga klasifikasi dan regresi *bounding box* dilakukan dalam satu langkah terpadu. Pendekatan ini memberikan hasil yang lebih cepat, meskipun akurasinya lebih rendah dibandingkan *two-stage detector* sehingga pendekatan ini lebih cocok untuk aplikasi *real-time*.

II.3.2 *Object Tracking*

Object tracking merupakan proses yang bertujuan untuk menentukan posisi suatu objek secara konsisten di setiap *frame* dalam sebuah video (Pappula 2023). Tujuan utamanya adalah membentuk lintasan (*trajectory*) pergerakan setiap objek sehingga sistem tidak hanya mengetahui di mana objek muncul pada satu *frame*, tetapi juga bagaimana objek tersebut bergerak sepanjang waktu.

II.3.3 *Pose Estimation*

Pose estimation merupakan proses yang bertujuan untuk menemukan lokasi bagian tubuh manusia dan membangun representasi kerangka tubuh (*skeleton*) dari data masukan seperti gambar atau video. Teknik ini mendeteksi titik-titik kunci (*keypoints*) seperti sendi bahu, siku, lutut, dan pergelangan tangan, kemudian menghubungkannya menjadi struktur rangka dua dimensi (2D) atau tiga dimensi (3D) (Zheng dkk. 2023).

II.4 *Aktivitas Mencurigakan*

Aktivitas mencurigakan merujuk pada perilaku yang menyimpang dari pola normal suatu lingkungan dan berpotensi menimbulkan dampak merugikan jika tidak segera ditangani, seperti berlari di area yang seharusnya tenang, berkelahi, berkeliaran terlalu lama, atau membawa objek berbahaya. Dalam literatur, topik ini umumnya dibahas sebagai *suspicious human activity recognition*, *abnormal event detection*, atau *video anomaly detection* dalam konteks sistem pemantauan (Zvereva 2022). Pendekatan deteksi aktivitas mencurigakan telah berkembang dari metode *rule-based* menjadi pendekatan berbasis *deep learning* seiring meningkatnya kemampuan kom-

putasi dan ketersediaan *dataset* video beranotasi.

II.5 Metrik Evaluasi

Evaluasi kinerja model deteksi objek dan aktivitas diperlukan untuk memastikan bahwa sistem mampu menghasilkan prediksi yang akurat dan konsisten dalam lingkungan operasional nyata. Pada sistem pengawasan berbasis CCTV, metrik evaluasi harus mampu mengukur kemampuan model dalam mengidentifikasi objek melalui *bounding box* dan kelas, serta kemampuan dalam mengenali aktivitas atau kejadian tertentu. Metrik evaluasi yang sering digunakan meliputi *confusion matrix*, *precision*, *recall*, *F1-score*, dan *mean Average Precision* (mAP) (Duong dkk. 2023).

II.5.1 *Confusion Matrix*

Confusion matrix adalah representasi performa model dalam bentuk tabel yang membandingkan hasil prediksi dengan label sebenarnya. Matriks ini terdiri atas empat komponen utama, yaitu *True Positive* (TP), *False Positive* (FP), *False Negative* (FN), dan *True Negative* (TN). Struktur ini memungkinkan analisis terhadap pola kesalahan model, seperti kecenderungan menghasilkan alarm palsu atau gagal mendeteksi kejadian penting.

II.5.2 *Precision*

Precision mengukur proporsi prediksi positif yang benar. Nilai *precision* yang tinggi menunjukkan bahwa model jarang memberikan deteksi positif yang keliru.

$$\text{Precision} = \frac{TP}{TP + FP}$$

II.5.3 *Recall*

Recall mengukur kemampuan model dalam mendeteksi seluruh kejadian positif yang benar.

$$\text{Recall} = \frac{TP}{TP + FN}$$

Dalam konteks sistem keamanan, nilai *recall* yang tinggi sangat penting untuk meminimalkan risiko aktivitas mencurigakan yang tidak terdeteksi.

II.5.4 *F1-score*

F1-score merupakan rata-rata harmonik dari *precision* dan *recall*, memberikan penilaian yang seimbang pada kedua aspek tersebut.

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Metrik ini ideal untuk kondisi dengan distribusi kelas yang tidak seimbang.

II.5.5 *mean Average Precision (mAP)*

Mean Average Precision (mAP) merupakan metrik evaluasi utama pada deteksi objek. Metrik ini menghitung rata-rata presisi pada berbagai nilai ambang *Intersection over Union (IoU)*. mAP menilai kemampuan model dalam memprediksi kelas objek sekaligus menghasilkan *bounding box* yang akurat. Penggunaan mAP relevan dalam penelitian ini karena performa deteksi objek menjadi komponen dasar dalam analisis perilaku dan aktivitas mencurigakan.

II.6 Penelitian Terkait

II.6.1 *Real-Time Building Management System Visual Anomaly Detection*

Penelitian ini mengusulkan metode deteksi anomali visual secara *real-time* pada sistem manajemen gedung dengan memanfaatkan kamera termal dan analisis titik panas (*heat points*) berbasis *machine learning*. Penelitian ini mereduksi data visual menjadi titik-titik kritis pergerakan dan distribusi panas sehingga beban komputasi lebih rendah dibanding pemrosesan citra secara penuh, namun tetap mampu mendeteksi anomali terkait keberadaan orang dan pola aktivitas di dalam gedung. Pendekatan ini terintegrasi dengan BMS untuk mendukung keamanan fisik dan manajemen energi, dan menunjukkan bahwa modul analitik visual dapat menjadi komponen bawaan BMS (Avci dan Bidollahkhani 2022).

II.6.2 *A Framework for the Video Surveillance Suspicious Activity Detection*

Rohitaksha dkk. mengembangkan kerangka kerja deteksi aktivitas mencurigakan pada *video surveillance* dengan mengelompokkan perilaku manusia menjadi dua kelas, yaitu aktivitas normal (misalnya duduk, berjalan, berlari, melambaikan tangan) dan aktivitas mencurigakan (misalnya penangkapan, *abuse*, *shoplifting*). Penelitian ini menggunakan *convolutional neural network (CNN)* untuk mengenali dan mengklasifikasikan aktivitas pada citra atau *frame* video, dan dilaporkan mencapai

akurasi sekitar 97,96% pada *dataset* CIFAR-100 sebagai bukti kemampuan model dalam membedakan pola visual berbagai tindakan. Hasil ini menunjukkan bahwa pendekatan klasifikasi berbasis CNN efektif untuk mendefinisikan ”mencurigakan” sebagai himpunan kelas perilaku eksplisit, yang dapat diadaptasi untuk konteks gedung tertentu seperti area kampus atau gedung inovasi (Rohitaksha, Narender, dan Faridi 2025).

II.6.3 *Suspicious Activity Detection Using Convolution Neural Network*

Penelitian ini merancang sistem *video surveillance* berbasis *deep learning* untuk mendeteksi aktivitas mencurigakan secara *real-time* menggunakan arsitektur *Long-term Recurrent Convolutional Network* (LRCN) yang menggabungkan CNN dan RNN. Sistem ini terdiri dari dua komponen utama, yaitu modul pengenalan aktivitas berbasis LRCN untuk menangkap informasi spasial dan temporal sekaligus, serta modul generasi peringatan *real-time* yang mengirim notifikasi ketika aktivitas seperti perkelahian, kecelakaan, atau perampokan terdeteksi pada *feed* kamera. Evaluasi pada *dataset* gabungan menunjukkan performa yang kompetitif dalam hal akurasi, presisi, dan *recall*, serta menegaskan bahwa arsitektur CNN-RNN cocok untuk diaplikasikan di lingkungan publik (bandara, stasiun, pusat perbelanjaan) (Quadri dan Katakdhond 2022).

BAB III

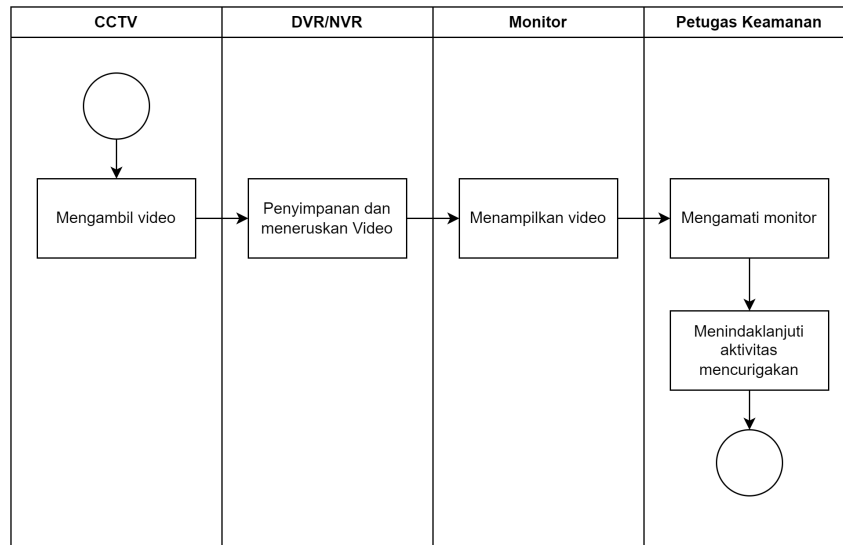
ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Kondisi keamanan di ITB Innovation Park saat ini masih hanya bergantung pada petugas keamanan yang berjaga selama 24 jam dengan sistem pergantian *shift*, tanpa adanya sistem *access control* untuk membatasi akses keluar masuk area. Infrastruktur pemantauan yang tersedia pada lantai 9 berupa delapan kamera CCTV konvensional yang terpasang di sepanjang koridor lantai 9 dan tidak mencakup area di dalam ruangan, sehingga cakupan pengawasannya terbatas.

Proses pemantauan rekaman CCTV dilakukan secara manual melalui layar monitor oleh petugas keamanan, di mana kamera hanya berfungsi sebagai perangkat perekam tanpa kemampuan analitik, deteksi otomatis, ataupun sistem peringatan dini. Dari sisi operasional, petugas yang memperhatikan delapan tampilan kamera secara simultan dalam durasi yang panjang, secara manusiawi berpotensi melewatkan kejadian penting akibat kelelahan dan penurunan fokus. Kondisi ini sistem keamanan yang seperti ini berpotensi tidak terdeteksinya kegiatan yang merugikan.

Berdasarkan wawancara dengan penghuni lantai 9, terdapat kekhawatiran terhadap keamanan barang-barang berharga seperti laptop dan perangkat elektronik lainnya, sehingga muncul kebutuhan agar sistem keamanan mampu memberikan deteksi dini terhadap potensi pencurian. Namun, sistem CCTV saat ini tidak memiliki fitur analitik yang dapat secara otomatis menandai pola perilaku mencurigakan.



Gambar III.1 Proses Bisnis Sistem Pengawasan Saat Ini (As-Is)

Diagram pada Gambar 3.1 menggambarkan alur kerja sistem pengawasan yang saat ini diterapkan di ITB Innovation Park. Sistem ini terdiri dari beberapa komponen utama, yaitu kamera CCTV, perangkat DVR/NVR, monitor, dan petugas keamanan.

Pertama, kamera CCTV yang terpasang di sepanjang lorong merekam aktivitas secara terus menerus dan mengirimkan video ke perangkat DVR/NVR. Perangkat tersebut berfungsi sebagai penyimpan rekaman sekaligus penghubung yang meneruskan tampilan video ke monitor di ruang keamanan.

Video yang ditampilkan pada monitor kemudian diamati oleh petugas keamanan. Proses ini dilakukan dengan cara memantau secara manual dan bergantung pada tingkat kewaspadaan serta konsentrasi petugas. Identifikasi suatu aktivitas yang dianggap tidak biasa sepenuhnya ditentukan oleh persepsi petugas terhadap tampilan video yang berlangsung. Tidak terdapat sistem peringatan otomatis yang dapat membantu menyoroti potensi kejadian tertentu.

Apabila petugas mencurigai adanya aktivitas yang tidak wajar, petugas akan menindaklanjuti secara manual, seperti mendatangi lokasi kejadian. Seluruh proses respons dilakukan tanpa dukungan sistem pendeteksi atau pencatat kejadian otomatis.

Berdasarkan diagram tersebut, dapat disimpulkan bahwa alur pengawasan bersifat linear dan sepenuhnya manual. Seluruh proses mulai dari pemantauan, identifikasi aktivitas, hingga tindakan lanjutan bergantung pada kemampuan dan perhatian

petugas. Kondisi ini menunjukkan belum adanya dukungan teknologi yang dapat membantu mengurangi beban pengawasan, meningkatkan konsistensi pemantauan, atau mempercepat deteksi aktivitas mencurigakan

III.2 Analisis Kebutuhan

Berdasarkan kondisi pengawasan yang telah dijelaskan sebelumnya, terdapat beberapa kesenjangan antara kebutuhan keamanan gedung dan kemampuan sistem yang tersedia saat ini. Kesenjangan utama terletak pada tidak adanya mekanisme analitik yang mampu membantu petugas dalam mengidentifikasi aktivitas yang berpotensi mencurigakan. Seluruh proses pemantauan dan pengenalan kejadian masih sepenuhnya bergantung pada pengamatan visual manusia, sehingga efektivitasnya dipengaruhi oleh faktor kelelahan, keterbatasan atensi, dan kemampuan individu. Situasi ini membuat potensi aktivitas tertentu tidak terdeteksi secara konsisten, terutama ketika beberapa tampilan kamera harus diamati secara simultan.

Selain ketiadaan kemampuan analisis otomatis, sistem saat ini juga tidak dilengkapi dengan fitur peringatan dini yang dapat menyoroti aktivitas tertentu sebelum berkembang menjadi insiden. Padahal, pola perilaku seperti keberadaan seseorang dalam durasi lama, pergerakan berulang pada satu area, atau aktivitas di luar jam operasional merupakan indikator umum dari perilaku mencurigakan yang seharusnya dapat dideteksi lebih awal. Tanpa mekanisme yang menandai pola tersebut, petugas hanya dapat bertindak setelah aktivitas teramati secara jelas, sehingga respons lebih bersifat reaktif.

III.2.1 Identifikasi Masalah Pengguna

Adapun pengguna sistem ini adalah petugas keamanan, pengelola gedung, dan penghuni lantai 9 ITB Innovation Park. Ketiga kelompok ini berinteraksi dengan lingkungan gedung dan memiliki kebutuhan yang berbeda terkait keamanan. Masalah yang dihadapi oleh masing-masing kelompok pengguna adalah sebagai berikut:

1. Petugas keamanan

Petugas harus memantau banyak kamera CCTV secara terus menerus dalam durasi panjang sehingga berisiko mengalami kehilangan fokus dan terlewatkan kejadian penting

2. Pengelola gedung

Pengelola gedung tidak memiliki dokumentasi aktivitas keamanan yang terpusat, sehingga evaluasi rutin terhadap potensi risiko atau kejadian tertentu

menjadi sulit dilakukan. Minimnya data terstruktur juga menghambat proses investigasi apabila terjadi laporan kehilangan atau insiden

3. Pengguna gedung

Penghuni merasa khawatir atas keamanan barang-barang berharga seperti laptop karena tidak adanya sistem keamanan lain selain mengandalkan petugas keamanan dan tidak adanya sistem yang dapat memberi deteksi dini terhadap aktivitas mencurigakan di lingkungan mereka untuk mencegah hal yang merugikan. Untuk mengatasi permasalahan tersebut, perlu dirumuskan kebutuhan fungsional dan nonfungsional yang dapat memenuhi kebutuhan ketiga kelompok pengguna. Subbab selanjutnya menjelaskan kebutuhan tersebut secara lebih rinci

III.2.2 Kebutuhan Fungsional

Kebutuhan fungsional menggambarkan fitur dan kemampuan yang harus dimiliki oleh sistem yang dirancang untuk menyelesaikan permasalahan yang telah diidentifikasi. Kebutuhan ini mencakup kemampuan sistem dalam menerima data, melakukan analisis perilaku, menampilkan hasil, serta mendukung proses pemantauan oleh petugas keamanan. Tabel berikut merangkum kebutuhan fungsional dari modul deteksi aktivitas mencurigakan yang akan dikembangkan

Tabel III.1 Kebutuhan Fungsional

Kode	Kebutuhan Fungsional	Deskripsi
FR-01	<i>Input</i> video	Sistem harus mampu menerima <i>input</i> berupa rekaman dari kamera CCTV yang telah terpasang pada ITB Innovation Park.
FR-02	Deteksi perilaku	Sistem harus mampu melakukan analisis terhadap video untuk mengenali pola aktivitas yang dikategorikan sebagai aktivitas mencurigakan.
FR-03	Visualisasi deteksi	Sistem harus mampu menampilkan hasil deteksi melalui <i>dashboard</i> dalam bentuk visualisasi sederhana yang mudah dipahami petugas.

Tabel III.1 Kebutuhan Fungsional

Kode	Kebutuhan Fungsional	Deskripsi
FR-04	Pencatatan Aktivitas	Sistem harus dapat mencatat dan menyimpan aktivitas yang terdeteksi dalam bentuk <i>log</i> agar dapat ditinjau kembali.
FR-05	Notifikasi peringatan	Sistem harus dapat memberikan notifikasi sederhana kepada petugas ketika terdeteksi aktivitas yang memerlukan perhatian.
FR-06	Akses <i>Dashboard</i> oleh Petugas	Sistem harus menyediakan <i>dashboard</i> yang dapat diakses oleh petugas keamanan untuk memantau hasil analitik secara <i>real-time</i> .

Dengan ini, diharapkan sistem yang dikembangkan mampu melakukan analisis terhadap rekaman CCTV dan mendeteksi pola perilaku yang dikategorikan sebagai aktivitas mencurigakan secara otomatis. Sistem juga diharapkan dapat menampilkan hasil deteksi melalui *dashboard* yang mudah dipahami, serta menyediakan pencatatan aktivitas dalam bentuk *log* untuk mendukung proses pelacakan dan evaluasi oleh petugas keamanan. Selain itu, kemampuan memberikan notifikasi sederhana diharapkan dapat membantu mengarahkan perhatian petugas terhadap kejadian tertentu sehingga proses pengawasan dapat berjalan lebih mudah

III.2.3 Kebutuhan Nonfungsional

Kebutuhan non-fungsional menjelaskan karakteristik kualitas yang harus dimiliki oleh sistem agar dapat berjalan secara optimal dan dapat digunakan secara efektif oleh petugas keamanan. Kebutuhan ini mencakup aspek kinerja, kemudahan penggunaan, keamanan data, serta keandalan deteksi yang dihasilkan. Tabel berikut merangkum kebutuhan non-fungsional tersebut.

Tabel III.2 Kebutuhan Nonfungsional

Kode	Kebutuhan Nonfungsional	Deskripsi
NFR-01	Ketersediaan sistem	Sistem harus memiliki <i>uptime</i> minimal 99,5% per bulan selama operasi 24 jam.
NFR-02	Waktu respon deteksi	<i>Latency</i> antara kejadian terekam kamera dan <i>alert</i> muncul di <i>dashboard</i> tidak boleh lebih dari 5 detik untuk 95% kasus.
NFR-03	Performa pemrosesan	Sistem harus mampu memproses <i>stream</i> dari 8 kamera secara paralel dengan penggunaan CPU di bawah 80%.
NFR-04	Akurasi deteksi	Sistem harus mencapai minimal 85% <i>detection rate</i> terhadap skenario aktivitas mencurigakan terdefinisi, dengan <i>false positive rate</i> tidak lebih dari 10% dari total <i>alert</i> harian.
NFR-05	Keamanan data video	Akses <i>dashboard</i> dibatasi dengan autentikasi dan <i>role-based access control</i> , dan hanya <i>metadata</i> penting (ID kamera, jenis <i>event</i> , <i>timestamp</i>) yang disimpan dalam <i>database</i> .
NFR-06	Kemudahan penggunaan	<i>Dashboard</i> harus memiliki tampilan yang sederhana, dengan tata letak elemen yang jelas dan mudah dipahami oleh petugas keamanan.

Dengan kebutuhan non-fungsional tersebut, sistem diharapkan dapat memberikan pemantauan yang stabil, cepat, dan aman, sekaligus menjaga akurasi serta efisien

III.3 Analisis Pemilihan Solusi

Sebelum menentukan pendekatan yang digunakan, diperlukan analisis terhadap beberapa alternatif metode analisis yang dapat digunakan untuk mengidentifikasi aktivitas pada video CCTV. Pemilihan metode ini penting karena setiap pendekatan memiliki kelebihan dan kekurangannya masing-masing. Oleh karena itu, subbab berikut membahas alternatif solusi serta dasar penentuan solusi terbaik.

III.3.1 Alternatif Solusi

Dalam merancang modul deteksi aktivitas mencurigakan, diperlukan pemilihan metode analisis video yang mampu mengenali perilaku tidak wajar. Berikut beberapa alternatif solusi yang dapat dipertimbangkan untuk mendeteksi aktivitas mencurigakan pada area yang dipantau CCTV

Tabel III.3 Alternatif Solusi

Metode	Kelebihan	Kelemahan
<i>Rule-based video analytics</i>	Bekerja dengan cepat karena ringan secara komputasi, mudah diterapkan	Tidak mampu memahami konteks perilaku, tidak cocok untuk aktivitas kompleks
Model ML <i>single object detection</i>	Mampu mengenali keberadaan orang, kendaraan, atau objek berbahaya	Tidak dapat memahami hubungan antar gerakan
<i>Machine Learning Multi-event Recognition</i>	Dapat mengenali berbagai jenis aktivitas mencurigakan berbasis pola gerakan, lebih <i>robust</i> untuk perilaku kompleks	Membutuhkan <i>dataset</i> lebih besar, komputasi lebih tinggi, model lebih kompleks
Pendekatan <i>Hybrid (Rule-based + ML)</i>	Mengurangi <i>false alarm</i> , dapat memahami konteks perilaku	Membutuhkan integrasi <i>pipeline</i> yang lebih rumit, membutuhkan <i>tuning parameter</i> lebih teliti

III.3.2 Analisis Penentuan Solusi

Dalam menentukan pendekatan terbaik, penelitian ini menggunakan metode *Weighted Scoring Matrix* (WSM). WSM merupakan teknik pengambilan keputusan yang membandingkan beberapa alternatif solusi berdasarkan sejumlah parameter yang diberi bobot sesuai tingkat kepentingannya. Metode ini dipilih karena sederhana dan cocok untuk mengambil keputusan yang mengharuskan mempertimbangkan banyak faktor.

Parameter yang digunakan pada WSM meliputi Akurasi, yang menilai sejauh mana setiap pendekatan mampu mengenali aktivitas mencurigakan dengan benar. Efisiensi digunakan untuk menilai seberapa optimal penggunaan komputasi pada masing-masing pendekatan. Kemudahan Implementasi dievaluasi berdasarkan tingkat kompleksitas integrasi solusi ke dalam lingkungan sistem yang sudah ada. Terakhir, Skalabilitas mencerminkan kemampuan pendekatan untuk diterapkan pada banyak kamera tanpa memerlukan perubahan besar pada konfigurasi atau *pipeline* proses. Hasil skor masing-masing pendekatan pada tiap parameter dapat dilihat pada tabel berikut.

Tabel III.4 Weighted Scoring Matrix

Parameter	<i>Rule-based</i>	ML De- teksi Objek	ML <i>Multi- event Recog- nition</i>	<i>Hybrid (Rule-based + ML)</i>
Akurasi (0.35)	2	2	4	4
Efisiensi (0.25)	5	4	3	3
Kemudahan Im- plementasi (0.25)	4	4	3	4
Skalabilitas (0.15)	3	4	4	3
Total	3.4	3.05	3.5	3.6

Setiap pendekatan diberi skor pada rentang 1 hingga 5, di mana nilai 1 menunjukkan kemampuan terendah dan nilai 5 menunjukkan kemampuan paling memenuhi kebutuhan parameter. Skor tersebut ditentukan secara kualitatif berdasarkan pemahaman teknis penulis terhadap karakteristik masing-masing pendekatan. Selanjutnya, skor dikalikan dengan bobot setiap parameter yang ditetapkan sesuai kebutuhan sistem di lapangan.

Berdasarkan hasil perhitungan pada tabel, pendekatan Hybrid (Rule-based + ML) memperoleh skor total tertinggi yaitu 3.60. Pendekatan ini dinilai paling seimbang karena mampu memberikan akurasi yang lebih baik dibanding rule-based, namun tetap mempertahankan efisiensi komputasi, kemudahan implementasi, dan skalabilitas yang tidak terlalu rumit.

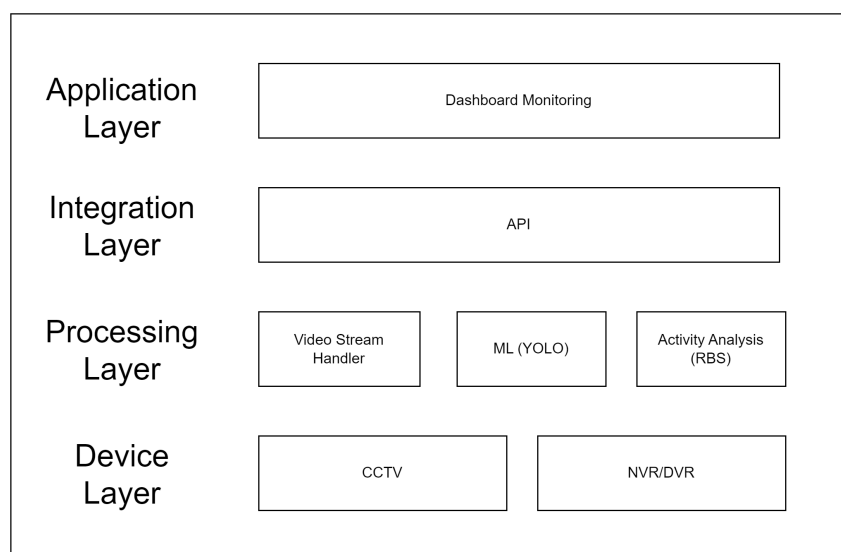
BAB IV

DESAIN KONSEP SOLUSI

Bab ini menjelaskan rancangan konsep solusi yang diusulkan berdasarkan pendekatan yang telah dipilih pada Bab sebelumnya. Desain ini menggambarkan bagaimana modul deteksi aktivitas mencurigakan diintegrasikan ke dalam alur kerja CCTV dan *Building Management System* (BMS) melalui kombinasi pemodelan *machine learning* dan *rule-based*.

IV.1 Arsitektur Konsep Solusi

Arsitektur konsep solusi dirancang untuk mengintegrasikan modul deteksi aktivitas mencurigakan berbasis *machine learning* ke dalam alur kerja CCTV yang telah tersedia pada ITB Innovation Park. Arsitektur ini terdiri dari empat lapisan utama, yaitu perangkat akuisisi video, pemrosesan video, integrasi sistem, dan antarmuka pengguna.



Gambar IV.1 Arsitektur Konsep Solusi

Pada lapisan perangkat, terdapat kamera CCTV untuk menangkap dan NVR/DVR berfungsi sebagai pengelola *stream* video yang kemudian diteruskan ke modul pemrosesan. Lapisan pemrosesan terdiri dari komponen *Video Stream Handler*, *Machine Learning* (menggunakan model YOLO), dan *Activity Analysis*. Pada komponen *Activity Analysis*, sistem mengekstraksi pola pergerakan dan interaksi objek untuk mengidentifikasi perilaku yang didefinisikan sebagai mencurigakan, seperti *loitering*, masuk ke area terbatas, atau membawa objek yang berpotensi berbahaya. Hasil pemrosesan kemudian diteruskan ke lapisan selanjutnya.

Lapisan selanjutnya adalah integrasi sistem, di mana hasil pendeteksian aktivitas mencurigakan dikirimkan ke *Building Management System* (BMS) melalui API. Terakhir, lapisan aplikasi menyediakan *dashboard* pemantauan *real-time* serta mekanisme notifikasi kepada operator keamanan.

IV.2 Pembuatan dan Penggunaan Model

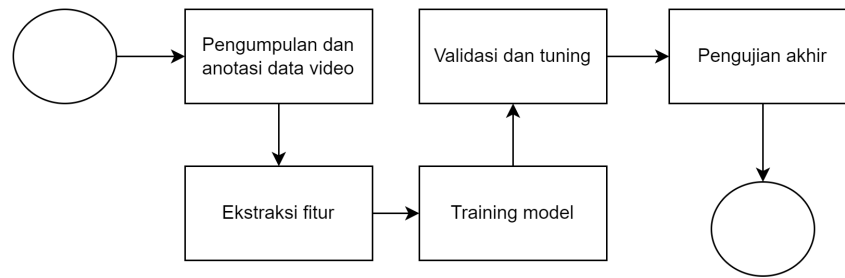
IV.2.1 Alur Pembuatan

Model dibangun dengan pendekatan *supervised learning* menggunakan arsitektur *object detection* sebagai fondasi utama. Sistem memanfaatkan model YOLO untuk mendeteksi objek manusia dan perilaku dasar pada setiap *frame* video. Hasil deteksi kemudian digunakan sebagai *input* bagi modul *activity analysis* yang bertugas menafsirkan pola gerak dan interaksi objek.

Untuk keperluan penelitian ini, aktivitas mencurigakan didefinisikan sebagai perilaku yang menyimpang dari pola aktivitas normal area, antara lain:

- a. *Loitering*
- b. Masuk area terbatas
- c. Gerakan agresif seperti berkelahi atau mendorong
- d. Membawa objek berbahaya
- e. Berlari di area yang seharusnya tenang

Berikut ini adalah alur pembuatan model deteksi aktivitas mencurigakan yang diusulkan:



Gambar IV.2 Alur Pembuatan Sistem

Setiap aktivitas tersebut direpresentasikan dalam bentuk fitur yang diekstraksi dari video, seperti posisi objek, durasi keberadaan, perubahan kecepatan, atau jarak antar individu. Model kemudian mempelajari pola ini melalui data pelatihan dan menghasilkan klasifikasi "normal" atau "mencurigakan".

Proses pembuatan model dimulai dengan mengumpulkan dan memberi anotasi pada data video yang memuat contoh aktivitas normal dan mencurigakan. Dari data tersebut, sistem mengekstraksi berbagai fitur seperti *bounding box* sebagai dasar pembelajaran model. Model kemudian dilatih menggunakan *dataset* berlabel agar mampu mengenali pola perilaku yang dianggap mencurigakan. Setelah itu dilakukan proses validasi dan *tuning*, termasuk pengaturan *threshold* deteksi dan evaluasi kinerja menggunakan metrik seperti *precision*, *recall*, dan *F1-score*. Tahap akhir berupa pengujian langsung pada rekaman CCTV ITB Innovation Park untuk memastikan bahwa model mampu berfungsi pada kondisi lingkungan nyata.

IV.2.2 Penggunaan Model

Setelah model mencapai performa yang memadai pada data uji, model diintegrasikan ke dalam *pipeline* pemrosesan video yang berjalan berdampingan dengan sistem CCTV yang sudah ada. Setiap alur video yang diterima dari NVR akan diproses melalui tiga tahapan:

1. **Object Detection**

Model mendeteksi manusia dan objek relevan pada setiap *frame* menggunakan YOLO. *Output* berupa *bounding box*, label objek, dan *confidence score*.

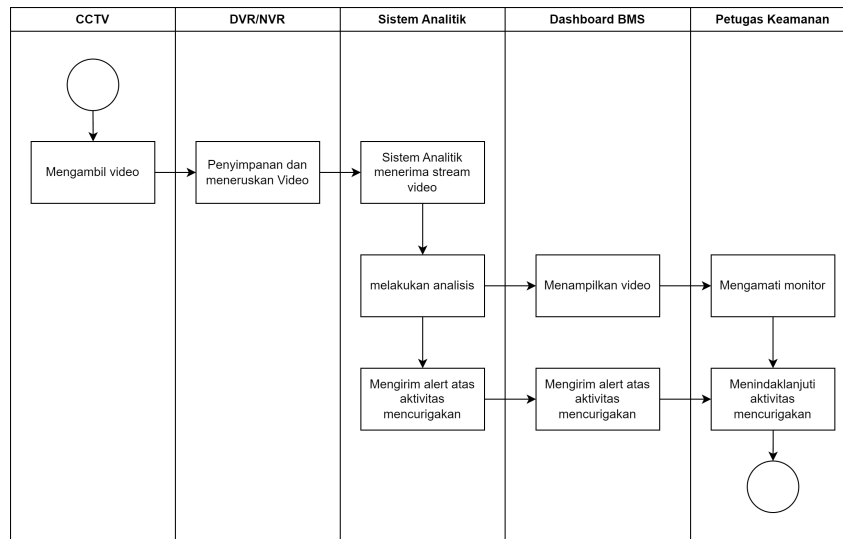
2. **Activity Interpretation**

Sistem melacak pergerakan objek dari waktu ke waktu dan mengidentifikasi pola yang sesuai dengan kriteria aktivitas mencurigakan. Sebagai contoh, jika seseorang berada di area yang sama lebih dari batas durasi tertentu, sistem menandainya sebagai *loitering*.

3. **Decision Engine dan Pengiriman Alert**

Jika sebuah aktivitas memenuhi kriteria mencurigakan, sistem menghasilkan *alert* yang memuat jenis aktivitas, waktu kejadian, dan potongan *frame* (*snapshot*). Informasi ini dikirimkan melalui API ke BMS.

IV.3 Perbandingan



Gambar IV.3 Proses Bisnis Sistem Pengawasan yang Diusulkan (To-Be)

Pada sistem yang diusulkan, alur kerja dimulai dengan CCTV merekam video kemudian DVR atau NVR meneruskan *stream* video ke modul analitik yang telah terintegrasi dengan *Building Management System* (BMS). Modul ini secara otomatis menerima *stream* video dan menjalankan analisis menggunakan model deteksi objek dan aktivitas mencurigakan. Proses analitik berlangsung secara *real-time*, sehingga setiap aktivitas mencurigakan dapat teridentifikasi secara terus menerus. Ketika sebuah aktivitas dikategorikan sebagai mencurigakan, sistem langsung menghasilkan *alert* dan mengirimkannya ke *dashboard* BMS. Petugas keamanan hanya perlu memverifikasi notifikasi yang muncul dan menindaklanjuti kejadian tersebut.

Kondisi ini berbeda dengan proses *as-is* yang berjalan saat ini, di mana observasi diserahkan sepenuhnya kepada petugas keamanan. CCTV hanya berfungsi sebagai perangkat pengambil gambar, sedangkan DVR atau NVR sebatas menyimpan dan menampilkan video ke monitor. Petugas harus mengamati banyak layar secara terus-menerus untuk mengenali potensi ancaman. Ketergantungan pada kemampuan manusia dalam memantau video secara terus menerus membuat risiko terjadinya kelalaian cukup tinggi. Tidak adanya pendeteksi otomatis menyebabkan efisiensi pengawasan bergantung sepenuhnya pada konsentrasi petugas.

Berdasarkan perbandingan tersebut, sistem usulan menawarkan peningkatan dalam membantu petugas keamanan mendeteksi aktivitas mencurigakan dengan menghadirkan pendekatan pengawasan yang lebih adaptif dibandingkan sistem *as-is* yang bersifat pasif dan reaktif.

BAB V

RENCANA SELANJUTNYA

V.1 Rencana Implementasi

V.1.1 Lini Masa

Tabel V.1 Lini Masa Rencana Implementasi

Aktivitas	Februari				Maret				April				Mei			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Observasi, wawancara pengguna																
Rumusan masalah & kebutuhan																
Desain konsep & arsitektur																
Pengembangan model & integrasi																
Pengujian & evaluasi																
Melakukan iterasi dan finalisasi																

Pengerjaan dimulai pada Februari dengan kegiatan observasi dan wawancara untuk memahami kebutuhan pengguna, kemudian dilanjutkan dengan perumusan masalah dan penyusunan kebutuhan sistem. Pada pertengahan Februari hingga Maret dilakukan perancangan konsep dan arsitektur solusi, yang menjadi dasar pengembangan model dan integrasi sistem pada akhir Maret hingga April. Memasuki April dan awal

Mei, sistem diuji dan dievaluasi untuk memastikan performa model serta kesesuaian integrasi dengan BMS. Tahap akhir berupa iterasi dan finalisasi dilakukan pada pertengahan hingga akhir Mei.

V.1.2 Alat dan Bahan

Rincian alat dan bahan yang digunakan pada pengembangan sistem ini disajikan pada tabel berikut.

Tabel V.2 Alat dan Bahan

Kategori	Alat / Bahan
Komputasi	Google Colab
Anotasi	Roboflow
Model & <i>Processing</i>	YOLO, Python, OpenCV
<i>Dataset</i>	Rekaman CCTV ITB Innovation Park, <i>Dataset</i> publik UCF-Crime

V.2 Desain Pengujian dan Evaluasi

Untuk mengukur performa sistem deteksi yang dikembangkan, digunakan beberapa metrik evaluasi standar dalam domain *computer vision*. Rincian metrik tersebut disajikan pada tabel berikut.

Tabel V.3 Metrik Evaluasi

Metrik	Penjelasan Singkat
<i>Confusion Matrix</i>	Menunjukkan jumlah prediksi benar dan salah untuk setiap kelas sehingga pola kesalahan model dapat terlihat jelas.
<i>Precision</i>	Mengukur ketepatan model dalam memprediksi kelas positif, terutama untuk menilai seberapa sering model menghasilkan <i>false positive</i> .
<i>Recall</i>	Mengukur kemampuan model mendeteksi seluruh kejadian positif dan melihat risiko <i>false negative</i> .
<i>F1 Score</i>	Kombinasi <i>precision</i> dan <i>recall</i> yang menunjukkan keseimbangan performa model.

Tabel V.3 Metrik Evaluasi

Metrik	Penjelasan Singkat
mAP	Ukuran utama dalam deteksi objek yang merangkum akurasi deteksi berdasarkan kurva <i>precision-recall</i> .

V.3 Analisis Risiko dan Mitigasi

Selain evaluasi performa model, penelitian ini juga mengidentifikasi sejumlah risiko yang dapat muncul selama proses pengembangan sistem deteksi. Risiko-risiko tersebut beserta strategi mitigasinya dijelaskan sebagai berikut.

1. Risiko Kualitas Data CCTV Rendah

Rekaman CCTV mungkin memiliki pencahayaan buruk, sudut kamera kurang ideal, noise tinggi, atau objek yang tertutup, sehingga menurunkan akurasi deteksi objek dan aktivitas.

Mitigasi: melakukan pengambilan data pada berbagai kondisi menggunakan augmentasi di Roboflow (*brightness, blur, noise, rotation*).

2. Risiko *False Positive* dan *False Negative*

Model dapat salah mendeteksi aktivitas mencurigakan (*false positive*) atau gagal mengenalinya (*false negative*), yang dapat mengurangi keandalan sistem.

Mitigasi: melakukan *tuning threshold confidence* dan IoU, menganalisis *error* menggunakan *confusion matrix*, menambah sampel pada kelas-kelas yang sering salah terdeteksi, serta memperbaiki anotasi yang kurang konsisten.

3. Risiko Keterbatasan Komputasi *Cloud (Runtime Colab/Kaggle)*

Google Colab atau Kaggle dapat memutus sesi saat *training* berlangsung, atau membatasi *runtime* GPU sehingga proses pelatihan tidak selesai.

Mitigasi: menyimpan *checkpoint* model secara berkala ke Google Drive, membagi proses *training* menjadi beberapa tahap, serta menggunakan Colab Pro jika dibutuhkan kestabilan akses GPU yang lebih tinggi.

4. Risiko Latensi Tinggi pada Inferensi Video

Model yang terlalu besar atau *pipeline* yang kurang optimal dapat menyebabkan inferensi video berjalan lambat sehingga tidak responsif.

Mitigasi: menggunakan model ringan seperti YOLOv8n/YOLOv8, mengoptimalkan *preprocessing*, serta menurunkan resolusi *input* jika tidak mempengaruhi akurasi secara signifikan.

5. Risiko Keamanan dan Privasi Data CCTV

Rekaman CCTV bersifat sensitif dan berpotensi menimbulkan pelanggaran

privasi apabila tidak dikelola dengan benar.

Mitigasi: menyimpan data hanya pada layanan *cloud* dengan akses terbatas, memastikan *dataset* di Roboflow menggunakan mode *private*, memberikan akses hanya kepada pihak yang berwenang, serta tidak mendistribusikan cuplikan video di luar kebutuhan penelitian.

DAFTAR PUSTAKA

- Aslam, Aneela. 2020. "Object Detection and Localization in Natural Scenes Through Single-Step and Two-Step Models", <https://doi.org/10.1109/ICETST49965.2020.9080728>.
- Avci, İsa, dan Michael Bidollahkhani. 2022. "Real-Time Building Management System Visual Anomaly Detection Using Heat Points Motion Analysis Machine Learning Algorithm". *Tehnički Vjesnik* 29 (6): 1852–1860. <https://doi.org/10.17559/TV-20220417151954>. <https://doi.org/10.17559/TV-20220417151954>.
- Domingues, Pedro, Paulo Carreira, Renato Vieira, dan Wolfgang Kastner. 2016. "Building Automation Systems: Concepts and Technology Review". *Computer Standards & Interfaces* 45. <https://doi.org/10.1016/j.csi.2015.11.005>.
- Duong, H. T., dkk. 2023. "Deep Learning-Based Anomaly Detection in Video Surveillance: A Survey". *Sensors* 23 (11): 5024. <https://doi.org/10.3390/s23115024>.
- Eini, Reza, dkk. 2022. "Smart Building Management System: Performance Specifications and Design Requirements". *Journal of Building Engineering* 39:102222. <https://doi.org/10.1016/j.jobe.2021.102222>.
- Hussain, Shahid, dkk. 2025. "Recent Innovations, Challenges, and Future Directions in Building Management Systems". *Ingénierie des Systèmes d'Information* 30 (9). <https://doi.org/10.18280/isi.300924>.
- Kumar, Ashish. 2024. "Object Detection using SSD and Efficient net B7 as base Network", <https://doi.org/10.1109/ICAC2N63387.2024.10894816>.
- Pappula, Praveen. 2023. "A Real Time Multiple Object Tracking in Videos using CNN Algorithm", <https://doi.org/10.1109/ICSSAS57918.2023.10331876>.

- Quadri, S. A., dan Komal S. Katakdhond. 2022. "Suspicious Activity Detection Using Convolution Neural Network". *Journal of Pharmaceutical Negative Results* 13 (Supplement 1): 151–158. <https://doi.org/10.47750/pnr.2022.13.S01.151>. <https://doi.org/10.47750/pnr.2022.13.S01.151>.
- Rohitaksha, K., M. Narender, dan Arman Rasool Faridi. 2025. "A Framework for the Video Surveillance Suspicious Activity Detection". *Engineering, Technology & Applied Science Research* 15 (4). <https://doi.org/10.48084/etasr.11437>. <https://doi.org/10.48084/etasr.11437>.
- Szeliski, Richard. 2022. *Computer Vision: Algorithms and Applications*. 2nd edisi. Cham: Springer. ISBN: 978-3-030-34372-9. <https://doi.org/10.1007/978-3-030-34372-9>.
- Zheng, Ce, Wenhan Wu, Chen Chen, Taojiannan Yang, Sijie Zhu, Ju Shen, Nasser Kehtarnavaz, dan Mubarak Shah. 2023. "Deep Learning-Based Human Pose Estimation: A Survey". *ACM Computing Surveys* 55 (13s): 1–37. <https://doi.org/10.1145/3603618>.
- Zvereva, Anna K. 2022. "Survey on Anomaly Detection in Surveillance Videos". *Results in Engineering*, <https://doi.org/10.1016/j.rineng.2025.104162>.