BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan merupakan salah satu aspek paling krusial dalam sebuah institusi atau Perusahaan Nalakhudin et al. (2021). Salah satu langkah yang dapat dilakukan untuk meningkatkan keamanan adalah dengan sistem pengawasan jarak jauh menggunakan kamera pengawas (Apriyani et al., 2020). Dalam era digital yang semakin berkembang, teknologi pengawasan seperti *Closed-Circuit Television* (CCTV) berbasis *Internet Protocol Camera* (*IP Camera*) telah menjadi komponen utama dalam system keamanan, khusunya di lingkungan perusahaan, pabrik, atau memastikan perlindungan asset dan kelancaran operasional (Tantoni & Zaen, 2020). Teknologi ini memungkinkan pengawasan secara *real-time*, termasuk pemantauan proses produksi, aktivitas di gudang, dan distribusi barang, sehingga dapat meminimalkan risiko kehilangan, kerusakan, atau ancaman lainnya.

Namun, keberhasilan sistem pengawasan ini sangat bergantung pada stabilitas dan kinerja jaringan yang mendukung transmisi data dari perangkat *IP Camera* ke server pusat. Masalah seperti *packet lost, latency,* atau perangkat yang *offline* tidak hanya menurunkan kualitas pengawasan, tetapi juga meningkatkan risiko keamanan. Kondisi saat ini untuk mengetahui adanya gangguan pada *IP Camera* masih bergantung pada laporan manual yang disampaikan oleh operator kepada tim pemeliharaan, terutama ketika terdapat *IP Camera* yang *offline* atau gangguan dalam tampilan visual, seperti kualitas gambar yang kurang baik atau hilangnya sinyal video. Pendekatan ini bersifat reaktif, memakan waktu, dan kurang efektif, terutama ketika jumlah perangkat yang dipantau sangat banyak. Dengan jumlah personil yang terbatas dan metode pemantauan manual yang masih mengandalkan pengamatan visual, kamera yang mengalami gangguan sering kali terlambat terdeteksi atau bahkan terlewatkan. Oleh karena itu, diperlukan metode yang mampu mendeteksi anomali pada jaringan *IP Camera* secara otomatis, sehingga dapat memberikan informasi dini kepada tim pemeliharaan untuk menangani anomali jaringan sebelum perangkat mengalami gangguan yang menyebabkan *offline*.

Dalam penelitian sebelumnya oleh Sadaf & Sultana (2020), penelitian tersebut menggunakan algoritma *Autoencoder* dan *Isolation Forest* dalam mendeteksi anomali. Hasil penelitian menunjukan metode tersebut mampu mencapai tingkat akurasi sebesar 95,4%, *precision* 94,8%, *recall* 97,2% dan *F-measure* 96%, yang mengindikasikan perfoma tinggi dalam mendeteksi *intrusi* secara efektif. Penelitian lain oleh Chua et al. (2024) menunjukan bahwa algoritma *Isolation Forest* memiliki perfoma yang baik dengan tingkat akurasi 93%, *precision* 95%, *recall* 90% dan *F1-score* 92%. Selain itu, model ini juga memiliki waktu eksekusi yang cepat, sekitar 23,62 detik. Sementara itu, penelitian yang dilakukan oleh Airlangga (2024), menyimpulkan bahwa model *Isolation Forest* memiliki kinerja yang kuat, dibuktikan dengan S*ilhouette Score* yang tinggi dan indeks *Davies-Bouldin* yang rendah, sehingga mampu mengisolasi anomali secara efektif. Penelitian oleh Kiran et al. (2020) juga menunjukan metode *Isolation Forest* lebih efektif dalam mendeteksi anomali pada transfer data dibandingkan dengan *Principal Component Analysis* (PCA) dan *Autoencoder*, dengan nilai *Error Rate* hanya sebesar 0,05%. Selain itu, penelitian oleh Yustanti & Mutmainah (2024) membandingkan algoritma *Local Outlier Factor* (LOF) dan *Isolation Forest* dalam analisis anomali kinerja dosen, menunjukan bahwa algoritma *Isolation Forest* berhasil mendeteksi 22 dosen terdeteksi anomali dengan S*ilhouette Score* sebesar 0,0377 dan *Rand Index* 0,441 yang menunjukan *Isolation Forest* memberikan hasil yang konsisten dalam mendeteksi anomali serta pemisahan klaster yang lebih baik dan akurat, penelitian ini menyimpulkan bahwa algoritma *Isolation Forest* lebih valid dibandingkan LOF.

Berdasarkan kajian dari penelitian sebelumnya, metode *Isolation Forest* terbukti mampu memberikan hasil yang baik dalam mendeteksi anomali. Oleh karena itu, penelitian ini akan menerapkan algoritma I*solation Forest* untuk mendeteksi anomali pada jaringan *IP Camera.* Penelitian ini diharapkan mampu memberikan kontribusi dalam mendeteksi anomali jaringan secara otomatis, sehingga dapat menyediakan informasi dini terkait gangguan yang terjadi atau status perangkat *offline*. Dengan adanya informasi tersebut, dapat mendukung terciptanya sistem pemeliharaan yang lebih responsif dan efektif.

1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini sebagai berikut :

1. Bagaimana menerapkan algoritma *Isolation Forest* untuk mendeteksi anomali pada jaringan *IP Camera* yang terindikasi menyebabkan perangkat *offline* atau mengalami gangguan pada jaringan?
2. Bagaimana tingkat akurasi algoritma *Isolation Forest* dalam mendeteksi anomali pada jaringan *IP Camera* melalui evaluasi menggunakan *confusion matrix?*

1.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah :

1. Menerapkan algoritma *Isolation Forest* untuk mendeteksi anomali pada jaringan *IP Camera* yang terindikasi menyebabkan perangkat *offline* atau mengalami gangguan pada jaringan.
2. Mengetahui hasil akurasi algoritma *Isolation Forest* dalam mendeteksi anomali pada jaringan *IP Camera* melalui evaluasi menggunakan *confusion matrix.*

1.4 Manfaat

Manfaat yang diharapkan dalam penelitian ini adalah :

1. Implementasi metode deteksi otomatis untuk jaringan *IP Camera* dapat membantu mengidentifikasi masalah secara dini. Sehingga mampu mengurangi risiko *downtime* dan meningkatkan responsivitas terhadap gangguan jaringan.
2. Penelitian ini mendukung program transformasi digital Perusahaan dengan memanfaatkan teknologi kecerdasan buatan melalui pendekatan *Machine Learning*, yang mengotomatisasi proses, meningkatkan akurasi, dan mempercepat pengambilan Keputusan.