BAB 1
PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, teknologi informasi berkembang dengan pesat dan telah membawa banyak perubahan dalam berbagai aspek di kehidupan manusia. Perkembangan teknologi seperti komputasi awan, kecerdasan buatan (AI), big data, dan jaringan nirkabel telah mendorong digitalisasi di berbagai sektor, mulai dari industri, kesehatan, transportasi, hingga kehidupan sehari-hari. Perubahan ini semakin didorong dengan adanya konsep Revolusi Industri 4.0, yang menekankan otomatisasi, konektivitas, dan integrasi sistem cerdas dalam berbagai proses. Salah satu inovasi teknologi yang berperan penting dalam revolusi ini adalah *Internet of Things* (IoT), yang memungkinkan perangkat saling terhubung dengan internet untuk mengumpulkan dan berbagi data secara *real-time* (Meindl & Mendonça, 2021).

Salah satu penerapan nyata dari teknologi IoT yang terus berkembang adalah pada sistem rumah pintar (*smart home*). Jaringan *smart home* yang semakin meluas dan kompleks memungkinkan pengguna mengakses berbagai aplikasi dan layanan, mulai dari pencahayaan pintar, pengaturan suhu otomatis, hingga sistem keamanan berbasis sensor dan kamera. Jaringan ini terdiri dari berbagai perangkat seperti sensor, aktuator, kamera, dan peralatan pintar yang saling berkomunikasi melalui protokol nirkabel maupun kabel (Rejito dkk., 2024). Kompleksitas dan konektivitas yang tinggi dalam sistem *smart home* ini menjadikannya semakin rentan terhadap serangan siber, sehingga upaya deteksi dini terhadap anomali lalu lintas jaringan menjadi semakin penting untuk menjaga keamanan dan kenyamanan pengguna.

Dibalik manfaatnya, teknologi IoT juga membawa tantangan keamanan yang signifikan, terutama dalam pertumbuhan lalu lintas data dalam ekosistem jaringan. Sistem ini mencakup berbagai perangkat yang berkomunikasi secara otomatis tanpa peran aktif manusia. Setiap perangkat dalam ekosistem IoT

berfungsi sebagai sumber data yang terus-menerus mengumpulkan, mengirim, dan menerima informasi melalui jaringan, sehingga volume data yang dihasilkan semakin besar dan kompleks. Namun, sifatnya yang terbuka dan terdistribusi menjadikan IoT rentan terhadap berbagai ancaman keamanan. Penyerang dapat menyalahgunakan lalu lintas data IoT untuk melakukan berbagai jenis serangan siber, seperti penyusupan jaringan, pencurian data, dan eksploitasi kerentanan sistem. Ancaman ini berpotensi membahayakan privasi pengguna, menyebabkan kebocoran informasi sensitif, dan juga dapat mengganggu fungsi operasional dari sistem IoT yang digunakan dalam sektor-sektor kritis seperti kesehatan, transportasi, dan manufaktur. Selain itu, lalu lintas tidak biasa dalam jaringan IoT sering kali menjadi indikator adanya aktivitas mencurigakan atau serangan siber yang dapat membahayakan sistem. Sehingga, pengelolaan keamanan data dan perlindungan privasi dalam jaringan IoT menjadi hal yang sangat penting untuk diperhatikan (Kurniabudi dkk., 2024).

Dalam trafik jaringan pada sistem IoT, anomali sering mengacu pada pola komunikasi yang menyimpang dari normal dan berpotensi membahayakan. Beberapa bentuk anomali yang umum terjadi pada jaringan IoT antara lain *Benign Scan* yaitu pemindaian tidak berbahaya namun bisa disebut anomali jika intensitasnya tinggi. *Port Scanning*, yaitu upaya mendeteksi port terbuka. ICMP *Flood* dan DNS *Flood* yaitu serangan DDoS dengan membanjiri jaringan dengan paket ICMP atau permintaan DNS. *Ping Sweep*, yaitu pemindaian dalam sejumlah besar IP untuk mencari target aktif. Berbagai bentuk anomali tersebut dapat menjadi celah bagi serangan siber, untuk itu diperlukan suatu pendekatan yang dapat mengatasi pola pola tidak wajar tersebut.

Untuk mengatasi permasalahan ini, salah satu teknik yang dapat digunakan adalah deteksi anomali. Deteksi anomali merupakan proses mengidentifikasi pola atau perilaku yang menyimpang dan berbeda dari biasanya, yang dapat menunjukkan adanya aktivitas mencurigakan dalam suatu sistem. Proses ini melibatkan analisis data yang memungkinkan sistem untuk mengidentifikasi pola trafik mencurigakan secara otomatis dan mencegah potensi serangan sebelum terjadi, sehingga dapat membantu dalam meningkatkan keamanan dan integritas

data (Saputra dkk., 2024). Teknik ini sering digunakan dalam keamanan siber, terutama untuk menganalisis lalu lintas jaringan untuk mendeteksi ancaman seperti serangan siber, akses tidak sah, dan penyalahgunaan sumber daya. Dengan meningkatnya ketergantungan pada analisis data, deteksi anomali kini menjadi bagian penting dalam berbagai bidang untuk meningkatkan keamanan.

Metode deteksi anomali tradisional berbasis aturan memiliki keterbatasan dalam mengenali pola yang beragam dan kompleks, terutama pada jaringan IoT yang terus berkembang. Metode ini sering kali kurang optimal dan memerlukan pembaruan aturan secara manual untuk menghadapi jenis ancaman baru. Dalam beberapa tahun terakhir, *machine learning* menjadi salah satu pendekatan utama karena mampu menangani dataset besar dan mengenali pola anomali secara otomatis. Penggunaan algoritma *machine learning* menjadi alternatif untuk mendeteksi anomali pada lalu lintas jaringan karena menunjukkan hasil yang lebih efektif. *Machine learning* mampu mengenali pola mencurigakan berdasarkan riwayat data dan secara otomatis menyesuaikan diri dengan ancaman baru. Sehingga, deteksi anomali berbasis *machine learning* lebih unggul dibandingkan metode tradisional, dan pendekatan ini banyak diterapkan dalam berbagai sistem keamanan lalu lintas jaringan, termasuk lingkungan IoT (Agustina dkk., 2024).

Dalam meningkatkan efektivitas, berbagai algoritma klasifikasi telah digunakan oleh penelitian terdahulu, namun masing-masing algoritma tersebut juga memiliki keterbatasan. Algoritma individu seperti *Decision Tree*, *Support Vector Machine* (SVM), *Logistic Regression*, *K-Nearest Neighbor* (KNN), *Naive Bayes* dan lain-lain memberikan performa yang baik, namun sering kali mengalami masalah seperti *overfitting*, ketidakseimbangan data, dan beban komputasi yang tinggi. Berdasarkan hal ini, model *Ensemble Learning* digunakan untuk mengatasi permasalah tersebut dengan menggabungkan beberapa model untuk menghasilkan prediksi yang lebih akurat dan stabil (Hermawan, 2021).

Pada penelitian sebelumnya (Hermawan, 2021), telah menggunakan model *ensemble learning* yaitu *Bagging*, *Boosting*, dan *Stacking* pada algoritma *base learner* yaitu *Decision Tree* (DT), *Random Forest* (RF), *Support Vector Machine* (SVM), *Naive Bayes* (NB), dan *Logistic Regression* (LR). Berdasarkan hasil

penelitian tersebut, teknik *Stacking* dengan SVM memiliki nilai performa paling tinggi dibandingkan *bagging* dan *boosting*. Maka, penelitian ini akan berfokus pada penggunaan model *ensemble learning* dengan teknik *Stacking* menggunakan *base learner* yang sama pada penelitian sebelumnya untuk menghasilkan prediksi awal, kemudian algoritma *Support Vector Machine* (SVM) digunakan sebagai *meta learner* untuk menggabungkan prediksi dari *base learner* dan menentukan prediksi akhir yang diharapkan dapat lebih akurat dalam mendeteksi anomali. Selain itu, penelitian ini juga menerapkan rekomendasi dari penelitian sebelumnya dengan menggunakan data yang lebih besar, menangani ketidakseimbangan data dengan metode SMOTE (*Synthetic Minority Over-sampling Technique*), serta menerapkan klasifikasi *multi-class* untuk tidak hanya mendeteksi keberadaan anomali tetapi juga mengelompokkan jenis anomalinya.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah pada penelitian ini adalah deteksi anomali pada lalu lintas jaringan IoT terdapat kendala karena pola lalu lintas semakin kompleks dan algoritma individu dalam *machine learning* sering mengalami masalah seperti overfitting dan ketidakseimbangan data, sehingga mengurangi akurasi dalam mendeteksi anomali.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah yang telah ditentukan, maka pertanyaan penelitian ini adalah:

1. Bagaimana penerapan algoritma *machine learning* dengan model *ensemble learning* dalam mendeteksi anomali pada trafik IoT?
2. Apakah teknik *stacking* dengan SVM sebagai *meta learner* dapat meningkatkan akurasi dalam mendeteksi anomali pada trafik IoT?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis penerapan algoritma *machine learning* dengan model *ensemble learning* menggunakan teknik *Stacking*

dengan menerapkan beberapa algoritma *base learner* dan algoritma SVM sebagai *meta learner* untuk mendeteksi anomali pada trafik IoT.

1.5 Manfaat Hasil Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Memberikan pemahaman mengenai penerapan algoritma *machine learning* menggunakan model *ensemble learning* dalam mendeteksi anomali pada trafik IoT.
2. Mendukung pengelolaan dan keamanan jaringan IoT, dengan hasil deteksi anomali sebagai bahan evaluasi dan mitigasi ancaman serangan siber.