BAB I

PENDAHULUAN

1.1 Latar Belakang

Meningkatnya jumlah pengguna internet di Indonesia menjadi indikator positif dalam hal adopsi teknologi, namun secara bersamaan juga membuka peluang yang lebih besar terhadap potensi serangan siber. Laporan dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pada tahun 2024 mencatat bahwa sekitar 221,5 juta penduduk atau 79,5% dari total populasi telah terhubung ke internet, menunjukkan tren pertumbuhan yang signifikan dibandingkan tahun sebelumnya (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024). Di sisi lain, laporan *CrowdStrike* tahun yang sama menyoroti pergeseran pola serangan siber secara global, di mana 75% aktivitas intrusi dilakukan tanpa menggunakan *malware*. Serangan ini tidak lagi bergantung pada penyisipan *file* berbahaya, melainkan memanfaatkan celah pada sistem seperti *API* (*Application Programming Interface*) yang tidak terlindungi, kelemahan dalam proses autentikasi atau kredensial yang berhasil dicuri (Crowdstrike, 2024). Strategi yang semakin halus ini membuat banyak sistem deteksi intrusi tradisional kurang optimal karena tidak mampu mengidentifikasi ancaman yang tidak tampak secara eksplisit. Kondisi ini menegaskan pentingnya penerapan pendekatan yang lebih canggih, seperti pemanfaatan algoritma *machine learning* untuk mengklasifikasi pola-pola anomali secara *real-time* dan merespons ancaman dengan lebih adaptif.

Situasi ini diperparah oleh tingginya jumlah insiden keamanan yang tercatat di dalam negeri. BSSN (Badan Siber dan Sandi Negara) dalam laporan tahunannya mengungkapkan bahwa sepanjang tahun 2023 terdapat lebih dari 403 juta anomali lalu lintas jaringan yang terdeteksi di Indonesia. Angka tertinggi terjadi pada bulan Agustus, sementara Indonesia sendiri menempati posisi pertama sebagai negara dengan jumlah

anomali terbanyak secara global. Selain itu, ditemukan ribuan kerentanan sistem, termasuk jenis celah keamanan seperti *IDOR* (*Insecure Direct Object Reference*) yang umum terjadi pada aplikasi web dan memungkinkan penyerang mengakses informasi tanpa otorisasi yang sah (Badan Siber dan Sandi Negara, 2023). Banyaknya volume data anomali dan kerentanan ini menandakan bahwa sistem deteksi tradisional yang umumnya berbasis *signature* (tanda tangan) tidak lagi memadai untuk menanggulangi serangan yang semakin kompleks dan tersembunyi. Oleh sebab itu, dibutuhkan model yang mampu mengotomatisasi proses klasifikasi dengan tingkat akurasi tinggi, salah satunya dengan mengadopsi pendekatan berbasis *machine learning* yang dapat mengenali pola serangan secara dinamis dan menangani volume data yang besar secara efisien.

Sistem *IDS* (*Intrusion Detection System*) berbasis tanda tangan dan aturan masih banyak digunakan dalam pengamanan jaringan komputer. Sistem ini bekerja dengan mendeteksi pola serangan yang telah diketahui sebelumnya, namun pendekatan ini memiliki kelemahan besar yaitu ketidakmampuan dalam mengenali serangan baru atau varian dari serangan yang sudah ada. Hal ini menyebabkan sistem *IDS* tradisional sering gagal mengidentifikasi ancaman modern seperti serangan *XSS* (*Cross-Site Scripting*) dan *SQL Injection* (*Structured Query Language Injection*) yang terus berkembang dalam bentuk dan tekniknya (Jemili dkk., 2024). Selain itu, data pelatihan yang tidak seimbang menjadi hambatan signifikan dalam proses pembelajaran mesin yang digunakan oleh *IDS* modern. Ketidakseimbangan ini menyebabkan menurunnya akurasi pendeteksian terhadap tipe serangan tertentu, sehingga meningkatkan potensi ancaman yang tidak terdeteksi. Oleh karena itu, pendekatan baru yang menggabungkan teknik klasifikasi berbasis kecerdasan buatan dan pemrosesan data besar menjadi sangat penting dalam upaya meningkatkan ketahanan sistem keamanan jaringan.

Pada data lalu lintas jaringan, model *machine learning* tradisional umumnya lebih cepat dan ringan, tetapi akurasi sering tidak stabil pada distribusi yang tidak seimbang sehingga kelas minor seperti *SQL Injection*, *XSS*, dan *Brute Force* cenderung

under-detected. Temuan komparatif terbaru menunjukkan kinerja ML yang bervariasi pada lintas dataset dan skenario operasional (Alharthi dkk., 2025). Di sisi lain, pendekatan *deep learning* kerap mencapai akurasi lebih tinggi, namun menuntut komputasi dan latensi yang lebih besar sehingga kurang ideal untuk kebutuhan *near-real-time* pada sumber daya terbatas (Chinnasamy dkk., 2025). Berdasarkan bukti empiris terkini, *stacking hybrid* menawarkan titik tengah yang pragmatis karena mampu meningkatkan akurasi secara konsisten sekaligus menjaga biaya komputasi tetap terukur; hasil yang kuat ditunjukkan pada beragam studi IDS berbasis *stacking hybrid* (Ali dkk., 2023).

Dalam konteks tersebut, *LightGBM* dipilih karena mampu menangani data berskala besar dan berdimensi tinggi dengan efisien sehingga sesuai untuk skenario *IDS* yang menuntut proses pelatihan dan inferensi yang cepat. *Random Forest* dipilih karena dikenal stabil terhadap *noise*, relatif tahan terhadap *overfitting*, dan mampu memberikan kinerja yang baik pada berbagai kombinasi fitur. Kombinasi keduanya sebagai *base-learner* diharapkan dapat menyatukan keunggulan efisiensi dan ketahanan model, sedangkan *Multi Layer Perceptron (MLP)* berperan sebagai *meta-learner* yang mempelajari pola dari keluaran kedua model tersebut sehingga menghasilkan keputusan klasifikasi yang lebih akurat dan konsisten untuk berbagai jenis serangan web.

Meskipun sejumlah studi telah menerapkan *stacking* untuk *IDS*, masih ada celah yang belum terjawab secara spesifik pada domain serangan web di *CIC-IDS 2017*. Belum ada kerangka yang secara terpadu mengombinasikan *LightGBM* dan *Random Forest* sebagai *base-learner* dengan *MLP* sebagai *meta-learner*, disertai kebijakan seleksi fitur berbasis *ANOVA F-Test* yang jelas target *Top-k*-nya untuk menekan latensi tanpa menurunkan akurasi. Penanganan ketidakseimbangan kelas umumnya dibahas, namun prosedur *SMOTE* yang tegas hanya pada data latih jarang didokumentasikan detail. Di sisi interpretabilitas, pemadanan daftar fitur penting versi *SHAP* dengan hasil *ANOVA* untuk memverifikasi konsistensi sinyal belum dievaluasi

sistematis pada kelas *SQL Injection*, *XSS*, dan *Brute Force*. Selain itu, pelaporan metrik sumber daya seperti latensi dan *memory footprint* pada lingkungan terbatas masih minim.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada pengembangan model klasifikasi serangan siber dengan pendekatan *stacking hybrid* yang mengombinasikan *LightGBM* dan *Random Forest* sebagai *base-learner* serta *MLP* sebagai *meta-learner*. Penelitian ini memanfaatkan teknik penyeimbangan kelas, seleksi fitur, dan skema evaluasi yang dirancang untuk mengatasi ketidakseimbangan distribusi data sekaligus menjaga efisiensi komputasi. Dengan mempertimbangkan kompleksitas serangan modern, tantangan data yang tidak seimbang, serta keterbatasan sistem deteksi tradisional, pendekatan *stacking hybrid* berbasis *machine learning* yang dikembangkan diharapkan mampu menjadi solusi yang lebih adaptif, akurat, dan aplikatif dalam mengklasifikasi serangan siber berbasis web.

Dengan mempertimbangkan kompleksitas serangan modern, tantangan data yang tidak seimbang, serta keterbatasan sistem deteksi tradisional, maka pendekatan *stacking hybrid* berbasis *machine learning* yang dikembangkan dalam penelitian ini diharapkan mampu menjadi solusi yang lebih adaptif, akurat dan aplikatif dalam mengklasifikasi serangan siber berbasis web.

1.2 Tujuan Penelitian

Secara umum, penelitian ini bertujuan untuk mengembangkan model klasifikasi serangan siber berbasis web dengan pendekatan *stacking hybrid* sehingga mampu meningkatkan kualitas deteksi pada lingkungan dengan distribusi data yang tidak seimbang. Secara khusus, tujuan penelitian ini adalah:

1) Merancang arsitektur model *stacking hybrid* yang mengombinasikan *LightGBM* dan *Random Forest* sebagai *base-learner* serta *MLP* sebagai *meta-learner* untuk klasifikasi serangan web.
2) Menilai kinerja model yang dikembangkan pada skenario klasifikasi biner dan multikelas dengan memperhatikan keadilan performa terhadap kelas-kelas minoritas.
3) Membandingkan kinerja model *stacking hybrid* dengan *base-learner* (model dasar) guna mengetahui besarnya peningkatan yang diperoleh.
4) Mengidentifikasi dan menjelaskan peran fitur-fitur penting yang memengaruhi keputusan model dalam membedakan lalu lintas normal dan berbagai jenis serangan web.
5) Menilai kebutuhan sumber daya komputasi serta potensi penerapan model pada lingkungan operasional yang memiliki keterbatasan sumber daya dan pada data dengan karakteristik yang berbeda.

1.3 Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan kontribusi dalam meningkatkan kemampuan klasifikasi serangan siber berbasis web dengan menggunakan pendekatan teknik *Stacking* yang menggabungkan *LightGBM* dan *Random Forest* sebagai *base-learner* dan *MLP* sebagai *meta-learner*, penelitian ini dapat memberikan solusi yang lebih akurat dalam mengidentifikasi serangan seperti *SQL Injection*, *XSS*, dan *Brute Force*. Hasil penelitian ini diharapkan dapat membantu dalam pengembangan sistem keamanan siber yang lebih efektif, terutama dalam menghadapi ancaman terhadap aplikasi web di lingkungan yang kompleks.