BAB VI

PENUTUP

6.1 Kesimpulan

Berdasarkan hasil penelitian yang berjudul "Penerapan *Machine Learning* untuk Menganalisis Kejahatan *Cyber* di Tengah Peringatan Serangan digital Menggunakan Algoritma *Random forest*", dapat disimpulkan bahwa sistem yang dibangun berhasil memenuhi tujuan yang telah direncanakan. Sistem mampu mendeteksi dan menganalisis aktivitas jaringan yang mencurigakan dengan memanfaatkan algoritma *random forest* sebagai metode klasifikasi. Melalui serangkaian pengujian, sistem dapat membedakan antara aktivitas normal dan aktivitas yang berpotensi sebagai serangan dengan tingkat akurasi yang memadai. Proses *input* data melalui file CSV, evaluasi prediksi dengan nilai *y_pred* dan *y_true*, serta penyajian hasil secara visual menunjukkan bahwa sistem berjalan secara fungsional dan informatif. Fitur tambahan seperti pengaturan ambang batas (t*hreshold*), *log IP* mencurigakan, dan validasi input juga berfungsi dengan baik, memberikan pengalaman penggunaan yang lebih stabil dan aman. Dengan demikian, penerapan *machine learning*, khususnya algoritma *random forest*, terbukti efektif dalam mendukung upaya deteksi dini terhadap serangan digital dalam sistem keamanan jaringan.

6.2 Saran

Untuk pengembangan dan penyempurnaan sistem di masa mendatang, penulis memberikan beberapa saran sebagai berikut:

1. Integrasi dengan Basis Data

   Sistem dapat dikembangkan lebih lanjut dengan menggunakan d*atabase* seperti MySQL agar data yang dianalisis dan hasil deteksi dapat disimpan dan dikelola dengan lebih efisien.

2. Penambahan Algoritma Pembanding

   Untuk meningkatkan akurasi dan efektivitas analisis, sistem dapat dibandingkan dengan algoritma *machine learning* lain seperti SVM, KNN, atau *Gradient Boosting* sebagai bahan evaluasi performa.

3. Peningkatan Visualisasi

   Visualisasi hasil deteksi dan log data dapat ditingkatkan dengan menggunakan grafik interaktif atau *dashboard* analitik agar memudahkan pemantauan secara *real-time.*

4. Penerapan di Lingkungan Nyata

   Sistem ini dapat diuji secara langsung di lingkungan jaringan nyata, seperti pada server institusi atau organisasi, guna mengukur efektivitas sistem dalam kondisi yang sebenarnya.

5. Penambahan Sistem Peringatan Otomatis

   Fitur peringatan otomatis (*alert)* seperti pengiriman notifikasi email atau *pop-up* saat ditemukan aktivitas mencurigakan dapat sangat membantu dalam tindakan *respons* cepat terhadap serangan.

Dengan perbaikan dan pengembangan lebih lanjut, sistem ini diharapkan dapat menjadi fondasi bagi solusi keamanan jaringan yang adaptif dan cerdas dalam menghadapi berbagai ancaman digital yang terus berkembang.