Implementasi Sistem Deteksi Anomali Jaringan Menggunakan Machine Learning untuk Keamanan Siber

Laporan Proyek Teknologi Informasi

Abstrak

Dalam era digital modern, ancaman terhadap keamanan jaringan meningkat secara signifikan seiring dengan pertumbuhan lalu lintas data di berbagai sektor. Penelitian ini mengusulkan sistem deteksi anomali berbasis Machine Learning untuk mengidentifikasi aktivitas mencurigakan di jaringan komputer. Dengan memanfaatkan algoritma klasifikasi seperti Random Forest dan XGBoost, sistem ini mampu membedakan pola normal dan anomali berdasarkan data lalu lintas jaringan. Hasil pengujian menunjukkan tingkat akurasi 94,6%, menunjukkan efektivitas pendekatan ini dalam mendeteksi potensi serangan siber secara dini.

Latar Belakang

Keamanan siber merupakan salah satu aspek paling krusial dalam infrastruktur teknologi informasi. Serangan siber seperti Denial of Service (DoS), phishing, dan malware dapat mengganggu stabilitas sistem dan menyebabkan kerugian finansial yang besar. Sistem deteksi anomali tradisional yang berbasis tanda tangan sering kali tidak efektif terhadap serangan baru yang belum dikenal. Oleh karena itu, penggunaan Machine Learning dalam mendeteksi pola lalu lintas abnormal menjadi solusi yang potensial untuk meningkatkan pertahanan jaringan.

Metodologi

1. **Pengumpulan Data**: Dataset diperoleh dari sumber publik seperti KDD Cup 99 dan UNSW-NB15. 2. **Pra-pemrosesan Data**: Meliputi pembersihan data, normalisasi nilai numerik, dan encoding fitur kategorikal. 3. **Pelatihan Model**: Model Machine Learning seperti Random Forest, Decision Tree, dan XGBoost digunakan untuk melatih sistem. 4. **Evaluasi Model**: Model dievaluasi menggunakan metrik akurasi, precision, recall, dan F1-score. 5. **Implementasi Sistem**: Sistem diintegrasikan ke dalam arsitektur jaringan untuk mendeteksi aktivitas anomali secara real-time.

Hasil dan Pembahasan

Hasil eksperimen menunjukkan bahwa model XGBoost memberikan performa terbaik dengan akurasi sebesar 94,6%, precision 93,8%, dan recall 92,7%. Kinerja ini menunjukkan kemampuan model dalam mengenali pola lalu lintas jaringan yang tidak biasa dengan tingkat kesalahan minimal. Integrasi sistem ini ke dalam jaringan lokal memungkinkan deteksi dini aktivitas berbahaya seperti port scanning dan brute force

login. Selain itu, sistem mampu menyesuaikan diri terhadap perubahan pola lalu lintas jaringan menggunakan pembelajaran berkelanjutan.

Kesimpulan dan Saran

Sistem deteksi anomali berbasis Machine Learning terbukti mampu meningkatkan keamanan jaringan dengan mendeteksi aktivitas mencurigakan secara lebih cepat dan akurat dibandingkan metode tradisional. Dalam pengembangan selanjutnya, sistem ini dapat diperluas dengan menerapkan Deep Learning serta integrasi dengan sistem manajemen keamanan informasi (SIEM). Selain itu, penelitian lanjutan disarankan untuk menguji performa sistem dalam lingkungan jaringan yang lebih kompleks dan dinamis.