BAB I
LATAR BELAKANG

1.1 Latar Belakang

Pada “Lanskap Keamanan Siber Indonesia 2024” keluaran BSSN, total trafik anomali di Indonesia selama 2024 tercatat 330 juta kejadian; jenis paling dominan adalah serangan botnet Mirai dengan 81 juta aktivitas. Laporan ini juga menyoroti bahwa trafik serangan tertinggi terjadi pada bulan Desember 2024 dengan 112 juta anomali, sedangkan anomali terendah pada bulan Mei dengan 12 juta anomali. Aktivitas anomali trafik berdampak pada penurunan kinerja perangkat dan jaringan, pencurian data sensitif, serta menurunnya kepercayaan terhadap organisasi.

Keberadaan sistem berbasis web membuka celah terhadap serangan seperti *SQL Injection*, XSS, LFI, serta serangan terkait lainnya; ancaman-ancaman ini bukan hanya menyebabkan kebocoran data, tetapi juga mengancam integritas dan ketersediaan layanan. Pemilihan ketiga jenis serangan ini sebagai target studi menunjukkan fokus pada kerentanan injeksi dan input yang umum dijumpai di aplikasi web.

Di sisi lain, arsitektur sebagian besar solusi keamanan yang ada masih berfokus pada analisis log secara pasif, bukan pada pemantauan trafik jaringan yang adaptif. Pendekatan ini cenderung mengakibatkan jeda waktu antara terjadinya serangan dengan proses deteksi dan respons. Padahal, penggunaan mekanisme pengawasan lalu lintas secara *real-time* menjadi krusial untuk mengungkap pola-pola serangan baru yang tidak terdefinisi dalam aturan atau tanda tangan konvensional. Hal tersebut mengindikasikan perlunya pengembangan sistem keamanan dengan agen *monitoring* yang terintegrasi dengan model klasifikasi cerdas, sehingga kemampuan deteksi dini terhadap serangan dapat ditingkatkan sebelum menimbulkan kerusakan yang lebih luas.

Penelitian ini mengembangkan sistem keamanan web berbasis *machine learning* yang memanfaatkan algoritma *K-Nearest Neighbor* untuk mengklasifikasikan serangan serta menyediakan dashboard interaktif guna memantau hasil deteksi. Fokus utamanya adalah mengenali serangan *SQL Injection,* XSS, dan LFI secara bersamaan.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang terindetifikasi diatas, maka dapat dirumuskan beberapa rumusan masalah sebagai berikut:

1. Bagaimana mengimplementasikan dashboard berbasis web yang dapat menampilkan hasil klasifikasi serangan dengan visualisasi yang mudah dipahami?
2. Bagaimana menerapkan metode K-Nearest Neighbor (KNN) pada aplikasi berbasis website untuk melakukan klasifikasi serangan?
3. Seberapa efektif aplikasi yang dikembangkan dalam mencegah serangan aplikasi web?

1.3 Batasan Masalah

Agar penelitian ini lebih terfokus dan dapat diselesaikan dengan baik, maka ditetapkan batasan-batasan sebagai berikut:

1. Dataset yang digunakan adalah kombinasi dataset yang diambil pada *repository openappsec,* dan *modsec-learn*, dan simulasi serangan yang telah ditentukan.
2. Metode yang digunakan untuk klasifikasi adalah *K-Nearest Neighbor* .
3. Fokus penelitian berada pada serangan *SQL Injection*, *Cross-Site Scripting*, dan *Local File Inclusion*.
4. Ruang lingkup analisis sistem keamanan meliputi mekanisme validasi input, dan teknik pendukung lainnya yang berfungsi untuk mengantisipasi terjadinya serangan siber.
5. Menggunakan bahasa pemrograman *python* sebagai pengklasifikasi model*,* dan sebagai *proxy* ke aplikasi.

1.4 Tujuan

Terdapat beberapa tujuan dari pembuatan aplikasi ini sebagai berikut:

1. Mengimplementasikan dashboard berbasis web yang menampilkan hasil klasifikasi serangan dengan visualisasi yang mudah dipahami.
2. Menerapkan metode *K-Nearest Neighbor* pada aplikasi berbasis website untuk klasifikasi serangan.
3. Menguji keefektifan aplikasi dalam mencegah serangan.

1.5 Manfaat

Adapun manfaat yang dapat diperoleh dari penelitian ini, diantaranya sebagai berikut:

1. Menyediakan informasi yang mendukung pengambilan keputusan dalam manajemen keamanan aplikasi web.
2. Diharapkan perancangan aplikasi ini dapat menambah referensi terhadap penelitian baru dengan topik terkait.
3. Memungkinkan alokasi sumber daya keamanan yang lebih efisien berdasarkan hasil klasifikasi.

1.6 Metode Penelitian

Untuk dapat mencapai keinginan dalam pembuatan aplikasi klasifikasi serangan *SQL Injection, Cross-Site Scripting,* dan *Local File Inclusion*, maka perlu dilakukan dengan langkah-langkah sebagai berikut:

1. Studi Literatur

   Studi literatur dilakukan dengan mengambil dan mempelajari berbagai sumber referensi seperti buku, jurnal ilmiah, dan artikel internet yang berkaitan dengan proses pada metode *K-Nearest Neighbor*.

2. Pengumpulan dan Pra-pemrosesan Data

   Dataset yang digunakan adalah dataset kombinasi yang diambil pada *repository* publik dan simulasi serangan di internet. Selanjutnya, data dibersihkan seperti, normalisasi data, dan pemberian label. Tahap ini penting untuk memastikan kualitas dari data.

3. Perancangan Sistem

   Secara umum tahapan ini dilakukan perancangan *flowchart K-Nearest Neighbor*, perancangan *flowchart* sistem, *formula* Metode *K-Nearest Neighbor*, dan perancangan struktur menu aplikasi prediksi pada serangan berbasis website.

4. Pelatihan Model

   Model *K-Nearest Neighbor* digunakan karena keunggulannya dalam klasifikasi yang akurat. Pelatihan dilakukan pada dataset terlabel, dan evaluasi awal dilakukan menggunakan *accuracy*, *precision*, *recall*, dan *F1-score* untuk mengukur performa.

5. Pengujian Sistem dan Evaluasi Model

   Sistem diuji dari sisi fungsional dan akurasi. Pengujian dilakukan menggunakan data uji untuk mengevaluasi efektivitas deteksi dan respons sistem terhadap skenario serangan. Hasil evaluasi menjadi dasar untuk penguatan sistem

1.7 Sistematika Penulisan

Sistematika penulisan dalam tugas akhir ini disusun sebagai berikut:

BAB I: Pendahuluan**,** Bab ini menjelaskan latar belakang, rumusan masalah, tujuan, atasan masalah, manfaat penelitian, serta sistematika penulisan sebagai basis pemahaman terhadap penelitian yang dilakukan.

BAB II: Tinjauan pustaka**,** Bab ini berisi penelitian terdahulu yang relevean, Kajian teori yang mendukung penelitian, seperti konsep dasar serangan *SQL Injection*, *Cross-Site Scripting*, *Local File Inclusion*, *Web Application Firewall*, TF-IDF, dan KNN.

BAB III: Analisis dan perancangan, bab ini berisi analisis kebutuhan fungsional dan non-fungsional, arsitektur sistem, proses pengambilan dataset, flowchart dari sistem WAF yang diimplementasikan.

BAB IV: Implementasi dan pengujian, Bab ini menjelaskan proses implementasi sistem deteksi serangan berbasis metode KNN serta pengujian kinerja dan fungsionalitas sistem, termasuk dashboard dan evaluasi hasil klasifikasi.

BAB V: Penutup, Bab ini berisi kesimpulan yang diperoleh berdasarkan hasil penelitian yang telah dilakukan. dan saran untuk pengembangan sistem lebih lanjut.