`

BAB I
PENDAHULUAN

Pada bab ini akan dibahas terkait latar belakang penelitian, rumusan masalah, tujuan, manfaat, dan batasan masalah.

1.1. Latar Belakang

Penggunaan aplikasi web telah menjadi bagian penting dari kehidupan sehari-hari, terutama dalam bidang pendidikan dan bisnis. Dalam bidang pendidikan, aplikasi web memungkinkan siswa untuk mengakses pembelajaran secara daring, berpartisipasi dalam diskusi, dan mengerjakan tugas dari mana saja. Di sisi bisnis, aplikasi web memfasilitasi komunikasi tim, dan manajemen proyek. Hal ini mencerminkan pergeseran paradigma dalam cara belajar dan berkolaborasi, memungkinkan akses yang lebih mudah dan fleksibel terhadap informasi serta memfasilitasi komunikasi dan kerja sama tim di seluruh dunia. Dengan terus berkembangnya teknologi dan kebutuhan akan keterlibatan digital yang lebih besar, penggunaan aplikasi web diperkirakan akan terus meningkat sebagai bagian penting dari kehidupan sehari-hari.

Pada sisi lain, keamanan aplikasi web menjadi perhatian utama karena meningkatnya jumlah pengguna aplikasi web, penting untuk memastikan bahwa data sensitif pengguna dilindungi. Serangan seperti *SQL Injection*, memanfaatkan celah keamanan dalam aplikasi web yang tidak memvalidasi atau menyaring input pengguna dengan benar, memungkinkan penyerang untuk memasukkan *SQL statement* untuk mengakses dan memodifikasi data pengguna (Elu, 2017). Untuk meningkatkan perlindungan terhadap serangan-serangan tersebut, penggunaan *Web Application Firewall* (WAF) menjadi salah satu solusi yang efektif. WAF bertindak sebagai filter antara pengguna dan aplikasi web, menganalisis setiap permintaan dan respons HTTP untuk mendeteksi dan mencegah serangan-serangan yang berpotensi merusak.

WAF memiliki dua pendekatan dalam mendeteksi serangan, yaitu *signature based* dan *anomaly based*. Dalam pendekatan *signature based*, WAF akan membandingkan setiap permintaan HTTP yang masuk dengan *database* pola yang sudah dikenal dari serangan-serangan sebelumnya. Pendekatan *signature based*

`

memiliki kelemahan yaitu tidak dapat mendeteksi serangan baru yang belum pernah dikenali sehingga memerlukan pembaruan setiap ditemukan pola serangan baru (Calvo & Beltrán, 2022). Dalam pendekatan *anomaly based,* WAF akan memantau setiap permintaan HTTP dan mencari pola yang tidak biasa atau mencurigakan yang mungkin menandakan serangan dengan menggunakan *machine learning*. Kelemahan dari pendekatan *anomaly based detection* adalah kecepatan dalam mendeteksi yang relatif lambat sehingga tidak disarankan digunakan sebagai sistem pendeteksi serangan *real-time* (Tekerek & Bay, 2019). Dari permasalahan yang muncul dari kedua pendekatan tersebut, solusi yang efektif adalah dengan menggabungkan kedua pendekatan sehingga dapat menutupi kelemahan satu sama lain. Pendeteksian awal menggunakan pendekatan *signature based*; jika pola yang terdeteksi tidak dikenali, maka pendekatan akan beralih ke *anomaly based* untuk analisis lebih lanjut. Hasil dari pendekatan *anomaly based* kemudian dapat digunakan untuk memperbarui database pola serangan yang digunakan dalam pendekatan *signature based*. Dengan demikian, WAF dapat secara adaptif meningkatkan kemampuannya dalam mendeteksi serangan baru dan yang belum pernah dikenali sebelumnya.

Berkaitan dengan hal itu, penggunaan pendekatan *hybrid signature based* dan *anomaly based* dengan SVM yang dioptimalkan PSO dipilih untuk mendeteksi serangan dari permintaan HTTP. Keputusan ini didasari oleh kemampuan kombinasi pendekatan *signature based*, yang mengandalkan pola serangan yang telah dikenali sebelumnya, dan pendekatan *anomaly based*, yang fokus pada pola yang tidak biasa atau anomali dalam lalu lintas web, untuk secara efektif mengidentifikasi serangan baru yang mungkin belum terdeteksi sebelumnya. Penggunaan PSO juga memberikan keuntungan tambahan dengan kemampuannya dalam mengoptimalkan parameter-parameter SVM untuk meningkatkan klasifikasi data normal dan data serangan. Dengan demikian, pendekatan ini diharapkan dapat memberikan tingkat deteksi serangan yang tinggi sambil meminimalkan jumlah serangan yang berhasil melewati sistem keamanan. SVM yang dioptimalkan PSO akan dievaluasi menggunakan semua skenario pengujian, dengan memanfaatkan *fitness function* untuk mengoptimalkan parameter SVM dan meningkatkan akurasi

`

deteksi. Dengan pendekatan ini, diharapkan dapat dicapai tingkat deteksi serangan yang lebih tinggi serta peningkatan performa sistem keamanan secara keseluruhan.

1.2. Rumusan Masalah

Berdasarkan dengan latar belakang yang telah dijelaskan sebelumnya, maka dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana kontribusi PSO dalam mengoptimalkan parameter SVM yang mempengaruhi kemampuan WAF dalam mendeteksi pola-pola serangan pada aplikasi web?
2. Bagaimana menerapkan PSO-SVM pada WAF dengan pendekatan *hybrid signature* dan *anomaly based* ?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan, maka tujuan dari penelitian ini sebagai berikut:

1. Menganalisis kontribusi algoritma PSO dalam mengoptimalkan parameter SVM untuk meningkatkan kemampuan WAF dalam mendeteksi pola-pola serangan pada aplikasi web.
2. Mengimplementasikan metode PSO-SVM pada WAF dengan pendekatan *hybrid signature* dan *anomaly based* untuk meningkatkan efisiensi dalam mendeteksi dan mencegah serangan pada aplikasi web.

1.4. Manfaat Penelitian

Pada penelitian ini, terdapat manfaat yang diharapkan dapat dicapai. Adapun manfaat penelitian yang ingin dicapai adalah sebagai berikut:

1. Meningkatkan deteksi serangan aplikasi web yang lebih efektif.
2. Memperkuat keamanan aplikasi web terhadap serangan baru dan berkembang.
3. Mengurangi risiko kerentanan keamanan yang tidak terdeteksi pada aplikasi web.
4. Menyediakan lapisan pertahanan tambahan terhadap serangan yang belum diketahui.

`

1.5. Batasan Masalah

Agar penelitian lebih terarah dan pembahasan tidak melebar, maka penelitian akan dibatasi sebagai berikut:

1. Data yang digunakan dalam penelitian adalah data ECML/PKDD 2007 dan CSIC 2010 dengan berupa data permintaan HTTP
2. Serangan yang dapat dideteksi adalah serangan *SQL Injection, XSS Injection, OS Command Injection, Buffer Overflow,* dan *Path Traversal*.
3. Pengembangan WAF dalam penelitian ini difokuskan pada penggunaan algoritma SVM yang dioptimalkan PSO untuk mendeteksi serangan siber dengan dua pendekatan: berdasarkan tanda-tanda serangan yang sudah dikenal *(signature based)* dan berdasarkan perilaku aneh yang mencurigakan *(anomaly based)*.