BAB I

PENDAHULUAN

Bab ini membahas Pendahuluan yang berisi penjelasan awal mengenai urgensi penelitian, konteks permasalahan yang melatarbelakanginya, serta tujuan dan manfaat yang ingin dicapai. Melalui bab ini, pembaca diberikan gambaran umum mengenai pentingnya pengembangan sistem keamanan pada aplikasi website, khususnya dalam menghadapi meningkatnya ancaman siber seperti *SQL Injection* dan *Cross-site Scripting* (*XSS*). Sistem keamanan yang dikembangkan dalam penelitian ini mengadopsi pendekatan *Web Application Firewall* (*WAF*) berbasis *Machine Learning*, yang bertujuan untuk mendeteksi dan mengantisipasi serangan secara otomatis dan adaptif. Selain itu, bab ini juga mencakup rumusan masalah, batasan penelitian, serta sistematika penulisan sebagai panduan untuk memahami struktur keseluruhan laporan penelitian.

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong hampir seluruh sektor untuk memanfaatkan aplikasi berbasis web sebagai sarana utama dalam pengelolaan data dan layanan digital. Namun, peningkatan penggunaan aplikasi web juga diiringi dengan meningkatnya ancaman keamanan siber, seperti serangan injeksi, *brute force*, dan eksploitasi kerentanan sistem. Kondisi ini menuntut adanya mekanisme perlindungan yang adaptif dan cerdas untuk menjaga integritas serta kerahasiaan data dalam aplikasi web. Menurut (Nair, 2024), keamanan aplikasi web memerlukan penerapan teknik deteksi serangan berbasis pembelajaran mesin untuk meningkatkan kemampuan identifikasi dan respons terhadap serangan injeksi *SQL Injection* dan *Cross-site Scripting* (*XSS*), sehingga kerentanan terhadap kebocoran data dapat dikurangi secara dinamis seiring evolusi pola serangan.

Lembaga pendidikan, termasuk universitas dan sekolah, semakin sering menjadi target serangan siber di tingkat global. Serangan yang ditujukan pada sistem akademik, portal mahasiswa, hingga sistem manajemen pembelajaran dapat mengakibatkan kebocoran data pribadi, manipulasi nilai, dan gangguan operasional

institusi. Fenomena ini menunjukkan bahwa sektor pendidikan memiliki risiko keamanan yang tinggi namun sering kali belum memiliki sistem pertahanan siber yang memadai. Menurut Kepuska dan Tomašević, *LMS* dan *platform* institusional lainnya menyimpan data sensitif seperti *Personal Identifiable Information* (PII) mahasiswa, sehingga peningkatan perlindungan berbasis risiko pada arsitektur keamanan menjadi kebutuhan kritis bagi institusi pendidikan tinggi (Kepuska & Tomašević, 2024).

Dalam konteks pendidikan di Indonesia, keamanan aplikasi web di lingkungan kampus masih menjadi aspek yang kurang mendapatkan perhatian utama. Banyak institusi pendidikan belum menerapkan standar keamanan web yang memadai, termasuk deteksi otomatis terhadap serangan dan sistem pencegahan berbasis kecerdasan buatan. Keberlanjutan operasional kampus sangat bergantung pada keandalan sistem informasi akademik yang mereka gunakan. Menurut (Budiman et al., 2021), peningkatan praktik keamanan pada aplikasi web di institusi pendidikan perlu dilakukan melalui evaluasi kerentanan dan penerapan kontrol keamanan berlapis untuk menjamin ketersediaan dan integritas layanan akademik.

Salah satu studi kasus yang menjadi perhatian dalam penelitian ini adalah penggunaan sistem *electronic voting (e-vote)* untuk pemilihan ketua organisasi kemahasiswaan di lingkungan kampus. Sistem *e-vote* sebagai aplikasi berbasis *web* memiliki tingkat risiko keamanan yang tinggi karena berperan dalam proses pengambilan keputusan yang bersifat penting dan sensitif. Potensi serangan siber seperti *brute force*, *SQL Injection,* dan *Cross-Site Scripting (XSS)* dapat dimanfaatkan untuk melakukan akses tidak sah, manipulasi data pemilih maupun hasil suara, serta mengganggu proses autentikasi pengguna. Dampak dari serangan tersebut tidak hanya merugikan secara teknis, tetapi juga dapat menurunkan tingkat kepercayaan *civitas* akademika terhadap legitimasi hasil pemilihan. Kondisi ini menunjukkan bahwa mekanisme keamanan berbasis aturan statis yang umum diterapkan pada aplikasi *web* belum sepenuhnya mampu menghadapi variasi pola serangan yang semakin kompleks dan dinamis.

Beberapa penelitian terkini telah mengusulkan penerapan teknik *Machine Learning (ML)* dalam pengembangan sistem *Web Application Firewall (WAF)*

untuk mengatasi keterbatasan metode berbasis aturan statis. Penelitian yang dilakukan oleh (Mani & Shenoy, 2025a) meninjau secara komprehensif bagaimana *model-ML* digunakan dalam aplikasi *WAF*, dan menunjukkan bahwa integrasi ML membuat *WAF* lebih adaptif terhadap pola serangan yang belum pernah dilihat sebelumnya.

Penelitian lain oleh *ML-Enhanced Behavioral & Anomaly Detection Web Application Firewall* (Asan Nainar & Sibikarthik, 2025) menegaskan bahwa sistem *WAF* berbasis *ML* yang memanfaatkan analisis perilaku mampu mendeteksi serangan seperti *brute-force*, *XSS*, dan *SQL Injection* dengan tingkat keberhasilan yang lebih tinggi dibanding pendekatan konvensional. Hasil-hasil tersebut memperkuat argumen bahwa pendekatan *Supervised Learning* dalam arsitektur *WAF* dapat secara signifikan meningkatkan kemampuan sistem untuk mengenali pola serangan baru, sekaligus mengurangi kebutuhan untuk terus-menerus memperbarui aturan manual.

Berdasarkan tinjauan tersebut, terdapat celah penelitian untuk mengembangkan *Web Application Firewall (WAF)* yang lebih dinamis dan adaptif, dengan memanfaatkan algoritma *Machine Learning*. Pendekatan ini memungkinkan sistem untuk belajar dari data serangan yang telah terjadi serta mengenali variasi serangan baru yang belum pernah dilihat sebelumnya. Teknik *Supervised Learning* menjadi solusi deteksi serangan web dengan belajar dari pola lalu lintas yang belum pernah dilihat sebelumnya, termasuk serangan seperti *SQL Injection* dan *Cross-site Scripting* (*XSS*) (Dawadi et al., 2023).

Berdasarkan penelitian-penelitian sebelumnya, masih terdapat keterbatasan pada integrasi model *Machine Learning* ke dalam sistem *Web Application Firewall (WAF)* yang adaptif dan teruji secara fungsional, khususnya pada lingkungan perguruan tinggi yang memiliki karakteristik pengguna dan pola akses yang dinamis. Sebagian besar penelitian berfokus pada evaluasi performa *model* secara teoritis melalui pengujian *dataset*, namun belum banyak yang mengkaji implementasi model *Machine Learning* secara langsung ke dalam sistem aplikasi *web* serta pengujian fungsionalnya secara menyeluruh.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan dan mengimplementasikan sistem *Web Application Firewall* berbasis *Machine Learning* yang terintegrasi dengan aplikasi *web e-vote* untuk pemilihan ketua organisasi kampus, serta mengevaluasi efektivitasnya melalui pengujian *model* dan pengujian sistem secara *end-to-end*. Diharapkan penelitian ini dapat memberikan kontribusi dalam meningkatkan keamanan aplikasi web di lingkungan perguruan tinggi, khususnya dalam mencegah serangan *SQL Injection* dan *Cross-Site Scripting (XSS)* secara adaptif dan andal.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana merancang dan mengembangkan sistem keamanan aplikasi website menggunakan *Web Application Firewall* (*WAF*) yang mampu mendeteksi serangan secara otomatis?
2. Bagaimana penerapan algoritma *Machine Learning* dapat digunakan untuk meningkatkan kemampuan deteksi terhadap serangan seperti *SQL Injection* dan *Cross-site Scripting* (*XSS*)?
3. Bagaimana perbandingan hasil kinerja antara algoritma *Decision Tree* dan *Random Forest* dalam mendeteksi serangan terhadap aplikasi web berdasarkan metrik evaluasi seperti akurasi, presisi, *recall*, dan *F1-score*?

1.3 Batasan Masalah

Batasan masalah pada penilitian ini adalah sebagai berikut:

1. Jenis serangan yang dideteksi dibatasi pada serangan berbasis input teks, yaitu *SQL Injection* dan *Cross-site Scripting* (*XSS*), yang termasuk dalam kategori umum dan sering terjadi pada aplikasi *website*.
2. Data yang digunakan untuk pelatihan dan pengujian model *Machine Learning* berasal dari *Dataset* publik yang berisi *log HTTP request* atau *Payload* publik.

3. Sistem *Web Application Firewall* yang dikembangkan bersifat simulatif dan berjalan pada lingkungan pengujian *(Testing environment)*, bukan langsung diimplementasikan pada sistem produksi atau *live server*.
4. *Model Machine Learning* yang digunakan terbatas pada model klasifikasi *supervised learning*, seperti *Decision tree*, *Random forest* tanpa menggunakan pendekatan *deep learning*.
5. Sistem *WAF* hanya melakukan deteksi dan pencegahan pada lapisan aplikasi (*Layer* 7) tanpa menerapkan pemblokiran IP secara langsung, untuk menghindari kemungkinan terblokirnya pengguna lain yang berada pada jaringan dengan alamat IP serupa.

1.4 Tujuan

Tujuan pada penelitian ini adalah sebagai berikut:

1. Merancang dan membangun sistem *Web Application Firewall* yang mampu mendeteksi serangan *SQL Injection* dan *Cross-site Scripting* (*XSS*) secara otomatis.
2. Menerapkan algoritma *Machine Learning* untuk mengklasifikasikan lalu lintas *HTTP* antara yang bersifat *normal* dan yang berpotensi sebagai serangan.
3. Menguji dan mengevaluasi perbandingan kinerja algoritma *Decision Tree* dan *Random Forest* dalam mendeteksi serangan terhadap aplikasi web berdasarkan metrik evaluasi seperti akurasi, presisi, *recall*, dan *F1-score*, untuk menentukan model yang paling optimal dalam pengembangan sistem *WAF* berbasis Machine Learning.

1.5 Manfaat

Adapun manfaat yang diperoleh dari penelitian ini sebagai berikut:

1. Bagi Peneliti (Mahasiswa): Penelitian ini memberikan pengalaman langsung dalam merancang dan mengembangkan sistem keamanan berbasis *Machine Learning*, serta memperluas pemahaman tentang penerapan teknologi kecerdasan buatan dalam konteks keamanan aplikasi web. Selain

itu, penelitian ini juga meningkatkan kemampuan analisis, pemrograman, dan pemecahan masalah secara sistematis.

2. Bagi Universitas Hayam Wuruk Perbanas: Penelitian ini dapat menjadi kontribusi dalam pengembangan keilmuan di bidang keamanan siber dan kecerdasan buatan, khususnya dalam lingkungan Program Studi Informatika. Selain itu, hasil penelitian ini juga dapat dijadikan referensi atau bahan ajar bagi dosen dan mahasiswa lain yang tertarik pada topik serupa.
3. Bagi Mitra: Bagi mitra atau pihak yang bekerja dalam pengembangan aplikasi *website*, hasil penelitian ini dapat memberikan gambaran dan solusi terkait sistem keamanan yang adaptif terhadap ancaman siber. Sistem yang dikembangkan dapat dijadikan sebagai prototipe awal untuk implementasi *Web Application Firewall* yang lebih cerdas dan responsif terhadap ancaman nyata.