ABSTRAK

Penelitian ini bertujuan untuk menerapkan metode Random Forest pada Web Application Firewall (WAF) untuk mendeteksi anomali serangan DDoS pada server web. Serangan DDoS (Distributed Denial of Service) merupakan ancaman serius bagi aplikasi web, di mana penyerang berusaha membanjiri server dengan volume trafik yang sangat tinggi sehingga mengganggu kestabilan dan kinerja sistem. Dalam menghadapi ancaman ini, WAF berfungsi sebagai penghalang pertama dengan menganalisis lalu lintas data yang masuk dan memblokir permintaan yang terdeteksi sebagai ancaman. Namun, seiring dengan perkembangan serangan yang semakin kompleks, diperlukan teknologi yang lebih adaptif dalam mendeteksi pola serangan baru, di mana metode machine learning seperti Random Forest menjadi solusi yang potensial.

Metode Random Forest digunakan dalam penelitian ini untuk menganalisis pola-pola anomali dalam lalu lintas web, yang dapat mengindikasikan adanya serangan DDoS. Random Forest merupakan algoritma machine learning berbasis ensemble yang mampu menghasilkan model klasifikasi yang akurat dengan menggabungkan hasil dari banyak pohon keputusan. Dalam penelitian ini, model Random Forest dilatih menggunakan dataset yang berisi data lalu lintas web dengan dua kategori utama, yaitu permintaan normal dan permintaan yang menunjukkan indikasi serangan DDoS. Dengan menggunakan teknik ini, penelitian ini berfokus pada kemampuan Random Forest untuk mendeteksi perbedaan signifikan antara lalu lintas yang sah dan yang mencurigakan, serta menilai efektivitasnya dalam aplikasi WAF untuk mendeteksi serangan secara real-time.

Hasil penelitian menunjukkan bahwa penerapan Random Forest pada WAF memberikan peningkatan yang signifikan dalam mendeteksi dan mencegah serangan DDoS. Akurasi model yang dihasilkan oleh Random Forest sangat tinggi, dengan tingkat deteksi yang lebih baik dibandingkan dengan sistem berbasis aturan tradisional yang sering kali kurang responsif terhadap serangan yang semakin canggih. Penggunaan Random Forest dalam WAF terbukti dapat meningkatkan keamanan aplikasi web dengan memberikan deteksi yang lebih akurat terhadap anomali yang mengindikasikan serangan DDoS, serta mengurangi jumlah false positive yang sering terjadi pada sistem deteksi berbasis aturan. Secara keseluruhan, penelitian ini menunjukkan bahwa metode Random Forest merupakan alat yang efektif untuk memperkuat sistem pertahanan web dalam menghadapi ancaman serangan DDoS.

Kata Kunci: Random Forest, Deteksi DDoS, Trafik Normal, Keamanan Jaringan, Pengujian Model.

ABSTRACT

This research aims to apply the Random Forest method to a Web Application Firewall (WAF) for detecting DDoS attack anomalies on web servers. DDoS (Distributed Denial of Service) attacks pose a significant threat to web applications, where attackers try to overwhelm the server with a high volume of traffic, disrupting the stability and performance of the system. In the face of this threat, WAF acts as the first line of defense by analyzing incoming traffic and blocking requests detected as threats. However, as attacks become more sophisticated, there is a growing need for adaptive technologies to detect new attack patterns, where machine learning methods like Random Forest provide a promising solution.

The Random Forest method is used in this study to analyze anomaly patterns in web traffic that may indicate a DDoS attack. Random Forest is an ensemble machine learning algorithm that creates a robust classification model by combining the outputs of multiple decision trees. In this study, the Random Forest model was trained using a dataset containing both normal web traffic and traffic showing signs of DDoS attacks. This method focuses on the ability of Random Forest to identify significant differences between legitimate and suspicious traffic and evaluates its effectiveness when applied to a WAF for real-time attack detection.

The results of this research show that the application of Random Forest in WAF significantly improves the detection and prevention of DDoS attacks. The accuracy of the model produced by Random Forest is exceptionally high, with detection rates outperforming traditional rule-based systems that are often less responsive to increasingly sophisticated attacks. The use of Random Forest in WAF has been shown to enhance the security of web applications by providing more accurate detection of anomalies indicating a DDoS attack, while reducing the number of false positives that are common in rule-based detection systems. Overall, this study demonstrates that the Random Forest method is an effective tool for strengthening web defense systems against DDoS threats.

Keywords: *Random Forest, DDoS Detection, Normal Traffic, Network Security, Model Evaluation.*