INTISARI

SISTEM DETEKSI SERANGAN *LOW AND SLOW DDOS* MENGGUNAKAN *DEEP LEARNING* PADA *APPLICATION LAYER*

Oleh

Ganjar Muhammad Parikesit

17/409434/PA/17741

Dalam era teknologi informasi yang maju, serangan *Distributed-Denial-of-Service (DDoS)* khususnya *jenis low and slow DDoS*, menjadi ancaman serius terhadap ketersediaan layanan pada website. Penelitian ini mengusulkan penggunaan algoritma *deep learning* untuk mendeteksi *serangan low and slow DDoS* pada *application layer*, sebuah pendekatan yang belum banyak diteliti sebelumnya. Dengan fokus pada analisis log traffic protokol HTTP, penelitian ini mengembangkan sistem berbasis *middleware* yang mampu mengidentifikasi client yang melakukan serangan *low and slow DDoS*. Implementasi sistem ini memungkinkan pembatasan akses terhadap *client* terduga serangan, sehingga meningkatkan ketersediaan layanan.

Melalui penelitian ini, ditemukan bahwa algoritma *deep learning*, khususnya model *Long Short-Term Memory (LSTM)* dengan panjang input 8, menunjukkan kinerja yang sangat baik dengan akurasi deteksi mencapai 99.18% dan waktu prediksi 4.912ms. Hasil ini menunjukkan efektivitas *deep learning* dalam mengenali pola serangan *low and slow DDoS* pada *application layer*. Selain itu, implementasi sistem deteksi yang dikembangkan berhasil mengurangi penggunaan sumber daya CPU dan memori, serta jumlah koneksi aktif, menandakan sistem ini efektif dalam mitigasi dampak *serangan low and slow DDoS* dan meningkatkan kinerja serta keamanan server.

Kata kunci: Serangan *DDoS, Low and slow DDoS,* Algoritma *deep learning, Application layer*

ABSTRACT

DEEP LEARNING-BASED DETECTION SYSTEM FOR SLOW AND LOW DDOS ATTACKS AT THE APPLICATION

by

Ganjar Muhammad Parikesit

17/409434/PA/17741

In the advanced era of information technology, Distributed-Denial-of-Service (DDoS) attacks, especially the low and slow DDoS type, pose a serious threat to the availability of services on websites. This study proposes the use of deep learning algorithms to detect low and slow DDoS attacks at the application layer, an approach that has not been extensively researched previously. Focusing on the analysis of HTTP protocol traffic logs, this research develops a system based on a middleware capable of identifying clients conducting low and slow DDoS attacks. The implementation of this system enables the restriction of access to suspected attacking clients, thereby enhancing service availability.

Through this research, it was found that deep learning algorithms, particularly the Long Short-Term Memory (LSTM) model with an input length of 8, demonstrated excellent performance with a detection accuracy reaching 99.18% and a prediction time of 4.912ms. These results indicate the effectiveness of deep learning in recognizing low and slow DDoS attack patterns at the application layer. Additionally, the implementation of the developed detection system successfully reduced CPU and memory resource usage, as well as the number of active connections, indicating its effectiveness in mitigating the impact of low and slow DDoS attacks and improving server performance and security.

Keyword: DDoS attack, Low and slow DDoS, Deep learning algorithms, Application layer