OPTIMALISASI SISTEM DETEKSI INTRUSI MENGGUNAKAN *MACHINE LEARNING* UNTUK DETEKSI SERANGAN TERDISTRIBUSI PADA SERVER

TESIS

Karya Ilmiah sebagai salah satu syarat untuk menyelesaikan jenjang magister di Departemen Teknik Elektro, Fakultas Teknik, Universitas Andalas

Oleh

Teddy Yuliswar

NIM. 2120952005

Dosen Pembimbing

Prof. Ikhwana Elfitri, Ph.D

NIP. 19750308 200003 1 002

Program Studi Magister

Departemen Teknik Elektro Fakultas Teknik

Universitas Andalas

2025

Judul	Optimalisasi Sistem Deteksi Intrusi Menggunakan *Machine Learning* Untuk Deteksi Serangan Terdistribusi Pada Server	Teddy Yuliswar
Program Studi	Magister Teknik Elektro	2120952005
Fakultas Teknik Universitas Andalas		

ABSTRAK

Peningkatan signifikan penggunaan internet di Indonesia seiring perkembangan teknologi digital turut meningkatkan risiko serangan siber, salah satunya serangan *Distributed Denial of Service (DDoS)* yang kian kompleks dan sulit dideteksi oleh sistem deteksi intrusi (IDS) konvensional. Penelitian ini bertujuan mengoptimalkan sistem deteksi intrusi berbasis algoritma *Decision Tree* melalui teknik seleksi fitur (*feature selection*) dengan memanfaatkan dataset CIC-DDoS2019, guna meningkatkan akurasi dan efisiensi deteksi serangan *DDoS*. Proses penelitian meliputi tahap pra-pemrosesan data, seleksi fitur, pelatihan model *Decision Tree*, serta integrasi notifikasi *real-time* melalui bot Telegram untuk meningkatkan kecepatan respons terhadap serangan. Hasil pengujian menunjukkan bahwa penerapan seleksi fitur secara signifikan meningkatkan akurasi model *Decision Tree* dibanding model tanpa seleksi fitur, sekaligus menurunkan false positive rate. Sistem notifikasi real-time melalui bot Telegram berhasil diimplementasikan, memungkinkan tim keamanan memperoleh informasi serangan secara cepat dan detail. Penelitian ini berkontribusi dalam menghadirkan sistem IDS yang lebih akurat, efisien, dan responsif dalam mendeteksi serangan *DDoS* pada server.

Kata Kunci : *Intrusion Detection System, DDoS, Machine Learning, Decision Tree, Feature Selection, CIC-DDoS2019, Bot Telegram*

Title	*Optimizing Intrusion Detection Systems Using Machine Learning For Distributed Attack Detection On Servers*	*Teddy Yuliswar*
Major	*Master of Electrical Engineering*	*2120952005*
Faculty of Engineering Andalas University		

ABSTRACT

The significant growth of internet usage in Indonesia, alongside digital technology advancements, has increased the risk of cyberattacks, including increasingly complex Distributed Denial of Service (DDoS) attacks that are difficult to detect using conventional Intrusion Detection Systems (IDS). This research aims to optimize an IDS based on the Decision Tree algorithm through feature selection techniques, utilizing the CIC-DDoS2019 dataset to enhance the accuracy and efficiency of DDoS attack detection. The research process involves data preprocessing, feature selection, Decision Tree model training, and the integration of real-time notifications via Telegram bot to improve response times against attacks. Experimental results indicate that applying feature selection significantly improves the Decision Tree model's accuracy compared to models without feature selection, while also reducing the false positive rate. The real-time notification system using Telegram bot was successfully implemented, enabling security teams to receive rapid and detailed attack information. This research contributes to delivering a more accurate, efficient, and responsive IDS for detecting DDoS attacks on servers.

Keywords : *Intrusion Detection System, DDoS, Machine Learning, Decision Tree, Feature Selection, CIC-DDoS2019, Telegram Bot*