INTISARI

SISTEM DETEKSI GANGGUAN JARINGAN PADA EKOSISTEM *INTERNET OF THINGS* DENGAN PENDEKATAN *MACHINE LEARNING*

Oleh

Remarezi Rafsanjani
20/459185/PA/19846

Network Intrusion Detection System (NIDS) merupakan sistem yang berfungsi untuk mendeteksi potensi serangan pada suatu jaringan komputer. Seiring dengan berkembangnya berbagai metode serangan dalam ranah keamanan siber, pengembangan teknik deteksi yang lebih ringan dan efisien menjadi semakin penting.

Penelitian ini berfokus pada pengembangan metode deteksi yang bersifat ringan namun tetap mampu mempertahankan tingkat akurasi yang tinggi, sehingga dapat diimplementasikan pada jaringan *Internet of Things* (IoT) yang umumnya menggunakan perangkat serta infrastruktur dengan keterbatasan sumber daya. Dalam penelitian ini digunakan dataset CSE-CIC-IDS2018 untuk melatih tiga algoritma *machine learning*, yaitu *Decision Tree*, *Random Forest*, dan *K-Nearest Neighbor* (KNN), yang selanjutnya dibandingkan performanya baik pada tahap pelatihan maupun pendeteksian serangan di skenario nyata.

Hasil penelitian menunjukkan bahwa ketiga algoritma memiliki perbedaan dalam waktu komputasi serta performa deteksi. Algoritma *K-Nearest Neighbor* menghasilkan waktu pelatihan tercepat yaitu 3.97 detik, sedangkan waktu pendeteksian tercepat diperoleh dari algoritma *Decision Tree* dengan durasi 1.04 detik. Dari sisi akurasi, algoritma *K-Nearest Neighbor* memberikan hasil pelatihan tertinggi sebesar 98.4%, sedangkan pada proses pendeteksian akurasi tertinggi dicapai oleh algoritma *Random Forest* dengan nilai 99.23%.

Hasil dari penelitian ini menunjukkan bahwa ketiga metode yang digunakan memiliki performa yang efisien dan sesuai untuk ekosistem IoT, khususnya apabila dikembangkan lebih lanjut dalam sistem yang lebih matang dan mudah diimplementasikan.

ABSTRACT

NETWORK INTRUSION DETECTION SYSTEM ON INTERNET OF THINGS ECOSYSTEM USING MACHINE LEARNING APPROACH

By

Remarezi Rafsanjani
20/459185/PA/19846

*A Network Intrusion Detection System (*NIDS*) is designed to detect potential attacks on computer networks. With the continuous emergence of new attack methods in the field of cybersecurity, the development of lighter and more efficient detection techniques has become increasingly important.*

This study focuses on developing a lightweight detection method that is still capable of maintaining high accuracy, making it suitable for implementation in Internet of Things (IoT) *environments, which generally operate under resource-constrained devices and infrastructures. The* CSE-CIC-IDS2018 *dataset was utilized to train three machine learning algorithms, namely Decision Tree, Random Forest, and K-Nearest Neighbor (KNN). The performance of these algorithms was then compared in terms of both training and real-world attack detection.*

The results indicate that the three algorithms differ in computational time and detection performance. The K-Nearest Neighbor algorithm achieved the fastest training time of 3.97 *seconds, while the fastest detection time was obtained by Decision Tree algorithm with* 1.04 *seconds of total detection time. In terms of accuracy, K-Nearest Neighbor achieved the highest training accuracy of* 98.4%, *whereas Random Forest reached the highest detection accuracy with a value of* 99.23%.

The results of this study indicate that the three methods used demonstrate efficient performance and are suitable for IoT *ecosystems, especially when further developed into more mature and user-friendly systems.*