Available *online* at : http://jnte.ft.unand.ac.id/

Jurnal Nasional Teknik Elektro

| ISSN (Print) 2302-2949 | ISSN (Online) 2407-7267 |

A B S T R A C T

The utilization of intrusion detection systems (IDS) holds the potential to significantly enhance the security of IT infrastructure. To improve the capabilities of IDS, Machine Learning (ML) methods have emerged as a promising approach. The primary objective of an IDS is to detect various types of malicious intrusions with a high detection rate while minimizing false alarms, surpassing the capabilities of a firewall. However, developing an IDS for IOT poses substantial challenges due to the massive volume of data that needs to be processed. To address this, an optimal approach is required to improve the accuracy of data containing numerous attacks. In this study, we propose a novel IDS model that employs the Random Forest, Decision Tree, and Logistic Regression algorithms, using a specialized ML technique known as Ensemble Learning. For this research, we used the BoT-IoT datasets as inputs for the IDS model to distinguish between malicious and benign network traffic. To determine the best model, we compared the performance metrics of each algorithm across different parameter combinations. The research findings demonstrate exceptional performance, with metric scores exceeding 99.995% for all parameter combinations. Based on these conclusive results, we deduce that the proposed model not only achieves remarkable success but also outperforms other traditional ML-based IDS models in terms of performance metrics. These outcomes highlight the potential of our novel IDS model to significantly enhance the security posture of IoT-based systems.

https://doi.org/10.25077/xxxxx