Efektifitas Sistem Deteksi Intrusi Berbasis Anomali Dalam Penanganan Zero-Day Attack Menggunakan Metode AdaBoost, J48, dan Random Forest

Nurul Fauzi[1], Fazmah Arif Yulianto[2], Hilal Hudan Nuha[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]nurulfauzi@students.telkomuniversity.ac.id, [2]fazmaharif@telkomuniversity.ac.id,
[3]hilalnuha@telkomuniversity.ac.id

Abstract

An intrusion detection system (IDS) is a crucial software or hardware application that employs security mechanisms to identify suspicious activity in a system or network. According to the detection technique, IDS is divided into two, namely signature-based and anomaly-based. Signature-based is said to be incapable of handling zero-day attacks, while anomaly-based is able to handle it. Machine learning techniques play a vital role in the development of IDS. There are differences of opinion regarding the most optimal algorithm for IDS classification in several previous studies, such as Random Forest, J48, and AdaBoost. Therefore, this study aims to evaluate the performance of the three algorithm models, using the NSL-KDD and UNSW-NB15 datasets used in previous studies. Empirical results demonstrate that utilizing AdaBoost+J48 with NSL-KDD achieves an accuracy of 99.86%, along with precision, recall, and f1-score rates of 99.9%. These results surpass previous studies using AdaBoost+Random Tree, with an accuracy of 98.45%. Furthermore, this research explores the effectiveness of anomaly-based systems in dealing with zero-day attacks. Remarkably, the results show that anomaly-based systems perform admirably in such scenarios. For instance, employing Random Forest with the UNSW-NB15 dataset yielded the highest performance, with an accuracy rating of 99.81%.

Keywords: IDS, Random Forest, J48, AdaBoost