ABSTRAK

Deteksi intrusi jaringan merupakan aspek penting dalam sistem informasi modern, terutama dengan meningkatnya penggunaan perangkat *Internet of Things* (*IoT*) yang rawan terhadap serangan siber. Penelitian ini bertujuan mengembangkan aplikasi PCAP *Analyzer* berbasis web (REST API) menggunakan pendekatan rekayasa perangkat lunak dan eksperimen kuantitatif, dengan integrasi model *Machine Learning* bertipe *ensemble* untuk klasifikasi otomatis *file packet capture* (PCAP). *Dataset* yang digunakan adalah CICIDS2018 yang merepresentasikan lalu lintas jaringan realistis dan berbagai tipe serangan. Tiga algoritma *ensemble* yang dilatih yaitu *Random Forest*, *AdaBoost*, dan *Gradient Boosting*, dengan tahapan praproses data yang menggunakan hasil dari *Exploratory Data Analysis* (EDA) secara intensif untuk dijadikan sebagai pedoman untuk melakukan teknik *feature engineering* seperti *log-transformation*, korelasi fitur, dan transformasi fitur kualitatif melalui *one-hot encoding*. Hasil evaluasi menunjukkan bahwa *Random Forest* mencapai akurasi tertinggi sebesar 99,76% dengan *macro average Precision*, *Recall*, dan *F1-score* masing-masing 98,22%, 98,55%, dan 98,39%, diikuti oleh *Gradient Boosting* dengan akurasi 99,55%, serta *AdaBoost* dengan akurasi 97,46% namun performa metrik *macro-avg* yang lebih rendah dikarenakan model *AdaBoost* gagal dalam mengklasifikasikan serangan *DoS*. Seluruh model diintegrasikan ke dalam aplikasi REST API yang ditulis menggunakan *FastAPI*, untuk melakukan konversi, aplikasi akan memanggil aplikasi berbasis terminal bernama *CICFlowMeter-v3* untuk kemudian diberikan ke model untuk diklasifikasi. Riset ini berkontribusi dalam penerapan *Machine Learning* untuk forensik digital dan investigasi serangan siber di jaringan *IoT*.

Kata Kunci : *PCAP Analyzer*, REST API, *Ensemble Machine Learning*, *CICFlowMeter-v3*, CICIDS2018

ABSTRACT

Network intrusion detection is a critical aspect of modern information systems, especially with the growing adoption of Internet of Things (IoT) devices that are highly vulnerable to cyberattacks. This research aims to develop a web-based (REST API) PCAP Analyzer application using a software engineering methodology with a quantitative experimental approach, integrating ensemble-based Machine Learning models to automatically classify packet capture (PCAP) files. The dataset used is CICIDS2018, which contains realistic network traffic representing various types of attacks. Three ensemble algorithms are trained, they are Random Forest, AdaBoost, and Gradient Boosting alongside a data preprocessor steps that heavily use the result of Exploratory Data Analysis (EDA) intensively as a base to do feature engineering techniques such as log-scaling, feature correlation analysis, and categorical transformation using one-hot encoding. Evaluation results on the validation dataset show that the Random Forest model achieved the highest accuracy at 99.76%, with macro averages for Precision, Recall, and F1-score of 98.22%, 98.55%, and 98.39%, respectively. Gradient Boosting followed with 99.55% accuracy, while AdaBoost reached 97.46%. However, AdaBoost failed to classify the DoS attack class, as the macro-avg metric is low, that is 65.58%. All models were integrated into a REST API built with FastAPI to enable automated analysis or classification of PCAP files. For the application to be able to convert PCAP file, it needs to call a terminal based application named CICFlowMeter-v3, the converted file then goes to the trained model to be classified. This research contributes to an application of Machine Learning in digital forensic and IoT network investigation.

Keywords : *PCAP Analyzer, REST API, Ensemble Machine Learning, CICFlowMeter-v3, CICIDS2018*