# ABSTRAK

Serangan terhadap jaringan komputer terus meningkat dan berpotensi menyebabkan kebocoran data serta kerugian besar. Intrusion Detection System (IDS) dikembangkan untuk mendeteksi ancaman ini, namun IDS konvensional masih menghadapi kendala berupa tingginya *false positive* dan *false negative*. Hal ini diperparah oleh ketidakseimbangan kelas pada *dataset* lalu lintas jaringan, seperti pada CIC-IDS2017, yang menyebabkan model sulit mengenali pola serangan minoritas. Penelitian ini bertujuan mengembangkan sistem deteksi intrusi menggunakan algoritma XGBoost yang dioptimasi dengan SMOTE untuk meningkatkan akurasi deteksi, khususnya dalam menurunkan tingkat kesalahan deteksi.

Metode yang digunakan dalam penelitian ini adalah pendekatan eksperimental. *Dataset* CIC-IDS2017 diproses melalui beberapa tahap, yaitu pembersihan data, pemetaan ulang label serangan, pembagian data latih dan uji dengan variasi proporsi, serta penyeimbangan data menggunakan SMOTE. Reduksi dimensi dilakukan dengan Principal Component Analysis (PCA) untuk meningkatkan efisiensi. Model dibangun menggunakan algoritma XGBoost dengan penyesuaian parameter dan *tuning* nilai k pada SMOTE. Evaluasi performa dilakukan berdasarkan metrik *precision, recall, f1-score,* AUPRC, FPR, dan FNR.

Hasil menunjukkan bahwa penerapan SMOTE mampu menurunkan nilai *false negative rate* dari 42,11% menjadi 1,82% pada data uji. Meskipun terjadi peningkatan *false positive,* model dengan parameter SMOTE terbaik (k = 3) dan proporsi data uji 30% menghasilkan dapat menekan tingkat *false positive* menjadi 4,13%. Penelitian ini menyimpulkan XGBoost yang dioptimasi dengan SMOTE memberikan solusi yang efektif untuk mengurangi *false negative*, terutama dalam menghadapi masalah ketidakseimbangan kelas dalam deteksi intrusi.



**Kata Kunci:** XGBoost, SMOTE, CIC-IDS2017, *False Negative, False Positive.*

## ABSTRACT

*Attacks on computer networks are increasing and have the potential to cause data leakage and huge losses. Intrusion Detection Systems (IDS) were developed to detect these threats, but conventional IDSs still face obstacles in the form of high false positives and false negatives. This is exacerbated by class imbalance in network traffic datasets, such as in CIC-IDS2017, which makes it difficult for models to recognize minority attack patterns. This research aims to develop an intrusion detection system using the XGBoost algorithm optimized with SMOTE to improve detection accuracy, especially in reducing the detection error rate.*

*The method used in this research is an experimental approach. The CIC-IDS2017 dataset is processed through several stages, namely data cleaning, re-mapping of attack labels, division of training and test data with varying proportions, and data balancing using SMOTE. Dimensionality reduction is performed with Principal Component Analysis (PCA) to improve efficiency. The model is built using XGBoost algorithm with parameter adjustment and tuning of k value in SMOTE. Performance evaluation was conducted based on precision, recall, f1-score, AUPRC, FPR, and FNR metrics.*

*The results show that the application of SMOTE can reduce the false negative rate from 42.11% to 1.82% on the test data. Despite the increase in false positives, the model with the best SMOTE parameters (k = 3) and 30% test data proportion resulted in reducing the false positive rate to 4.13%. This study concludes that XGBoost optimized with SMOTE provides an effective solution to reduce false negatives, especially in dealing with the problem of class imbalance in intrusion detection.*



***Keywords:*** *XGBoost, SMOTE, CIC-IDS2017, False Negative, False Positive.*