ABSTRAK

Insider attack merupakan ancaman keamanan yang sulit dideteksi karena pelaku memiliki akses sah terhadap sistem organisasi, sehingga aktivitasnya menyerupai perilaku pengguna normal. Meskipun sejumlah penelitian telah menerapkan *machine learning* pada deteksi *insider threat*, optimasi *hyperparameter* secara sistematis menggunakan *Grid Search* yang dikombinasikan dengan SMOTE pada *multiple* versi CERT dataset, serta evaluasi kemampuan generalisasi lintas versi, masih belum banyak dieksplorasi secara komprehensif.

Penelitian ini mengusulkan model deteksi *insider threat* berbasis algoritma *Extreme Gradient Boosting* (XGBoost) dengan optimasi *hyperparameter Grid Search* dan penanganan ketidakseimbangan kelas menggunakan SMOTE. Sebanyak 13 fitur perilaku pengguna diekstraksi dari enam sumber log aktivitas pada CERT *Insider Threat Dataset* versi r4.2, r5.2, dan r6.2, yang merepresentasikan skenario ketidakseimbangan kelas dengan rasio hingga 800:1. Model dilatih menggunakan skema *Stratified 3-Fold Cross-Validation* dengan optimasi tujuh *hyperparameter* utama XGBoost, dan dievaluasi menggunakan metrik *precision*, *recall*, *F1-Score*, dan AUC-ROC.

Hasil pengujian menunjukkan bahwa XGBoost dengan SMOTE mencapai *F1-Score* 0.9655 dan AUC-ROC 0.9992 pada r4.2, serta F1-Score 0.9000 dan AUC-ROC 0.9964 pada r5.2, membuktikan efektivitas penanganan ketidakseimbangan kelas melalui peningkatan *recall*. Pada r6.2 dengan ketidakseimbangan ekstrem, model gagal menghasilkan prediksi positif pada *threshold default* (F1=0.0000) meskipun AUC-ROC mencapai 0.9725, yang mengindikasikan isu kalibrasi probabilitas bukan kegagalan pembelajaran. Evaluasi lintas versi mengungkapkan degradasi performa yang signifikan, menunjukkan sensitivitas model terhadap *distributional shift*. Temuan ini mengindikasikan bahwa XGBoost dengan SMOTE efektif pada lingkungan distribusi statis, namun memerlukan mekanisme *threshold* adaptif dan strategi *domain adaptation* untuk penerapan pada lingkungan deteksi *insider threat* yang dinamis.

Kata Kunci: Deteksi *Insider Attack*, XGBoost, SMOTE, Optimasi *Hyperparameter, Grid Search,* CERT *Dataset,* Analisis Perilaku, Klasifikasi Tidak Seimbang

ABSTRACT

Insider attacks constitute a security threat that is difficult to detect because perpetrators possess legitimate access to organizational systems, causing their activities to resemble normal user behavior. Although numerous studies have applied machine learning techniques to insider threat detection, systematic hyperparameter optimization using Grid Search combined with SMOTE across multiple versions of the CERT dataset, as well as the evaluation of cross-version generalization capability, remains insufficiently explored in a comprehensive manner.

This study proposes an insider threat detection model based on the Extreme Gradient Boosting (XGBoost) algorithm, incorporating Grid Search hyperparameter optimization and Synthetic Minority Oversampling Technique (SMOTE) to address class imbalance. A total of 13 behavioral features were extracted from six activity log sources in the CERT Insider Threat Dataset versions r4.2, r5.2, and r6.2, representing class imbalance scenarios with ratios of up to 800:1. The model was trained using a Stratified 3-Fold Cross-Validation scheme with optimization of seven key XGBoost hyperparameters and evaluated using precision, recall, F1-score, and AUC-ROC metrics.

The experimental results demonstrate that XGBoost combined with SMOTE achieved an F1-score of 0.9655 and an AUC-ROC of 0.9992 on r4.2, as well as an F1-score of 0.9000 and an AUC-ROC of 0.9964 on r5.2, indicating the effectiveness of class imbalance handling through improved recall. Under the extreme imbalance condition of r6.2, the model failed to generate positive predictions at the default threshold (F1 = 0.0000), despite achieving an AUC-ROC of 0.9725, suggesting a probability calibration issue rather than a learning failure. Cross-version evaluation revealed significant performance degradation, indicating the model's sensitivity to distributional shift. These findings suggest that XGBoost with SMOTE is effective in static distribution environments; however, adaptive threshold mechanisms and domain adaptation strategies are required for deployment in dynamic insider threat detection environments.

Keywords: *Insider Threat Detection, XGBoost, SMOTE, Hyperparameter Optimization, Grid Search, CERT Dataset, Behavioral Analytics, Imbalanced Classification*