ABSTRAK

Penggunaan enkripsi secara luas pada komunikasi internet menyebabkan isi paket jaringan tidak dapat dianalisis secara langsung, sehingga klasifikasi lalu lintas jaringan menjadi semakin kompleks. Permasalahan ini semakin menantang pada aliran trafik berdurasi pendek (*short flow*) karena proses normalisasi memerlukan *zero-padding* yang berpotensi menurunkan kualitas representasi data. Permasalahan penelitian ini adalah belum diketahuinya pengaruh penggunaan data sintetik yang dihasilkan oleh Conditional Generative Adversarial Network (cGAN) sebagai augmentasi terhadap kinerja Convolutional Neural Network (CNN) dalam mengklasifikasikan lalu lintas jaringan terenkripsi pada kondisi *short flow*.

Penelitian menggunakan *dataset* publik USTC-TFC2016 yang terdiri atas 20 kelas, yaitu 10 kelas *benign* dan 10 kelas *malware*. Data diperoleh dari sumber publik, kemudian diekstraksi menjadi *session*, dinormalisasi berdasarkan panjang *session*, dan dikonversi menjadi citra *grayscale* berukuran 28×28 piksel. Model cGAN dilatih secara kondisional berdasarkan label kelas dan menghasilkan 150.000 citra sintetik. Data tersebut digunakan dalam lima skenario augmentasi, yaitu 0, 1.000, 1.500, 3.000, dan 7.500 citra per kelas. Setiap skenario digunakan untuk melatih dan menguji model CNN. Kinerja model dievaluasi menggunakan *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix*. Metode SHAP diterapkan untuk menginterpretasikan kontribusi piksel terhadap keputusan model. Pengembangan sistem dilakukan menggunakan metode *prototyping* serta dilengkapi antarmuka web sebagai sarana demonstrasi inference.

Hasil pengujian menunjukkan bahwa cGAN mampu menghasilkan citra sintetik secara terkontrol berdasarkan kelas, tetapi augmentasi belum mampu melampaui kinerja model *baseline*. Pada klasifikasi *benign*, *baseline* mencapai *accuracy* 94,790% dan *macro F1-score* 95,367%, sedangkan model augmented terbaik dengan 3.000 citra per kelas mencapai *accuracy* 94,768% dan *macro F1-score* 95,348%. Pada klasifikasi *malware*, *baseline* mencapai *accuracy* 97,892% dan *macro F1-score* 97,890%, sedangkan model *augmented* terbaik dengan 1.000 citra per kelas mencapai *accuracy* 97,740% dan *macro F1-score* 97,747%. Hasil tersebut menunjukkan bahwa pengaruh augmentasi tidak bersifat linear dan tidak selalu meningkatkan kinerja klasifikasi. Efektivitasnya bergantung pada kualitas, keragaman, dan kesesuaian distribusi data sintetik terhadap data asli. Penelitian ini memberikan evaluasi empiris penggunaan cGAN untuk augmentasi trafik terenkripsi, dilengkapi analisis SHAP dan antarmuka web untuk demonstrasi klasifikasi.

Kata Kunci: lalu lintas terenkripsi, *Conditional* GAN, CNN, augmentasi data sintetik, SHAP.

ABSTRACT

The widespread use of encryption in internet communications makes network packet contents inaccessible for direct analysis, thereby increasing the complexity of network traffic classification. This challenge becomes more significant in short-duration traffic flows (short flows) because normalization requires zero-padding, which may reduce data representation quality. This study evaluated the effect of synthetic data generated by a Conditional Generative Adversarial Network (cGAN) as an augmentation method on the performance of a Convolutional Neural Network (CNN) in classifying encrypted network traffic under short-flow conditions.

The study used the public USTC-TFC2016 dataset, which consists of 20 classes: 10 benign and 10 malware classes. The data were acquired from a public source, extracted into sessions, normalized according to session length, and converted into 28×28-pixel grayscale images. The cGAN was conditionally trained using class labels and generated 150,000 synthetic images. These images were applied through five augmentation scenarios: 0, 1,000, 1,500, 3,000, and 7,500 images per class. Each scenario was used to train and test the CNN. Performance was evaluated using accuracy, precision, recall, F1-score, and confusion matrix. SHAP was applied to interpret pixel contributions to model decisions. The system was developed using the prototyping method and included a web interface for inference demonstrations.

The results showed that the cGAN generated class-controlled synthetic images, but augmentation did not outperform the baseline models. For benign classification, the baseline achieved 94.790% accuracy and a 95.367% macro F1-score, whereas the best augmented model with 3,000 images per class achieved 94.768% accuracy and a 95.348% macro F1-score. For malware classification, the baseline achieved 97.892% accuracy and a 97.890% macro F1-score, whereas the best augmented model with 1,000 images per class achieved 97.740% accuracy and a 97.747% macro F1-score. The results indicate that augmentation is not linear and does not necessarily improve classification performance. Its effectiveness depends on the quality, diversity, and distributional similarity of synthetic data to original data. This study provides an empirical evaluation of cGAN-based augmentation for encrypted traffic classification, supported by SHAP analysis and a web interface for classification demonstrations.

Keywords: *encrypted network traffic, Conditional GAN, CNN, synthetic data augmentation, SHAP.*