Modifikasi arsitektur Deep Convolutional Generative Adversarial Network (DCGAN) untuk oversampling data tabel serta pengaruhnya terhadap performa deteksi Anomaly-Based Network Intrusion Detection System (ANIDS) = Modification of Deep Convolutional Generative Adversarial Network (DCGAN) architecture for tabular data oversampling and its effect on Anomaly-Based Network Intrusion Detection System (ANIDS) detection performance

Hada Melino Muhammad, author

Abstrak

Anomaly-Based Network Intrusion Detection System (ANIDS) memegang peranan yang sangat penting dengan berkembangnya teknologi internet. ANIDS digunakan untuk mendeteksi trafik jaringan yang membahayakan pengguna internet. Metode tradisional yang digunakan untuk membuat ANIDS masih sulit untuk mengekstrak fitur dari trafik yang banyak dan berdimensi tinggi. Selain itu, jumlah sampel yang sedikit pada beberapa jenis trafik menyebabkan ketidakseimbangan dataset dan mempengaruhi performa deteksi ANIDS. Ketidakseimbangan dataset dapat diatasi dengan oversampling dan atau undersampling. Penulis mengusulkan metode oversampling menggunakan modifikasi dari Deep Convolutional Generative Adversarial Network (DCGAN) yang dapat mengekstrak fitur trafik data secara langsung dan menghasilkan sampel baru untuk menyeimbangkan dataset. Modifikasi DCGAN bertujuan untuk menghindari adanya pemetaan data tabular menjadi data gambar sebelum masuk ke DCGAN. Selain itu, modifikasi DCGAN bertujuan untuk menstabilkan pelatihan model untuk data tabular sehingga data yang dihasilkan lebih berkualitas. Pengujian efek modifikasi DCGAN dilakukan dengan melatih model ANIDS yang terdiri dari model Deep Neural Network (DNN) dan Convolutional Neural Network (CNN). Evaluasi performa deteksi dilakukan dengan confusion matrix serta metrik accuracy, precision, recall, dan F1-Score. Hasil yang didapatkan adalah oversampling menggunakan modifikasi DCGAN meningkatkan validation accuracy dari 75.77% menjadi 81.41% pada model DNN dan 73.94% menjadi 80.76% pada model CNN. Peningkatan metrik lain juga terjadi akibat dari peningkatan validation accuracy.
.....Anomaly-Based Network Intrusion Detection System (ANIDS) plays a very important role with the development of internet technology. ANIDS is used for detecting network traffic that endangers internet users. The traditional methods used to create ANIDS are still difficult to extract features from high-dimensional traffic. In addition, the small number of samples in some types of traffic causes imbalanced dataset and affects ANIDS detection performance. Imbalanced dataset can be overcome by oversampling and or undersampling. The author proposes an oversampling method using a modification of the Deep Convolutional Generative Adversarial Network (DCGAN) which can extract data traffic features directly and generate new samples to balance the dataset. DCGAN modification aims to avoid mapping tabular data into image data before entering DCGAN. In addition, the DCGAN modification aims to stabilize the training model for tabular data so that the resulting data is of higher quality. Testing the effects of the DCGAN modification was carried out by training the ANIDS model consisting of the Deep Neural Network (DNN) and Convolutional Neural Network (CNN) models. Evaluation of detection performance is carried out using a confusion matrix and the metrics of accuracy, precision, recall, and F1-Score. The results

obtained are oversampling using the DCGAN modification increases the validation accuracy from 75.77% to 81.41% in the DNN model and 73.94% to 80.76% in the CNN model. Improvements in other metrics also occurred as a result of the increase in validation accuracy.