Rancang Bangun Algoritma Machine Learning Menggunakan Arsitektur Autoencoder Untuk Reduksi Dimensi Serta Pengaruhnya Terhadap Performa Deteksi Intrusion Detection System (IDS) = Development of Machine Learning Algorithm Using Autoencoder Architecture for Dimensionality Reduction and Its Impact on Intrusion Detection System (IDS) Performance

Muhammad Wafiyulloh, author

Abstrak

Serangan jaringan semakin beragam seiring berkembangnya internet. Dalam menghadapi serangan-serangan tersebut, diperlukan juga pengembangan sistem keamanan internet terhadap pengguna salah satunya adalah IDS. Intrusion detection system (IDS) merupakan sistem keamanan dalam mengawasi aktivitas jaringan yang berbahaya bagi pengguna. Metode yang umum digunakan yaitu signature-based IDS. Signature-based IDS menggunakan daftar serangan siber yang diketahui dalam menentukan jaringan berbahaya atau normal. Akan tetapi, IDS hanya mengetahui serangan yang diketahui saja dan membutuhkan input secara manual untuk mengubah daftar serangan sehingga tidak efektif dalam mengatasi serangan yang tidak ketahui. Oleh karena itu, penelitian ini berfokus pada pengembangan IDS dengan pendekatan machine learning menggunakan model autoencoder untuk reduksi dimensi dan pengaruhnya terhadap model IDS. Autoencoder yang digunakan pada penelitian ini terdapat 2 model yaitu non-symmetric deep autoencoder (NDAE) dan modifikasi dari NDAE menggunakan metode variational autoencoder (VAE) yang disebut sebagai V-NDAE, serta model PCA. Modifikasi NDAE bertujuan untuk mengambil informasi penting dengan menggunakan distribusi probabilistik sehingga menjadi data yang berkualitas untuk pelatihan model IDS. Pengujian reduksi dimensi dari model-model ini dilakukan dengan melatih model IDS yaitu model random forest. Penelitian ini dilakukan pada 2 dataset yang berbeda yaitu dataset CICIDS2017 dan dataset dari simulasi serangan jaringan. Metrik yang digunakan adalah metrik accuracy, precision, recall, F-1 score, ROC curve. Berdasarkan pengujian yang telah dilakukan terhadap dataset CICIDS2017, model NDAE memiliki nilai rata-rata akurasi validasi sebesar 90.85% sehingga memiliki nilai yang lebih besar daripada model V-NDAE yang memiliki nilai rata-rata akurasi validasi sebesar 87.65%. Pelatihan model NDAE menggunakan hyperparameter yang paling optimal yaitu dengan optimizer RMSProp dan batch size sebesar 128. Pada pengujian terhadap dataset dari simulasi serangan jaringan, model NDAE memiliki performa yang lebih baik daripada model V-NDAE dan model PCA. Model NDAE memiliki nilai rata-rata akurasi validasi sebesar 94.66% dan model V-NDAE memiliki nilai rata-rata akurasi validasi sebesar 66.32%. Pelatihan model NDAE menggunakan hyperparameter yang paling optimal yaitu dengan optimizer Adam dan batch size sebesar 32.

.....The variety of network attacks increases as the internet evolves. In dealing with these attacks, the development of an internet security system for users is necessary, one of which is IDS.

An intrusion detection system (IDS) is a security system designed to monitor network activity that is dangerous for users. The commonly used method is signature-based IDS. Signature-based IDS uses a signature database of known cyber attacks to determine whether a network is dangerous or normal. However, this IDS only recognizes known attacks and requires manual input to change the signature database of attacks, making it ineffective in dealing with unknown attacks. Therefore, this research focuses on developing an IDS using a machine learning approach, specifically using an autoencoder model for dimensionality reduction and its impact on the IDS model. The models used in this research consists of a non-symmetric deep autoencoder (NDAE), modification of NDAE using the variational autoencoder (VAE) method, and PCA model. The modified NDAE can capture important information from the latent distribution, which helps stabilize the training of the model. Dimensionality reduction testing for both models is performed by training an IDS model, specifically a random forest model. This research is conducted on two different datasets: the CICIDS2017 dataset and a dataset from network attack simulations. The evaluation metrics used are accuracy, precision, recall, F-1 score, and ROC curve. Based on the testing performed on the CICIDS2017 dataset, the NDAE model achieves an average validation accuracy of 90.85%, which is higher than the average validation accuracy of 87.65% for the V-NDAE model and PCA model. The NDAE model's training is done using the most optimal hyperparameters, specifically the RMSProp optimizer and a batch size of 128. In the testing on the dataset from network attack simulations, the NDAE model outperforms the V-NDAE model and PCA model. The NDAE model achieves an average validation accuracy of 94.66%, while the V-NDAE model achieves an average validation accuracy of 66.32%. The NDAE model's training is done using the most optimal hyperparameters, specifically the Adam optimizer and a batch size of 32.