

INTISARI

DETEKSI INTRUSI PADA JARINGAN MENGGUNAKAN *ENCODER DAN K-NEAREST NEIGHBOR(KNN)*

Sarah Anjani

22/501675/PPA/06394

Jaringan komputer merupakan salah satu komponen sistem informasi yang banyak digunakan saat ini. Penggunaan jaringan komputer semakin populer mengakibatkan meningkatnya risiko dan gangguan (Intrusi) pada penggunaan jaringan tersebut dan keamanan jaringan menurun. Penelitian ini bertujuan untuk mendeteksi intrusi pada jaringan dengan menggunakan *Encoder* dan *K-Nearest Neighbor* (KNN). *Dataset* yang digunakan untuk membangun model deteksi intrusi adalah dataset yang di ambil dari *archive.ics.uci.edu* yang berisi data jaringan normal dan jaringan anomaly yang berjumlah total lebih dari 494.021 data. *Encoder* merupakan salah satu layer pada *Autoencoder* yang digunakan untuk menghasilkan dimensi data yang lebih rendah, dimana diterapkan fungsi aktivasi pada setiap *layers* tersebut. Kemudian, fitur laten yang dihasilkan dari *Encoder* tersebut digunakan sebagai *input* klasifikasi KNN. Klasifikasi KNN dilakukan dengan menghitung jarak data dengan menggunakan rumus *Euclidean distance*, kemudian memilih *K* tetangga terdekat, menghitung frekuensi kelas dan langkah terakhir menentukan label mayoritas dari data tersebut. Untuk evaluasi model deteksi ini akan menggunakan ukuran kinerja model yaitu *accuracy*, *precision*, *recall*, dan *f1-score*. Berdasarkan penelitian yang dilakukan, model yang diusulkan mendapatkan hasil akurasi sebesar 0.99 (99%), *precision* 0.99 (99%), *recall* 0.99 (99%) dan *f1-score* 0.99 (99%) dengan waktu komputasi paling cepat dibandingkan dengan model perbandingan lainnya. Hasil dari penelitian ini menunjukkan bahwa model *Encoder* dan KNN yang diusulkan dapat secara efektif dan efisien dalam mendeteksi intrusi pada jaringan.

Kata Kunci: intrusi jaringan, deteksi intrusi, *Encoder*, *Autoencoder*, KNN

ABSTRACT

INTRUSION DETECTION ON THE NETWORK USING ENCODER AND K-NEAREST NEIGHBOR (KNN)

Sarah Anjani

22/501675/PPA/06394

Computer networks are one of the components of information systems that are widely used today. The increasingly popular use of computer networks results in increased risks and interference (Intrusion) in the use of these networks and decreased network security. This research aims to detect intrusion on the network using Encoder and K-Nearest Neighbor (KNN). The dataset used to build the intrusion detection model is a dataset taken from archive.ics.uci.edu which contains normal network and anomaly network data totaling more than 494,021 data. The encoder is one of the layers in the Autoencoder which is used to produce lower dimensional data, where an activation function is applied to each layer. Then, the latent features generated from the Encoder are used as input for KNN classification. KNN classification is carried out by calculating the distance of the data using the Euclidean distance formula, then selecting the K nearest neighbors, calculating the class frequency and the final step determining the majority label of the data. To evaluate this detection model, we will use model performance measures, namely accuracy, precision, recall and f1-score. Based on research conducted, the proposed model obtained accuracy results of 0.99 (99%), precision 0.99 (99%), recall 0.99 (99%) and f1-score 0.99 (99%) with the fastest computing time compared to other comparison models. The results of this research show that the proposed Encoder and KNN models can effectively and efficiently detect intrusions on the network.

Keywords: network intrusion, intrusion detection, Encoder, Autoencoder, KNN