Penerapan Data Mining Untuk Klasifikasi Intrusi Melalui Jaringan Internet: Studi Kasus Badan Meteorologi Klimatologi Dan Geofisika = Application of Data Mining for Intrusion Classification through the Internet Network: Case Study of Meteorology Climatology and Geophysics Agency

Bima Tri Ariyanto, author

Abstrak

Aktivitas anomali pada jaringan internet BMKG belum seluruhnya dapat dianalisis secara manual, sehingga beberapa sistem BMKG terdampak oleh aktivitas siber ini. Deteksi dan klasifikasi intrusi merupakan upaya penting yang dapat dilakukan BMKG dalam menangani serangan siber. Penelitian ini bertujuan untuk membuat model klasifikasi terbaik untuk mengklasifikasikan intrusi. Dataset yang digunakan adalah dataset CICIDS2017 dan data internet BMKG yang kemudian dilakukan penanganan data tidak seimbang menggunakan SMOTE. Untuk meningkatkan performa klasifikasi, dilakukan seleksi fitur dan diusulkan tiga variasi jumlah fitur, yaitu 7 fitur, 18 fitur, dan 82 atau keseluruhan fitur. Klasifikasi yang dilakukan mencakup klasifikasi biner untuk membedakan serangan dan normal, serta multikelas untuk mengklasifikasikan beberapa jenis serangan. Algoritma klasifikasi yang digunakan dalam penelitian ini adalah KNearest Neighbor (KNN), Decision Tree (DT), dan Random Forest (RF). Hasil model klasifikasi terbaik untuk kelas biner adalah DT dengan 82 atau keseluruhan fitur dengan akurasi 99,1%. Sedangkan model terbaik untuk multikelas adalah DT dengan 82 atau keseluruhan fitur dengan akurasi 99,2%. Penelitian ini menunjukkan bahwa model klasifikasi berbasis pembelajaran mesin dapat meningkatkan deteksi dan klasifikasi serangan siber dengan akurasi tinggi. BMKG dapat mengimplementasikan model ini untuk deteksi otomatis dan respons cepat terhadap ancaman, melakukan uji coba lapangan, memberikan pelatihan staf, dan memastikan pemeliharaan serta pemantauan rutin model. Langkah-langkah ini dapat membantu BMKG dalam meningkatkan keamanan jaringan dan melindungi data serta layanan dari serangan siber di masa mendatang.

..... Anomalous activity on the BMKG's internet network cannot be fully analyzed manually, so several BMKG systems have been affected by this cyber activity. Intrusion detection and classification is an important effort that can be made by BMKG in dealing with cyber attacks. This research aims to create the best classification model to classify intrusions. The datasets used are the CICIDS2017 dataset and BMKG internet data, which are then handled with unbalanced data using SMOTE. To improve classification performance, feature selection is performed, and three variations in the number of features are proposed, namely 7 features, 18 features, and 82 or all features. The classification includes binary classification to distinguish between normal and attack and multiclass classification to classify multiple types of attacks. The classification algorithms used in this research are K-Nearest Neighbor (KNN), Decision Tree (DT), and Random Forest (RF). The best classification model for binary classes is DT with 82 or all features with 99.1% accuracy. While the best model for multiclass is DT with 82 or all features with 99.2% accuracy. This research shows that a machine learning-based classification model can improve cyberattack detection and classification with high accuracy. BMKG can implement this model for automated detection and rapid response to threats, conduct field trials, provide staff training, and ensure regular model maintenance and

monitoring. These steps can help BMKG improve network security and protect data and services from future cyberattacks.