Klasifikasi Jenis Cyber-attack pada Jaringan Wi-Fi dan Internet of Things Menggunakan Metode Decision Tree dengan Reduced Error Pruning = Classification of Cyber-attack Types on Wi-Fi Networks and the Internet of Things Using the Decision Tree Method with Reduced Error Pruning

Daniel Roberto, author

Abstrak

Tren cyber-attack atau serangan siber terus bertambah banyak setiap tahunnya. Menurut data dari patrolisiber.id, terdapat 61 laporan penipuan melalui e-mail dengan jumlah kerugian mencapai lebih dari 144 miliar rupiah dan merupakan modus penipuan dengan kerugian terbesar pada tahun 2019. Teknik machine learning telah diadaptasi pada algoritma deteksi dalam Intrusion Detection System (IDS) sebagai perangkat untuk memeriksa semua traffic jaringan karena dapat membawa manfaat dalam pengembangan performanya yang berskala besar dalam meningkatkan detection rate dan pengurangan processing time. Salah satu metode machine learning pada IDS adalah decision tree, yaitu metode yang dapat bekerja dengan cepat, menghasilkan akurasi yang baik, dan mudah untuk diinterpretasi. Penelitian ini bertujuan untuk melakukan klasifikasi jenis serangan cyber-attack terhadap jaringan Wi-Fi dan Internet of Things melalui penerapan teknik machine learning dengan metode decision tree. Untuk menghindari overfitting pada model, akan digunakan teknik lanjutan yaitu post-pruning dengan menggunakan algoritma reduced error pruning. Hasil yang diperoleh dari penelitian ini adalah pengembangan performa model decision tree setelah dilakukan metode reduced error pruning dibanding model yang tidak dilakukan pruning. Evaluasi kinerja model yang sudah dilakukan pruning dengan ukuran nilai metrik accuracy, F1 score, recall, dan precision pada data testing masing-masing adalah sebesar 94.67%, 94.79%, 94.9%, dan 94.69%.
.....The trend of cyber-attacks continues to increase every year. According to data from patrolsiber.id, there are 61 reports of fraud via e-mail with a total loss of more than 144 billion rupiahs and is the mode of fraud with the biggest losses in 2019. Machine learning techniques have been adapted to the detection algorithms in the Intrusion Detection System (IDS) as a tool to examine all network traffic because they can bring benefits in the development of large-scale performance in increasing the detection rate and reducing processing time. One of the machine learning methods in the IDS is the decision tree, which is a method that works quickly, produces good accuracy, and is easy to interpret. This study aims to classify types of cyber-attacks against Wi-Fi networks and the Internet of Things through the application of machine learning techniques with the decision tree method. To avoid overfitting on the model, an advanced technique will be used, namely post-pruning using the reduced error pruning algorithm. The results obtained from this study are the development of the performance of the decision tree model after the reduced error pruning method is used compared to the model without pruning. Evaluation of the performance of the model that has been pruned with the metrics measurement of accuracy, F1 score, recall, and precision in data testing is 94.67%, 94.79%, 94.9%, and 94.69%, respectively.