

IMPLEMENTASI ALGORITMA DECISION TREE UNTUK KLASIFIKASI POLA SERANGAN PADA LOG FILE

Miftarullah Firdaus¹, Triawan Adi Cahyanto²

Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Jember
miftah.ustad@gmail.com, triawanac@unmuhjember.ac.id

ABSTRAK

Sistem Deteksi Intrusi merupakan sebuah mekanisme dalam usaha menyediakan keamanan bagi jaringan komputer. Oleh karena itu diperlukan suatu cara proses identifikasi serangan dalam usaha menjaga keamanan jaringan. Algoritma Machine Learning untuk deteksi intrusi jaringan dilakukan, dimana performa harus berada pada level yang dapat diterima untuk berbagai tipe serangan pada jaringan. Dari semakin meningkatnya teknologi komputer data dalam jumlah yang besar dapat dikumpulkan dan disimpan. Akan tetapi data ini baru berguna jika dianalisa dan dependensi korelasinya ditemukan. Hal ini dapat dicapai dengan menggunakan klasifikasi yang tepat, perlu diperhatikan metode klasifikasi yang tepat. Karena adanya pemrosesan data yang besar dan kompleks serta sifat dinamis dari tipe serangan, metode Data Mining diterapkan dalam Sistem Deteksi Intrusi dalam jaringan berdasarkan trafik data. Salah satu algoritma yang diharapkan mampu digunakan dalam proses klasifikasi serangan ini yakni algoritma Decision tree. Performa dari akurasi diukur dari algoritma machine learning dengan menggunakan test KDDCUP 1999 intrusi dataset untuk menemukan klasifikasi serangan. Dalam percobaan ini deteksi intrusi jaringan dievaluasi performa dengan memanfaatkan benchmark KDDCUP 1999 dari 10000 Training Dataset. Melihat lebih jauh sebuah Decision Tree sebagai model intrusi. Dan pada akhirnya percobaan dibantu dengan Classifier J48 yang berasal dari alat perangkat lunak WEKA untuk mendapatkan akurasi dari performa dalam mencapai deteksi serangan. Dari hasil analisis didapatkan tingkat akurasi dicapai dengan sangat baik menggunakan algoritma ini dalam proses klasifikasi serangan dengan tingkat akurasi 99.76 % pada sistem.

Kata kunci : Sistem Deteksi Intrusi, Klasifikasi, Data Mining, Decision Tree, KDDCUP 1999, Akurasi.

IMPLEMENTASI ALGORITMA DECISION TREE UNTUK KLASIFIKASI POLA SERANGAN PADA LOG FILE

Miftarullah Firdaus¹, Triawan Adi Cahyanto²

Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Jember
miftah.ustad@gmail.com, triawanac@unmuhjember.ac.id

ABSTRACT

Intrusion Detection System is a mechanism in an effort to provide security for computer networks. Therefore we need a method of identifying attacks in an effort to maintain network security. Machine Learning algorithms for network intrusion detection are carried out, where performance must be at an acceptable level for various types of attacks on the network. From the increasing computer technology, large amounts of data can be collected and stored. However, this data is only useful if it is analyzed and the correlation criteria found. This can be achieved by using the right classification, it is necessary to consider the appropriate classification method. Due to the large and complex data processing and the dynamic nature of the type of attack, the Data Mining method is applied in Intrusion Detection Systems in networks based on data traffic. One algorithm that is expected to be able to be used in this attack classification process is the Decision Tree algorithm. The performance of the measured accuracy of the machine learning algorithm using the KDDCUP 1999 test intrusion dataset to find the classification of attacks. In this experiment the performance of network intrusion was evaluated by utilizing the KDDCUP 1999 benchmark of 10000 Dataset Training. Look further at a Decision Tree as an intrusion model. And in the end the experiment was assisted by a J48 Classifier that came from a WEKA software tool to get accuracy from performance in achieving attack detection. From the results of the analysis it was found that the level of accuracy was very well achieved using this algorithm in the process of classification of attacks with system of accuracy 99.76 %.

Keywords : Intrusion Detection System, Classification, Data Mining, Decision Tree, KDDCUP 1999, Accuracy.