# IMPLEMENTASI *DATA MINING* MENGGUNAKAN ALGORITMA C4.5 UNTUK KLASIFIKASI SERANGAN PADA *INTRUSION DETECTION SYSTEM* (IDS)

Isnaini Syarifatun Nisa[1], Alfirna Rizqi Lahitani[2], Adkhan Sholeh[3]

## INTISARI

**Latar Belakang**: *Intrusion Detection System* (IDS) merupakan komponen penting dalam keamanan jaringan komputer, yang berfungsi untuk mengidentifikasi dan merespon ancaman atau serangan yang terjadi. Seiring dengan meningkatnya kompleksitas serangan siber, metode deteksi tradisional seringkali kurang mampu menghadapi volume data yang besar dan variasi serangan yang terus berkembang. Serangan siber yang tidak terdeteksi dapat menyebabkan kerugian besar bagi organisasi, baik dari segi finansial maupun reputasi. Oleh karena itu, diperlukan pendekatan yang lebih efektif untuk mengklasifikasikan dan mendeteksi serangan dengan lebih akurat.

**Tujuan**: Penelitian ini bertujuan untuk mengimplementasikan *data mining* menggunakan algoritma C4.5 untuk klasifikasi serangan pada IDS.

**Metode Penelitian**: Metode yang digunakan pada penelitian ini yaitu klasifikasi dengan menggunakan algoritma C4.5 dan membuat pohon keputusan (*decision tree*) untuk menentukan tingkat akurasi dalam mengklasifikasikan serangan.

**Hasil**: Hasil dari penelitian ini menunjukkan bahwa algoritma C4.5 mampu menghasilkan model klasifikasi dengan tingkat akurasi yang tinggi yaitu sebesar 99% dengan jumlah data uji sebanyak 125.973 data. Model ini dapat mengidentifikasi dan mengklasifikasikan serangan dengan efektif, sehingga dapat meningkatkan performa dan efisiensi IDS dalam mendeteksi ancaman. Implementasi *data mining* menggunakan algoritma C4.5 ini diharapkan dapat menjadi solusi yang handal untuk meningkatkan keamanan jaringan komputer dari serangan yang semakin kompleks dan canggih.

**Kesimpulan**: Dari pohon keputusan (*decision tree)* yang terbentuk, informasi tentang komponen utama yang memengaruhi jenis serangan terdapat pada atribut flag dengan nilai *gain* tertinggi sebesar 0,516. Jenis serangan yang termasuk anomali atau tidak pada dataset ini bisa diketahui dengan menggunakan seleksi 3 fitur yang saling berhubungan yaitu: *protocol_type*, *service*, dan *flag.*

**Kata-kunci**: *Data Mining*, *Intrusion Detection System*, Klasifikasi Serangan, Algoritma C4.5, Keamanan Jaringan

# *IMPLEMENTATION OF DATA MINING USING THE C4.5 ALGORITHM FOR ATTACK CLASSIFICATION IN AN INTRUSION DETECTION SYSTEM (IDS)*

Isnaini Syarifatun Nisa[1], Alfirna Rizqi Lahitani[2], Adkhan Sholeh[3]

## *ABSTRACT*

***Background**: Intrusion Detection System (IDS) is a critical component in computer network security, functioning to identify and respond to threats or attacks that occur. With the increasing complexity of cyber attacks, traditional detection methods often struggle to cope with the large volume of data and the evolving variety of attacks. Undetected cyber attacks can lead to significant losses for organizations, both financially and reputationally. Therefore, a more effective approach is needed to classify and detect attacks more accurately.*

***Objective**: This research aims to implement data mining using the C4.5 algorithm for attack classification in an IDS.*

***Method**: The method used in this research is classification using the C4.5 algorithm and creating a decision tree to determine the accuracy in classifying attacks.*

***Result**: The results of this research show that the C4.5 algorithm is capable of producing a classification model with a high accuracy rate of 99% using a test data set of 125,973 instances. This model can effectively identify and classify attacks, thereby improving the performance and efficiency of IDS in detecting threats. The implementation of data mining using the C4.5 algorithm is expected to be a reliable solution for enhancing computer network security against increasingly complex and sophisticated attacks.*

***Conclusion**: From the formed decision tree, information about the main components affecting the type of attack is found in the flag attribute, which has the highest gain value of 0.516. The type of attack that is classified as an anomaly or not in this dataset can be determined using the selection of three interrelated features: protocol_type, service, and flag.*

***Keywords**: Data Mining, Intrusion Detection System, Attack Classification, C4.5 Algorithm, Network Security*