Jurnal Sistem Informasi dan Teknologi
Vol. 7, No. 4, November 2025

https://journalversa.com/s/index.php/jsit

KLASIFIKASI INTRUSI DETEKSI SYSTEM PADA SISTEM JARINGAN KOMPUTER DENGAN ALGORITMA NAÏVE BAYES

Rivaldi Hamzah[1], Ahmad Turmudi Zy[2], Edora[3]
[1,2,3]Universitas Pelita Bangsa
Email: rivaldihamzah15@gmail.com[1], turmudi@pelitabangsa.ac.id[2],
edora@pelitabangsa.ac.id[3]

Abstrak

Intrusi deteksi system pada sistem jaringan computer merupakan sebuah sistem perangkat lunak atau perangkat keras yang dapat digunakan untuk mendeteksi adanya aktivitas yang mencurigakan dalam sistem atau jaringan *compute*r, data dan informasi dapat diproses dalam sebuah jaringan komputer. kemanan data salah satu aspek yang penting dalam masalah internet khususnya jaringan computer. Setiap hasil yang didapat dari setiap pengujian dengan menggunakan algoritma Naïve Bayes, data dalam mendeteksi aktivitas mencurigakan dalam suatu jaringan komputer atau *intrusi deteksi system* pada sistem jaringan komputer masuk dalam kelas No yang berarti dalam prediksi data *intrusi deteksi system* pada sistem jaringan komputer tidak adanya serangan pada suatu jaringan. Dari hasil pengujian dalam deteksi lalu lintas atau serangan yang mencurigakan dalam sebuah jaringan dengan algoritma *naïve bayes* menghasilkan tingkat accuracy 95.00 % sehingga data dapat di klasifikasi kedalam katagori cukup baik karena hasil dari pengujian menghasilkan tinggkat *accuracy* di atas 50%, dan dapat mempermudah dalam pengambilan keputusan dan upaya pencegahan terhadap *intrusi deteksi system* pada sistem jaringan komputer. Berdasarkan hasil yang sudah didapatkan dalam penelitian ini maka hasil pengujian data dapat di bandingan dari penelitian sebelumnya. dan hasil dari pengujian data *intrusi deteksi system* pada sistem jaringan computer, menghasilkan tingkat accuracy 95.00 %.

Kata Kunci: *Data Mining*, Klasifikasi, *Naïve Bayes*, *Intrusion Detection System*,Komputer.

Abstract

An intrusion detection system on a computer network system is a software or hardware system that can be used to detect suspicious activity in a computer system or network, data and information can be processed in a computer network. Data security is an important aspect of internet problems, especially computer networks. Every result obtained from each test using the Naïve Bayes algorithm, data in detecting suspicious activity in a computer network or intrusion detection system on a computer network system is included in class No, which means that in the prediction of intrusion detection system data on a computer network system there are no attacks on a network. From the test results in detecting suspicious traffic or attacks in a network with the Naïve Bayes algorithm, it produces an accuracy level of 95.00% so that the data can be classified into a fairly good category because the results of the test produce an accuracy level of above 50%, and can make decision making easier. and efforts to prevent

intrusion detection systems on computer network systems. Based on the results obtained in this research, the results of data testing can be compared with previous research. and the results of testing data on intrusion detection systems on computer network systems, resulted in an accuracy rate of 95.00%.

***Keywords**: Data Mining, Classification, Naïve Bayes, Intrusion Detection System, Computer*

PENDAHULUAN

Intrusi deteksi system pada sistem jaringan computer merupakan sebuah sistem perangkat lunak atau perangkat keras yang dapat digunakan untuk mendeteksi adanya aktivitas yang mencurigakan dalam sistem atau jaringan *comput*er, data dan informasi dapat diproses dalam sebuah jaringan komputer. kemanan data salah satu aspek yang penting dalam masalah internet khususnya jaringan komputer . Sebuah jaringan komputer harus mampu memberikan rasa aman terhadap akses yang dilakukan oleh seorang user, dengan memberikan jaminan informasi atau data pribadi aman dari pengaksesan komputer (M. Khudadad and Z. Huang, 2023)**.**

Salah satu supaya melindungi jaringan dari ancaman *intruder (penyerang)* membangun sistem deteksi intrusi atau *Intrusi deteksi system* pada sistem jaringan computer. Deteksi intrusi proses memonitor kejadian pada sistem komputer atau jaringan dan menganalisanya untuk memberikan tanda insiden yang mungkin, yang mana yang merupakan pelanggaran atau mendekati pelanggaran sebuah kebijakan keamanan komputer dan dapat berfungsi untuk mengidentifikasi traffic atau lalu-lintas data pada sebuah jaringan komputer dimana IDS dapat menentukan apakah *traffic* aman, mencurigakan atau bahkan terindikasi merupakan serangan

(A. Essra, Rahmadani, and Safriadi, 2020). Permasalahan muncul ketika aktifitas yang mencurigakan atau serangan dalam pengambilan data dan penyerang mengirim email phishing ke karyawan dengan file berbahaya atau tautan ke situs berisi *exploit*, namun tidak terdaftar pada rule atau aturan yang diinputkan sehingga hal itu sangat membahayakan sebuah jaringan komputer (Dhanabal and S. P. Shantharajah, 2021) . Oleh karena itu dibutuhkan sebuah *clustering* untuk pengelompokan data *Intrusi deteksi system* pada sistem jaringan *computer)* di hangkook indonesia, dalam satu set objek fisik atau abstrak ke dalam kelas-kelas yang serupa (Jupriyadi, 2022). Intrusi jaringan merupakan upaya untuk mendapatkan akses, *Intrution Detection System* digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan dan Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis

untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan *Intrution Detection System* umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada pintu masuk jaringan (H. Tianfield, 2020).

Naive Bayes merupakan salah satu algoritma klasifikasi dalam pembelajaran mesin (machine learning) yang berbasis pada Teorema Bayes, dengan asumsi bahwa fitur-fitur input bersifat independen satu sama lain *(naive).* berfungsi untuk melakukan prediksi jaringan dan diketahui apakah sebuah aktifitas pada sebuah *traffic* jaringan tersebut serangan atau bukan serangan. Dari hasil tersebut juga dapat digunakan menjadi dasar untuk membuat rule baru yang akan diinputkan menjadi aturan-aturan pada *Intrusi deteksi system* pada sistem jaringan *computer* yang digunakan. Sehingga suatu sistem keamanan dalam jaringan komputer yang tahan dan toleran terhadap intrusi jaringan (M. Khudadad and Z. Huang, 2023).

Data mining adalah bentuk penggalian data yang digunakan untuk menggali pengetahuan dari jumlah data yang besar. Salah satu algoritma yang digunakan dalam teknik data mining yang memakai teori klasifikasi. Klasifikasi digunakan untuk menilai data dengan memasukkan data tersebut ke dalam sejumlah kelas yang tersedia. klasifikasi yaitu pembangunan model dengan melakukan pelatihan data *testing* dan *training* untuk disimpan sebagai penerapan model untuk melakukan klasifikasi data (M. Surahman *et al, 2020)*. Sistem deteksi intrusi merupakan proses memonitor trafik jaringan dalam sebuah sistem untuk mendeteksi adanya pola data yang mencurigakan yang memungkinkan adanya serangan dalam sistem tersebut. Sistem yang dirancang untuk mendeteksi aktivitas mencurigakan atau tidak sah dalam jaringan komputer atau sistem informasi. IDS bertugas untuk mengawasi lalu lintas jaringan atau aktivitas sistem, dan memberikan peringatan *(alert)* jika terdeteksi adanya potensi ancaman, Proses menguraikan dan mengidentifikasi informasi dengan teknik dan diharapkan dapat digali suatu potensi dan informasi atau pengetahuan serta dapat menganalisa serangan terhadap keamanan *IDS Intrution Detection System* pada komputer dan mencari pola dari sekumpulan data yang terdapat dalam data untuk di analisis sehingga menghasilkan informasi tertentu untuk di manfaatkan pengetahuannya. Salah satu pendekatan yang dapat digunakan untuk menganalisis sekumpulan data.

METODE PELAKSANAAN

Dalam melakukan penelitian penulis mengikuti aturan yang telah ditetapkan agar penelitian dapat bertahap dan konsisten dan peneliti untuk mengumpulkan, menganalisis, dan menginterpretasikan data guna menjawab pertanyaan penelitian atau menguji data. Berikut ini merupakan gambaran umum langkah yang dilakukan pada saat penelitian ini:

1. Mengindentifikasi Masalah

   Melakukan identifikasi masalah dan menentukan batasan-batasannya terlebih dahulu, tujuannya agar mendapatkan solusi permasalahan serta menentukan tujuan dan manfaat yang akan dicapai.
2. Menganalisis Masalah

   Menganalisis masalah merupakan langkah untuk memahami ruang lingkup atau batasan-batasan masalah dengan harapan masalah tersebut dapat dipahami dengan baik.
3. Pengumpulan Data

   Tujuan untuk mendapatkan data yang dapat mendukung penelitian ini. Dalam melakukan pengumpulan data dilakukan antara lain dengan :

   a. Studi Lapangan

      Kegiatan ini dilakukan dengan cara melakukan observasi terhadap data untuk melihat keadaan nyata, kemudian mengumpulkan data terkait penelitian.

   b. Studi Pustaka

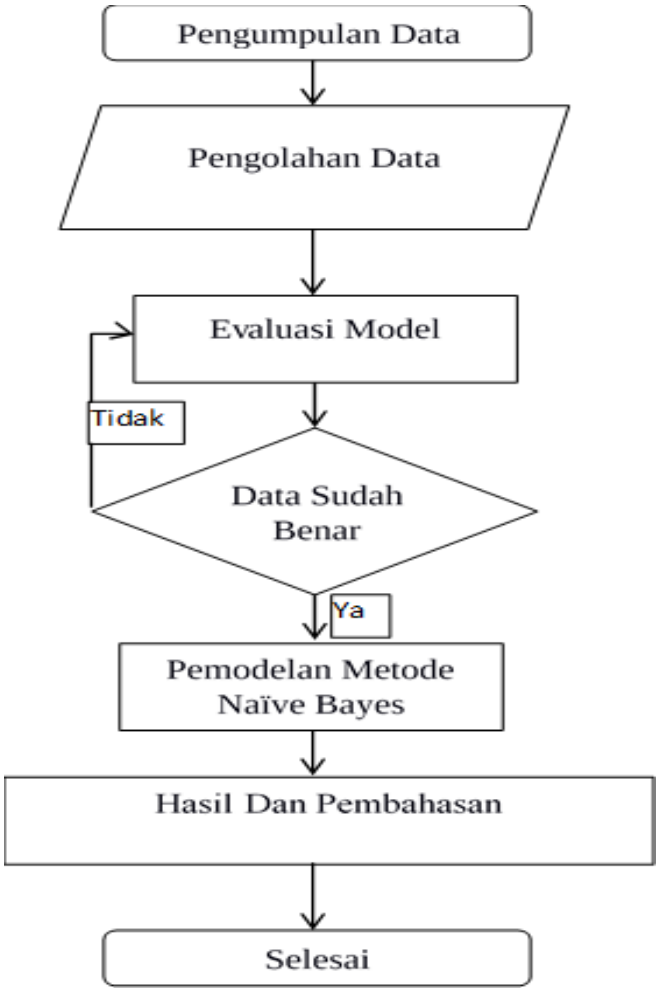
      Kegiatan ini dilakukan dengan mempelajari buku, jurnal, atau penelitian terdahulu terkait topik penelitian. Hal ini dilakukan agar
      penelitian memiliki dasar pengetahuan yang sesuai dengan arah penelitian yang akan dilakukan.
4. Pengolahan Data

   Pengolahan data pada penelitian ini berdasarkan proses yang terdapat pada KDD (*knowledge discovery in database*).
5. Melakukan analisa dan Pembahasan

   Bagaimana proses analisa d*ata mining* dengan algoritma naïve bayes, kemudian bagaimana mengembangkan proses analisa *data mining*. Berdasarkan hasil analisa data tersebut penulis mengimplementasikan penggunaan algoritma naïve

bayes dengan menggunakan colab.

Dalam melakukan penelitian seorang peneliti memiliki pedoman yang secara bertahap yang akan dilakukan sebagai berikut:



Gambar 1 Tahapan Penelitian

HASIL DAN PEMBAHASAN

1. Evaluasi Pengujian pada *Colaboratory*

Pada proses ini metode kelasifikasi dengan algoritma naïve bayes diterapkan untuk pembentukan klasifikasi shingga dapat menghasilkan suatu prediksi dengan keakurasian yang tepat . Dalam penelitian ini penulis menggunakan pengujian perhitungan dengan bantuan *Colaboratory* . Pengujian model yang didapat dengan menggunakan *Colaboratory* adalah dengan tahapan langkah - langkah sebagai berikut :

a. Melakukan import libery yang diperlukan untuk proses pada ***Colaboratory***., kemudian ketikan libery yang di butuhkan dalam pengujian data.

```
import numpy as np
import pandas as pd

from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import accuracy_score
```

Gambar 2 Import Libery

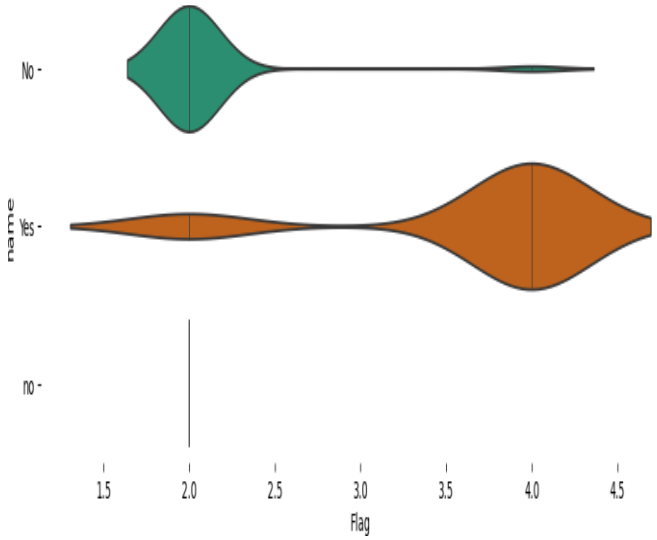
b. Melakukan import data, pada tampilan proses, tambahkan dataset pada folder ke layar tampilan dalam bentuk data xlsx.

```
dataset=pd.read_excel('pengujian.xlsx')
dataset.head()
```

	Protocol Type	dst_host_srv_count	dst_host_count	Flag	Attack	name
0	1	225	4	2	2	No
1	3	255	255	2	2	No
2	1	255	255	4	1	Yes
3	1	1	4	2	2	No
4	1	255	255	2	2	No

Gambar 3 Tampilan Data

c. Langkah berikutnya menentukan hasil grafik *intrusi deteksi system* pada sistem jaringan komputer untuk menampilkan



Gambar 3 Tampilan Data intrusi deteksi system *pada sistem jaringan komputer*

d. Lakukan *Running Process* untuk mendapatkan hasil klelasifikasi dari 100 *record* dataset yang digunakan tersebut.

```
dataset.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 100 entries, 0 to 99
Data columns (total 6 columns):
 #   Column              Non-Null Count  Dtype
---  ------              --------------  -----
 0   Protocol Type       100 non-null    int64
 1   dst_host_srv_count  100 non-null    int64
 2   dst_host_count      100 non-null    int64
 3   Flag                100 non-null    int64
 4   Attack              100 non-null    int64
 5   name                100 non-null    object
dtypes: int64(5), object(1)
memory usage: 4.8+ KB
```

Gambar 4 Tampilan Data

2. Analisa Hasil Pengujian

Setelah melakukan tahapan dalam kelasifikasi data melalui algoritma naïve bayes, pemanfaatan algoritma naïve bayes yang digunakan menghasilkan suatu klasifikasi untuyk dapat di prediksi terhadap masing-masing data. Dataset hasil pencatatan proses data *intrusi deteksi system* pada sistem jaringan komputer yang digunakan adalah sebanyak 100 record data yang akan diuji pada proses pembentukan kelasifikasi dengan algoritma naïve bayes. Hasil *klasifikasi model* pada pengujian pada *colaboratory* dapat dilihat pada gambar berikut.

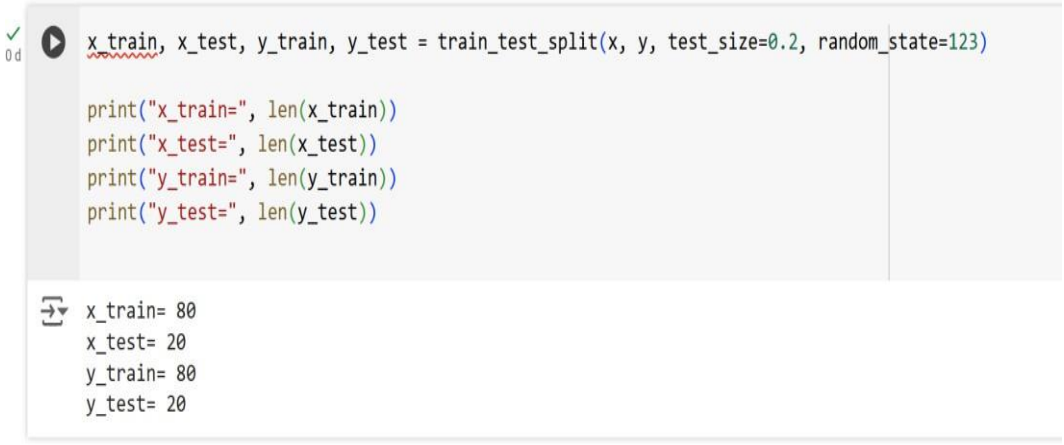
```
from sklearn.preprocessing import LabelEncoder # Assuming LabelEncoder was intended
en = LabelEncoder()

dataset['name'] = en.fit_transform(dataset['name']) # Remove extra space(s)/tab(s) before this line
dataset.head()
```

	Protocol Type	dst_host_srv_count	dst_host_count	Flag	Attack	name
0	1	225	4	2	2	0
1	3	255	255	2	2	0
2	1	255	255	4	1	1
3	1	1	4	2	2	0
4	1	255	255	2	2	0

Gambar 5 Hasil klasifikasi Model data intrusi deteksi system *pada sistem jaringan komputer*

Dari hasil diatas dapat dilihat bahwa pembentukan data traning dan data testing yang didapat melalui pengujian dengan *Colaboratory* ini relevan. Pembentukan dari masing – masing variabel data juga memiliki kemiripan dengan perhitungan manual yang dilakukan. Hanya saja dalam proses menggunakan *colaboratory* tidak ditentukan nilai dari data training dan testing awal sebagaimana yang dilakukan dalam proses perhitungan manual. Hasil *klasifikasi model* pada pengujian pada *colaboratory* dapat dilihat pada gambar berikut.



Gambar 6 Hasil Pembagian Data Training Dan Testing

Pengujian metode dilakukan dengan maksud mengetahui hasil yang dianalisa dan mengukur metode serta algoritma yang digunakan apakah berfungsi dengan baik atau tidak. Proses pengujian menggunakan *colaboratory* dan melihat data apakah sesuai dengan hasil yang diperoleh melalui *colaboratory* tersebut. Sedangkan validasi metode dan algoritma *Naive Bayes* dilakukan dengan mengukur hasil *accuracy, percision dan recall* dan dapat dihitung dengan menggunakan *Confusion Matrix* sebagai berikut :

a. Naïve Bayes

Nilai accuracy dihitung dengan cara menjumlah data benar yang bernilai positif (True Positive) ditambah dengan nilai Negatif (True Negatif) dibagi dengan jumlah data benar yang bernilai positif (True Positive), Negatif (True Negatif) dan ditambah dengan data salah yang bernilai positif (False Positif), Negatif (False Negatif). Dari data pengujian kemudian hasil dari data tersebut menyatakan tingkat *accuracy, recall* dan *persicion* dari algoritma *Naïve Bayes*. Berikut ini hasil dari nilai *accuracy, recall* dan *persicion.*

```
akurasi = classification_report(y_test,y_pred)
print(akurasi) # Removed the extra indent and aligned with the previous line
```

```
              precision    recall  f1-score   support

           0       1.00      0.91      0.95        11
           1       1.00      1.00      1.00         9
           2       0.00      0.00      0.00         0

    accuracy                           0.95        20
   macro avg       0.67      0.64      0.65        20
weighted avg       1.00      0.95      0.97        20
```

Gambar 7 Hasil *accuracy, recall dan persicion dari algoritma Naïve Bayes*

Dari data pengujian kemudian hasil dari data tersebut menyatakan tingkat *accuracy* algoritma *Naive Bayes*. Berikut ini hasil dari nilai *accuracy.*

```
akurasi = accuracy_score(y_test,y_pred)
print("Tingkat Akurasi : %d persen"%(akurasi*100))
```

```
Tingkat Akurasi : 95 persen
```

Gambar 8 Hasil *accuracy Algoritma Naïve Bayes*

Pengujian performa terhadap model dan algoritma dilakukan dengan maksud mengetahui hasil *accuracy* yang dianalisa dan mengukur metode serta algoritma yang digunakan apakah berfungsi dengan baik dapat menghasilkan tingkat *Accuracy* 95.00% .

3. Analisa Hasil

Hasil percobaan penelitian *Aji Sudibyo, Taufik Asra, Bakhtiar Rifai*. menunjukan bahwa penerapan *naive bayes* pada klasifikasi data yang telah melewati proses diskritisasi mampu memberikan akurasi hingga 89%, sedangkan peneltian *Arief Prasetyo, Luqman Affandi , Dedi Arpandi*, Penelitian Yang Menggunakan Metode Naive Bayes Ini Telah Berhasil Melakukan Klasifikasi Serangan-Serangan Baru Dengan Akurasi Kebenaran Adalah Sebesar 81- 84,67 %. Berdasarkan hasil yang sudah didapatkan dalam penelitian ini maka hasil pengujian dari algoritma Naïve Bayes yang menghasilkan tingkat *Accuracy* 95.00%, karena atribut (attack) normal, dos, probe dan r2l, normal (tidak ada serangan), setiap data berdasarkan hasil dari penentuan label atau atribut mendapatkan hasil yang baik dalam suatu data atau semua atribut dalam meningkatkan hasil *accuracy*. Dan hasil pengujian dalam mengklasifikasi data *intrusi*

deteksi system pada sistem jaringan komputer masuk dalam kelas No yang berarti dalam prediksi data *intrusi deteksi system* pada sistem jaringan komputer tidak adanya serangan pada suatu jaringan. Meningkatnya akurasi ini dapat mempermudah dalam pengambilan keputusan dan upaya pencegahan dari setiap algoritma merupakan salah satu faktor yang menyebabkan nilai akurasi tinggi karena setiap atribut dan kelas atau label memiliki pengaruh pada algoritma.

KESIMPULAN DAN SARAN

Dari analisis dan hasil pengolahan data *Intrusion Detection System* maka dapat diambil kesimpulan. Setiap hasil yang didapat dari setiap pengujian dengan menggunakan algoritma Naïve Bayes, data dalam mendeteksi aktivitas mencurigakan dalam suatu jaringan komputer atau *intrusi deteksi system* pada sistem jaringan komputer masuk dalam kelas No yang berarti dalam prediksi data *intrusi deteksi system* pada sistem jaringan komputer tidak adanya serangan pada suatu jaringan. Dari hasil pengujian dalam deteksi lalu lintas atau serangan yang mencurigakan dalam sebuah jaringan dengan algoritma *naïve bayes* menghasilkan tingkat accuracy 95.00 % sehingga data dapat di klasifikasi kedalam katagori cukup baik karena hasil dari pengujian menghasilkan tinggkat *accuracy* di atas 50%, dan dapat mempermudah dalam pengambilan keputusan dan upaya pencegahan terhadap *intrusi deteksi system* pada sistem jaringan komputer. Berdasarkan hasil yang sudah didapatkan dalam penelitian ini maka hasil pengujian data dapat di bandingan dari penelitian sebelumnya. dan hasil dari pengujian data *intrusi deteksi system* pada sistem jaringan computer, menghasilkan tingkat accuracy 95.00 %..

DAFTAR PUSTAKA

M. Khudadad and Z. Huang, “Intrusion Detection with Tree-Based Data Mining Classification Techniques by Using KDD,” *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 227 LNICST, no. 6, pp. 294–303, 2020, doi: 10.1007/978-3-319-73447-7_33.

A. Essra, Rahmadani, and Safriadi, “Analisis Information Gain Attribute Evaluation Untuk Klasifikasi Serangan,” *J. Inf. Syst. Dev.*, vol. 2, no. 2, pp. 9–14, 2020.

I. N. T. Wirawan and I. Eksistyanto, “Penerapan Naive Bayes Pada Intrusion Detection System Dengan Diskritisasi Variabel,” *JUTI J. Ilm. Teknol. Inf.*, vol. 13, no. 2, p. 182, 2015, doi: 10.12962/j24068535.v13i2.a487.

L. Dhanabal and S. P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 6, pp. 446–452, 2021, doi: 10.17148/IJARCCE.2015.4696.

Jupriyadi, "Implementasi Seleksi Fitur Menggunakan Algoritma FVBRM Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids)," *Semin. Nas. Teknol. Inf.*, vol. 17, no. January 2020, pp. 1–6, 2020. N. Rosli *et al.*, "Jurnal Teknologi," vol. 1, pp. 1–6, 2022.

H. Tianfield, "Data Mining Based Cyber-Attack Detection," *Univ. Glas.*, vol. 13, no. 2, pp. 90–104, 2020, doi: 10.1063/1.2975179.

M. Surahman *et al.*, "PENERAPAN METODE SVM-BASED MACHINE LEARNING UNTUK," pp. 196–206, 2020.

I. Rahmadani, H. S. Tambunan, and I. S. Damanik, "Penerapan Data Mining Dalam Pengelompokan Kota Berdasarkan Provinsi Yang Tanggap Terhadap Ancaman Narkotika Dengan Menggunakan K-Medoids," vol. 2, pp. 93–99, 2020.

G. widi N. Dicky Nofriansyah, *Algoritma Data Mining Dan pengujian*. Yogyakarta: Cv Budi Utama, 2021.

Suyanto, *Data Mining*. Yogyakarta: Informatika, 2022.

O. Villacampa, "(Weka - Thesis) Feature Selection and Classification Methods for Decision Making: A Comparative Analysis," *ProQuest Diss. Theses*, no. 63, p. 188, 2023.

Retno Tri vulandari, *Data Mining*. Yogyakarta: Gava Media, 2019.

Y. Silalahi, Kristiani Silalahi., Murfi, Hendri., Satria, "Studi Perbandingan Pemilihan Fitur untuk Support Vector Machine pada Klasifikasi Penilaian Risiko Kredit," vol. 1, no. 2, pp. 119–136, 2021.

Wirawan, I. N. T., & Eksistyanto, I. (2015). Penerapan Naive Bayes Pada Intrusion Detection System Dengan Diskritisasi Variabel. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *13*(2), 182. https://doi.org/10.12962/j24068535.v13i2.a487