Penerapan Naïve Bayes untuk Klasifikasi Serangan Pada Jaringan Komputer (Studi Kasus : Laboratorium Jaringan Komputer Politeknik Negeri Bengkalis)

Ryci Rahmatil Fiska[1], Wahyat[2], Dedi Hermawan[3], Via Laurenz[4], Izatul Fateha[5]
Politeknik Negeri Bengkalis
rycirf@polbeng.ac.id[1], wahyat@polbeng.ac.id[2]

Abstract

Server security on a computer network is very important, maintaining the security of a computer network in order to maintain information, data and maintain infrastructure so that it can work and function properly and provide access rights to registered users, this research, aims to build an IDS (Intrusion Detection System) on the network and Server using Raspberry Pi with SNORT which is useful for monitoring Server activity when an attempted attack occurs. With the increasing complexity of network attacks carried out by attackers, intelligent and adaptive approaches are needed to detect and overcome these threats. Traditional methods such as rule-based or signatures are often not effective enough in the face of evolving attacks. The large amount of network traffic data makes it difficult to manually analyze and detect attacks.

Naive Bayes has a very important role in the classification and detection of network attacks, both considered malicious and highly malicious, By using Naive Bayes, network security systems can become more proactive and adaptive to attacks. This technology not only helps in detecting familiar attacks but also enables identification and response to new or unknown attack techniques. Through proper classification, the system can provide better protection and reduce the impact of attacks.

Keywords : Naïve Bayes, Raspberry Pi, Server, IDS, Snort

1. PENDAHULUAN

Keamanan jaringan komputer telah menjadi salah satu prioritas utama di era digital yang semakin berkembang pesat. Dengan meningkatnya ancaman siber seperti *malware*, *denial of service* (DoS), *phishing*, dan serangan *zero-day*, kebutuhan akan sistem yang mampu mendeteksi dan menanggulangi serangan secara cepat dan akurat sangat penting. Salah satu teknologi utama yang digunakan untuk mengatasi masalah ini adalah *Intrusion Detection System* (IDS), yang dirancang untuk memonitor dan menganalisis lalu lintas jaringan guna mendeteksi aktivitas mencurigakan atau serangan.IDS tradisional, yang umumnya berbasis tanda tangan (*signature-based*) atau berbasis aturan (*rule-based*), sering kali tidak cukup efektif dalam menghadapi serangan baru atau serangan yang tidak diketahui sebelumnya. Untuk mengatasi kekurangan ini, pendekatan berbasis *machine learning* (ML) telah diperkenalkan. Salah satu algoritma ML yang paling sederhana namun efektif dalam klasifikasi data adalah *Naive Bayes*.

Naive Bayes adalah algoritma pembelajaran mesin berbasis probabilistik yang didasarkan pada Teorema Bayes dengan asumsi independensi bersyarat antara fitur. Algoritma ini memiliki beberapa karakteristik yang membuatnya cocok untuk diterapkan pada IDS, antara lain:
Kesederhanaan dan Kecepatan: *Naive Bayes* adalah algoritma yang relatif sederhana dan cepat dalam melakukan komputasi. Dalam lingkungan jaringan yang membutuhkan deteksi cepat terhadap potensi serangan, efisiensi komputasi sangatlah penting.
Kemampuan Mengolah Data Multikelas: Dalam jaringan komputer, lalu lintas dapat melibatkan berbagai jenis serangan yang berbeda. *Naive Bayes* sangat efektif dalam menangani tugas klasifikasi multikelas, yang berguna dalam mendeteksi berbagai jenis serangan sekaligus.

Penanganan Dataset Besar: Serangan jaringan sering kali terjadi dalam volume data yang besar, dan *Naive Bayes* mampu menangani dataset yang besar dengan efisiensi tinggi karena skema perhitungan probabilistiknya yang sederhana.

Kemampuan dalam Anomaly Detection: IDS sering harus mendeteksi serangan yang jarang terjadi atau serangan baru yang belum diketahui sebelumnya (*zero-day attacks*). Algoritma *Naive Bayes*, terutama dalam mode deteksi anomali, dapat membantu mengenali aktivitas yang tidak biasa berdasarkan distribusi probabilitas dari data yang dilatih.

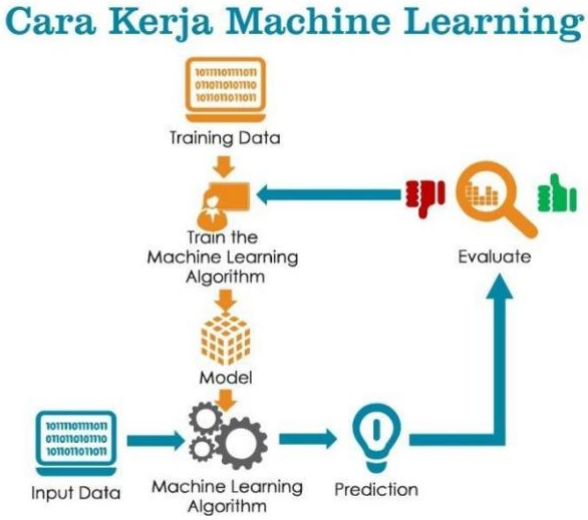
2. TINJAUAN PUSTAKA

Tinjauan Pustaka memuat penelitian terdahulu dan teori pendukung terkait dengan permasalahan yang dibahas. Sumber pustaka yang digunakan harus dicantumkan pada daftar pustaka. Penulisan acuan menggunakan pola "penulis, tahun" yang mengacu pada karya di daftar pustaka. Dalam teks, karya yang diacu menggunakan ketentuan berikut:

a. *Intrusion Detection System* bisa di definisikan sebagai perangkat lunak, perangkat keras atau gabungan keduanya yang berfungsi sebagai pendeteksi adanya serangan illegal yang masuk kedalam jaringan computer (Anis et al., 2022);
b. Naive Bayes memprediksi kelas atau label untuk data baru dengan menghitung probabilitas kelas berdasarkan distribusi fitur fitur yang diamati. Meskipun sederhana, Naive Bayes dapat memberikan hasil yang baik dalam banyak situasi dan sering digunakan sebagai baseline untuk membandingkan kinerja model klasifikasi yang lebih kompleks(Ananda & Suryono, 2024);

3. METODE PENELITIAN

Tahapan penelitian terdiri dari beberapa langkah, dimulai dengan pengumpulan data yang dibutuhkan untuk membuat rancangan Machine Learning. Pada tahap ini, dilakukan identifikasi data yang relevan untuk penelitian, serta penentuan kebutuhan fungsional dan non-fungsional, seperti tujuan yang harus dicapai oleh sistem dan batasan kinerja yang diinginkan. Setelah data terkumpul dan kebutuhan ditetapkan, langkah selanjutnya adalah membuat rancangan model Machine Learning yang baik, mencakup pemilihan algoritma dan metode yang sesuai. Rancangan ini kemudian diimplementasikan, sehingga menghasilkan model Machine Learning yang mampu melakukan klasifikasi sesuai dengan tujuan penelitian dengan menggunakan salah satu dari model Machine Learning yaitu Naïve Bayes. Langkah terakhir yaitu membuat dokumentasi dan laporan hasil penelitian.



Gambar 1. Rencana Pembuatan Machine Learning

Lokasi penelitian saat melakukan riset berada di Laboratorium Jaringan Komputer, Jurusan Teknik Informatika, Politeknik Negeri Bengkalis.

Analisa kebutuhan dilakukan untuk mendapatkan kebutuhan pengguna, untuk membangun Intrusion Detection System (IDS) memerlukan perangkat keras dan perangkat lunak sebagai berikut :

Tabel 1. Perangkat Keras dan Perangkat Lunak yang digunakan

Hardware/Software	**Penggunaan**
Komputer PC	Sebagai Web Server yang akan di uji untuk diserang
Raspberry Pi (Sd Card dan case)	Intrusion Detection System (IDS)
Router	Manajemen Bandwith
Kabel UTP	Kabel LAN
Laptop	Perangkat Penyerang
Google Colab	Proses Klasifikasi MachineLearning
Snort	Aplikasi IDS
Raspbian	Sistem Operasi
Smartphone	Bot Telegram

4. HASIL PENELITIAN DAN PEMBAHASAN

Tipe Serangan di Lab Jaringan Komputer

Setelah dilakukan pendeteksian serangan pada laboratorium jaringan komputer Politeknik Negeri Bengkalis, terdapat beberapa jenis serangan yang sering muncul seperti pada table di bawah ini:

Tabel 2. Pelabelan jenis serangan

Tipe	Label
ICMP Ping	Berbahaya
ICMP Ping	Sangat Berbahaya
ICMP Ping	Berbahaya
ICMP Ping	Sangat Berbahaya
SCAN FIN	Berbahaya
SCAN FIN	Berbahaya
DDOS TCP Attack	Sangat Berbahaya
SCAN FIN	Sangat Berbahaya
SCAN FIN	Berbahaya
DDOS TCP Attack	Berbahaya
DDOS TCP Attack	Sangat Berbahaya
DDOS TCP Attack	Sangat Berbahaya

DDOS TCP Attack	Berbahaya
DDOS TCP Attack	Sangat Berbahaya
DDOS TCP Attack	Berbahaya
DDOS TCP Attack	Sangat Berbahaya
SCAN FIN	Berbahaya
SCAN FIN	Berbahaya
ICMP Ping	Sangat Berbahaya
ICMP Ping	Sangat Berbahaya
ICMP Ping	Berbahaya
ICMP Ping	Berbahaya
SCAN FIN	Sangat Berbahaya
SCAN FIN	Sangat Berbahaya
ICMP Ping	Sangat Berbahaya
SCAN FIN	Sangat Berbahaya
DDOS TCP Attack	Berbahaya
DDOS TCP Attack	Berbahaya
DDOS TCP Attack	Sangat Berbahaya
SCAN FIN	Sangat Berbahaya

Klasifikasi Naïve bayes

Menghitung probabilitas Berbahaya dan Sangat Berbahaya dari serangan SCAN FIN

Kemungkinan Berbahaya

1. Hitung prior probability
   P (SCAN FIN) = 10/30 = 0,33
   P (Berbahaya) = 14/30 = 0,46
2. Hitung probabilitasposterior
   P (SCAN FIN|Berbahaya) = 5/14 = 0,35
3. Masukkan Probabilitas Prior dan Posterior dalam persamaan
   P (Berbahaya|SCAN FIN) =0,35*0,46/0,33 = 0,48

Kemungkinan serangan sangat berbahaya

1. Hitung prior probability
   P (SCAN FIN) = 10/30 = 0,33
   P (Sangat Berbahaya) = 16/30 = 0,53
2. Hitung probabilitas posterior
   P (SCAN FIN|Sangat Berbahaya) = 5/16 = 0,31
3. Masukkan Probabilitas Prior dan Posterior dalam persamaan
   P (Sangat Berbahaya|SCAN FIN) =0,31*0,53/0,33 = 0,49

Menghitung probabilitas Berbahaya dan Sangat Berbahaya dari serangan ICMP PING

Kemungkinan Berbahaya

1. Hitung prior probability
   P (ICMP PING) = 9/30 = 0,3
   P (Berbahaya) = 14/30 = 0,46
2. Hitung probabilitas posterior
   P (ICMP PING|Berbahaya) = 4/14 = 0,28
3. Masukkan Probabilitas Prior dan Posterior dalam persamaan
   P (Berbahaya|ICMP PING)
   =0,28*0,46/0,3 = 0,42

Kemungkinan serangan sangat berbahaya

1. Hitung prior probability
   P (ICMP PING) = 9/30 = 0,3
   P (Sangat Berbahaya) = 16/30 = 0,53
2. Hitung probabilitas posterior
   P (ICMP PING|Sangat Berbahaya) = 5/16 = 0,31
3. Masukkan Probabilitas Prior dan Posterior dalam persamaan
   P (Sangat Berbahaya|ICMP PING) =0,31*0,53/0,3 = 0,54

Menghitung probabilitas Berbahaya dan Sangat Berbahaya dari serangan DDOS

Kemungkinan Berbahaya

1. Hitung prior probabilityP (DDOS) = 11/30 = 0,36

P (Berbahaya) = 14/30
= 0,46

2. Hitung probabilitas posterior

P (DDOS |Berbahaya) = 5/14 = 0,35

3. Masukkan Probabilitas Prior dan Posterior dalam persamaanP (Berbahaya| DDOS) =0,35*0,46/0,36 = 0,44

Kemungkinan serangan sangat berbahaya

1. Hitung prior probabilityP (DDOS) = 11/30 = 0,36

P (Sangat Berbahaya) = 16/30 = 0,53

2. Hitung probabilitas posterior
   P (DDOS |Sangat Berbahaya) = 6/16 = 0,37
3. Masukkan Probabilitas Prior dan Posterior dalam persamaanP (Sangat Berbahaya| DDOS) =0,37*0,53/0,36 = 0,54

Klasifikasi Naïve Bayes Menggunakan Google Colab

Setelah dilakukan perhituangan secara manual maka dilakukan lagi perhitungan menggunakan Google Colab untuk memudahkan melihat hasil klasifikasi berdasarkan grafik Evaluasi Model Naïve Bayes.

+ Kode + Teks

```
# Fungsi untuk menghitung probabilitas posterior
def calculate_posterior(prob_prior, prob_posterior, prob_evidence):
    return (prob_posterior * prob_prior) / prob_evidence

# Data
total_attacks = 30

# SCAN FIN
scan_fin = 10
dangerous_scan_fin = 5
very_dangerous_scan_fin = 5

# Probabilitas prior dan posterior untuk SCAN FIN
p_scan_fin = scan_fin / total_attacks
p_dangerous = 14 / total_attacks
p_very_dangerous = 16 / total_attacks

p_scan_fin_given_dangerous = dangerous_scan_fin / 14
p_scan_fin_given_very_dangerous = very_dangerous_scan_fin / 16

# Menghitung probabilitas Berbahaya dan Sangat Berbahaya dari SCAN FIN
p_dangerous_given_scan_fin = calculate_posterior(p_dangerous, p_scan_fin_given_dangerous, p_scan_fin)
p_very_dangerous_given_scan_fin = calculate_posterior(p_very_dangerous, p_scan_fin_given_very_dangerous, p_scan_fin)

# ICMP PING
icmp_ping = 9
dangerous_icmp_ping = 4
very_dangerous_icmp_ping = 5

# Probabilitas prior dan posterior untuk ICMP PING
p_icmp_ping = icmp_ping / total_attacks
```

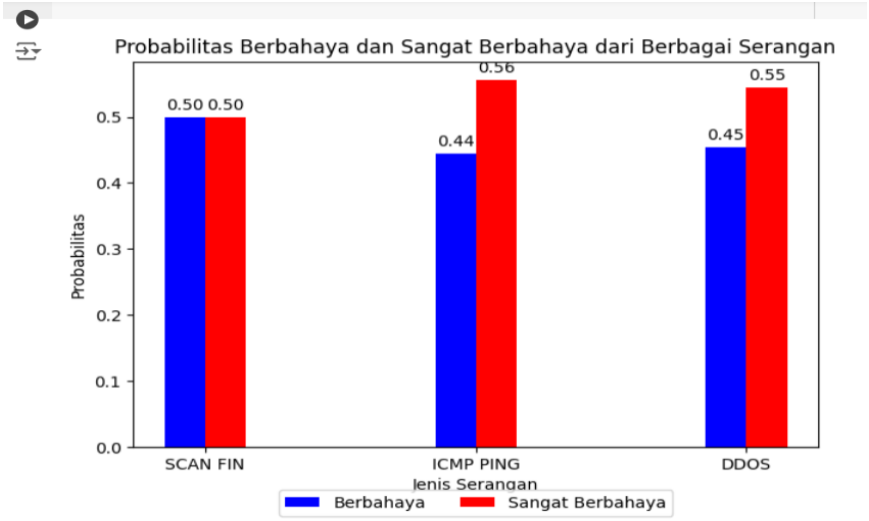
Gambar 2. Evaluasi Model Naïve Bayes

```
+ Kode  + Teks

p_dangerous_given_icmp_ping = dangerous_icmp_ping / 14
p_very_dangerous_given_icmp_ping = very_dangerous_icmp_ping / 16

# Menghitung probabilitas Berbahaya dan Sangat Berbahaya dari ICMP PING
p_dangerous_given_icmp_ping = calculate_posterior(p_dangerous, p_dangerous_given_icmp_ping, p_icmp_ping)
p_very_dangerous_given_icmp_ping = calculate_posterior(p_very_dangerous, p_very_dangerous_given_icmp_ping, p_icmp_ping)

# DDOS
ddos = 11
dangerous_ddos = 5
very_dangerous_ddos = 6

# Probabilitas prior dan posterior untuk DDOS
p_ddos = ddos / total_attacks
p_dangerous_given_ddos = dangerous_ddos / 14
p_very_dangerous_given_ddos = very_dangerous_ddos / 16

# Menghitung probabilitas Berbahaya dan Sangat Berbahaya dari DDOS
p_dangerous_given_ddos = calculate_posterior(p_dangerous, p_dangerous_given_ddos, p_ddos)
p_very_dangerous_given_ddos = calculate_posterior(p_very_dangerous, p_very_dangerous_given_ddos, p_ddos)

# Print hasil
print(f"P(Berbahaya | SCAN FIN) = {p_dangerous_given_scan_fin:.2f}")
print(f"P(Sangat Berbahaya | SCAN FIN) = {p_very_dangerous_given_scan_fin:.2f}")
print(f"P(Berbahaya | ICMP PING) = {p_dangerous_given_icmp_ping:.2f}")
print(f"P(Sangat Berbahaya | ICMP PING) = {p_very_dangerous_given_icmp_ping:.2f}")
print(f"P(Berbahaya | DDOS) = {p_dangerous_given_ddos:.2f}")
print(f"P(Sangat Berbahaya | DDOS) = {p_very_dangerous_given_ddos:.2f}")
```

Gambar 3. Evaluasi Model Naïve Bayes Lanjutan

OUTPUT :

```
P(Berbahaya | SCAN FIN) = 0.50
P(Sangat Berbahaya | SCAN FIN) = 0.50
P(Berbahaya | ICMP PING) = 0.44
P(Sangat Berbahaya | ICMP PING) = 0.56
P(Berbahaya | DDOS) = 0.45
P(Sangat Berbahaya | DDOS) = 0.55
```



Gambar 4. Klasifikasi Menggunakan Google Colab

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian yang dilakukan dapat disimpulkan bahwa :

1. Pengujian dilakukan dilakukan dengan 3 Skenario yaitu: *PING Attack, Port Scanning*, dan *DOS/DDoS Attack.*
2. *Naive Bayes* sering menunjukkan performa yang baik dalam mendeteksi serangan-serangan umum, seperti serangan *Denial of Service* (DoS) atau *Probing*, yang memiliki pola yang lebih jelas dalam lalu lintas jaringan.
3. Secara keseluruhan penggunaan *Naive Bayes* untuk IDS telah menunjukkan beberapa kelebihan, seperti akurasi yang layak, efisiensi komputasi, dan kemudahan implementasi.

5.2 Saran

Saran dari penelitian ini adalah meskipun naïve bayes memiliki beberapa kelebihan namun kekurangannya dalam menangani fitur yang saling bergantung dan kinerjanya pada dataset yang tidak seimbang menjadikan algoritma ini lebih cocok untuk kasus tertentu atau sebagai bagian dari pendekatan hibrida. Penelitian lebih lanjut dalam pengembangan dan kombinasi *Naive Bayes* dengan metode lain diharapkan dapat mengatasi kelemahan ini untuk meningkatkan performa dalam mendeteksi serangan jaringan yang lebih kompleks.

6. DAFTAR PUSTAKA

Anis, M., Hilmi, A., & Khujaemah, E. (2022). Network Security Monitoring With Intrusion Detection System. *Jurnal Teknik Informatika (JUTIF)*, *3*(2), 249– 253. https://doi.org/10.20884/1.jutif.2022.3.2.117

A. T. Zy, A. T. Sasongko, and A. Z. Kamalia, "Penerapan Naïve Bayes Classifier, Support Vector Machine, dan Decision Tree untuk Meningkatkan Deteksi Ancaman Keamanan Jaringan," *Media Online)*, vol. 4, no. 1, pp. 610–617, 2023, doi: 10.30865/klik.v4i1.1134.

Ananda, D., & Suryono, R. R. (2024). *Analisis Sentimen Publik Terhadap Pengungsi Rohingya di Indonesia dengan Metode Support Vector Machine dan Naïve Bayes*. *8*(April), 748–757. https://doi.org/10.30865/mib.v8i2.7517

Dwivedi, N., Katiyar, D., & Goel, G. (2022). A Comparative Study of Various Software Development Life Cycle (SDLC) Models. *International Journal of Research in Engineering, Science and Management, 5*(3), 141–144.

F. Veriarinal, "Klasifikasi Sistem Deteksi Kerusakan Mesin Komputer Menggunakkan Metode Naive Bayes," *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 2, no. 10, pp. 5–24, 2024.

Ferdinand Louis, M. Ficky Duskarnaen, & Hamidillah Ajie. (2021). Uji Kecepatan Raspberry Pi Sebagai Private Cloud Storage Untuk Small Office Home Office: Dengan Studi Kasus Di Upt Tik. *PINTER : Jurnal Pendidikan Teknik Informatika DanKomputer*, *5*(2), 42–49. https://doi.org/10.21009/pinter.5.2.7

Mahesh, B. (2020). Machine Learning Algorithms - A Review. *International Journal of Science and Research*, *9*(1), 381–386. https://doi.org/10.21275/ART20203995

Ridwan, R., Lubis, H., & Kustanto, P. (2020). Implementasi Algoritma Neural Network dalam Memprediksi Tingkat Kelulusan Mahasiswa. *Jurnal Media Informatika Budidarma*, *4*(2), 286. https://doi.org/10.30865/mib.v4i2.2035

Satwika, I. K. S., Sudiarsa, I. W., & Swari, M. H. P. (2020). Intrusion Detection System (Ids) Menggunakan Raspberry Pi 3 Berbasis Snort Studi Kasus: Stmik Stikom Indonesia. *SCAN - Jurnal Teknologi Informasi Dan Komunikasi*, *15*(3), 2–7. https://doi.org/10.33005/scan.v15i3.2279

Suharyanto, C. E., & Maulana, A. (2020). Perancangan Network Attached Storage (Nas) Menggunakan Raspberry Pi Untuk Usaha Mikro Kecil Dan Menengah (Umkm). *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *5*(2),

S. Jaelani, “the Role of Information System Attack Classification in Strengthening National Security and Combating Cyberwarfare,” 2024.