1 JURNAL DESAIN DAN ANALISIS TEKNOLOGI (JDDAT)

Full Paper

Klasifikasi Serangan Denial-of-Service (DoS) pada Jaringan Komputer Menggunakan Algoritma Machine Learning: Studi Komparatif K-Nearest Neighbors (K-NN) dan Naive Bayes

Veranny Arianty Putri[1], Surgiwe[2], Frengki Hotsabar Parmonangan Simatupang[3] , Yudhistira Andilie[4], Viriya Marhan Cunis[5] , Mhd Adi Setiawan Aritonang[6], Deosa Putra Caniago[7]
Program Studi Teknik Komputer, Institut Teknologi Batam, Indonesia

Informasi Artikel

Terbit: Juli 2026

Kata Kunci:

Denial-of-Service (DoS), K-Nearest Neighbors, Machine Learning, Naive Bayes, Network Security

ABSTRAK

Keamanan jaringan komputer menghadapi tantangan besar akibat peningkatan serangan siber, khususnya serangan *Denial-of-Service* (DoS) yang mengganggu ketersediaan layanan. Tantangan utama dalam mendeteksi serangan ini adalah kemiripan pola trafik serangan dengan trafik normal serta ketidakseimbangan kelas pada data. Penelitian ini bertujuan melakukan studi komparatif antara algoritma *Machine Learning* K-Nearest Neighbors (K-NN) dan Naive Bayes untuk mengklasifikasikan serangan DoS menggunakan *subset* dataset CIC-DDoS. Evaluasi kinerja dilakukan berdasarkan metrik akurasi, *precision*, *recall*, *F1-score*, dan waktu prediksi. Hasil pengujian menunjukkan bahwa K-NN unggul dalam akurasi mencapai 99,95% dan mampu mendeteksi kelas minoritas dengan sangat baik, namun memiliki waktu prediksi yang lambat (±16,89 detik). Sebaliknya, Naive Bayes menawarkan efisiensi komputasi yang tinggi dengan waktu prediksi sangat cepat (±0,034 detik) dan akurasi 99,21%, meskipun memiliki kelemahan dalam *precision* pada kelas normal. Kesimpulannya, K-NN lebih direkomendasikan untuk sistem yang memprioritaskan akurasi maksimal, sedangkan Naive Bayes lebih sesuai untuk sistem deteksi dini yang membutuhkan respons *real-time*. Penelitian ini memberikan wawasan bagi pengembang sistem IDS dalam memilih model yang sesuai dengan prioritas kebutuhan keamanan jaringan.

Corresponding Author:

Veranny Arianti Putri,
Email: verranygumay@gmail.com

1. PENDAHULUAN

Keamanan jaringan komputer merupakan aspek penting dalam mendukung infrastruktur digital modern. Peningkatan trafik data, layanan daring, komputasi awan, serta teknologi Internet of Things (IoT) turut meningkatkan ancaman siber, khususnya serangan Denial-of-Service (DoS) dan Distributed Denial-of-Service (DDoS). Serangan ini bekerja dengan membanjiri server menggunakan trafik berlebih sehingga mengganggu ketersediaan layanan dan menghabiskan sumber daya sistem. Tantangan utama dalam deteksi DoS adalah kemiripan pola trafik serangan dengan trafik normal, yang menyulitkan proses identifikasi secara akurat [1].

Beberapa Pendekatan berbasis machine learning banyak digunakan untuk mengatasi permasalahan tersebut karena mampu mempelajari pola trafik jaringan secara otomatis. Beberapa penelitian menunjukkan bahwa algoritma Naive Bayes dan K-Nearest Neighbors (K-NN) memiliki performa yang baik dalam mendeteksi serangan DoS/DDoS[2]. Penelitian menggunakan dataset CICIDS2018 melaporkan bahwa Naive Bayes dapat mencapai akurasi hingga 95% setelah dilakukan prapemrosesan dan seleksi fitur yang tepat. Sementara itu, algoritma K-NN dilaporkan mampu mencapai akurasi yang sangat tinggi pada berbagai lingkungan jaringan dengan pemilihan parameter yang sesuai [3].

Salah satu dataset yang menjadi standar dalam riset deteksi serangan adalah CIC-DDoS, yang menyediakan detail trafik serangan modern dengan variasi flow yang kompleks. Pemilihan subset dari dataset

CIC-DDoS dalam penelitian ini didasarkan pada kebutuhan untuk mengevaluasi efektivitas algoritma dalam menangani noise pada fitur-fitur kritis yang belum banyak dikaji secara mendalam pada penelitian sebelumnya. Selain itu, performa machine learning sangat dipengaruhi oleh karakteristik dataset, terutama permasalahan ketidakseimbangan kelas (class imbalance). Dalam kondisi nyata, trafik normal dan trafik serangan sering kali memiliki rasio yang sangat timpang, yang berpotensi menyebabkan model mengalami bias terhadap kelas mayoritas.

Eksperimen awal yang dilakukan pada penelitian ini menunjukkan adanya ketimpangan ekstrem antara trafik normal dan trafik DoS. Pada kondisi tersebut, ditemukan perbedaan perilaku yang signifikan: algoritma K-NN menunjukkan kemampuan adaptasi yang lebih baik dalam mengenali pola pada kelas minoritas, sementara Naive Bayes cenderung menunjukkan bias dengan salah mengklasifikasikan sebagian trafik normal sebagai serangan.

Berdasarkan celah tersebut, penelitian ini melakukan studi komparatif mendalam antara algoritma K-Nearest Neighbors dan Naive Bayes dalam mengklasifikasikan serangan DoS pada subset dataset CIC-DDoS. Evaluasi dilakukan secara komprehensif menggunakan metrik accuracy, precision, recall, F1-score, serta time complexity (waktu prediksi). Hasil penelitian ini diharapkan memberikan kontribusi empiris dalam pemilihan algoritma yang paling efektif dan efisien untuk diintegrasikan ke dalam sistem deteksi serangan pada jaringan modern yang dinamis.

2. METODE PENELITIAN

Metodologi penelitian ini dirancang untuk melakukan klasifikasi serangan Denial-of-Service (DoS) pada jaringan komputer menggunakan pendekatan machine learning. Penelitian berfokus pada studi komparatif dua algoritma klasifikasi, yaitu K-Nearest Neighbors (K-NN) dan Naive Bayes, dengan tujuan mengevaluasi performa keduanya dari aspek akurasi, ketepatan klasifikasi per kelas, serta efisiensi waktu prediksi.

2.1 Dataset

Dataset yang digunakan pada penelitian ini berasal dari CIC-DDoS dataset, yang merupakan dataset standar dan banyak digunakan dalam riset keamanan jaringan[4]. Dataset asli memiliki ukuran sangat besar (±30 GB), sehingga untuk keperluan eksperimen dan efisiensi komputasi dilakukan pengambilan subset data sebanyak 100.000 baris pertama.
Dataset terdiri dari dua kelas, yaitu:

Table 1 *kelas dataset*

Class 0	Class 1
Trafik normal (benign)	Trafik serangan DoS/DDoS

Distribusi kelas pada dataset sangat tidak seimbang (*class imbalance*), dengan jumlah data sebagai berikut:

Table 2 *jumlah dataset*

Class	Jumlah Data
Class 0 (Normal)	161 data
Class 1 (DoS/DDoS)	19.598 data

Kondisi ini sengaja dipertahankan untuk menguji robustitas algoritma dalam menangani data dunia nyata yang umumnya tidak seimbang**.**

2.2 Pemrosesan data

Tahapan *preprocessing* dilakukan untuk memastikan kualitas data sebelum digunakan dalam proses pelatihan dan pengujian model. Tahapan ini meliputi:

1. Pembersihan Data :Data yang memiliki nilai kosong atau duplikat dihapus untuk mencegah bias pada proses klasifikasi.
2. Transformasi Label :Label kelas dikonversi ke dalam bentuk numerik, dengan nilai 0 untuk trafik no rmal dan 1 untuk trafik serangan.
3. Normalisasi Fitur :Normalisasi dilakukan pada fitur numerik menggunakan metode *scaling* untuk m

enyamakan rentang nilai antar fitur.Proses ini sangat penting terutama untuk algoritma K-NN yang berbasis jarak antar data.

4. Pembagian Data :Dataset dibagi menjadi dua bagian, yaitu data latih (*training set*) dan data uji (*testing set*) dengan rasio 80:20.

2.3 Algoritma K-Nearest Neighbors (K-NN)

K-Nearest Neighbors merupakan algoritma klasifikasi non-parametrik yang bekerja berdasarkan kedekatan jarak antar data[5]. Pada penelitian ini, perhitungan jarak dilakukan menggunakan Euclidean Distance.

Proses kerja K-NN adalah sebagai berikut:

1. Menghitung jarak antara satu data uji dengan seluruh data latih.
2. Menentukan sejumlah *K* tetangga terdekat.
3. Menetapkan kelas berdasarkan mayoritas kelas tetangga tersebut.

Kelebihan K-NN dalam penelitian ini terlihat pada kemampuannya mendeteksi kelas minoritas (trafik normal) dengan sangat baik meskipun dataset tidak seimbang. Namun, algoritma ini memiliki kelemahan pada sisi waktu prediksi karena harus menghitung jarak terhadap seluruh data latih.

2.4 Algoritma Naive Bayes

Naive Bayes merupakan algoritma klasifikasi probabilistik yang bekerja berdasarkan Teorema Bayes dengan asumsi bahwa setiap fitur bersifat independen satu sama lain[6]. Algoritma ini menentukan kelas suatu data dengan menghitung probabilitas posterior dari masing-masing kelas berdasarkan probabilitas fitur-fitur yang dimiliki data tersebut. Proses klasifikasi diawali dengan perhitungan probabilitas awal (prior) untuk setiap kelas, kemudian dilanjutkan dengan perhitungan probabilitas bersyarat (likelihood) dari tiap fitur terhadap kelas yang bersangkutan[7]. Selanjutnya, nilai probabilitas posterior dihitung, dan kelas dengan nilai probabilitas tertinggi ditetapkan sebagai hasil klasifikasi. Keunggulan utama dari algoritma Naive Bayes terletak pada efisiensi komputasi yang sangat tinggi serta waktu prediksi yang relatif cepat, sehingga algoritma ini sangat sesuai untuk diterapkan pada sistem deteksi serangan jaringan yang membutuhkan respons cepat atau bekerja secara real-time[8].

2.5 Evaluasi Kinerja Model

Evaluasi kinerja model pada penelitian ini dilakukan menggunakan confusion matrix yang dikombinasikan dengan beberapa metrik evaluasi standar untuk menilai performa klasifikasi. Metrik accuracy digunakan untuk mengukur tingkat ketepatan model secara keseluruhan dalam mengklasifikasikan data uji. Precision digunakan untuk mengevaluasi ketepatan model dalam memprediksi kelas serangan, sedangkan recall digunakan untuk mengukur kemampuan model dalam mendeteksi seluruh data yang benar-benar merupakan serangan. Selain itu, F1-score digunakan untuk menilai keseimbangan antara precision dan recall sehingga memberikan gambaran performa model yang lebih komprehensif. Di samping metrik kualitas prediksi, waktu prediksi juga diukur untuk mengevaluasi efisiensi komputasi dari masing-masing algoritma, yang menjadi faktor penting dalam pertimbangan implementasi sistem deteksi serangan berbasis machine learning.

2.6 Prosedur Eksperimen

Prosedur eksperimen dalam studi ini dimulai dengan memuat dan mengolah bagian dari dataset CIC-DDoS yang berfungsi sebagai sumber data utama. Data yang dikumpulkan selanjutnya melalui proses preprocessing yang mencakup pembersihan serta normalisasi fitur agar setiap atribut memiliki skala yang seimbang dan tidak mendominasi pelatihan model. Kemudian, dataset dibagi menjadi dua bagian: data latih dan data uji, di mana model K-Nearest Neighbor (K-NN) dan Naive Bayes dilatih menggunakan data latih tersebut. Setelah selesai pelatihan, kedua model tersebut diujikan menggunakan data uji untuk menilai kemampuan klasifikasinya. Kinerja model dievaluasi dengan menghitung confusion matrix dan laporan klasifikasi yang mencakup metrik akurasi, presisi, recall, serta F1-score. Di samping itu, waktu prediksi masing-masing algoritma juga diukur untuk mengevaluasi efisiensi komputasi. Semua hasil evaluasi ini kemudian dipergunakan untuk membandingkan kinerja K-NN dan Naive Bayes secara menyeluruh, baik dari perspektif akurasi maupun kecepatan prediksi.

2.7 Parameter Evaluasi

Laporan Detail K-NN:

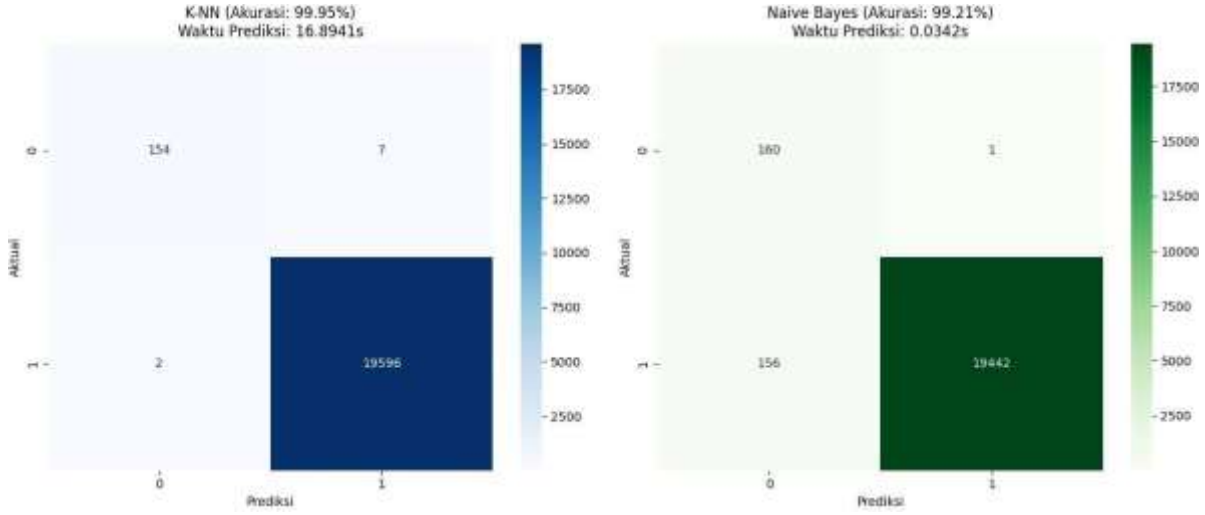
	precision	recall	f1-score	support
0	0.99	0.96	0.97	161
1	1.00	1.00	1.00	19598
accuracy			1.00	19759
macro avg	0.99	0.98	0.99	19759
weighted avg	1.00	1.00	1.00	19759

Laporan Detail Naive Bayes:

	precision	recall	f1-score	support
0	0.51	0.99	0.67	161
1	1.00	0.99	1.00	19598
accuracy			0.99	19759
macro avg	0.75	0.99	0.83	19759
weighted avg	1.00	0.99	0.99	19759

Gambar 2.1 Hasil Akurasi K-NN dan Naïve Bayes

Gambar tersebut menyajikan perbandingan kinerja klasifikasi antara algoritma K-Nearest Neighbors (K-NN) dan Naive Bayes pada dataset dengan ketidakseimbangan kelas yang ekstrem (class imbalance), di mana kelas 1 (serangan) mendominasi secara signifikan dibandingkan kelas 0 (normal). Hasil evaluasi menunjukkan bahwa K-NN memiliki performa yang sangat superior dan stabil dengan skor precision, recall, dan f1-score yang hampir sempurna pada kedua kelas, sementara Naive Bayes mengalami penurunan performa drastis pada kelas 0—tercermin dari rendahnya precision (0.51) dan f1-score (0.67)—yang mengindikasikan bahwa model Naive Bayes cenderung memberikan banyak false positive dengan mengklasifikasikan trafik normal secara keliru sebagai serangan.



Gambar 2.2 Confusion Matrix K-NN dan Naïve Bayes

Hasil dari penelitian menunjukkan adanya perbedaan yang signifikan dalam karakteristik performa antara algoritma K-Nearest Neighbor (K-NN) dan Naive Bayes berdasarkan parameter yang digunakan untuk evaluasi. Model K-NN mencapai tingkat akurasi yang sangat tinggi, yakni 99,95%, dan memperlihatkan kemampuan luar biasa dalam mendeteksi kelas minoritas, sehingga efektif untuk mengenali berbagai jenis serangan. Meski begitu, kelebihan ini disertai dengan waktu prediksi yang cukup lama, yaitu sekitar ±16,89 detik, yang bisa menjadi kendala pada sistem yang memerlukan respons secara real-time. Di sisi lain, algoritma Naive Bayes meraih akurasi sebesar 99,21% dengan waktu prediksi yang sangat cepat, yaitu sekitar ±0,034 detik, sehingga lebih unggul dalam efisiensi komputasi. Namun, model ini menunjukkan kelemahan dalam mendeteksi kelas normal, yang disebabkan oleh adanya ketidakseimbangan data dalam dataset. Parameter-parameter evaluasi tersebut menjadi dasar utama dalam analisis perbandingan antara akurasi klasifikasi dan

efisiensi waktu prediksi dalam konteks pengembangan sistem untuk deteksi serangan DoS.

3. HASIL DAN ANALISIS

Berdasarkan hasil pengujian, algoritma K-NN mencapai akurasi tertinggi (99,95%), sedikit lebih unggul dibandingkan Naive Bayes (99,21%). Keunggulan utama K-NN terlihat tidak hanya pada akurasi total, tetapi juga pada ketepatan deteksi per-kelas, yang menunjukkan kemampuan K-NN dalam mengenali pola serangan DoS secara lebih konsisten pada setiap kategori lalu lintas jaringan [9].

3.1. Hasil K-NN

K-NN melakukan klasifikasi berdasarkan kedekatan jarak antar data pada ruang fitur beserta dengan memecah data menjadi dua kelas berbeda yang dapat dikelompokkan dengan baik, sehingga sangat efektif dalam memisahkan pola trafik normal dan trafik serangan yang memiliki karakteristik berbeda secara signifikan [9].

Berdasarkan analisis klasifikasi dan confusion matrix, algoritma K-NN menunjukkan kinerja yang luar biasa dalam mengidentifikasi serangan DoS, dengan tingkat akurasi mencapai 99,95% dan nilai F1-score yang hampir menyentuh 1,00 untuk kedua kategori. Pada kategori minoritas (kelas 0), K-NN mencatat precision sebesar 0,99 dan recall mencapai 0,96, yang menunjukkan kemampuan yang tinggi dalam mengenali serangan tanpa menghasilkan banyak false positive ataupun false negative.

Confusion matrix milik K-NN menunjukkan bahwa dari total 161 data untuk kelas 0, sebanyak 154 data berhasil dikelompokkan dengan benar, hanya 7 data yang salah klasifikasi, dan terdapat kesalahan yang sangat minimal pada kelas mayoritas (hanya 2 data). Ini mengindikasikan bahwa K-NN bukan hanya unggul dalam akurasi keseluruhan, tetapi juga konsisten dalam ketepatan deteksi pada masing-masing kelas, yang sangat penting dalam konteks Sistem Deteksi Intrusi (IDS).

Meskipun demikian, keunggulan dalam hal akurasi dari K-NN dibayarkan dengan waktu prediksi yang relatif lambat (sekitar 16,89 detik). Hal ini disebabkan oleh sifat K-NN sebagai pembelajar malas, di mana perhitungan jarak dilakukan untuk seluruh data pelatihan pada saat fase prediksi.

3.2. Hasil Naive Bayes

Sebaliknya, algoritma Naive Bayes menunjukkan performa yang sangat cepat, dengan waktu prediksi hanya 0,0342 detik, jauh lebih cepat dibandingkan K-NN. Tingkat akurasi secara keseluruhan yang dicapai juga tetap tinggi, yaitu 99,21%, yang menunjukkan bahwa Naive Bayes masih sangat cocok digunakan dalam klasifikasi serangan DoS.

Namun, jika dianalisis lebih lanjut pada laporan klasifikasi per kelas, terlihat bahwa precision pada kelas 0 hanya mencapai 0,51, meskipun recall mencapai 0,99. Ini menunjukkan bahwa Naive Bayes cenderung menghasilkan false positive yang lebih tinggi pada kelas minoritas, yaitu mengidentifikasi lalu lintas normal sebagai serangan. Hal ini juga terlihat pada confusion matrix, di mana terdapat 156 instance kelas 1 yang salah diklasifikasikan sebagai kelas 0.

Fenomena ini dapat dipahami melalui asumsi independensi antar fitur yang dipakai oleh Naive Bayes, yang sering kali tidak sepenuhnya dipenuhi dalam data lalu lintas jaringan yang kompleks dan saling berhubungan. Penelitian mengenai deteksi botnet dan DDoS menunjukkan bahwa meskipun Naive Bayes memiliki keunggulan dalam efisiensi komputasi, kinerjanya dapat menurun pada dataset yang memiliki ketidakseimbangan kelas dan ketergantungan fitur yang tinggi.

Naive Bayes menunjukkan keunggulan signifikan dalam hal kecepatan pemrosesan, menjadikannya sangat sesuai untuk kebutuhan deteksi dini (early warning system). Kompleksitas komputasi Naive Bayes yang rendah serta asumsi independensi antar fitur memungkinkan algoritma ini melakukan klasifikasi dalam waktu yang sangat singkat.

Berdasarkan hasil diskusi tersebut, dapat ditarik Kesimpulan bahwa efektivitas algoritma sangat bergantung pada metrik evaluasi dan kebutuhan sistem. Jika efektivitas diukur berdasarkan akurasi, sensitivitas, dan ketepatan deteksi per-kelas, maka K-NN merupakan algoritma yang lebih unggul. Namun, jika efektivitas didefinisikan dari sisi kecepatan respons dan efisiensi komputasi, maka Naive Bayes menjadi pilihan yang lebih tepat. Oleh karena itu, dalam implementasi nyata, pemilihan algoritma perlu disesuaikan dengan kebutuhan operasional sistem IDS, apakah lebih menekankan akurasi maksimal atau respons real-time [10].

DAFTAR PUSTAKA

[1] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes,” 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[2] M. N. Faiz, R. H. Maharrani, L. Sari, A. W. Muhammad, and A. R. Supriyono, “Classification of DDoS Attacks based on Network Traffic Patterns Using the k-Nearest Neighbor (k-NN) Algorithm,” *J. Informatics Inf. Syst. Softw. Eng. Appl.*, vol. 7, no. 2, pp. 173–182, May 2025, doi: 10.20895/inista.v7i2.1834.

[3] A. Irfani, N. Iman, F. Dwi Sumadi, and Z. Sari, "Low Rate DDOS Attack Detection Using KNN On SD-IOT," *REPOSITOR*, vol. 5, no. 1, pp. 603–608, 2023.

[4] J. Parez, M. Alamsyah, F. Rahma, and A. Kurniawardhani, "Sains dan Teknologi KLASIFIKASI SERANGAN DISTRIBUTED DENIAL OF SERVICE MENGGUNAKAN ENSEMBLE STACKING," vol. 12, no. 4, pp. 1874–1893, 2025.

[5] R. S. Daulay, "Analisis Kritis dan Pengembangan Algoritma K-Nearest Neighbor (KNN): Sebuah Tinjauan Literatur," *J. Pendidik. Sains dan Komput.*, vol. 4, no. 02, pp. 131–141, Dec. 2024, doi: 10.47709/jpsk.v4i02.5055.

[6] K. S. Arlandy, A. Faqih, and A. R. Rinaldi, "Mengoptimalkan Kinerja Naïve Bayes Pada Ancaman Modern Dengan Menggunakan PCA Pada Data Intrusion Detection System (IDS)," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 1, pp. 25–37, 2025, doi: 10.47324/ilkominfo.v8i1.303.

[7] 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.

[8] A. Z. Macfud, A. P. Kusuma, and W. D. Puspitasari, "Analisis Algoritma Naive Bayes Classifier (Nbc)," *J. Mhs. Tek. Inform.*, vol. 7, no. 1, pp. 87–94, 2023.

[9] A. D. Afifaturahman, F. Maulana, and S. Artikel, "Perbandingan Algoritma K-Nearest Neighbour (KNN) dan Naive Bayes pada Intrusion Detection System (IDS) INFORMASI ARTIKEL ABSTRACT," *Innov. Res. INFORMATICS*, vol. 3, no. 1, pp. 17–25, 2021, [Online]. Available: http://innovatics.unsil.ac.id

[10] F. Azhari, B. Hananto, and I. Ernawati, "Perbandingan Kinerja Algoritma Dalam Klasifikasi Serangan DDoS Berdasarkan Data CIC IoMT Dataset," Aug. 2025.