JURNAL TAMPIASIH
INSTITUT TEKNOLOGI DAN KESEHATAN ASPIRASI
E-ISSN : 2986 - 8742

ANALISIS PERBANDINGAN ALGORITMA KNN DAN NAIVE BAYES UNTUK IDENTIFIKASI SERANGAN BERDASARKAN DATA LOG JARINGAN

Muh. Yusril Hidayat[1], Olva Routania[2]
[1]Prodi Teknologi Informasi, Institut Teknologi dan Kesehatan Aspirasi Lombok Timur, Indonesia
[2]Prodi Ilmu Komunikasi Universitas Slamet Riyadi Surakarta, Indonesia

Article Information

Article history:
Received: 16/07/2026

Approved: 30/07/2026

Keywords:
K-Nearest Neighbor (KNN); Naive Bayes; machine learning; network security; network log data; attack identification.

Kata Kunci:
K-Nearest Neighbor (KNN); Naive Bayes; machine learning; keamanan jaringan; data log jaringan; identifikasi serangan.

Corresponding author:
muhyusrilhidayat23@gmail.com

ABSTRAK

Peningkatan aktivitas jaringan komputer menyebabkan semakin besarnya volume data log yang perlu dianalisis untuk membedakan aktivitas normal dan serangan siber. Pemanfaatan machine learning dapat membantu proses identifikasi serangan secara lebih cepat dan terukur. Penelitian ini bertujuan menerapkan dan membandingkan algoritma K-Nearest Neighbor (KNN) dan Naive Bayes dalam mengidentifikasi serangan berdasarkan data log jaringan serta mengevaluasi kinerja kedua algoritma menggunakan accuracy, precision, recall, F1-score, AUC, dan waktu komputasi. Metode penelitian menggunakan dataset log jaringan sintetis sebanyak 2.000 record yang terdiri atas 12 atribut prediktor dan satu atribut target dengan dua kelas, yaitu normal dan attack. Data dibagi menjadi 80% data latih dan 20% data uji, kemudian dilakukan transformasi fitur kategorikal, standardisasi menggunakan StandardScaler, serta pemberian noise pada data uji. Algoritma KNN diuji dengan nilai K=1 sampai 20 dan diperoleh K optimal sebesar 5, sedangkan algoritma pembanding menggunakan Gaussian Naive Bayes. Hasil penelitian menunjukkan bahwa KNN memperoleh accuracy 90,25%, precision 89,69%, recall 92,59%, dan F1-score 91,12%, sedangkan Naive Bayes memperoleh accuracy 90,00%, precision 89,64%, recall 92,13%, dan F1-score 90,87%. Nilai AUC KNN sebesar 0,9074 dan Naive Bayes sebesar 0,9060. Naive Bayes memiliki waktu komputasi lebih singkat, sementara hasil 5-fold cross-validation menunjukkan accuracy 92,31% untuk Naive Bayes dan 92,13% untuk KNN. Dengan demikian, kedua algoritma mampu mengidentifikasi serangan dengan performa yang relatif berdekatan, dengan karakteristik keunggulan yang berbeda pada performa klasifikasi dan efisiensi komputasi.

ABSTRACT

Increased computer network activity has led to a growing volume of log data requiring analysis to distinguish between normal activity and cyberattacks. Machine learning can facilitate faster and more scalable attack identification. This study aims to implement and compare the K-Nearest Neighbor (KNN) and Naive Bayes algorithms in identifying attacks based on network log data, evaluating their performance using accuracy, precision, recall, F1-score, AUC, and computation time. The research methodology utilizes a synthetic network log dataset of 2,000 records, comprising 12 predictor attributes and one target attribute with two classes: normal and attack. The data was split into 80% training data and 20% testing data, followed by categorical feature

transformation, standardization using StandardScaler, and the introduction of noise to the testing data. The KNN algorithm was tested with K values ranging from 1 to 20, identifying an optimal K of 5, while Gaussian Naive Bayes was used as the comparative algorithm. The results show that KNN achieved an accuracy of 90.25%, precision of 89.69%, recall of 92.59%, and F1-score of 91.12%, whereas Naive Bayes achieved an accuracy of 90.00%, precision of 89.64%, recall of 92.13%, and F1-score of 90.87%. The AUC values were 0.9074 for KNN and 0.9060 for Naive Bayes. Naive Bayes demonstrated shorter computation time, while 5-fold cross-validation results showed an accuracy of 92.31% for Naive Bayes and 92.13% for KNN. Thus, both algorithms are capable of identifying attacks with relatively similar performance levels, though they exhibit distinct strengths regarding classification performance and computational efficiency..

© 2026 TAMPIASIH

PENDAHULUAN

Perkembangan teknologi informasi dan semakin luasnya penggunaan jaringan komputer menyebabkan volume aktivitas jaringan yang harus dipantau semakin besar. Setiap aktivitas komunikasi pada jaringan dapat menghasilkan data log yang merekam informasi mengenai koneksi, alamat sumber dan tujuan, protokol, port, durasi komunikasi, serta karakteristik lalu lintas lainnya. Data tersebut dapat dimanfaatkan sebagai sumber informasi untuk mengidentifikasi aktivitas normal maupun aktivitas yang mengindikasikan adanya serangan siber. Dalam konteks keamanan jaringan, kemampuan untuk mendeteksi serangan secara cepat dan akurat menjadi bagian penting dari Intrusion Detection System (IDS). Penelitian mengenai deteksi intrusi menunjukkan bahwa pendekatan machine learning banyak digunakan karena mampu mempelajari pola dari karakteristik lalu lintas jaringan dan mengklasifikasikan aktivitas ke dalam kategori normal atau serangan (Lysenko et al., 2022). Dengan demikian, pemanfaatan data log jaringan sebagai sumber data klasifikasi memiliki relevansi yang kuat dalam pengembangan mekanisme deteksi serangan berbasis data.

Salah satu pendekatan yang banyak digunakan dalam klasifikasi serangan jaringan adalah machine learning terawasi (supervised learning). Algoritma seperti K-Nearest Neighbor (KNN) dan Naive Bayes memiliki karakteristik yang relatif sederhana dibandingkan sejumlah model pembelajaran mesin yang lebih kompleks. KNN melakukan klasifikasi berdasarkan kedekatan suatu data terhadap sejumlah data tetangga terdekat, sedangkan Naive Bayes menggunakan pendekatan probabilistik berdasarkan probabilitas kelas dan karakteristik fitur. Penelitian tentang deteksi serangan pada jaringan Internet of Things menunjukkan bahwa algoritma KNN termasuk algoritma yang dapat digunakan untuk menganalisis karakteristik lalu lintas jaringan, sementara Naive Bayes juga menjadi salah satu algoritma klasifikasi yang digunakan dalam penelitian IDS (Lysenko et al., 2022). Penggunaan dua algoritma tersebut menjadi menarik untuk dibandingkan karena keduanya memiliki mekanisme klasifikasi yang berbeda, sehingga kinerjanya dapat dipengaruhi oleh karakteristik data log jaringan yang digunakan.

Permasalahan dalam identifikasi serangan jaringan tidak hanya berkaitan dengan kemampuan algoritma menghasilkan klasifikasi, tetapi juga dengan karakteristik data yang digunakan. Data jaringan dapat memiliki jumlah fitur yang banyak, distribusi data yang tidak seragam, serta ketidakseimbangan jumlah antara aktivitas normal dan berbagai jenis serangan. Kondisi tersebut dapat memengaruhi kinerja model klasifikasi dan menyebabkan nilai akurasi saja tidak cukup untuk menggambarkan kemampuan model dalam mendeteksi serangan. Kajian dan penelitian terkini mengenai IDS memperlihatkan perhatian yang semakin besar terhadap pemilihan

fitur, ketidakseimbangan data, serta evaluasi menggunakan berbagai metrik kinerja (Özgül et al., 2025). Oleh karena itu, penelitian mengenai perbandingan algoritma KNN dan Naive Bayes perlu mempertimbangkan tidak hanya akurasi, tetapi juga precision, recall, F1-score, dan apabila memungkinkan waktu pemrosesan sebagai dasar evaluasi performa.

Data log jaringan juga memiliki karakteristik yang berbeda dari data klasifikasi pada domain umum karena setiap catatan dapat merepresentasikan suatu aktivitas komunikasi atau kejadian pada jaringan. Informasi tersebut dapat digunakan untuk membentuk fitur yang merepresentasikan pola serangan, misalnya frekuensi koneksi, durasi koneksi, protokol yang digunakan, jumlah paket, atau karakteristik lalu lintas lainnya. Penelitian Lysenko et al. (2022) memperlihatkan bahwa fitur lalu lintas dapat digunakan untuk mendeteksi serangan siber dengan pendekatan machine learning. Penelitian yang lebih baru juga menunjukkan bahwa sistem pemantauan jaringan berbasis pembelajaran mesin dapat menggabungkan berbagai algoritma klasifikasi untuk mendeteksi ancaman keamanan (Eshmawi et al., 2026). Hal ini menunjukkan bahwa pengolahan data jaringan menjadi fitur yang representatif merupakan tahapan penting sebelum algoritma klasifikasi diterapkan.

Kajian teoretis juga menegaskan bahwa IDS berbasis machine learning dapat menggunakan pendekatan berbasis aturan maupun berbasis data, dengan data log jaringan diproses menjadi fitur yang membedakan aktivitas normal dari aktivitas serangan. Literatur terbaru mengenai IDS menunjukkan penggunaan berbagai sumber data, termasuk network traffic, system logs, dan host activity, sebagai sumber fitur untuk proses klasifikasi (Ahmed & Askar, 2026). Meskipun penelitian tentang IDS berbasis machine learning telah berkembang, sebagian besar penelitian berfokus pada pengembangan model hibrida, ensemble, optimasi fitur, atau algoritma yang lebih kompleks (Özgül et al., 2025; Eshmawi et al., 2026), sehingga perbandingan langsung dua algoritma klasifikasi yang relatif sederhana seperti KNN dan Naive Bayes pada sumber data dan prosedur evaluasi yang sama masih belum menjadi fokus utama.

RUMUSAN MASALAH

Berdasarkan latar belakang tersebut, terdapat beberapa permasalahan yang dapat diidentifikasi. Pertama, data log jaringan yang berukuran besar dan memiliki karakteristik fitur yang beragam membutuhkan metode klasifikasi yang mampu membedakan aktivitas normal dan aktivitas serangan secara konsisten. Kedua, perbedaan mekanisme antara KNN dan Naive Bayes dapat menghasilkan performa yang berbeda ketika diterapkan pada data log jaringan tertentu. Ketiga, penggunaan akurasi sebagai satu-satunya indikator evaluasi dapat memberikan gambaran yang kurang lengkap ketika dataset memiliki distribusi kelas yang tidak seimbang. Keempat, terdapat kebutuhan untuk mengetahui bagaimana karakteristik data jaringan memengaruhi hasil klasifikasi masing-masing algoritma.

Kesenjangan penelitian juga terletak pada kebutuhan untuk menghubungkan hasil performa algoritma dengan karakteristik data yang digunakan. Model yang menghasilkan akurasi tinggi belum tentu memiliki kemampuan yang sama dalam mengenali seluruh kategori serangan, terutama apabila terdapat ketidakseimbangan kelas (Lysenko et al., 2022; Özgül et al., 2025). Oleh sebab itu, penelitian ini diarahkan tidak hanya untuk menentukan nilai metrik performa, tetapi juga menganalisis perbedaan karakteristik KNN dan Naive Bayes ketika diterapkan pada data log jaringan, sehingga dapat memberikan gambaran yang lebih terukur mengenai kelebihan dan keterbatasan masing-masing algoritma.

Berdasarkan uraian tersebut, rumusan masalah penelitian ini adalah sebagai berikut.

1) Bagaimana penerapan algoritma KNN untuk mengidentifikasi serangan berdasarkan data log jaringan?

2) Bagaimana penerapan algoritma Naive Bayes untuk mengidentifikasi serangan berdasarkan data log jaringan?
3) Bagaimana perbandingan kinerja algoritma KNN dan Naive Bayes berdasarkan metrik accuracy, precision, recall, dan F1-score?
4) Bagaimana karakteristik hasil klasifikasi kedua algoritma dalam membedakan aktivitas normal dan aktivitas serangan pada data log jaringan?

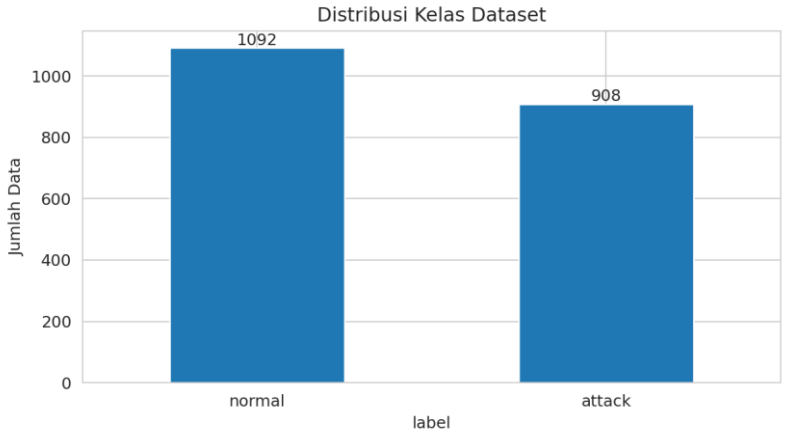
Tujuan Penelitian

Penelitian ini bertujuan untuk menerapkan dan membandingkan algoritma KNN dan Naive Bayes dalam mengidentifikasi serangan berdasarkan data log jaringan serta mengevaluasi performanya menggunakan accuracy, precision, recall, dan F1-score. Secara akademik, penelitian ini diharapkan memberikan kontribusi berupa analisis empiris mengenai penerapan dua algoritma klasifikasi dengan pendekatan berbeda pada data keamanan jaringan.

Secara praktis, hasil penelitian dapat menjadi bahan pertimbangan dalam memilih metode klasifikasi untuk pengembangan mekanisme identifikasi serangan berbasis data log, khususnya pada lingkungan yang membutuhkan model relatif sederhana dan dapat dievaluasi secara terukur. Penelitian ini juga dapat menjadi dasar bagi penelitian berikutnya untuk mengembangkan perbandingan dengan algoritma lain, melakukan seleksi fitur, menangani ketidakseimbangan kelas, atau mengembangkan model IDS yang lebih kompleks.

HASIL DAN PEMBAHASAN PENELITIAN

C.1 Karakteristik Data Penelitian



Gambar 1. Distribusi Kelas Dataset

Penelitian ini menggunakan data log jaringan sintetis yang dibangkitkan secara terprogram untuk merepresentasikan karakteristik data intrusion detection. Dataset terdiri atas 2.000 record dengan 13 kolom, yaitu 12 atribut prediktor dan satu atribut target berupa label. Atribut yang digunakan meliputi duration, protocol_type, service, flag, src_bytes, dst_bytes, count, srv_count, serror_rate, same_srv_rate, dst_host_count, dan dst_host_srv_count. Label klasifikasi terdiri atas dua kelas, yaitu normal dan attack.

Dataset dirancang agar lebih realistis daripada data yang terpisah secara sempurna. Pada proses pembangkitan data terdapat overlap distribusi antara kelas normal dan attack, korelasi antarfitur seperti src_bytes dengan dst_bytes serta count dengan srv_count, dan label noise sebesar 8%. Korelasi antarfitur tersebut secara khusus berpotensi memengaruhi Naive Bayes karena algoritma ini menggunakan asumsi independensi bersyarat antarfitur.

Setelah proses pembangkitan dan penambahan noise, distribusi label terdiri atas 1.078 data normal (53,90%) dan 922 data attack (46,10%). Dengan demikian, dataset relatif seimbang sehingga evaluasi tidak hanya mengandalkan accuracy, tetapi juga precision, recall, dan F1-score.

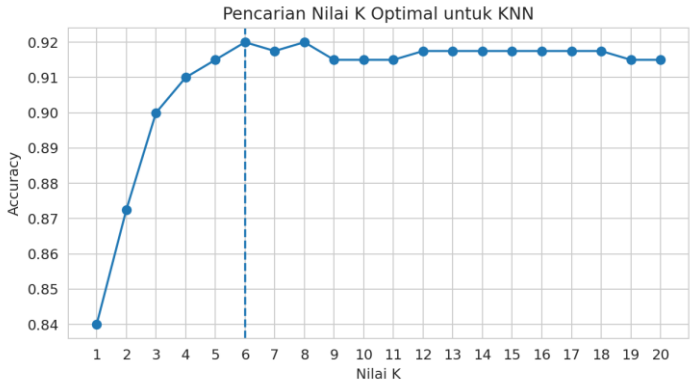
Tabel 1. Data Presentase Kelas Data Set

Kelas Data	Jumlah Data	Persentase
Normal	1.078	53,90%
Attack	922	46,10%
Total	2.000	100,00%

Pemeriksaan struktur dataset menunjukkan bahwa seluruh 2.000 record memiliki nilai non-null. Dari 13 kolom, lima atribut bertipe float64, empat atribut bertipe int64, dan empat atribut bertipe object. Fitur kategorikal protocol_type, service, dan flag kemudian dikonversi menggunakan LabelEncoder, sedangkan label normal dan attack juga dikodekan menjadi nilai numerik.

Selanjutnya, data dibagi menjadi 80% data latih dan 20% data uji dengan stratified split. Sebanyak 1.600 record digunakan sebagai data latih dan 400 record sebagai data uji. Fitur kemudian distandardisasi menggunakan StandardScaler. Untuk mensimulasikan kondisi data lapangan yang tidak sepenuhnya bersih, data uji diberi derau pengukuran dengan distribusi normal dan standar deviasi 0,6.

C.2 Hasil Klasifikasi Algoritma KNN dan Naive Bayes



Gambar 2. Pencarian Nilai K Optimal untuk KNN

Model K-Nearest Neighbors (KNN) diuji menggunakan nilai K dari 1 sampai 20. Berdasarkan pencarian nilai K, diperoleh K optimal sebesar 5 dengan accuracy pengujian sebesar 90,25%. Model KNN kemudian dilatih kembali menggunakan K=5 dan digunakan untuk menghasilkan prediksi pada 400 data uji.

Model kedua adalah Gaussian Naive Bayes. Algoritma ini dipilih karena fitur yang digunakan telah ditransformasikan ke bentuk numerik/kontinu dan Gaussian Naive Bayes sesuai untuk memodelkan distribusi fitur numerik.

Tabel 2. Data Perbandingan

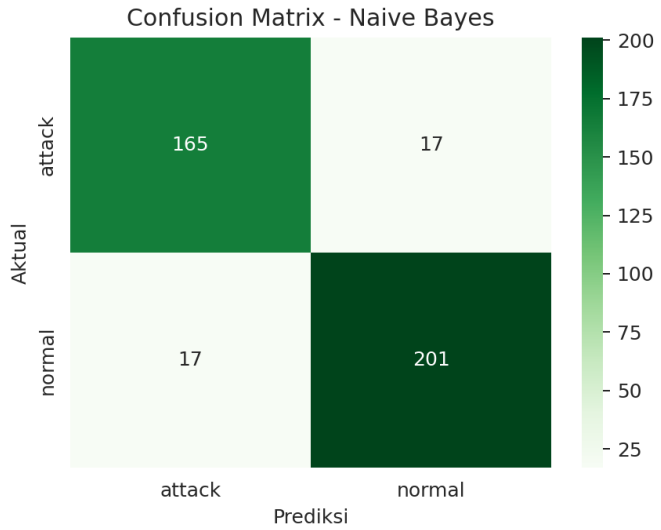
Algoritma	Accuracy	Precision	Recall	F1-score
KNN	90,25%	89,69%	92,59%	91,12%
Naive Bayes	90,00%	89,64%	92,13%	90,87%

Tabel tersebut menunjukkan bahwa kedua algoritma menghasilkan performa yang relatif berdekatan. KNN memperoleh accuracy 90,25%, precision 89,69%, recall 92,59%, dan F1-score 91,12%. Sementara itu, Naive Bayes memperoleh accuracy 90,00%, precision 89,64%, recall 92,13%, dan F1-score 90,87%. Perbedaan performa yang relatif kecil menunjukkan bahwa kedua

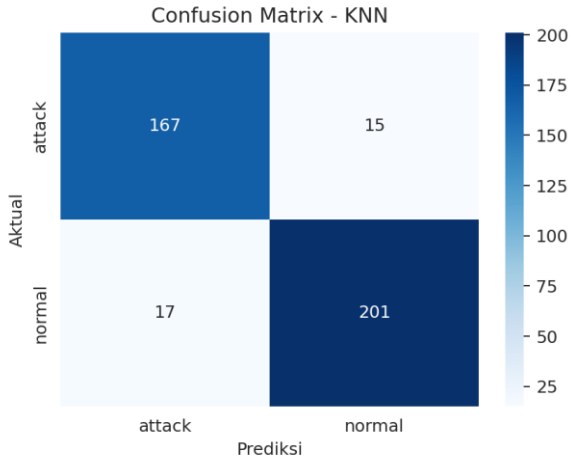
pendekatan mampu mengenali pola antara trafik normal dan serangan pada dataset yang digunakan.

Dalam konteks identifikasi serangan, recall menjadi metrik penting karena menunjukkan proporsi serangan yang berhasil dikenali oleh model. Recall KNN sebesar 92,59% berarti sebagian besar data serangan pada data uji berhasil diidentifikasi. Recall Naive Bayes sebesar 92,13% juga menunjukkan kemampuan deteksi yang tinggi, meskipun sedikit lebih rendah dibandingkan KNN.

C.2.1 Confusion Matrix



Gambar 4. Confusion Matrix Naive Bayes



Gambar 3. Confusion Matrix KNN

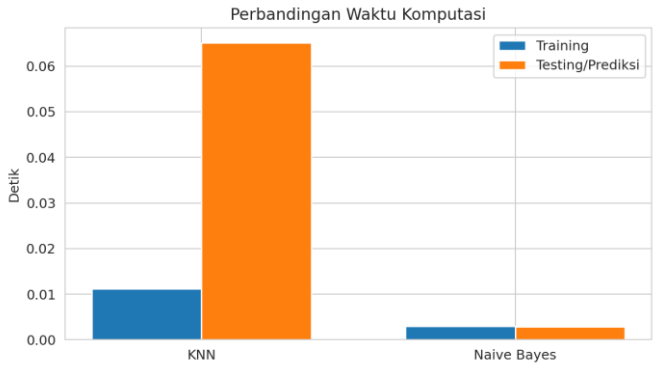
Tabel 3. Cnfusion Matrix

Model	Aktual Attack → Prediksi Attack	Aktual Attack → Prediksi Normal	Aktual Normal → Prediksi Attack	Aktual Normal → Prediksi Normal
KNN	161	23	16	200
Naive Bayes	161	23	17	199

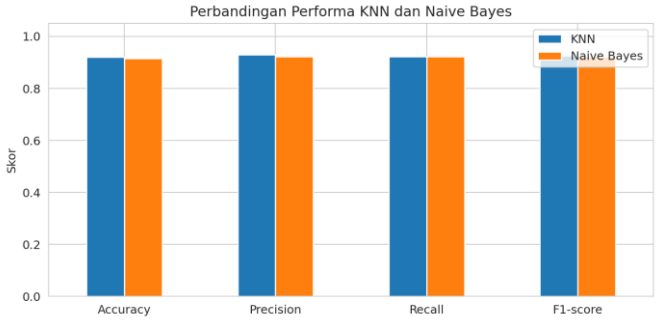
Confusion matrix menunjukkan bahwa KNN mengklasifikasikan 161 data attack dengan benar dan 200 data normal dengan benar. Terdapat 23 data attack yang diprediksi sebagai normal (false negative) dan 16 data normal yang diprediksi sebagai attack (false positive). Naive Bayes juga berhasil mengidentifikasi 161 data attack dan 199 data normal, dengan 23 false negative dan 17

false positive. Dengan demikian, pada data uji ini KNN menghasilkan satu false positive lebih sedikit dibandingkan Naive Bayes, sedangkan jumlah false negative keduanya sama.

C.2.2 Waktu Komputasi



Gambar 6. Perbandingan Waktu Komputasi



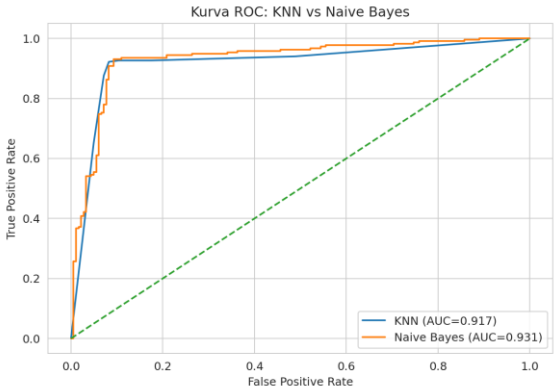
Gambar 5. Perbandingan Performa KNN dan Naive Bayes

Tabel 3. Perbandingan Waktu

Algoritma	Waktu Training	Waktu Testing/Prediksi
KNN	0,01119 detik	0,06513 detik
Naive Bayes	0,00292 detik	0,00283 detik

Dari sisi waktu komputasi, Naive Bayes membutuhkan waktu training dan testing yang jauh lebih singkat daripada KNN pada eksperimen ini. KNN membutuhkan 0,01119 detik untuk training dan 0,06513 detik untuk testing, sedangkan Naive Bayes membutuhkan 0,00292 detik untuk training dan 0,00283 detik untuk testing. Perbedaan waktu testing berkaitan dengan karakteristik KNN sebagai lazy learner yang melakukan perhitungan berdasarkan kedekatan data saat prediksi, sedangkan Naive Bayes telah membentuk parameter probabilistik pada tahap training.

C.2.3 ROC dan AUC



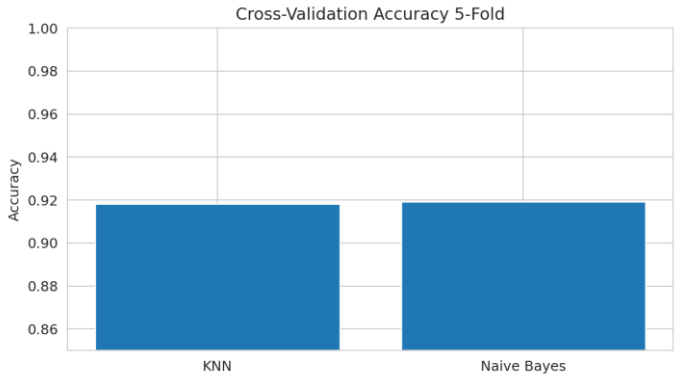
Gambar 7. Kurva ROC dan AUC

Tabel 4. Nilai KKN & Naïve Bayes

Algoritma	AUC
KNN	0,9074
Naive Bayes	0,9060

Nilai AUC KNN sebesar 0,9074 dan Naive Bayes sebesar 0,9060 menunjukkan bahwa kedua model memiliki kemampuan diskriminasi yang baik dalam membedakan kelas normal dan attack pada data uji. Nilai AUC KNN sedikit lebih tinggi, tetapi selisihnya kecil sehingga perbedaan kemampuan diskriminasi kedua model pada eksperimen ini relatif terbatas.

C.2.4 Cross-Validation



Gambar 8. Cross-Validation Accuracy 5-Fold

Algoritma	Rata-rata Accuracy 5-Fold	Standar Deviasi
KNN	92,13%	0,0078
Naive Bayes	92,31%	0,0070

Hasil validasi silang 5-fold pada data latih menunjukkan rata-rata accuracy KNN sebesar 92,13% dengan standar deviasi 0,0078, sedangkan Naive Bayes memperoleh rata-rata accuracy 92,31% dengan standar deviasi 0,0070. Hasil ini memperlihatkan bahwa performa Naive Bayes pada validasi silang sedikit lebih tinggi dan variasinya sedikit lebih rendah. Temuan tersebut juga menunjukkan bahwa hasil pada satu pembagian data uji tidak sepenuhnya menggambarkan seluruh variasi performa model.

C.3 Temuan Utama

- Dataset penelitian terdiri atas 2.000 data sintetis dengan dua kelas, yaitu normal dan attack, dan distribusi kelas setelah penambahan label noise relatif seimbang.
- KNN dengan K=5 menghasilkan accuracy 90,25%, precision 89,69%, recall 92,59%, dan F1-score 91,12%.
- Naive Bayes menghasilkan accuracy 90,00%, precision 89,64%, recall 92,13%, dan F1-score 90,87%.
- Pada data uji, kedua model memiliki jumlah false negative yang sama, yaitu 23 data, sedangkan KNN menghasilkan false positive 16 data dan Naive Bayes 17 data.
- Naive Bayes memiliki waktu training dan testing yang lebih singkat dibandingkan KNN.
- Hasil cross-validation menunjukkan rata-rata accuracy Naive Bayes 92,31% dan KNN 92,13%, sehingga performa keduanya tetap berdekatan ketika dievaluasi pada beberapa subset data.
- Nilai AUC KNN sebesar 0,9074 dan Naive Bayes sebesar 0,9060 menunjukkan kemampuan diskriminasi kedua model yang relatif serupa pada eksperimen ini.

C.4 Pembahasan

C.4.1 Interpretasi Temuan

Hasil penelitian menunjukkan bahwa KNN dan Naive Bayes sama-sama dapat digunakan untuk mengklasifikasikan data log jaringan menjadi trafik normal dan trafik yang terindikasi serangan. Kinerja KNN yang sedikit lebih tinggi pada data uji dapat dikaitkan dengan kemampuannya memanfaatkan kedekatan antarobservasi setelah fitur distandardisasi. Dengan K=5, keputusan klasifikasi ditentukan berdasarkan lima tetangga terdekat sehingga pola lokal pada ruang fitur dapat dimanfaatkan.

Naive Bayes menghasilkan kinerja yang hampir sama dengan KNN. Hal ini menunjukkan bahwa meskipun terdapat korelasi antarfitur, pendekatan probabilistik masih mampu menangkap informasi yang cukup untuk membedakan dua kelas. Namun, asumsi independensi bersyarat pada Naive Bayes tidak sepenuhnya sesuai dengan karakteristik dataset yang memang dirancang memiliki korelasi antara beberapa fitur.

Perbedaan kecil antara kedua algoritma perlu dipahami bersama dengan hasil validasi silang. Pada satu data uji, KNN memiliki accuracy 90,25%, sedangkan Naive Bayes 90,00%. Sebaliknya, pada 5-fold cross-validation, Naive Bayes memperoleh rata-rata accuracy 92,31%, sedikit lebih tinggi daripada KNN sebesar 92,13%. Perbedaan ini menunjukkan bahwa perubahan subset data dapat memengaruhi urutan performa kedua model.

C.4.2 Analisis Recall dalam Identifikasi Serangan

Recall merupakan metrik yang relevan untuk sistem identifikasi serangan karena false negative berarti aktivitas yang sebenarnya termasuk attack diklasifikasikan sebagai normal. Pada eksperimen ini, recall KNN sebesar 92,59% dan Naive Bayes sebesar 92,13%. Keduanya menunjukkan kemampuan deteksi serangan yang tinggi, dengan KNN menghasilkan recall sedikit lebih tinggi pada data uji. Meskipun demikian, masih terdapat 23 data attack yang tidak terdeteksi oleh masing-masing model, sehingga tidak dapat dikatakan bahwa model mampu mendeteksi seluruh serangan.

C.4.3 Analisis Efisiensi Komputasi

Perbedaan paling jelas antara kedua algoritma terlihat pada waktu komputasi. Naive Bayes memiliki waktu training 0,00292 detik dan waktu testing 0,00283 detik, sedangkan KNN membutuhkan 0,01119 detik untuk training dan 0,06513 detik untuk testing. Kondisi ini sesuai dengan karakteristik algoritma masing-masing. KNN tidak membentuk parameter klasifikasi kompleks pada saat training dan melakukan perhitungan kedekatan pada saat prediksi. Sebaliknya, Naive Bayes menghitung parameter probabilistik pada tahap training sehingga prediksi dapat dilakukan dengan sangat cepat.

Dengan demikian, pemilihan algoritma tidak hanya mempertimbangkan accuracy atau F1-score, tetapi juga kebutuhan waktu komputasi. Pada lingkungan yang membutuhkan prediksi cepat dan berulang, waktu inferensi menjadi aspek penting dalam evaluasi.

C.4.4 Kesesuaian dengan Karakteristik Data

Dataset dibuat dengan overlap antarkelas, korelasi fitur, dan label noise sebesar 8%. Kondisi tersebut membuat klasifikasi tidak menjadi persoalan yang sepenuhnya terpisah secara linear atau sempurna. Hasil accuracy sekitar 90% menunjukkan bahwa kedua algoritma mampu memanfaatkan pola yang terdapat pada fitur, namun tetap menghasilkan kesalahan klasifikasi. Hal ini sesuai dengan tujuan pembangkitan data sintetis untuk memberikan kondisi eksperimen yang lebih realistis dibandingkan dataset yang dapat dipisahkan secara sempurna.

C.4.5 Implikasi Hasil Penelitian

Secara akademis, penelitian ini menunjukkan perbedaan karakteristik dua algoritma klasifikasi dalam mengolah data log jaringan. KNN memberikan hasil sedikit lebih tinggi pada data uji untuk accuracy, precision, recall, F1-score, dan AUC, sedangkan Naive Bayes memberikan efisiensi komputasi yang jauh lebih tinggi dan rata-rata cross-validation yang sedikit lebih baik. Oleh karena itu, hasil penelitian menunjukkan bahwa evaluasi model perlu dilakukan menggunakan beberapa indikator secara bersamaan.

Secara praktis, kedua algoritma dapat dijadikan pendekatan awal untuk klasifikasi aktivitas jaringan berdasarkan data log. Namun, hasil ini belum dapat langsung digeneralisasikan sebagai kinerja pada jaringan produksi karena dataset yang digunakan merupakan data sintetis. Penggunaan dataset nyata seperti NSL-KDD, CICIDS2017, UNSW-NB15, atau log IDS/firewall yang relevan diperlukan untuk menguji kemampuan generalisasi.

C.4.6 Keterbatasan Penelitian

- Dataset yang digunakan bersifat sintetis sehingga karakteristiknya belum tentu sepenuhnya mencerminkan trafik jaringan nyata.
- Penelitian hanya membandingkan KNN dan Gaussian Naive Bayes sehingga belum mencakup algoritma lain seperti Decision Tree, Random Forest, Support Vector Machine, atau ensemble.
- Data uji diberi noise pengukuran secara sintetis; kondisi noise pada jaringan nyata dapat memiliki karakteristik berbeda.
- Evaluasi dilakukan pada satu dataset dan satu skenario eksperimen, sehingga generalisasi ke jaringan, perangkat, dan jenis serangan lain masih memerlukan pengujian tambahan.

- Nilai K optimal dipilih berdasarkan accuracy pada data uji dalam notebook, sehingga pada penelitian lanjutan pemilihan hyperparameter sebaiknya dilakukan menggunakan validasi silang pada data training agar data uji tetap menjadi evaluasi akhir yang independen.

Ringkasan Hasil Penelitian

Secara keseluruhan, eksperimen menunjukkan bahwa KNN dan Naive Bayes memiliki performa klasifikasi yang sangat berdekatan. Pada data uji, KNN memperoleh accuracy 90,25%, precision 89,69%, recall 92,59%, dan F1-score 91,12%, sedangkan Naive Bayes memperoleh accuracy 90,00%, precision 89,64%, recall 92,13%, dan F1-score 90,87%. KNN juga memperoleh AUC sedikit lebih tinggi, yaitu 0,9074 dibandingkan 0,9060. Namun, Naive Bayes jauh lebih cepat dalam training dan testing serta memperoleh rata-rata cross-validation sedikit lebih tinggi, yaitu 92,31% dibandingkan 92,13% pada KNN. Temuan tersebut memperlihatkan bahwa pemilihan model perlu mempertimbangkan kombinasi performa klasifikasi, kemampuan mendeteksi serangan, konsistensi, dan efisiensi komputasi.

KESIMPULAN

Berdasarkan hasil penelitian mengenai analisis perbandingan algoritma K-Nearest Neighbor (KNN) dan Naive Bayes untuk identifikasi serangan berdasarkan data log jaringan, dapat disimpulkan bahwa kedua algoritma mampu mengklasifikasikan aktivitas jaringan ke dalam kategori normal dan attack dengan performa yang relatif berdekatan. Pada data uji, algoritma KNN dengan nilai K=5 memperoleh accuracy sebesar 90,25%, precision 89,69%, recall 92,59%, dan F1-score 91,12%. Sementara itu, Naive Bayes memperoleh accuracy sebesar 90,00%, precision 89,64%, recall 92,13%, dan F1-score 90,87%.

Hasil confusion matrix menunjukkan bahwa kedua algoritma memiliki jumlah false negative yang sama, yaitu 23 data attack yang diklasifikasikan sebagai normal. KNN menghasilkan 16 false positive, sedangkan Naive Bayes menghasilkan 17 false positive. Hal tersebut menunjukkan bahwa kedua algoritma memiliki kemampuan yang relatif serupa dalam mengidentifikasi serangan pada dataset yang digunakan.

Dari sisi kemampuan diskriminasi, KNN memperoleh nilai AUC sebesar 0,9074, sedangkan Naive Bayes sebesar 0,9060. Perbedaannya relatif kecil sehingga kemampuan kedua model dalam membedakan aktivitas normal dan serangan dapat dikatakan berdekatan. Hasil cross-validation juga menunjukkan bahwa Naive Bayes memperoleh rata-rata accuracy sebesar 92,31%, sedangkan KNN sebesar 92,13%, sehingga performa kedua algoritma tetap relatif stabil dan berdekatan pada beberapa subset data.

Perbedaan yang lebih jelas terlihat pada aspek efisiensi komputasi. Naive Bayes membutuhkan waktu training sebesar 0,00292 detik dan testing sebesar 0,00283 detik, sedangkan KNN membutuhkan waktu training 0,01119 detik dan testing 0,06513 detik. Dengan demikian, karakteristik kedua algoritma memiliki implikasi yang berbeda dalam penerapannya: KNN menunjukkan performa yang sedikit lebih tinggi pada sebagian besar metrik data uji, sedangkan Naive Bayes memberikan efisiensi komputasi yang lebih tinggi.

Secara keseluruhan, penelitian ini menunjukkan bahwa KNN dan Naive Bayes dapat digunakan sebagai pendekatan awal untuk mengidentifikasi serangan berdasarkan data log jaringan. Namun, hasil penelitian belum dapat digeneralisasikan langsung pada jaringan produksi karena dataset yang digunakan merupakan data sintetis. Penelitian selanjutnya perlu menggunakan dataset jaringan nyata dan membandingkan lebih banyak algoritma,

serta mempertimbangkan seleksi fitur, ketidakseimbangan kelas, dan optimasi hyperparameter untuk memperoleh gambaran kemampuan model yang lebih komprehensif.

REFERENSI

Ababneh, J., Al-Nsour, E. Y. A., & Al-Shaikh, A. A. (2026). Enhancing DevOps continuous monitoring phase: Hybrid intrusion detection and ensemble learning system (HIDELS). IEEE. https://ieeexplore.ieee.org/abstract/document/11326691/

Ahmed, A. A., Mahmood, M. M., et al. (2026). Enhanced network intrusion detection and classification based on ensemble learning techniques: A study on the NSL-KDD dataset. Sistemasi: Jurnal Sistem Informasi. https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/view/6308

Ahmed, Z. R., & Askar, S. K. (2026). Advances in intrusion detection systems: Emerging trends, intelligent techniques, and future directions. Engineering Research Express. https://iopscience.iop.org/article/10.1088/2631-8695/ae812d/meta

Chishti, F., & Rathee, G. (2026). An autonomous intrusion detection framework leveraging multi-layered stacking ensemble architectures with dynamic machine learning-driven feature subset. Peer-to-Peer Networking and Applications. https://doi.org/10.1007/s12083-025-02172-9

Ebrahem, O., Dowaji, S., & Alhammoud, S. (2026a). A lightweight machine learning approach for DDoS detection and classification. Scientific Reports. https://www.nature.com/articles/s41598-026-48535-x

Ebrahem, O., Dowaji, S., & Alhammoud, S. (2026b). On the limited generalizability of a universal features set for DDoS detection across network environments. IEEE Access. https://ieeexplore.ieee.org/abstract/document/11346938/

Eshmawi, A. A., Al-Nowami, A., & Mirza, M. (2026). Machine learning-based network monitoring for cybersecurity threat detection. Journal of Network and Systems Management. https://doi.org/10.1007/s10922-025-10001-w

Kamaruddin, A., Chin, T. S., & Galán-Jiménez, J. (2026). The F-ELV-based privacy-preserving framework for intrusion detection in SDN-IoT network. IEEE. https://ieeexplore.ieee.org/abstract/document/11563315/

Kumar, L. K. S., Nethi, S. R., Uyyala, R., Vurubindi, P., et al. (2026). Anomaly-based intrusion detection on benchmark datasets for network security: A comprehensive evaluation. Scientific Reports. https://www.nature.com/articles/s41598-026-38317-w

Lysenko, S., Bobrovnikova, K., Kharchenko, V., & Savenko, O. (2022). IoT multi-vector cyberattack detection based on machine learning algorithms: Traffic features analysis, experiments, and efficiency. Algorithms, 15(7), 239. https://doi.org/10.3390/a15070239

Makhdoomi, P. M. S., Ikhlas, M., Khursheed, A., et al. (2026). Network-based intrusion detection: A comparative analysis of machine learning approaches for improved security. Journal of Cyber Security. https://doi.org/10.1080/23742917.2024.2447119

Mallick, C., Nayak, S., Singh, K. N., & Senapati, M. R. (2026). Securing the Internet of Things through intrusion detection system utilizing machine ensemble learning and feature extraction techniques. SN Computer Science. https://doi.org/10.1007/s42979-025-04648-0

Misriati, T., & Aryanti, R. (2026). Explainable machine learning for multi-class classification of internet firewall traffic. Bulletin of Informatics and Data Science. https://www.ejurnal.pdsi.or.id/index.php/bids/article/view/163

Norouzi, M., Gürkaş-Aydın, Z., Turna, Ö. C., Yağci, M. Y., et al. (2023). A hybrid genetic algorithm-based random forest model for intrusion detection approach in internet of medical things. Applied Sciences, 13(20), 11145. https://www.mdpi.com/2076-3417/13/20/11145

Nourildean, S. W., Mefteh, W., & Frihida, A. M. (2026). Intrusion detection system-based ensemble machine learning to improve IoT network against cyber attacks. The Journal of Supercomputing. https://doi.org/10.1007/s11227-026-08529-y

Ogab, M., Zaidi, S., Bourouis, A., & Calafate, C. T. (2025). Machine learning-based intrusion detection systems for the internet of drones: A systematic literature review. IEEE Access. https://ieeexplore.ieee.org/abstract/document/11018757/

Özgül, M. A., Demirbaş, Ş., & Vadi, S. (2025). A hybrid machine learning approach for cyberattack detection and classification in SCADA systems: A hydroelectric power plant application. Electronics, 15(1), 10. https://www.mdpi.com/2079-9292/15/1/10

Ronanki, S. K., & Killi, B. R. (2026). Machine learning based cyber attack detection and classification in O-RAN. Journal of Network and Systems Management. https://doi.org/10.1007/s10922-026-10035-8

Sharma, H., & Kumar, P. (2026). Security solutions for the Internet of Things using machine learning and deep learning: Current trends and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. https://doi.org/10.1002/widm.70059

Sundar, R., Sandhya, K. S., & Rajpoot, N. K. (2026). Machine learning enabled intrusion detection for terabit optical networks. IEEE. https://ieeexplore.ieee.org/abstract/document/11525652/