Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)

IMPLEMENTASI METODE NAÏVE BAYES DALAM DETEKSI AKSES TIDAK SAH MENGGUNAKAN DATASET UNSW-NB15

Implementation Of The Naïve Bayes Method For Unauthorized Access Detection Using The UNSW-NB15 Dataset

Ahmad Rizeki[1], Yumi Novita Dewi[2*], Imam Syafi'i[3]

Program Studi Sistem Informasi[1,3], Program Studi Informatika[2*]
Fakultas Teknik & Informatika[1,2*,3]
Universitas Bina Sarana Informatika[1,2*,3]

Correspondent Author : yumi.ymd@bsi.ac.id

Authors Email: ahmadrizeki10@gmail.com[1],
yumi.ymd@bsi.ac.id[2*], syafiimam92052@gmail.com[3]

Received: January 07, 2026**. Revised:** May 25, 2026**. Accepted: June** 05, 2026**. Issue Period:** Vol.10 No.3 (2026), Pp.714-720

Abstrak: Perkembangan teknologi informasi dan meningkatnya aktivitas digital telah menyebabkan tingginya risiko serangan terhadap jaringan komputer. Berbagai bentuk serangan siber, seperti akses tidak sah dan aktivitas berbahaya, dapat mengancam keamanan serta kerahasiaan data. Oleh karena itu, diperlukan sebuah mekanisme keamanan yang mampu mendeteksi serangan secara efektif, salah satunya melalui penerapan *Intrusion Detection System* (IDS). Penelitian ini bertujuan untuk mengimplementasikan algoritma Naïve Bayes dalam mendeteksi akses tidak sah pada jaringan komputer. Dataset yang digunakan adalah UNSW-NB15, yang telah melalui tahap praproses data sehingga menghasilkan sebanyak 82.332 record yang siap digunakan untuk proses klasifikasi. Metode evaluasi yang diterapkan adalah 10-Fold Cross Validation dengan bantuan perangkat lunak RapidMiner. Hasil pengujian menunjukkan bahwa algoritma Naïve Bayes mampu memberikan kinerja yang sangat baik dalam mengklasifikasikan trafik jaringan. Model yang dihasilkan memperoleh nilai akurasi sebesar 95,96%, precision 94,11%, recall 98,85%, serta nilai Area Under Curve (AUC) sebesar 0,964. Nilai AUC yang tinggi menunjukkan bahwa model memiliki kemampuan yang sangat baik dalam membedakan antara trafik normal dan trafik serangan. Berdasarkan hasil tersebut, dapat disimpulkan bahwa algoritma Naïve Bayes layak digunakan sebagai metode klasifikasi dalam sistem deteksi intrusi untuk meningkatkan keamanan jaringan komputer.

DOI: 10.52362/jisamar.v10i3.2247

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)

Kata Kunci: Naïve Bayes; Sistem Deteksi Intrusi; Akses Tidak Sah; Keamanan Siber; Dataset UNSW-NB15; Pembelajaran Mesin.

Abstract: *The rapid growth of information technology and digital activities has led to an increasing number of attacks on computer networks. Various types of cyberattacks, such as unauthorized access and malicious activities, pose serious threats to data security and confidentiality. Therefore, an effective security mechanism is required to detect such attacks, one of which is through the implementation of an Intrusion Detection System (IDS). This study aims to apply the Naïve Bayes algorithm to detect unauthorized access in computer networks. The dataset used in this research is the UNSW-NB15 dataset, which was preprocessed to obtain 82,332 records suitable for classification. The evaluation was conducted using the 10-Fold Cross Validation method with the assistance of RapidMiner software. The experimental results indicate that the Naïve Bayes algorithm achieves excellent performance in classifying network traffic. The proposed model attained an accuracy of 95.96%, a precision of 94.11%, a recall of 98.85%, and an Area Under the Curve (AUC) value of 0.964. The high AUC value demonstrates that the model is highly effective in distinguishing between normal traffic and attack traffic. Based on these findings, it can be concluded that the Naïve Bayes algorithm is a reliable and effective method for intrusion detection systems to enhance network security.*

Keywords: *Naïve Bayes; Intrusion Detection System; Unauthorized Access; Cybersecurity; UNSW-NB15 Dataset; Machine Learning.*

I. PENDAHULUAN

Keamanan jaringan komputer merupakan aspek yang sangat krusial dalam infrastruktur teknologi informasi modern. Meningkatnya jumlah pengguna internet, pesatnya perkembangan layanan digital, serta keterbukaan akses terhadap berbagai sistem jaringan telah memperbesar potensi terjadinya serangan siber. Salah satu ancaman yang paling sering terjadi adalah aktivitas akses tidak sah, yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Oleh karena itu, diperlukan mekanisme keamanan yang mampu mendeteksi dan mengidentifikasi serangan secara efektif. Salah satu solusi yang banyak digunakan adalah *Intrusion Detection System* (IDS), yang berfungsi untuk memantau lalu lintas jaringan dan mendeteksi aktivitas yang mencurigakan [1].

Secara umum, IDS diklasifikasikan ke dalam dua pendekatan utama, yaitu *signature-based* dan *anomaly-based*. Pendekatan *signature-based* mendeteksi intrusi berdasarkan pola serangan yang telah diketahui, sedangkan pendekatan *anomaly-based* mengidentifikasi aktivitas yang menyimpang dari perilaku normal jaringan sehingga lebih adaptif terhadap serangan baru atau *zero-day attacks* [2]. Seiring meningkatnya kompleksitas dan volume data jaringan, pendekatan *anomaly-based* banyak dikembangkan dengan memanfaatkan algoritma *machine learning* yang mampu mengolah data dalam jumlah besar dan menghasilkan model klasifikasi yang akurat [3].

Dalam beberapa tahun terakhir, dataset UNSW-NB15 banyak digunakan sebagai dataset modern dalam penelitian IDS karena mampu merepresentasikan karakteristik lalu lintas jaringan serta berbagai jenis serangan siber terkini, seperti DoS, Exploits, Backdoor, Fuzzers, dan Generic [4]. Dataset ini dikembangkan sebagai alternatif terhadap dataset lama, seperti KDD99 dan DARPA, yang dinilai sudah tidak lagi mencerminkan pola serangan jaringan modern. Dengan demikian, penggunaan dataset UNSW-NB15 diharapkan dapat memberikan hasil evaluasi yang lebih relevan dan realistis.

Penelitian-penelitian sebelumnya menunjukkan bahwa algoritma Naïve Bayes, sebagai algoritma klasifikasi berbasis probabilistik, memiliki keunggulan dalam hal kesederhanaan model, efisiensi komputasi,

DOI: 10.52362/jisamar.v10i3.2247

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)

serta kemampuan menangani dataset berdimensi besar [5]. Meskipun memiliki asumsi independensi antar fitur, Naïve Bayes tetap mampu memberikan performa yang kompetitif dalam berbagai studi klasifikasi, termasuk pada bidang keamanan jaringan.

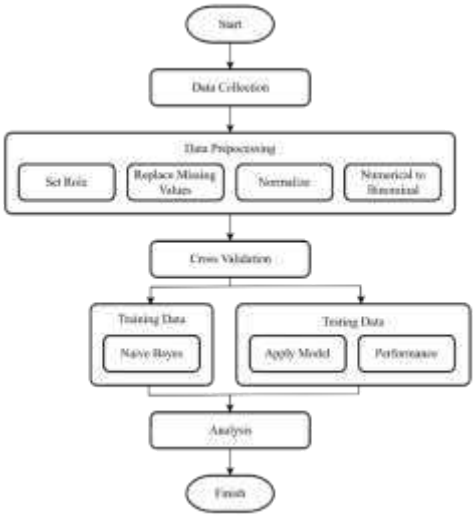
Berdasarkan permasalahan dan peluang yang telah diuraikan, penelitian ini bertujuan untuk menerapkan dan mengevaluasi performa algoritma Naïve Bayes dalam mendeteksi aktivitas akses tidak sah pada jaringan komputer menggunakan dataset UNSW-NB15. Evaluasi kinerja model dilakukan menggunakan metrik *accuracy*, *precision*, *recall*, dan *Area Under Curve* (AUC) guna mengukur kemampuan model dalam membedakan antara trafik normal dan trafik serangan.

Adapun kontribusi utama dari penelitian ini adalah penyajian analisis kinerja algoritma Naïve Bayes pada dataset UNSW-NB15 yang telah dipraproses, serta pemberian gambaran empiris mengenai efektivitas algoritma tersebut sebagai metode klasifikasi dalam sistem deteksi intrusi berbasis *machine learning*. Hasil penelitian ini diharapkan dapat menjadi referensi bagi penelitian selanjutnya dalam pengembangan sistem keamanan jaringan.

Sistematika penulisan dalam penelitian ini disusun sebagai berikut. Bagian pertama berisi pendahuluan yang menguraikan latar belakang, permasalahan, tujuan, dan kontribusi penelitian. Bagian kedua membahas tinjauan pustaka dan landasan teori yang berkaitan dengan IDS, algoritma Naïve Bayes, serta dataset UNSW-NB15. Bagian ketiga menjelaskan metodologi penelitian yang digunakan. Bagian keempat menyajikan hasil pengujian dan pembahasan. Terakhir, bagian kelima berisi kesimpulan dan saran untuk penelitian selanjutnya.

II. METODE DAN MATERI

Penelitian ini menggunakan pendekatan eksperimental dengan menerapkan algoritma Naïve Bayes untuk mendeteksi aktivitas akses tidak sah pada jaringan komputer. Tahapan penelitian meliputi pengumpulan data, praproses data, pemodelan, dan evaluasi performa. Seluruh proses eksperimen dilakukan menggunakan perangkat lunak RapidMiner untuk memastikan konsistensi alur pemodelan dan evaluasi. Alur metodologi penelitian ditunjukkan pada Gambar 1.



Gambar 1. Metodologi Penelitian untuk Pemodelan Naïve Bayes Menggunakan RapidMiner

2.1. Dataset

Dataset yang digunakan dalam penelitian ini adalah UNSW-NB15 yang dikembangkan oleh Australian Cyber Security Centre. Dataset ini dipilih karena merepresentasikan karakteristik lalu lintas jaringan modern dan mencakup berbagai jenis serangan siber, seperti DoS, Exploits, Fuzzers, Backdoor, Reconnaissance, Worm, dan Shellcode. Setelah dilakukan proses pembersihan data, dataset yang digunakan berjumlah 82.332 record dengan 45 atribut, yang terdiri atas fitur numerik, kategorikal, dan statistik lalu lintas jaringan. Dataset ini kemudian digunakan sebagai dasar dalam proses pelatihan dan pengujian model klasifikasi Naïve Bayes.

DOI: 10.52362/jisamar.v10i3.2247

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)

2.2. Praproses Data

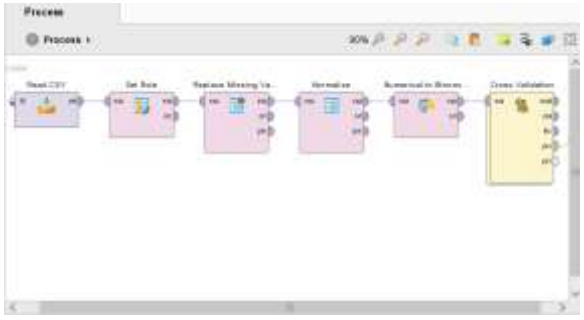
Tahap praproses data bertujuan untuk meningkatkan kualitas data sebelum digunakan dalam proses pemodelan. Tahapan ini meliputi pembersihan data, normalisasi fitur numerik, serta penentuan label target, yang seluruhnya dilakukan menggunakan RapidMiner. Pembersihan data mencakup penanganan *missing values*, penghapusan data duplikat, penyesuaian delimiter, dan penyesuaian tipe data agar sesuai dengan kebutuhan algoritma Naïve Bayes. Normalisasi dilakukan untuk menyamakan skala fitur numerik guna mencegah dominasi atribut tertentu dalam proses klasifikasi. Penentuan label target dilakukan menggunakan operator *Set Role*, dengan membagi kelas data menjadi dua kategori, yaitu *Normal* dan *Attack*. Proses praproses ini menghasilkan dataset yang lebih terstruktur dan siap digunakan dalam proses pelatihan dan pengujian model.

2.3. Pemodelan dan Evaluasi Menggunakan Naïve Bayes

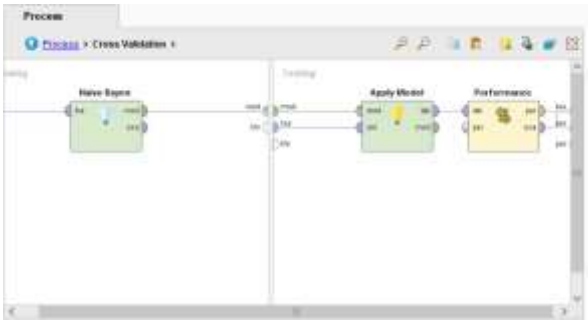
Algoritma Naïve Bayes digunakan untuk mengklasifikasikan trafik jaringan ke dalam dua kelas, yaitu trafik normal dan trafik serangan. Algoritma ini bekerja berdasarkan Teorema Bayes dengan asumsi independensi antar fitur, sehingga memiliki kompleksitas komputasi yang rendah dan efisien untuk dataset berukuran besar.

Untuk mengevaluasi kinerja model secara objektif dan menghindari bias, penelitian ini menerapkan metode 10-Fold Cross Validation. Dataset dibagi menjadi sepuluh bagian (*fold*), di mana pada setiap iterasi sembilan fold digunakan sebagai data pelatihan dan satu fold sebagai data pengujian. Proses ini dilakukan secara berulang hingga seluruh fold digunakan sebagai data uji.

Evaluasi performa model dilakukan menggunakan beberapa metrik, yaitu *accuracy*, *precision*, *recall*, dan *Area Under Curve* (AUC). Metrik-metrik ini dipilih untuk memberikan gambaran menyeluruh mengenai kemampuan model dalam mengklasifikasikan trafik jaringan serta membedakan antara trafik normal dan serangan.



Gambar 2. Alur Preprocessing dan Pemodelan Naive Bayes Menggunakan RapidMiner



Gambar 3. Struktur Cross Validation pada RapidMiner untuk Algoritma Naive Bayes

Alur preprocessing dan pemodelan Naive Bayes ditunjukkan pada **Gambar 2**, sedangkan struktur internal Cross Validation yang digunakan pada proses pelatihan dan pengujian model ditunjukkan pada **Gambar 3**.

III. PEMBAHASAN DAN HASIL

DOI: 10.52362/jisamar.v10i3.2247

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)

3.1. Hasil Evaluasi Model Naïve Bayes

Evaluasi kinerja algoritma Naïve Bayes dilakukan menggunakan metode 10-Fold Cross Validation untuk memperoleh hasil pengujian yang stabil dan tidak bias. Nilai rata-rata hasil evaluasi model ditunjukkan pada Tabel 1.

Tabel 1. Hasil Evaluasi Model Naïve Bayes

Metode	Accuracy (%)	Precision (%)	Recall (%)	AUC
10-fold CV (average)	95.96	94.11	98.85	0.964

Berdasarkan hasil evaluasi tersebut, dapat disimpulkan bahwa algoritma Naïve Bayes mampu melakukan klasifikasi trafik jaringan dengan sangat baik. Nilai *accuracy* yang tinggi menunjukkan konsistensi model dalam melakukan prediksi secara benar. Selain itu, nilai *precision* dan *recall* yang sama-sama tinggi mengindikasikan bahwa model mampu mendeteksi serangan secara akurat dengan tingkat kesalahan yang relatif rendah. Nilai AUC sebesar 0,964 menunjukkan bahwa model memiliki kemampuan yang sangat baik dalam membedakan antara trafik normal dan trafik serangan.

3.2. Analisis Confusion Matrix

Confusion matrix digunakan untuk mengevaluasi distribusi hasil prediksi model terhadap kelas aktual, sehingga memberikan gambaran lebih rinci mengenai performa klasifikasi. Confusion matrix model Naïve Bayes ditunjukkan pada Tabel 2.

Table 2. Confusion Matrix Model Naive Bayes

Prediksi / Aktual	Normal	Attack
Normal (pred. false)	34.194	522
Attack (pred. true)	2.806	44.810

Berdasarkan confusion matrix, nilai True Positive (TP) dan True Negative (TN) relatif tinggi, sedangkan False Negative (FN) berada pada tingkat yang rendah. Hal ini menunjukkan bahwa model mampu mendeteksi sebagian besar serangan dengan risiko kesalahan yang minimal, sehingga sesuai untuk sistem IDS dapat dijelaskan bahwa:

a. **True Positive = 44.810**
   Data serangan yang berhasil diprediksi sebagai serangan.
b. **True Negative = 34.194**
   Data normal yang berhasil diprediksi sebagai normal.
c. **False Positive = 2.806**
   Data normal yang salah diprediksi sebagai serangan. Masih dapat diterima dalam sistem IDS karena false alarm lebih aman dibanding serangan yang lolos.
d. **False Negative = 522**
   Data serangan yang salah diprediksi sebagai normal. Nilai false negative yang relatif kecil menunjukkan model cukup baik dalam menangkap serangan.

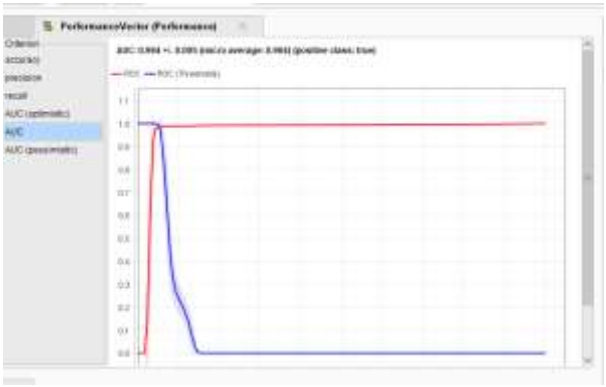
Secara keseluruhan, True Positive yang tinggi dan False Negative yang rendah menunjukkan bahwa Naive Bayes mampu mendeteksi akses tidak sah dengan baik dan dapat diterapkan pada sistem keamanan jaringan.

3.3. Kurva ROC dan Nilai AUC

Kurva Receiver Operating Characteristic (ROC) menggambarkan hubungan antara *True Positive Rate* (TPR) dan *False Positive Rate* (FPR) pada berbagai nilai ambang (*threshold*). Kurva ROC dan nilai AUC untuk algoritma Naïve Bayes ditunjukkan pada Gambar 4.

DOI: 10.52362/jisamar.v10i3.2247

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)



Gambar 4. Kurva ROC dan Nilai AUC untuk Algoritma Naïve Bayes

Nilai AUC sebesar 0,964 menunjukkan bahwa model memiliki kemampuan diskriminasi yang sangat baik dalam membedakan antara trafik normal dan trafik serangan. Semakin mendekati nilai 1, semakin baik kemampuan model dalam melakukan klasifikasi, sehingga hasil ini menegaskan efektivitas algoritma Naïve Bayes dalam konteks sistem deteksi intrusi.

3.4. Evaluasi

Hasil evaluasi menunjukkan bahwa algoritma Naïve Bayes memiliki performa yang konsisten dan stabil pada dataset UNSW-NB15. Nilai *recall* yang sangat tinggi menunjukkan bahwa model mampu mendeteksi hampir seluruh serangan yang terdapat dalam dataset, sementara nilai *precision* yang tinggi mengindikasikan rendahnya tingkat alarm palsu. Dengan nilai AUC di atas 0,9, model ini dapat dikategorikan sebagai *excellent classifier*. Beberapa poin penting yang dapat dibahas dari hasil penelitian ini adalah sebagai berikut:

1. **Akurasi Tinggi Menunjukkan Konsistensi dan Stabilitas Model**
   Nilai akurasi sebesar 95,96% menunjukkan bahwa model bekerja secara konsisten dalam mengklasifikasikan trafik jaringan. Hal ini menandakan bahwa algoritma Naïve Bayes mampu memanfaatkan fitur-fitur dalam dataset UNSW-NB15 secara efektif.
2. **Precision Tinggi Mengindikasikan Rendahnya False Positive**
   Nilai precision sebesar 94,11% menunjukkan bahwa sebagian besar prediksi serangan merupakan serangan yang sebenarnya. Kondisi ini sangat penting dalam sistem IDS, karena tingginya false positive dapat mengganggu operasional jaringan dan menurunkan kepercayaan terhadap sistem keamanan.
3. **Recall Sangat Tinggi Menunjukkan Kemampuan Deteksi Serangan yang Optimal**
   Recall sebesar 98,85% menunjukkan bahwa model berhasil mendeteksi hampir seluruh serangan. Dalam konteks IDS, recall merupakan metrik yang sangat krusial karena serangan yang tidak terdeteksi (*false negative*) dapat menimbulkan dampak yang serius terhadap keamanan jaringan. Nilai FN yang relatif rendah menunjukkan bahwa risiko serangan yang lolos dapat diminimalkan.
4. **Nilai AUC Tinggi Menunjukkan Kemampuan Diskriminasi yang Sangat Baik**
   Nilai AUC sebesar 0,964 mengindikasikan bahwa model memiliki kemampuan generalisasi yang kuat dan mampu membedakan kelas normal dan serangan secara akurat pada berbagai nilai ambang. Hal ini menunjukkan bahwa model tidak hanya bergantung pada satu threshold tertentu.
5. **Efektivitas Naïve Bayes sebagai Metode IDS**
   Kombinasi nilai accuracy, precision, recall, dan AUC menunjukkan bahwa algoritma Naïve Bayes merupakan metode yang efektif, ringan secara komputasi, dan sesuai untuk digunakan pada dataset berskala besar seperti UNSW-NB15. Hasil ini sejalan dengan karakteristik Naïve Bayes sebagai algoritma probabilistik yang efisien dan mampu menangani variasi fitur dalam sistem deteksi intrusi.

   Hasil ini sejalan dengan karakteristik Naive Bayes yang dikenal memiliki performa baik pada data berdimensi besar dan bersifat probabilistik, sehingga dapat menangani variasi fitur pada dataset UNSW-NB15.

IV. KESIMPULAN

DOI: 10.52362/jisamar.v10i3.2247

e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.3 (August 2026)

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa algoritma Naïve Bayes mampu mendeteksi aktivitas akses tidak sah pada jaringan komputer dengan performa yang sangat baik. Evaluasi kinerja menggunakan metode 10-Fold Cross Validation menunjukkan nilai akurasi sebesar 95,96%, precision 94,11%, recall 98,85%, serta nilai Area Under Curve (AUC) sebesar 0,964. Nilai-nilai tersebut mengindikasikan bahwa model memiliki kemampuan klasifikasi yang tinggi dalam membedakan antara trafik normal dan trafik serangan.

Hasil penelitian ini menunjukkan bahwa algoritma Naïve Bayes merupakan metode yang efektif, efisien, dan andal untuk diterapkan dalam sistem *Intrusion Detection System* (IDS) pada jaringan modern. Meskipun memiliki asumsi independensi antar fitur dan kompleksitas komputasi yang relatif rendah, algoritma ini tetap mampu menghasilkan performa yang kompetitif pada dataset IDS modern seperti UNSW-NB15. Selain itu, penelitian ini memberikan kontribusi praktis dengan menunjukkan bahwa algoritma Naïve Bayes dapat dijadikan sebagai solusi IDS yang ringan dan efisien, terutama pada lingkungan jaringan dengan keterbatasan sumber daya komputasi. Dengan demikian, Naïve Bayes berpotensi menjadi alternatif yang layak dalam pengembangan sistem keamanan jaringan berbasis *machine learning*.

REFERENSI

[1] F. Veriarinal, "Klasifikasi Sistem Deteksi Kerusakan Mesin Komputer Menggunakan Metode Naive Bayes," *SNIT – Seminar Nasional Industri dan Teknologi*, pp. 5–24, 2024.
[2] M. H. Rifai, D. A. Pramudya, and R. R. Narfandi, "Analisis peran teknologi kecerdasan buatan dalam mengoptimalkan proses deteksi terhadap serangan siber," in *Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, 2024.
[3] A. F. Mahmud and S. Wirawan, "Deteksi Phishing Website menggunakan Machine Learning Metode Klasifikasi," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 4, pp. 1368–1380, 2024.
[4] Japit et al., "Deteksi Anomali Transaksi E-Commerce Menggunakan SVM," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1976–1980, 2024.
[5] Yokkampon et al., "Anomaly Detection Using Support Vector Machines for Time Series Data," *Journal of Robotics, Networking and Artificial Life*, vol. 8, no. 1, pp. 41–46, 2021.
[6] M. Darip and B. R. S. Permana, "Analysis and Design of a Sales Application System," *Journal of Advances in Information and Industrial Technology*, vol. 6, no. 1, pp. 11–20, 2024.
[7] R. Faurina et al., "Pengembangan Chatbot Menggunakan Deep Feed-Forward Neural Network," *Jurnal Eksplora Informatika*, vol. 11, no. 2, pp. 120–129, 2023.
[8] A. Baradja and T. I. Tjendrowasono, "Pengaplikasian Deep Reinforcement Q-Learning," *Jurnal Rekayasa Sistem Informasi dan Teknologi*, vol. 1, no. 3, 2024.

DOI: 10.52362/jisamar.v10i3.2247