Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 1, Maret 2026
DOI : https://doi.org/10.33395/jmp.v15i1.15956
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Analisis Perbandingan Metode Machine Learning KNN dengan Naive Bayes pada Log Serangan Jaringan

[1]Agus Fs Ndruru, [2] Rika Rosnelly, [3]Bob Subhan Riza
[1*,2,3]Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia
*Korespondensi: agusndruru1999@gmail.com

Submit : 28 Feb 2026 | **Diterima** : 14 Mar 2026 | **Terbit** : 20 Mar 2026

ABSTRACT

Massive cybercrimes, such as Distributed Denial of Service (DDoS) attacks, demand rapid and accurate preventive measures through an Intrusion Detection System (IDS). This research aims to analyze and compare the performance of machine learning algorithms, specifically K-Nearest Neighbor (KNN) and Naive Bayes, in classifying network attack logs. The research methodology utilizes the public CIC-IDS2017 dataset through the stages of data preprocessing, model design, parameter optimization, and confusion matrix-based evaluation. The test results show that the KNN method with an optimal neighborhood value of K=3 achieved an accuracy rate of 99.92%, outperforming the Gaussian Naive Bayes algorithm, which recorded an accuracy of 99.52%. The superiority of KNN is also consistent across precision, recall, and F1-score metrics, as its distance-based approach (Euclidean) is capable of capturing the correlation of complex, nonlinear attack patterns. Conversely, the probabilistic approach of Naive Bayes has much lighter computational efficiency, but its performance is slightly hindered by the assumption of attribute independence. The implications of this research provide a strategic guideline that KNN is highly recommended for security systems that prioritize absolute accuracy and minimal false negatives, while Naive Bayes is ideal as an efficient initial monitoring filter. The conclusion of the study affirms that KNN is significantly more adaptive and accurate than Naive Bayes in detecting network anomalies. For future research, it is recommended to conduct tests using hybrid models, the application of deep learning, or the implementation of real-time detection on network traffic to comprehensively examine the system's scalability and computational load.

***Keywords**: CIC-IDS2017, Intrusion Detection System, K-Nearest Neighbor, Machine Learning, Naive Bayes.*

ABSTRAK

Kejahatan siber seperti serangan *Distributed Denial of Service* (DDoS) yang masif menuntut adanya tindakan preventif yang cepat dan akurat melalui sistem deteksi intrusi (IDS). Penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja algoritma *machine learning*, yaitu *K-Nearest Neighbor* (KNN) dan *Naive Bayes*, dalam mengklasifikasikan *log* serangan jaringan. Metodologi penelitian menggunakan *dataset* publik CIC-IDS2017 melalui tahapan *preprocessing* data, perancangan model, optimasi parameter, hingga evaluasi berbasis *confusion matrix*. Hasil pengujian menunjukkan bahwa metode KNN dengan nilai ketetanggaan optimal K=3 memperoleh tingkat akurasi sebesar 99,92%, mengungguli algoritma *Gaussian Naive Bayes* yang mencatatkan akurasi 99,52%. Keunggulan KNN juga terlihat konsisten pada metrik presisi, *recall*, dan *F1-score* karena pendekatannya yang berbasis jarak (*Euclidean*) mampu menangkap korelasi pola serangan nonlinier yang kompleks. Sebaliknya, pendekatan probabilistik *Naive Bayes* memiliki efisiensi komputasi yang jauh lebih ringan, namun kinerjanya sedikit terhambat oleh asumsi independensi antaratribut. Implikasi dari penelitian ini memberikan panduan strategis bahwa KNN sangat direkomendasikan untuk sistem keamanan yang memprioritaskan akurasi mutlak dan minim *false negative*, sementara *Naive Bayes* ideal sebagai filter pemantauan awal yang efisien. Kesimpulan penelitian menegaskan bahwa KNN secara signifikan lebih adaptif dan akurat dibandingkan *Naive Bayes* dalam mendeteksi anomali jaringan. Untuk penelitian selanjutnya, disarankan agar melakukan pengujian menggunakan model *hybrid*, penerapan *deep learning*, atau implementasi deteksi secara *real-time* pada lalu lintas jaringan guna menguji skalabilitas dan beban komputasi sistem secara komprehensif.

Kata Kunci: *CIC-IDS2017, Intrusion Detection System, K-Nearest Neighbor, Machine Learning, Naive Bayes*.

PENDAHULUAN

Badan Siber dan Sandi Negara mencatat bahwasanya pada bulan Mei tahun 2025, ada sebanyak 755.639.091 anomali trafik yang terjadi. Klasifikasi anomali trafik tersebut meliputi *malware* sebanyak 723.959.783, *unauthorized access* sebanyak 23.581.719, *exploit* sebanyak 3.781.568, APT sebanyak 1.445.361, *information leak* sebanyak 1.380.054, *denial of service* sebanyak 1.343.379, *web application attack* sebanyak 143.568, dan *information gathering* sebanyak 3.659. Pada tanggal 31 Juli 2021, situs Sekretariat Kabinet Republik Indonesia juga mengalami peretasan yang menyebabkan web tidak dapat diakses oleh masyarakat. Hal tersebut menandakan bahwasanya kejahatan digital (siber) masih sangat masif terjadi. Kejahatan siber merupakan aktivitas kriminal kompleks yang dilakukan dengan menggunakan teknologi komputer, mencakup upaya mencari dan menyebarkan informasi untuk intimidasi (*doxing*), penghinaan melalui media *online* (*cyberbullying*), penyebaran berita bohong, hingga penyerangan *website* atau *server* seperti DDoS (Purba & Mauluddin, 2023).

Selain DDoS, ancaman lain yang kerap terjadi adalah *bruteforce*, yaitu teknik serangan peretas yang dilakukan dengan paksaan pada sistem keamanan web melalui percobaan menebak *username* dan *password*. Peretas menggunakan teknik ini untuk menemukan kerentanan kode dan mendapatkan informasi dari halaman web yang tersembunyi, sehingga eksploitasi dapat dilakukan untuk menyusup ke dalam sistem (Fachri, 2023). Penyajian informasi pada sistem berbasis *website* harus mengikuti aturan standarisasi keamanan informasi yang terdiri dari tiga prinsip utama: kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Kerahasiaan memastikan web tidak diakses oleh pihak tanpa wewenang; integritas menjamin keaslian data tidak diubah secara ilegal; dan ketersediaan memberikan jaminan autentikasi kepada pengguna sah (Hermawan et al., 2022). Adanya serangan DDoS atau *bruteforce* akan merusak ketiga prinsip tersebut. Oleh karena itu, diperlukan tindakan preventif yang efektif, salah satunya melalui pengolahan log data serangan menggunakan metode *machine learning*.

Dua metode *machine learning* yang banyak digunakan dalam analisis log serangan adalah *K-Nearest Neighbor* (KNN) dan *Naive Bayes*. K-NN merupakan metode klasifikasi berbasis kedekatan data (*lazy learning*) yang tidak mempelajari model dari data *testing*, melainkan menghitung kedekatan antara kasus baru (data uji) dan kasus lama (data latih) berdasarkan pencocokan bobot fitur menggunakan penghitungan jarak *Euclidean* (Rahayu et al., 2022; Setiyorini & Asmono, 2019). Sementara itu, *Naive Bayes* merupakan algoritma klasifikasi probabilistik yang didasarkan pada Teorema Bayes, dengan asumsi "naif" bahwa setiap fitur bersifat independen satu sama lain. Metode ini menghitung probabilitas suatu data masuk ke dalam kelas tertentu dan dikenal sederhana, cepat, serta efisien untuk data berskala besar.

Keandalan kedua metode ini dalam mengklasifikasikan data telah dibuktikan oleh beberapa peneliti terdahulu. Penelitian yang dilakukan oleh Churcher et al. (2021) menyimpulkan bahwa pada klasifikasi multi-kelas, metode KNN unggul dengan tingkat akurasi mencapai 99%, mengungguli model lain termasuk *Random Forest* (RF), serta menunjukkan performa yang sangat baik dalam mengenali berbagai jenis serangan secara simultan. Di sisi lain, penelitian oleh Astofa (2020) menunjukkan bahwa metode *Naive Bayes* memiliki kinerja yang sangat kompetitif, di mana metode ini mampu menghasilkan nilai akurasi sebesar 91,16%, lebih tinggi dibandingkan metode *Support Vector Machine* berbasis *Particle Swarm Optimization* yang menghasilkan akurasi 85,92%. Berbagai penelitian ini menegaskan bahwa baik KNN maupun *Naive Bayes* memiliki karakteristik dan keunggulan yang berbeda, sehingga evaluasi komparatif pada domain data yang spesifik menjadi sangat krusial.

Berdasarkan perbedaan karakteristik tersebut, perlu dilakukan analisis perbandingan antara KNN dan *Naive Bayes* untuk mengetahui tingkat akurasi, kecepatan komputasi, dan efektivitas masing-masing metode dalam mendeteksi dan mengklasifikasikan log serangan jaringan. Agar pembahasan lebih terarah, penelitian ini dibatasi pada penggunaan log serangan jaringan yang diperoleh dari *dataset* publik (CICIDS), tanpa membahas mekanisme mitigasi atau respons terhadap serangan. Evaluasi difokuskan pada parameter *Accuracy*, *Precision*, *Recall* (*Sensitivity*), dan *F1-Score*. Melalui penelitian ini, diharapkan dapat diperoleh hasil analisis identifikasi pola aktivitas berbahaya pada lalu lintas jaringan, serta memberikan rekomendasi

mengenai metode algoritma yang paling optimal untuk diterapkan dalam sistem deteksi serangan jaringan.

METODE PENELITIAN

Studi Literatur

Tahap awal penelitian dilakukan dengan mengumpulkan landasan teori dan tinjauan dari hasil-hasil penelitian terdahulu. Sumber literatur utama bersumber dari jurnal ilmiah tingkat nasional maupun internasional yang berfokus pada pembahasan *Machine Learning* (khususnya algoritma KNN dan *Naive Bayes*), analisis serangan DDoS, serta forensik digital.

Pengumpulan Data

Penelitian ini menggunakan data primer yang diperoleh dari *Intrusion Detection System* (IDS) publik, yaitu dataset CIC-IDS2017. Dataset ini merekam aktivitas lalu lintas jaringan yang merepresentasikan kondisi normal maupun saat terjadi serangan.

Tabel 1. Sampel Dataset Serangan Jaringan

Jenis Log	Atribut Data	Keterangan
DDOS Attack	Src IP, Dst IP, Flows, Packet Rate, Bytes	Traffic Berlebihan
Normal Traffic	Src IP, Dst IP, Bytes, Packets, Service	Aktivitas jaringan normal

Preprocessing Dataset

Preprocessing merupakan tahapan pembersihan dan transformasi data mentah menjadi format yang ideal untuk diproses oleh algoritma KNN dan *Naive Bayes*. Karena dataset CIC-IDS2017 berukuran sangat besar, tahapan ini mengatasi *missing value*, menghapus data duplikat, serta menangani nilai tidak valid (seperti NaN atau Inf) yang kerap muncul pada kolom perhitungan durasi aliran (*flow*). Selain itu, atribut yang tidak memiliki relevansi terhadap proses klasifikasi seperti *Flow ID*, alamat IP (sumber dan tujuan), serta *timestamp* dihapus (dieliminasi).

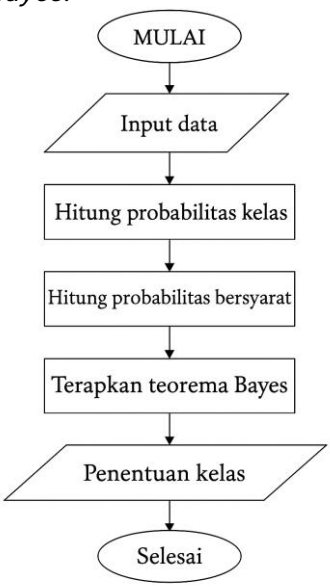
Tabel 2. Sampel Hasil Preprocessing Dataset

Flow Duration	Total Fwd Pkts	Total Bwd Pkts	Flow Bytes/s	Flow Pkts/s	Fwd Pkt Len Mean	Bwd Pkt Len Mean	Protocol	Fwd IAT Mean	Bwd IAT Mean	Subflow Fwd Bytes	Subflow Bwd Bytes	Label
-215	-314	-287	-412	-297	-358	-404	0	-323	-312	-287	-341	0
574	613	491	867	742	523	601	6	682	754	795	698	1
-124	-172	-0.19	-202	-156	-188	-213	6	-202	-219	-205	-182	0
932	888	942	1.011	997	962	945	6	1.073	1.024	981	1.002	1
-364	-421	-398	-473	-432	-419	-436	0	-442	-407	-438	-451	0

Perancangan Model

Penelitian ini merancang sistem klasifikasi serangan jaringan dengan mengimplementasikan dua metode perbandingan. Pengujian diawali dengan membangun model *Naive Bayes*, lalu dilanjutkan dengan model KNN.

a. Rancangan Model *Naive Bayes*:



Gambar 1. Rancangan Model Penelitian Metode Naïve Bayes

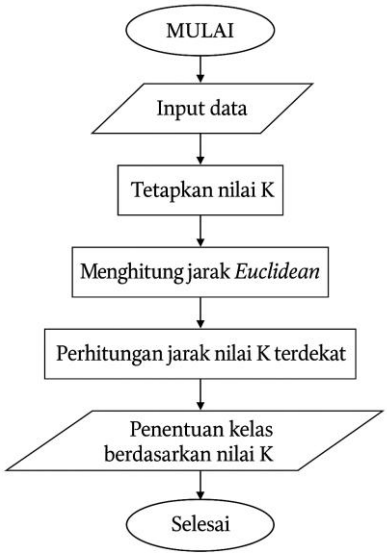
Input data terdiri dari fitur numerik kontinu dan label kelas (*Normal* atau *Attack*). Model bekerja dengan menghitung probabilitas awal (*prior*) setiap kelas, yaitu rasio jumlah data pada suatu kelas terhadap total data keseluruhan. Selanjutnya, sistem menghitung probabilitas bersyarat fitur terhadap kelas $\mathrm{P}(\mathrm{X} \mid \mathrm{C})$ menggunakan asumsi distribusi Gaussian. Model menggabungkan probabilitas *prior* dan probabilitas bersyarat melalui pendekatan Teorema Bayes:

$$\mathrm{P}(\mathrm{C} \mid \mathrm{X}) = \frac{\mathrm{P}(\mathrm{X} \mid \mathrm{C}) \times \mathrm{P}(\mathrm{C})}{\mathrm{P}(\mathrm{X})}$$

Mengingat nilai $\mathrm{P}(\mathrm{X})$ bersifat konstan pada semua kelas, proses klasifikasi dipersingkat dengan membandingkan nilai proporsionalnya:

$$\mathrm{P}(\mathrm{C} \mid \mathrm{X}) \propto \mathrm{P}(\mathrm{X} \mid \mathrm{C}) \times \mathrm{P}(\mathrm{C})$$

b. Rancangan Model *K-Nearest Neighbor* (KNN):



Gambar 2. Rancangan Model Penelitian Metode KNN

Data hasil *preprocessing* menjadi input awal sistem. Peneliti menentukan nilai *K* (misalnya $\mathrm{K} = 3\ 5$ atau 7) yang berfungsi sebagai batas jumlah tetangga terdekat yang

dievaluasi. Jarak setiap data uji terhadap seluruh data latih dikalkulasi menggunakan persamaan *Euclidean Distance*:

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$$

Sistem kemudian mengurutkan jarak dari yang terpendek hingga terpanjang, lalu mengisolasi K data terdekat. Klasifikasi akhir ditentukan melalui *majority voting*; apabila mayoritas dari tetangga K berlabel *Attack*, maka data uji tersebut diprediksi sebagai *Attack*, begitu pula sebaliknya.

Evaluasi Model

Hasil prediksi dari model *Naive Bayes* dan KNN dievaluasi menggunakan *Confusion Matrix*. Evaluasi ini berdasar pada perhitungan nilai *True Positive* (TP), *False Positive* (FP), *True Negative* (TN), dan *False Negative* (FN) untuk mendapatkan tingkat Akurasi, Presisi, dan *Recall* (Ramayu et al., 2022). Rumus yang digunakan adalah sebagai berikut:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

Analisa Hasil

Kinerja klasifikasi dari kedua model komputasi dianalisis secara mendalam. Analisis dititikberatkan pada pengujian berbagai rasio pembagian data latih dan data uji untuk menemukan skenario yang menghasilkan nilai metrik (Akurasi, Presisi, dan *Recall*) tertinggi, guna menentukan model yang paling optimal.

Menarik Kesimpulan

Tahap akhir melibatkan penarikan kesimpulan berdasarkan hasil evaluasi dan komparasi secara komprehensif. Hasil kesimpulan ini akan merekomendasikan algoritma *Machine Learning* yang paling andal dalam mengidentifikasi dan mengklasifikasikan anomali pada *log* lalu lintas jaringan.

HASIL DAN PEMBAHASAN

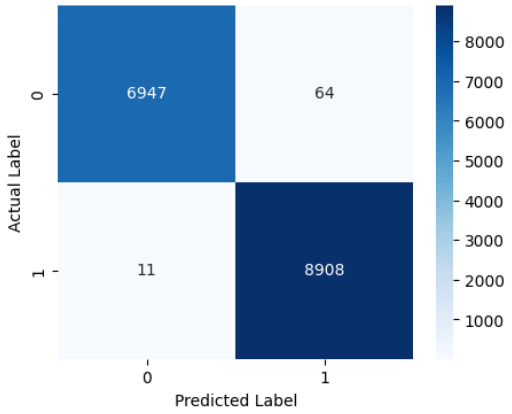
Hasil Klasifikasi Menggunakan *Naive Bayes*

Model *Naive Bayes* mencapai tingkat akurasi sebesar 99,52%. Nilai presisi dan *recall* yang mendekati angka 1 menunjukkan bahwa tingkat kesalahan *false positive* relatif rendah, sekaligus mampu mendeteksi sebagian besar data serangan secara tepat.

Tabel 3. Hasil Evaluasi Kinerja Model Naive Bayes

Kelas	Precision	Recall	F1-Score	Support
Normal (0)	01.00	0,06875	0,06875	7.011
Serangan DDoS (1)	0,06875	01.00	01.00	8.919
Macro Average	01.00	0,06875	01.00	15.930
Weighted Average	01.00	01.00	01.00	15.930

Hasil visualisasi *Confusion Matrix* menunjukkan bahwa model berhasil mengklasifikasikan 6.947 data normal (TN) dan 8.908 data serangan (TP). Terdapat tingkat kesalahan minor berupa 64 data *False Positive* dan 11 data *False Negative*.



Gambar 3. Confusion Matrix Model Naïve Bayes

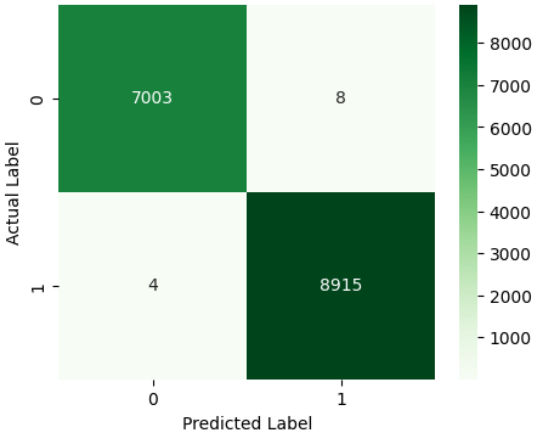
Hasil Klasifikasi Menggunakan *K-Nearest Neighbor* (KNN)

Evaluasi dilakukan menggunakan parameter persamaan metrik yang sama dengan *Naive Bayes*. Hasil evaluasi menunjukkan bahwa KNN memperoleh nilai akurasi yang lebih tinggi, yakni 99,92%, dengan nilai presisi, *recall*, dan *F1-score* yang sangat stabil di angka 1.00.

Tabel 4. Evaluasi Model KNN

Kelas	Precision	Recall	F1-Score	Support
Normal (0)	01.00	01.00	01.00	7.011
Serangan DDoS (1)	01.00	01.00	01.00	8.919
Macro Average	01.00	01.00	01.00	15.930
Weighted Average	01.00	01.00	01.00	15.930

Visualisasi *Confusion Matrix* mengonfirmasi kinerja superior KNN. Model berhasil mengidentifikasi 7.003 data normal (TN) dan 8.915 data serangan (TP), dengan kesalahan klasifikasi yang sangat minim (hanya 8 *False Positive* dan 4 *False Negative*).



Gambar 4. Confusion Matrix Model KNN

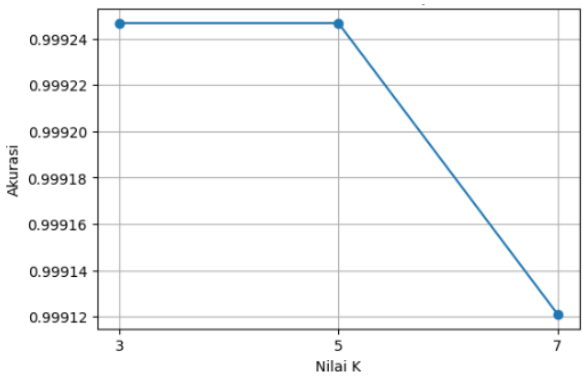
Optimasi Parameter Nilai K pada KNN

Kinerja KNN sangat bergantung pada nilai K (jumlah tetangga terdekat). Pengujian sensitivitas dilakukan pada variasi K = 3, 5, dan 7 untuk menentukan parameter paling optimal.

Tabel 5. Akurasi Skor

Total K	Nilai K
K3	0.9992467043314501
K5	0.9992467043314501
K7	0.9991211550533584

Hasil menunjukkan bahwa K=3 dan K=5 menghasilkan tingkat akurasi identik yang paling tinggi (99,92%), sedangkan K=7 mengalami sedikit penurunan (99,91%). Peningkatan nilai K tidak selalu berbanding lurus dengan performa karena model dapat kehilangan sensitivitas terhadap pola lokal. Berdasarkan pertimbangan efisiensi komputasi dan kestabilan, nilai **K=3** ditetapkan sebagai parameter terbaik untuk klasifikasi akhir model.



Gambar 5. Grafik Akurasi Nilai K

Perbandingan Kinerja *Naive Bayes* dan KNN

Perbandingan kinerja secara langsung memperlihatkan keunggulan metode KNN atas *Naive Bayes* pada seluruh metrik pengujian. KNN unggul dengan selisih akurasi, presisi, dan *recall* yang lebih konsisten, menjadikannya model yang lebih tangguh dalam meminimalkan deteksi palsu maupun kegagalan deteksi.

Tabel 6. Perbandingan Naive Bayes Dengan KNN

	Metode	Accuracy	Precision	Recall	F1-Score
0	Naive Bayes	0.995292	0.995310	0.995292	0.995290
1	KNN	0.999247	0.999247	0.999247	0.999247

Pembahasan

Secara keseluruhan, kedua model *machine learning* terbukti mampu membedakan pola aktivitas normal dan anomali (serangan DDoS) secara efektif dari *dataset* CICIDS2017. Namun, perbedaan karakteristik dasar algoritma sangat memengaruhi hasil akhirnya.

Naive Bayes, dengan pendekatan probabilistiknya, terbukti sangat cepat dan efisien untuk digunakan pada *dataset* berukuran besar. Kelemahannya terletak pada asumsi probabilitas independen antaratribut (naif). Pada *log* jaringan aktual, atribut seperti durasi koneksi dan laju paket memiliki korelasi alami. Karena asumsi independensi ini tidak sepenuhnya terpenuhi, akurasi *Naive Bayes* sedikit tertinggal, terutama pada fitur-fitur yang saling tumpang tindih.

Sebaliknya, KNN yang beroperasi menggunakan pendekatan spasial berbasis jarak (*Euclidean*) tidak bergantung pada asumsi distribusi. Algoritma ini mempertimbangkan korelasi antardata secara implisit sehingga jauh lebih fleksibel dalam menangkap pola nonlinier dan pola lokal spesifik dari serangan jaringan. Kekuatan ini dibuktikan dengan minimnya nilai *False Negative* pada KNN. Meskipun demikian, keunggulan akurasi KNN harus dibayar dengan biaya komputasi yang lebih berat pada tahap pengujian (*lazy learning*), karena model harus menghitung jarak dari data uji ke seluruh data latih.

KESIMPULAN

Metode *K-Nearest Neighbor* (KNN) dan *Naive Bayes* menunjukkan kapabilitas yang sangat baik dalam mengklasifikasikan log serangan jaringan, namun dengan karakteristik performa yang berbeda. Algoritma KNN, melalui pendekatan klasifikasi berbasis kedekatan spasial antar data, terbukti sangat adaptif dan tangguh dalam menangkap pola serangan yang bersifat nonlinier dan kompleks. Kinerja optimal KNN sangat bergantung pada proses normalisasi fitur dan pemilihan nilai *K* yang tepat (seperti K=3), yang berfungsi menyeimbangkan sensitivitas model terhadap *noise* di dalam variasi lalu lintas data jaringan. Di

sisi lain, metode *Naive Bayes* menawarkan keunggulan komparatif dari segi efisiensi komputasi dan kecepatan pemrosesan karena menggunakan pendekatan probabilistik yang lebih sederhana. Meskipun demikian, asumsi independensi antaratribut pada *Naive Bayes* sedikit membatasi kinerjanya, mengingat atribut pada log jaringan (seperti durasi aliran dan jumlah paket) secara alami memiliki keterkaitan yang kuat.

Secara komparatif, algoritma KNN terbukti lebih unggul dan akurat dibandingkan *Naive Bayes* dalam mendeteksi dan mengklasifikasikan anomali jaringan. Hal ini menegaskan bahwa KNN adalah pilihan yang jauh lebih efektif untuk sistem yang memprioritaskan ketepatan klasifikasi mutlak dan menuntut tingkat *false negative* yang sangat rendah. Sebaliknya, efisiensi tinggi dari *Naive Bayes* menjadikannya lebih ideal sebagai lapis penyaring pertama pada lingkungan jaringan dengan sumber daya terbatas. Oleh karena itu, pemilihan metode *machine learning* untuk *Intrusion Detection System* (IDS) harus disesuaikan dengan infrastruktur yang ada—menyeimbangkan antara kebutuhan akan ketepatan analisis pola serangan yang kompleks (KNN) dan tuntutan efisiensi beban komputasi (*Naive Bayes*).

REFERENSI

Abdullah, R. K., Fudhail, M. T., & Mujahidin, S. (2024). Penggunaan Snort dan Fail2ban sebagai IDS untuk mengatasi brute force attack dengan notifikasi Telegram: Studi kasus pada Institusi XYZ. *JUSTIN (Jurnal Sistem dan Teknologi Informasi), 12*(3), 530–542. https://doi.org/10.26418/justin.v12i3.79617

Aminudin, A., Hakim, L., Nuryasin, I., & Santiyas, H. R. (2024). Kriptosistem hybrid algoritme RSA dan El-Gamal menggunakan socket TCP pada instant messaging. *JRST (Jurnal Riset Sains dan Teknologi), 8*(1), 1. https://doi.org/10.30595/jrst.v8i1.17124

Anwar, N., Munawwar, M., Abduh, M., & Santosa, N. B. (2018). Komparatif performance model keamanan menggunakan metode algoritma AES 256 bit dan RSA. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 2*(3), 783–791. https://doi.org/10.29207/resti.v2i3.606

Ardiansyah, Suradi, A. A. M., & Saputra, W. (2025). Strategi keamanan router MikroTik: Deteksi dan mitigasi serangan brute force berbasis scripting. *JUKI: Jurnal Komputer dan Informatika, 7*, 12–19.

Arief, A., & Saputra, R. (2016). Implementasi kriptografi kunci publik dengan algoritma RSA-CRT pada aplikasi instant messaging. *Scientific Journal of Informatics, 3*(1), 46–54. https://doi.org/10.15294/sji.v3i1.6115

Chaloop, S. G., & Abdullah, M. Z. (2021). Enhancing hybrid security approach using AES and RSA algorithms. *Journal of Engineering and Sustainable Development, 25*(4), 58–66. https://doi.org/10.31272/jeasd.25.4.6

Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. *Sensors, 21*(2), 1–32. https://doi.org/10.3390/s21020446

Fachri, F. (2023). Optimasi keamanan web server terhadap serangan brute-force menggunakan penetration testing. *Jurnal Teknologi Informasi dan Ilmu Komputer, 10*(1), 51–58. https://doi.org/10.25126/jtiik.20231015872

Fauzi, A., Firmansyah, F., & Sandi, T. A. A. (2024). Perancangan keamanan router MikroTik dari serangan FTP dan SSH brute force. *Jurnal Infortech, 6*(1), 9–14. https://doi.org/10.31294/infortech.v6i1.21697

Geta Putri, G., Styorini, W., & Dian Rahayani, R. (2015). Analisis kriptografi simetris AES dan kriptografi asimetris RSA pada enkripsi citra digital. *Ethos (Jurnal Penelitian dan Pengabdian Masyarakat), 3*(8), 197–207.

Ghori, K. M. U., Imran, M., Nawaz, A., Abbasi, R. A., Ullah, A., & Szathmary, L. (2023). Performance analysis of machine learning classifiers for non-technical loss detection. *Journal of Ambient Intelligence and Humanized Computing, 14*(11), 15327–15342. https://doi.org/10.1007/s12652-019-01649-9

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi algoritma kriptografi RSA untuk enkripsi dan dekripsi email. *Jurnal Teknologi dan Sistem Komputer, 3*(2), 253–258. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258

Hermawan, A., Hartati, T., & Wijaya, Y. A. (2022). Analisa keamanan data melalui website Zahra Software menggunakan metode keamanan informasi CIA triad. *Jurnal Informatika: Jurnal Pengembangan IT, 7*(3), 125–130. https://doi.org/10.30591/jpit.v7i3.3428

Kurniawan, D., & Saputra, A. (2019). Penerapan K-Nearest Neighbour dalam penerimaan peserta didik dengan sistem zonasi. *Jurnal Sistem Informasi Bisnis, 9*(2), 212–219. https://doi.org/10.21456/vol9iss2pp212-219

Laksono, E., Basuki, A., & Bachtiar, F. (2020). Optimization of K value in KNN algorithm for spam and ham email classification. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 4*(2), 377–383. https://doi.org/10.29207/resti.v4i2.1845

Mulyanto, Y., Herfandi, H., & Candra Kirana, R. (2022). Analisis keamanan wireless local area network (WLAN) terhadap serangan brute force dengan metode penetration testing (Studi kasus: RS H.L Manambai Abdulkadir). *Jurnal Informatika Teknologi dan Sains, 4*(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Nolly, R. A., Fitria, A., & Saputra S., K. (2023). Penerapan algoritma K-Nearest Neighbors untuk klasifikasi fragmen metagenom berdasarkan ekstraksi fitur k-mers. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 17*(1), 52. https://doi.org/10.30872/jim.v17i1.5779

Purba, Y. O., & Mauluddin, A. (2023). Kejahatan siber dan kebijakan identitas kependudukan digital: Sebuah studi tentang potensi pencurian data online. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial, 5*(2), 55–66. https://doi.org/10.51486/jbo.v5i2.113

Rahayu, S., MZ, Y., Bororing, J. E., & Hadiyat, R. (2022). Implementasi metode K-Nearest Neighbor (K-NN) untuk analisis sentimen kepuasan pengguna aplikasi teknologi finansial FLIP. *Edumatic: Jurnal Pendidikan Informatika, 6*(1), 98–106. https://doi.org/10.29408/edumatic.v6i1.5433

Rahmawati, L., Rifki Arrosid, M., & Gugus Azhari, M. (2023). Pemanfaatan teknologi computer vision untuk implementasi deteksi masker menggunakan metode supervised learning. *Jurnal JEETech, 4*(2), 75–80. https://doi.org/10.32492/jeetech.v4i2.4201

Ramayu, I. M. S., Susanto, F., & Mahendra, G. S. (2022). Penerapan data mining dengan algoritma C4.5 dalam pemesanan obat guna meningkatkan keuntungan apotek. *Prosiding Seminar Nasional Manajemen, Desain & Aplikasi Bisnis Teknologi (SENADA), 5*, 237–245.

Setiyorini, T., & Asmono, R. T. (2019). Penerapan metode K-Nearest Neighbor dan Gini index pada klasifikasi kinerja siswa. *Jurnal Techno Nusa Mandiri, 16*(2), 121–126. https://doi.org/10.33480/techno.v16i2.747

Srinivasan, K., & Budda, R. (2025). Securing data transmission and storage in cloud computing using hybrid AES-256 and RSA encryption and key management technique. *International Journal of Science and Engineering Applications, 14*(3), 64–69. https://doi.org/10.7753/ijsea1403.1013

Trisnawati, T. T., Yurinanda, S., Syafmen, W., & Multahadah, C. (2023). Penerapan algoritma Rivest-Shamir-Adleman (RSA) pada enkripsi Uniform Resource Locator (URL) website untuk keamanan data. *Euler: Jurnal Ilmiah Matematika, Sains dan Teknologi, 11*(2), 205–215. https://doi.org/10.37905/euler.v11i2.21169

Wahyadyatmika, A. P., Isnanto, R. R., & Somantri, M. (2014). Implementasi algoritma kriptografi RSA pada surat elektronik (e-mail). *Transient, 3*(4), 1–9.