Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

Simulasi dan Analisis Strategi Hybrid Teaming Menggunakan Algoritma Naive Bayes dalam Deteksi Serangan Distributed Denial of Service (DDoS)

Aprilian Gevindo*, Yuhandri, Billy Hendrik

Fakultas Ilmu Komputer, Magister Teknik Informatika, Universitas Putra Indonesia YPTK Padang, Padang, Indonesia
Jl. Raya Lubuk Begalung, Padang, Sumatera Barat 25221
Email: [1,*]liando1801@email.com, [2]yuyu@upiyptk.ac.id, [3]billy_hendrik@upiyptk.ac.id
Email Penulis Korespondensi: liando1801@email.com
Submitted: **31/01/2026**; Accepted: **30/04/2026**; Published: **30/04/2026**

Abstrak−Serangan *cyber*, khususnya *Distributed Denial of Service* (DDoS) telah menjadi ancaman serius bagi ketersediaan *server* dan infrastruktur jaringan lainnya. Serangan ini mampu melumpuhkan layanan pada jaringan berskala besar, dengan cara membanjiri sistem target menggunakan lalu lintas yang sangat tinggi. Berdasarkan hal tersebut, tujuan dari penelitian ini berupa simulasi dan analisis strategi *Hybrid Teaming* dengan menggunakan algoritma *Naïve Bayes*. Strategi ini mensimulasikan kolaborasi terstruktur antara metode *Red Team* (penyerang), *Blue Team* (pertahanan), dan *Purple Team* (evaluator) untuk menguji ketahanan sekaligus memperkuat postur keamanan secara menyeluruh. Algoritma *Naive Bayes* salah satu algoritma terbaik dalam *Machine Learning*, dan sangat baik dalam melakukan proses pengklasifikasian data. Kinerja algoritma *Naïve Bayes* dengan strategi *Hybrid Teaming* yang dibangun menjadi suatu sistem deteksi cerdas. Sistem ini dilatih menggunakan 10.000 data dari dataset publik serta 1.688 dari *log* jaringan Rumah Sakit Umum Daerah (RSUD) Tapan. Berdasarkan hasil analisis data, hasil pelatihan model masuk dalam kategori sempurna yaitu akurasi, presisi, *recall*, dan *F1-score* mendapat hasil 100%. Model tersebut kemudian diimplementasikan pada *server* serta *router MikroTik* dalam lingkungan simulasi yang mereplikasi jaringan RSUD Tapan. Hasil pengujian pada kedua komponen ini menunjukkan sistem berhasil mendeteksi berbagai pola serangan *Flooding* dengan akurasi deteksi 100%. Sistem mampu merespons secara otomatis dengan memblokir alamat IP (*Internet Protocol*) penyerang pada kedua lapisan tersebut serta mengirimkan notifikasi *real-time* melalui *WhatsApp* dan *Email*. Kontribusi penelitian ini menghasilkan sebuah kerangka kerja pertahanan siber yang komprehensif dan efektif.

Kata Kunci: Strategi Hybrid Teaming; Algoritma Naïve Bayes; Ketahanan Jaringan; Sistem Cerdas; Serangan DDoS

Abstract−Cyber attacks, particularly Distributed Denial of Service (DDoS), have become a serious threat to the availability of servers and other network infrastructure. These attacks can paralyze services on large-scale networks by flooding the target system with extremely high traffic. Based on this, the objective of this research is to simulate and analyze a Hybrid Teaming strategy using the Naïve Bayes algorithm. This strategy simulates structured collaboration between the Red Team (attackers), Blue Team (defenders), and Purple Team (evaluators) to test resilience while comprehensively strengthening the security posture. The Naïve Bayes algorithm is one of the best algorithms in Machine Learning and excels at performing data classification processes. The performance of the Naïve Bayes algorithm combined with the Hybrid Teaming strategy is developed into an intelligent detection system. This system is trained using 10,000 data points from a public dataset and 1,688 data points from the network logs of the Tapan Regional General Hospital (RSUD). Based on the data analysis results, the model training outcomes fall into the perfect category, with accuracy, precision, recall, and F1-score achieving a result of 100%. The model was then implemented on a server and a MikroTik router within a simulation environment that replicates the Tapan RSUD network. The test results on these two components show that the system successfully detected various Flooding attack patterns with a detection accuracy of 100%. The system is capable of responding automatically by blocking the attacker's IP (Internet Protocol) address at both layers, as well as sending real-time notifications via WhatsApp and Email. The contribution of this research results in a comprehensive and effective cybersecurity defense framework.

Keywords: Hybrid Teaming Strategy; Naïve Bayes Algorithm; Network Resilience; Intelligent Systems; DDoS Attacks

1. PENDAHULUAN

Serangan siber khususnya *Distributed Denial of Service* (DDoS), kini menjadi ancaman serius bagi *server* [1]. DDoS dapat dikatakan semacam serangan yang tampak sederhana namun sangat merusak [2]. Triwulan 3 tahun 2019, terjadi peningkatan serangan DDoS dengan serangan terbanyak terjadi pada bulan September. Serangan *Distributed Denial of Service* (DDoS) yang telah diteliti sebelumnya oleh Syujak ddk., 2024 digambarkan sebagai salah satu ancaman yang serius dalam keamanan jaringan *modern* [3]. Akibat serangan *Distributed Denial of Service* (DDoS) ditegaskan dalam penelitian lainnya yang telah di teliti oleh Ruswandi ddk., 2024 yang menyatakan bahwa serangan tersebut dikategorikan serangan yang sangat berbahaya [4].

Variasi dari serangan *Distributed Denial of Service* (DDoS) khususnya tipe *Flooding* yang diteliti oleh Munawarah & Winanto, 2024 menyatakan serangan tersebut yang dianggap lebih merusak. Lingkup serangan *Distributed Denial of Service* (DDoS) yang semakin sering terjadi mendorong perlunya strategi pertahanan siber yang inovatif dan proaktif untuk mengantisipasi ancaman [6]. Pencapaian kinerja tugas yang sukses pada penelitian Hedley ddk., 2023, operator manusia harus menyesuaikan tindakan mereka sesuai dengan perilaku rekan kerja *Artificial Intelligence* (AI) mereka [7]. Kombinasi AI dengan keahlian manusia pada penelitian Sarker ddk., 2023 sebagai strategi yang telah muncul sebagai solusi potensial untuk mengatasi lanskap keamanan jaringan yang terus berubah [8].

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

Konteks strategi pertahanan siber, *Red Teaming* menonjol sebagai strategi utama untuk memahami risiko yang terlibat dalam berbagai macan serangan. Pelatihan dari *Red Teaming*, dapat mensimulasikan serangan untuk meningkatkan kesiapan dalam pertahanan jaringan [9]. Personil *Red Teaming* merancang pendekatan dalam simulasi dengan berpura-pura sebagai penyerang nyata, hingga melakukan pengujian penetrasi [10]. *Red Teaming* sudah digunakan dalam penelitian yang dilakukan oleh Beutel et al., 2024 yang menunjukkan bahwa *Red Teaming* mampu menemukan kelemahan model yang jarang terjadi [12]. Pengujian serangan terhadap ketahanan jaringan menggunakan mekanisme *Red Teaming* yang sudah diteliti oleh Al-Azzawi et al., 2025 menegaskan bahwa mekanisme tersebut menjadi pendekatan penting dalam mengidentifikasi kelemahan sistem keamanan siber [14].

Sebagai pelengkap dari pendekatan ofensif *Red Team*, *Blue Teaming* berperan dalam aspek defensif dengan fokus melindungi aset organisasi melalui pemantauan, deteksi, dan respons insiden secara proaktif [15]. Seiring meningkatnya kompleksitas ancaman siber, kebutuhan akan metrik evaluasi yang kuat, proses otomatis, serta wawasan objektif terhadap kinerja *Blue Team* menjadi semakin mendesak [16]. Penelitian yang membahas tentang *Blue Teaming* yang telah diteliti oleh Wang ddk., 2024 menghasilkan simulasi menunjukkan peningkatan signifikan dalam kecepatan deteksi, akurasi respons, serta ketahanan jaringan dibandingkan metode tradisional [17]. Penggunaan mekanisme *Blue Teaming* yang dilakukan oleh Bianchi ddk., 2024 dapat dimanfaatkan pada *cyber ranges* sebagai lingkungan *virtual* untuk simulasi serangan dan pengujian pertahanan [18].

Melengkapi hubungan antara *Red* dan *Blue Team*, *Purple Teaming* hadir sebagai bentuk kolaboratif yang menjembatani keduanya dalam satu siklus pengujian dan umpan balik yang berkesinambungan [19]. Solusi kerja sama tim dari *Purple Teaming* untuk saran pertahanan yang ditingkatkan, dan penilaian risiko pada keseimbangan [20]. *Purple Teaming* telah di teliti oleh Svotwa ddk., 2025 dengan menekankan pentingnya kolaborasi antara *Red Team* dan *Blue Team* untuk meningkatkan efektivitas pertahanan siber [21]. Strategi dari *Purple Teaming* yang telah diteliti oleh Muchina., 2025 menjelaskan bahwa strategi ini menggunakan kolaborasi langsung antara *Red Team* dan *Blue Team* [22].

Berbagai konsep teknologi *modern* berbasis *Artificial Intelligence* (AI) telah dikembangkan untuk membantu identifikasi hingga mendeteksi suatu objek [23]. *Machine Learning* dapat diterapkan pada berbagai bidang seperti lalu lintas kendaraan darat, industri, medis dan teknologi [24]. Penerapan teknik *Machine Learning* pada penelitian Sitip ddk., 2024 telah muncul sebagai solusi yang menjanjikan untuk mengekstrak wawasan berharga dari berbagai macam data [25]. Penerapan *Machine Learning* pun dapat di terapkan dan mengahsil metode yang akurat akurat pada penelitian Triya ddk., 2024 hingga dapat digunakan dalam melakukan identifikasi hingga prediksi objek dengan metode dan algoritma dari *Machine Learning* [26].

Naïve Bayes termasuk dalam algoritma yang digunakan dengan teknik *Machine Learning* yang berasal dari *teorema bayes*. Berdasarkan konsep yang dikemukakan oleh ilmuan Inggris yaitu Thomas Bayes, bahwa teknik pendekatan ini menggunakan probabilitas dan *statistic* [27]. Pendekatan algoritma Naïve Bayes dengan distribusi *Gaussian* memungkinkan model menangani fitur numerik yang mengikuti distribusi normal [28] Algoritma *Naive Bayes* pada penelitian Aryanti ddk., 2023 berpendapat bahwa algoritma ini salah satu algoritma terbaik dalam *Machine Learning*, dan sangat baik dalam melakukan proses pengklasifikasian data [29]. *Naïve Bayes* terbilang yang paling efektif dan efisien. Meskipun asumsi bahwa atribut dalam data adalah independen pada penelitian Firmansyach ddk., 2023, kinerja klasifikasi *Naïve Bayes* tetap cukup tinggi [30].

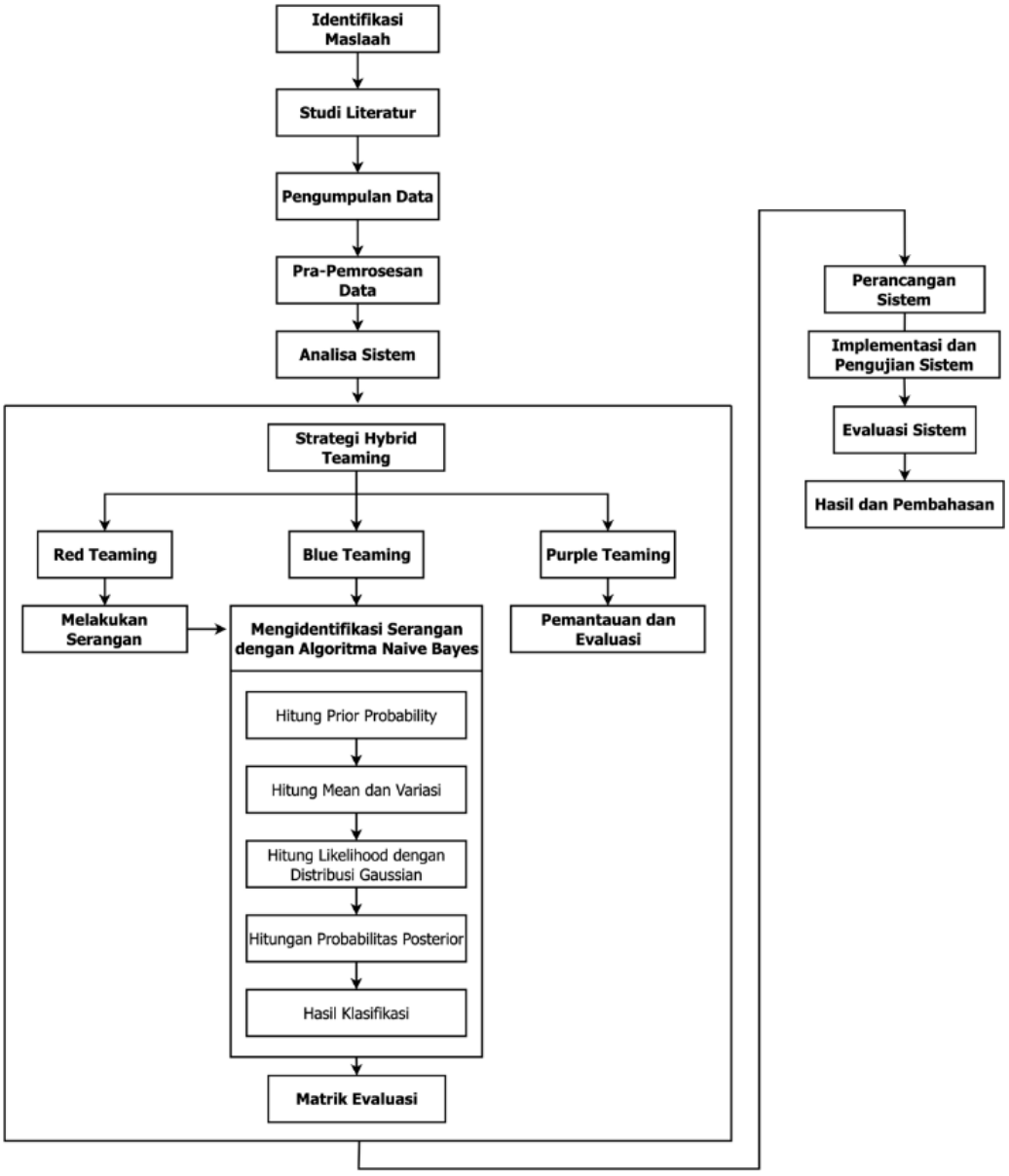
Melihat kemampuan *Naïve Bayes* dalam melakukan klasifikasi serangan siber dengan akurasi yang baik serta kemampuan strategi dari *Hybrid Teaming* yang menggabungkan kekuatan ofensif *Red Team*, defensif *Blue Team*, dan kolaboratif *Purple Team*. Upaya ini bertujuan untuk mengidentifikasi serta menguji pertahanan terhadap ancaman, Kombinasi dari kemampuan klasifikasi *Naïve Bayes* dan pendekatan pengujian komprehensif *Hybrid Teaming* dapat menghasilkan metode analisis ketahanan jaringan yang lebih adaptif, responsif, dan proaktif dalam menghadapi ancaman siber. Kolaborasi kedua pendekatan tersebut tidak hanya memberikan manfaat yanh berpotensi menjadi solusi praktis.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

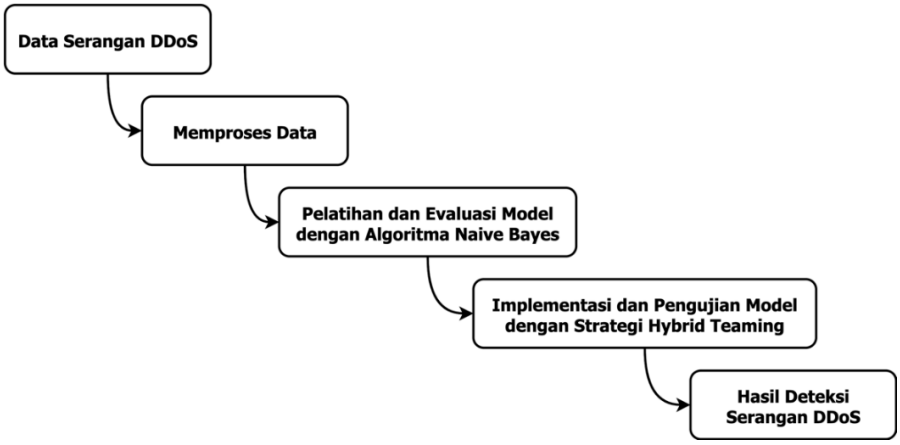
Metodologi penelitian berfungsi sebagai fondasi dan peta jalan yang kritis dalam setiap investigasi ilmiah, terdiri dari serangkaian langkah sistematis yang dirancang secara logis untuk merancang, melaksanakan, dan mengevaluasi suatu penelitian demi mencapai tujuan spesifik yang telah ditetapkan. Inti dari metodologi ini adalah pemilihan jenis penelitian yang tepat, apakah bersifat kualitatif, kuantitatif, atau campuran, serta penetapan pendekatan filosofis atau teoritis yang mendasarinya, seperti deskriptif, eksperimental, atau studi kasus. Setelah data terkumpul, metodologi menentukan penerapan metode analisis data yang ketat dan sesuai, yang dapat berupa analisis statistik, analisis tematik, atau pemodelan, untuk mengolah dan menafsirkan temuan secara objektif. Aspek yang tidak kalah pentingnya adalah penyusunan prosedur pengujian dan validasi hasil yang robust, yang meliputi uji reliabilitas, uji validitas, atau *peer review*, metodologi penelitian sering kali digambarkan secara visual dalam bentuk diagram alur atau kerangka kerja terstruktur. Kerangka kerja visual ini berfungsi sebagai alat bantu yang sangat penting. Sebuah ilustrasi konkret dari kerangka kerja penelitian yang dimaksud dapat diamati pada Gambar 1 yang disajikan di bawah ini:

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323



Gambar 1. Tahapan Penelitian

Gambar 1 mengilustrasikan tahapan-tahapan yang penulis lakukan dalam penelitian ini. Tahapan-tahapan tersebut kemudian dibagi menjadi sub tahapan untuk memudahkan penulis dalam melakukan penelitian. Bagian selanjutnya akan menjelaskan secara terperinci tahapan-tahapan yang penulis lakukan dalam penelitian ini seperti Gambar 2.



Gambar 2. Metode Intelligent System

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

Gambar 2 menjelaskan tahapan-tahapan dari metode yang di gunakan. Tahapan ini memastikan bahwasannya sistem dapat dikembangkan dengan semestinya. Semua konsep yang digunakan akan di jelaskan seperti berikut ini.

2.2 Data Serangan DDoS

Data dikumpulkan dari dua sumber utama untuk memastikan variasi dan keakuratan dalam proses analisis serangan *Distributed Denial of Service* (DDoS). Data terdiri dari data latih dan data uji. Pengumpulan data digunakan untuk persiapan dalam pelatihan dan pengujian pada sistem yang akan dibangun dengan total 11.688 *record* data.

2.2.1 Data Pelatihan

Data pelatihan digunakan untuk membangun model deteksi serangan agar sistem mampu mengenali pola serangan secara akurat. Data ini bersifat primer yang diambil melalui *platform Kaggle* dengan jumlah total 10.000 data. Setiap data berisi atribut serangan dan normal seperti Tabel 1.

Tabel 1. Data Pelatihan

No	Protokol	Rate	Length	Count	TTL	Status
1	ICMP	70	500	25669	64	DDOS-Attack
2	UDP	848	112	6562	128	Normal
3	UDP	70	10272	614990	64	DDOS-Attack
4	TCP	301	68	3883	255	Normal
5	ICMP	63	6184	372962	64	DDOS-Attack

Sumber : https://www.kaggle.com/datasets/easycatch/ddos-flood

Tabel 1 menunjukkan sebagian sampel data pelatihan yang digunakan dalam proses pembelajaran model. Data tersebut terdiri dari 7.000 data serangan (*DDOS-Attack*) dan 3.000 data normal. Keberagaman data pelatihan ini untuk meningkatkan kemampuan model dalam mengenali pola serangan pada berbagai kondisi.

2.2.2 Data Pengujian

Data pengujian digunakan untuk mengevaluasi kinerja model deteksi serangan *Distributed Denial of Service* (DDoS) yang telah dilatih sebelumnya. Data bersifat sekunder yang dikumpulkan langsung dari *log server* Rumah Sakit Umum Daerah Tapan. Total data yang diperoleh berjumlah 1.688 *record* dan ditampilkan secara sampel seperti Tabel 2.

Tabel 2. Data Pengujian

No	Protocol	Length	Rate	Count	TTL	Status
1	ICMP	73	1000	59078	64	DDOS-Attack
2	TCP	83	1000	59151	64	DDOS-Attack
3	TCP	901	140	8515	32	Normal
4	UDP	74	2713	163581	64	DDOS-Attack
5	UDP	527	52	3221	128	Normal

Sumber: Rumah Sakit Umum Daerah Tapan

Tabel 2 menunjukkan sebagian sampel data pengujian yang digunakan dalam tahap evaluasi model. Data tersebut terdiri dari 1.147 *record* berlabel *DDoS-Attack* dan 541 *record* berlabel Normal. Komposisi data ini membantu dalam menilai kemampuan model untuk mengenali pola serangan secara akurat.

2.3 Memproses Data

Data serangan DDoS digunakan sebagai bahan utama dalam proses analisis. Data ini menjadi dasar untuk mengidentifikasi pola serangan. Tahapan pra-pemrosesan dilakukan untuk memastikan data memiliki kualitas yang baik. Proses pra-pemrosesan meliputi pembersihan data dari anomali dan kesalahan. Data yang telah diproses siap untuk dianalisis lebih lanjut. Seluruh tahapan bertujuan agar data sesuai dengan kebutuhan sistem seperti Gambar 3.

Gambar 3. Tahapan Pra-Pemrosesan Data

Gambar 3 menjelaskan alur proses pra-pemrosesan data yang dimulai dari tahap untuk mengumpulkan data serangan dari berbagai sumber. Tahap berikutnya adalah Data *Cleaning* yang berfungsi untuk menghapus data duplikat atau tidak relevan. Setelah itu dilakukan Data *Selection* untuk memilih atribut penting yang dibutuhkan, kemudian dilanjutkan dengan Data *Transformation* agar data dapat digunakan dalam tahap analisis berikutnya.

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

2.4 Pelatihan dan Evaluasi Model

Tahapan ini menggunakan algoritma *Naive Bayes*. Proses ini untuk menganalisis data dan mengklasifikasikan apakah suatu aktivitas jaringan termasuk kategori normal atau terindikasi serangan DDoS. Hasil identifikasi kemudian diuji menggunakan Matrik Evaluasi untuk menilai tingkat efektivitas model dalam mendeteksi serangan.

2.4.1 Naïve Bayes

Algoritma *Naive* Bayes termasuk salah satu algoritma klasifikasi yang menggunakan pendekatan probabilistik berdasarkan Teorema Bayes. Model ini mengasumsikan bahwa setiap fitur bersifat independen satu sama lain. Rumus dasar *Naïve Bayes* ditunjukkan pada persamaan berikut ini:

a. Persiapan Dataset
Proses memasukkan *dataset* dimulai dengan tahap persiapan data. Seluruh data kemudian melalui proses pembersihan dan pengolahan awal agar siap digunakan dalam tahap pelatihan model. Tahap berikutnya adalah pra-pemrosesan, yaitu mengonversi data ke format analisis dengan penghapusan *stopwords*, *stemming*, serta vektorisasi pada data teks, dan melakukan *encoding* pada data kategorikal [34].

b. Menghitung Probabilitas Awal (Prior Probability)
Probabilitas awal untuk mengetahui kemungkinan dasar suatu dokumen termasuk dalam kelas tertentu. Nilai ini diperoleh dari proporsi jumlah pada setiap kelas yang dihitung pada setiap kelas yang ada. Perhitungan probabilitas awal dijelaskan lebih rinci pada Persamaan 1:

$$P(C_i) = \frac{N_{C_i}}{N} \tag{1}$$

Persamaan 1 menampilkan C_i sebagai kelas target yang ingin diprediksi atau dianalisis dalam suatu proses klasifikasi. $P(C_i)$ adalah peluang awal dari kelas target yang diperoleh berdasarkan proporsi jumlah data pada kelas tersebut terhadap keseluruhan data. N_{C_i} menyatakan jumlah data yang termasuk ke dalam kelas target, sedangkan N adalah jumlah total seluruh data yang terdapat dalam dataset dan digunakan sebagai dasar perhitungan peluang [35].

c. Menghitung Mean dan Variansi
Probabilitas setiap fitur dalam kelas dihitung untuk menentukan kontribusi masing-masing fitur terhadap klasifikasi dokumen. Perhitungan ini dilakukan secara terpisah untuk setiap fitur menggunakan data. Rumus perhitungan *Mean* dan Variasi dijelaskan melalui Persamaan 2 dan Persamaan 3:

$$\mu_{ij} = \frac{\sum_{i=1}^{N_{C_i}} x_i}{N_{C_i}} \tag{2}$$

$$\sigma_{ij}^2 = \frac{\sum_{k=i}^{N_{C_i}} (x_i - \mu_{ij})}{N_{C_i}} \tag{3}$$

Persamaan 2 menampilkan μ_{ij} yang merujuk pada peluang atau nilai rata-rata dari fitur X_j pada kelas C_i yang digunakan sebagai parameter dalam proses perhitungan probabilitas. Sedangkan Persamaan 3 menampilkan σ_{ij}^2 yang menyatakan varian dari fitur X_j pada kelas C_i yang berfungsi untuk menggambarkan sebaran data terhadap nilai rata-ratanya. x_{jk} adalah nilai fitur X_j pada data ke-k dalam kelas C_i yang digunakan sebagai *input* untuk menghitung peluang suatu data termasuk ke dalam kelas tertentu [36].

d. Menghitung Likelihood Menggunakan Distribusi Gaussian
Setiap fitur X_j pada data baru dihitung probabilitasnya terhadap kelas C_i. Perhitungan ini digunakan untuk menentukan seberapa besar kemungkinan data baru termasuk dalam kelas tertentu berdasarkan fitur yang dimilikinya. Rumus perhitungannya dijelaskan pada Persamaan 4 [36]:

$$P(X_j = x_j | C_i) = \frac{1}{\sqrt{2\pi\sigma_{ij}^2}} . \exp\left(-\frac{(x_j - \mu_{ij})^2}{2\sigma_{ij}^2}\right) \tag{4}$$

Persamaan 4 menampilkan x_j yang merupakan nilai fitur ke-j dari suatu data yang diklasifikasikan dan digunakan sebagai input dalam proses perhitungan model klasifikasi. Nilai ini merepresentasikan karakteristik spesifik dari data tersebut berdasarkan fitur yang diamati. Informasi dari x_j berperan penting dalam menentukan kelas target yang paling sesuai dengan data yang dianalisis [36].

e. Menghitung Probabilitas Posterior
Peluang akhir suatu data termasuk dalam kelas tertentu dihitung dengan menggabungkan probabilitas awal kelas dan probabilitas masing-masing fitur. Perhitungan ini menentukan kelas yang paling mungkin untuk data tersebut. Rumus perhitungannya dijelaskan pada Persamaan 5:

$$P(C_i|X_n) = P(C_i) \cdot \prod_{j=1}^{n} P(X_j = x_j | C_i) \tag{5}$$

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

Persamaan 5 menampilkan $P(C_i|X)$ sebagai penjelasan simbol probabilitas bahwa suatu data dengan vektor fitur X termasuk ke dalam kelas C_i berdasarkan hasil perhitungan model klasifikasi. $P(X_j = X_j \mid C_i)$ adalah nilai *likelihood* yang menunjukkan peluang munculnya nilai fitur X_j tertentu apabila data tersebut berasal dari kelas C_i. Nilai *likelihood* ini digunakan sebagai komponen utama dalam menentukan besarnya probabilitas akhir suatu data terhadap kelas target [35].

f. Menentukan Hasil Klasifikasi
Kelas data ditentukan dengan memilih kelas yang memiliki peluang akhir tertinggi. Proses ini memastikan data baru diklasifikasikan ke kelas yang paling sesuai berdasarkan perhitungan probabilitas. Penentuan kelas dijelaskan secara formal pada Persamaan 6:

$$Prediksi = arg\ max_{C_i}\ P(C_i|X) \tag{6}$$

Persamaan 6 menampilkan symbol prediksi yang ditentukan menggunakan fungsi arg max terhadap $P(C_i|X)$, yaitu dengan memilih kelas C_i yang memiliki nilai probabilitas *posterior* paling besar. Pendekatan ini memastikan bahwa data diklasifikasikan ke dalam kelas yang paling mungkin. Proses *arg max* berperan penting dalam pengambilan keputusan akhir pada metode klasifikasi probabilistic [37].

2.4.2 Evaluasi Kinerja Model

Pengukuran kinerja model merupakan proses evaluasi yang digunakan untuk menilai seberapa baik model dalam melakukan tugas kategorisasi. Metrik yang umum digunakan dalam evaluasi ini meliputi *precision*, *recall*, *F-measure*, dan *accuracy*. Nilai *True Positive* (TP), *False Positive* (FP), *True Negative* (TN), dan *False Negative* (FN) digunakan untuk menghitung metrik-metrik tersebut, yang menggambarkan hasil prediksi dan performa model pada setiap kelas. Berikut ini adalah parameter perhitungan pengukuran kinerja model [38]:

a. Accuracy
Accuracy merupakan ukuran evaluasi yang menunjukkan seberapa banyak prediksi yang benar (baik positif maupun negatif) dibandingkan dengan seluruh jumlah data. Semakin tinggi nilai akurasi, semakin baik model dalam mengklasifikasikan data secara keseluruhan. Rumus untuk menghitung *accuracy* ditunjukkan pada Persamaan 7:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{7}$$

Persamaan 7 menunjukkan bahwa *accuracy* dihitung berdasarkan jumlah prediksi benar (*True Positive* dan *True Negative*) dibandingkan dengan total seluruh prediksi. Meskipun metrik ini sangat umum digunakan, akurasi bisa menjadi menyesatkan apabila data tidak seimbang.

b. Precision
Precision menunjukkan seberapa tepat model dalam memprediksi kelas positif. Nilai *precision* tinggi menunjukkan bahwa sebagian besar prediksi positif yang dihasilkan oleh model memang benar-benar positif. Hal ini penting terutama ketika kesalahan positif (*false positive*) harus diminimalkan. Rumus precision ditunjukkan pada Persamaan 8:

$$Precision = \frac{TP}{TP+FP} \tag{8}$$

Persamaan 8 menekankan pentingnya meminimalkan kesalahan prediksi positif (*False Positive*), terutama kasus berdampak besar, seperti prediksi fraud atau penyakit. *Precision* berguna saat biaya dari kesalahan positif sangat tinggi.

c. Recall
Recall atau sensitivitas merupakan tahapan mengukur kemampuan model dalam menemukan semua data yang termasuk dalam kelas positif. Nilai *recall* tinggi menunjukkan bahwa model mampu mendeteksi sebagian besar data positif yang ada. Metrik ini sangat penting pada konteks yang mengutamakan deteksi semua kasus positif. Rumus *recall* ditunjukkan pada Persamaan 9:

$$Recall = \frac{TP}{TP+Fn} \tag{9}$$

Persamaan 9 dinyatakan bahwa *recall* yang tinggi berarti model berhasil mengidentifikasi sebagian besar kasus positif. Rumus ini penting untuk situasi yang menuntut deteksi lengkap terhadap kelas positif, seperti dalam sistem peringatan dini atau diagnosis penyakit berbahaya.

d. F1-Score
F1-Score adalah *harmonic* mean dari *precision* dan *recall*. Metrik ini memberikan gambaran seimbang antara kedua metrik tersebut, terutama saat diperlukan kompromi antara keduanya. *F1-Score* berguna ketika distribusi kelas tidak seimbang dan kita ingin mempertimbangkan baik *precision* maupun *recall*. Rumus *F1-Score* ditunjukkan pada Persamaan 10:

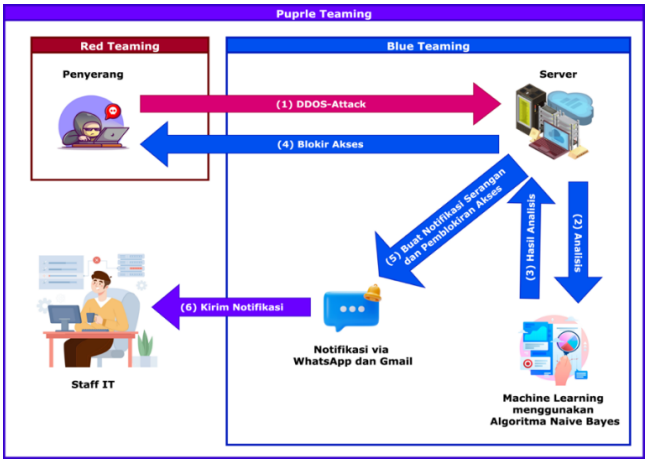
$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{10}$$

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

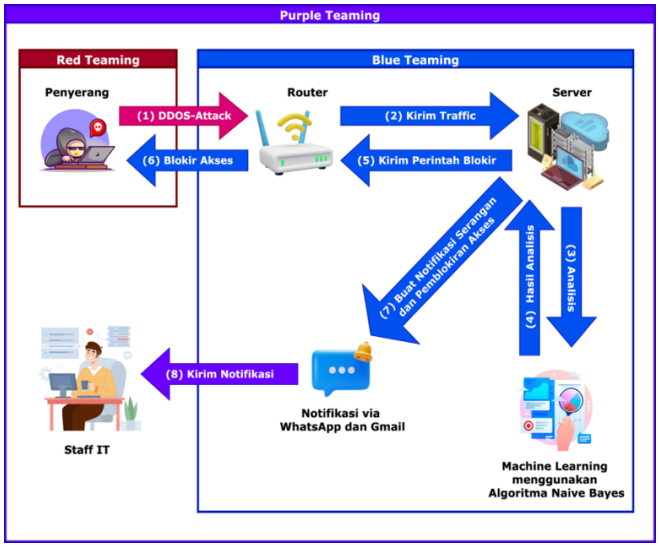
Persamaan 10 ini digunakan ketika terdapat ketidak seimbangan kelas dan diperlukan kompromi antara kemampuan menemukan kelas positif (*recall*) dan ketepatan prediksi kelas positif (*precision*). *F1-Score* menjadi pilihan utama saat ingin menilai kinerja model secara menyeluruh berdasarkan hasil yang di dapati.

2.5 Implementasi dan Pengujian Model

Bagian ini menjelaskan tahapan dari penerapan/implementasi serta pengujian model dengan Strategi *Hybrid Teaming*. Implementasi model dilakukan melalui penggunaan hasil dari pengolahan data. Setelah itu model diuji melalui *server* dan *router* untuk mengidentifikasi serangan nyata dengan model tersebut. Proses ini di rancang seperti skenario yg di ilustrasikan melalui Gambar 4 berikut:



(a) Skenario pada Server



(b) Skenario pada Router

Gambar 4. Skenario Implementasi dan Pengujian Model

Gambar 4 menjelaskan kondisi pengujian yang dilakukan dengan melakukan serangan terhadap *server* dan *router*. Serangan diarahkan dari dua *client* berbeda, di mana satu *client* menargetkan *gateway server* dan *client* lainnya menargetkan *gateway router*. Proses ini digunakan untuk menganalisis kemampuan sistem dalam mendeteksi dan merespons ancaman berbasis kecerdasan buatan.

2.5.1 Red Teaming

Strategi ini merupakan suatu pendekatan dalam dunia keamanan siber yang mengadopsi perspektif penyerang untuk menguji ketahanan sistem, jaringan, atau organisasi secara menyeluruh. Tim yang disebut *Red Team* bertugas mensimulasikan serangan nyata dengan menggunakan berbagai teknik dan metode yang sama seperti yang digunakan oleh pelaku ancaman sesungguhnya, seperti hacker atau kelompok kriminal siber. Aktivitas ini tidak hanya berfokus pada aspek teknis, tetapi juga bisa meliputi pengujian sosial engineering, pengujian fisik, serta pengujian proses internal. Tujuan utama dari *Red Teaming* adalah untuk mengidentifikasi dan mengekspos kelemahan-kelemahan kritis yang bisa dieksploitasi oleh pihak jahat sebelum mereka benar-benar menyerang, sehingga dapat mengambil langkah tepat untuk meningkatkan keamanan [32].

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

2.5.2 Blue Teaming

Strategi ini merupakan pendekatan dalam keamanan siber yang berfokus pada pertahanan sistem dari berbagai jenis serangan. Tim ini bertanggung jawab untuk menjaga keamanan jaringan, sistem, dan data dengan cara memantau aktivitas, mendeteksi ancaman, serta merespons insiden secara cepat dan efektif. Mereka menggunakan berbagai alat dan teknik seperti *firewall*, antivirus, IDS/IPS (*Intrusion Detection/Prevention Systems*), dan SIEM (*Security Information and Event Management*) untuk mengidentifikasi serta menganalisis potensi ancaman yang masuk ke dalam sistem [16].

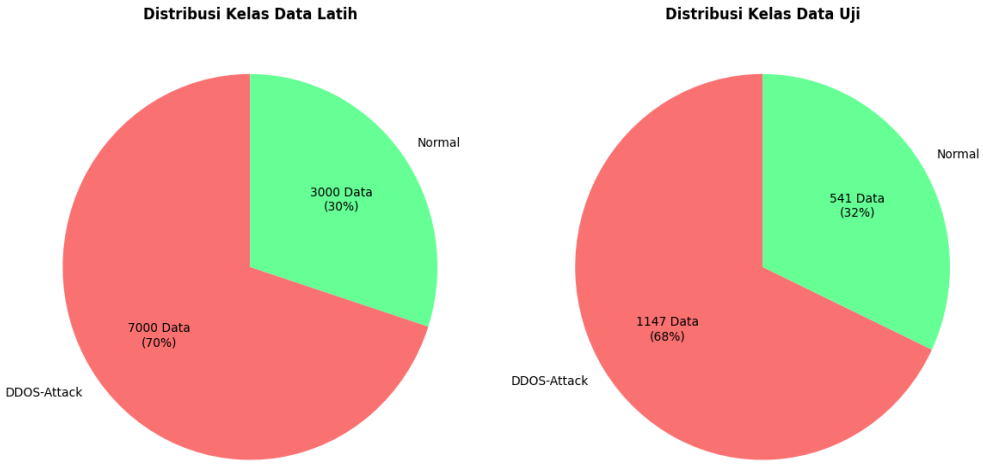
2.5.3 Purple Teaming

Strategi ini *merupakan* konsep yang berkembang sebagai jembatan kolaboratif antara *Red Team* dan *Blue Team*, tim yang bertanggung jawab atas pertahanan dan mitigasi serangan. Berbeda dengan pendekatan tradisional yang memisahkan tugas dan tanggung jawab kedua tim tersebut, Purple Teaming menekankan pentingnya komunikasi dan kerja sama yang erat selama proses pengujian keamanan. Melalui interaksi langsung ini, *Red Team* dapat berbagi taktik, teknik, dan prosedur yang mereka gunakan secara real-time kepada *Blue Team*, sementara *Blue Team* dapat segera merespons dan menguji efektivitas pertahanan mereka terhadap serangan tersebut [33].

3. HASIL DAN PEMBAHASAN

3.1 Hasil Distribusi Data

Hasil ini dilakukan untuk melihat distribusi kelas pada *dataset* sebelum memasuki tahap pelatihan model. Informasi distribusi diperlukan untuk memastikan keseimbangan antara kelas *DDOS-Attack* dan Normal pada data latih maupun data uji. Bentuk visualisasi distribusi tersebut ditampilkan pada Gambar 5 berikut:



Gambar 5. Visualisasi Distribusi Kelas pada Dataset

Gambar 5 menunjukkan perbandingan jumlah data antara kelas *DDOS-Attack* dan kelas Normal pada kedua jenis *dataset*. Tampilan visual membantu memastikan tidak adanya ketimpangan ekstrem yang dapat memengaruhi performa model. Data ini siap digunakan dalam proses pemangunan model sistem deteksi.

3.2 Hasil Pra-Pemrosesan Data

Pemrosesan data dilakukan agar data bisa di olah oleh sistem. Proses ini mencakup 5 (lima) variabel sebagai indikator dalam pemrosesan data. Indikator tersebut di gunakan agar sistem dapat mengenali pola sistem dalam mendeteksi seperti berikut:

a. Protocol (X1).
b. Packet Length (X2).
c. Packet Rate (X3).
d. Packet Count (X4).
e. IP TTL (X5).
f. Status (Y).

Proses ini bertujuan untuk menyeragamkan format data sehingga seluruh variabel memiliki nilai numerik yang dapat dihitung secara matematis. Variabel seperti *Protocol* dan *Status* dikonversi ke dalam bentuk angka. Nilai X1 dan Y dikonversi menjadi menjadi suatu bilangan. Setelah proses konversi dilakukan, seluruh data pelatihan dan pengujian disajikan dalam bentuk numerik, seperti Tabel 3.

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

Tabel 3. Hasil Pra-Processing Data

No	Data Latih						Data Uji					
	X1	X2	X3	X4	X5	Y	X1	X2	X3	X4	X5	Y
1	0	70	500	25669	64	0	0	73	1000	59078	64	0
2	2	848	112	6562	128	1	1	83	1000	59151	64	0
3	2	70	10272	614990	64	0	1	901	140	8515	32	1
4	1	301	68	3883	255	1	2	74	2713	163581	64	0
5	0	63	6184	372962	64	0	2	527	52	3221	128	1

Tabel 3 menunjukkan hasil akhir transformasi data dari kedua sumber. Semua variabel telah diubah ke dalam format numerik sehingga dapat digunakan pada tahap analisis dan penerapan algoritma klasifikasi. Proses transformasi ini memastikan bahwa data memiliki struktur yang seragam dan siap diproses.

3.3 Hasil Pelatihan dan Evaluasi Model

Serangan dilakukan melalui *red teaming* seperti pada Tabel 2. Identifikasi serangan dilakukan oleh *Blue Teaming* yang berperan sebagai pihak pertahanan dalam sistem keamanan jaringan. Tim ini menggunakan algoritma *Naive Bayes* untuk menganalisis data dan mengklasifikasikan apakah suatu aktivitas jaringan termasuk kategori normal atau terindikasi serangan *Distributed Denial of Service* (DDoS). Hasil Mean dan Variasi disajikan pada Tabel 4.

Tabel 4. Hasil Mean dan Variasi

No	Kode	Mean		Variasi	
		Y_0	Y_1	Y_0	Y_1
1	X1	0,988	1,203	0,901	0,366
2	X2	69,522	602,707	215,459	88512,048
3	X3	2416,137	80,635	6820983,247	3109,589
4	X4	144974,03	4841,955	24569607967	11156433,03
5	X5	64,009	83,87	0,585	2405,47

Tabel 4 menunjukkan bahwa terdapat perbedaan signifikan antara nilai *mean* dan variasi pada kedua kelas. Nilai tersebut dihitungan menggunakan Persamaan 2 dan Persamaan 3 melalui Persamaan 1. Nilai *mean* dan variasi akan digunakan sebagai dasar dalam perhitungan *likelihood* seperti Tabel 5.

Tabel 5. Hasil Likelihood

No	X1		…….	X5	
	Y_0	Y_1		Y_0	Y_1
1	0,24450639	0,09131511	…….	0,52155735	0,00749297
2	0,24450639	0,09131511	…….	0,52155735	0,00749297
3	0,23807943	0,276886	…….	0	0,00464981
4	0,24450639	0,09131511	…….	0,52155735	0,00749297
5	0,23807943	0,276886	…….	0	0,00542632

Tabel 5 menunjukkan hasil perhitungan *Likelihood* menggunakan distribusi *Gaussian* pada setiap atribut. Nilai probabilitas tersebut menghasilkan nilai E- (Notasi Ilmiah) di dalam hasil penjumlahan, ini dikarenakan angka sangatlah kecil, dan juga ini bertujuan supaya lebih ringkas dan mudah dibaca. Perhitungan juga menghasilkan nilai 0 (nol) karena nilai eksponensialnya sangat kecil akibat pangkat negatif yang besar, sehingga hasil akhirnya mendekati nol. Nilai yang lebih tinggi pada salah satu kelas digunakan untuk menentukan keputusan klasifikasi akhir. Hasil perhitungan *posterior* ini dikumpulkan untuk seluruh sampel. Ringkasan hasil perhitungan disusun dan ditampilkan pada Tabel 6.

Tabel 6. Hasil Probabilitas Posterior

No	Y_0	Y_1
1	6,81353E-13	2,5431E-130
2	4,59827E-13	1,8918E-130
3	0	8,29827E-14
4	8,88261E-13	0
5	0	3,89566E-13

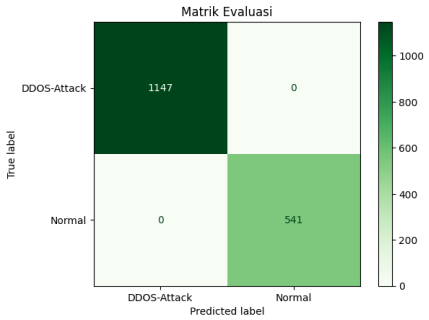
Tabel 6 menunjukkan hasil perhitungan probabilitas *posterior* yang merepresentasikan probabilitas masing-masing kelas. Nilai-nilai sangat kecil pada beberapa entri menggambarkan perbedaan skala *likelihood*. Hasil p*osterior probability* menjadi dasar untuk pengambilan keputusan klasifikasi akhir pada sistem. Hasil akhir dari proses klasifikasi ditampilkan seperti Tabel 7.

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

Tabel 7. Hasil Klasifikasi

No	Y_0	Y_1	Y	Status
1	6,81353E-13	2,5431E-130	0	DDOS-Attack
2	4,59827E-13	1,8918E-130	0	DDOS-Attack
3	0	8,29827E-14	1	Normal
4	8,88261E-13	0	0	DDOS-Attack
5	0	3,89566E-13	1	Normal

Tabel 7 menyatakan hasil dari proses deteksi serangan menggunakan algoritma *Naive Bayes*, di mana nilai Y menunjukkan hasil keputusan akhir. Apabila nilai Y_0 lebih besar dari Y_1, maka aktivotas dikategorikan sebagai *DDOS-Attack*, sedangkan jika nilai Y_1 lebih besar, maka dikategorikan sebagai Normal. Hasil klasifikasi menjadi dasar evaluasi kinerja sistem deteksi serangan *Distributed Denial of Services* (DDoS). Nilai aktual merepresentasikan kategori sebenarnya, sedangkan prediksi menunjukkan hasil klasifikasi sistem. Evaluasi ini yaitu *True Positive (TP)*, *False Positive (FP)*, *False Negative (FN), dan True Negative (TN)*. Nilai-nilai tersebut ditampilkan pada Gambar 6.



Gambar 6. Hasil Pelatihan Model Naïve Bayes

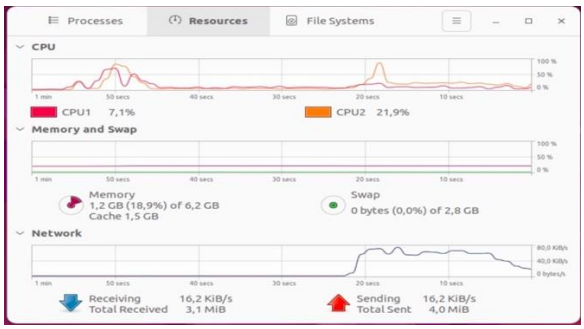
Gambar 6 menunjukkan matriks evaluasi yang menggambarkan performa model pada data latih. Setiap nilai pada matriks tersebut memperlihatkan kemampuan model dalam memprediksi kelas secara akurat. Seluruh metrik menghasilkan *accuracy*, *precision*, *recall*, dan *F1-Score* dengan presentase 100% yang menandakan bahwa model mampu mengklasifikasikan seluruh data latih dengan sempurna. Hasil ini mengindikasikan bahwa pola data pada kelas serangan dan normal dapat dipelajari dengan sangat baik oleh model.

3.4 Hasil Implementasi dan Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh komponen yang telah diimplementasikan mampu berjalan sesuai fungsi yang direncanakan. Proses pengujian mencakup verifikasi kinerja sistem pada *server* dan pengecekan stabilitas koneksi pada *router*. Sistem memberikan respons yang berbeda sesuai parameter trafik yang terdeteksi. Informasi ini menjadi dasar penilaian mengenai kinerja model *Naive Bayes* dalam pengklasifikasian. Pengujian ini bertujuan untuk memastikan bahwa proses deteksi dan klasifikasi dapat berjalan dengan akurat menggunakan bahasa pemograman *Python*. Hasil deteksi serangan dari server dan router disajikan pada Gambar 7.

```
root@atk-VirtualBox:/home/atk# hping3 -1 --flood 10.10.18.1
HPING 10.10.18.1 (enp0s3 10.10.18.1): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

(a) Serangan dari Red Teaming

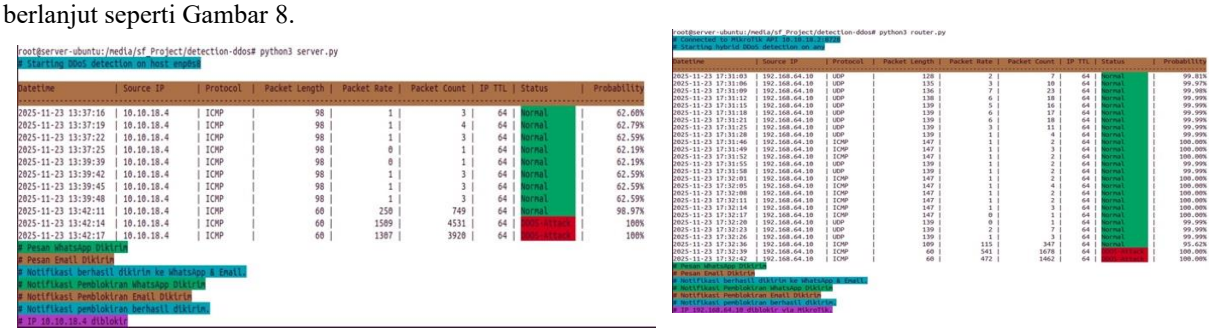


(b) Dampak Serangan

Gambar 7. Serangan dari Red Teaming

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

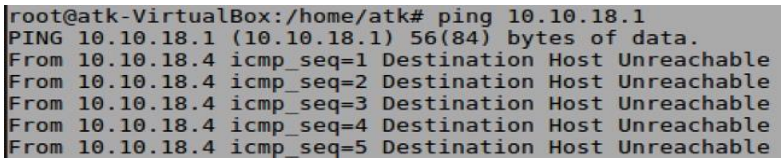
Gambar 7 menampilkan skenario serangan yang diluncurkan oleh tim *Red Teaming* terhadap infrastruktur jaringan. Visualisasi ini memperlihatkan pola trafik mencurigakan yang berhasil diarahkan ke *server* dan *router*. Pola serangan dirancang untuk menguji ketahanan sistem dalam membedakan trafik normal dan anomali. Hasil tangkapan paket data menunjukkan lonjakan permintaan dalam waktu singkat yang mengindikasikan upaya DDoS. Informasi ini menjadi masukan kritis bagi tim Blue Teaming dalam menyusun strategi pertahanan. Pengujian berlanjut seperti Gambar 8.



(a) Hasil Deteksi Serangan ke Server (b) Hasil Deteksi Serangan ke Router

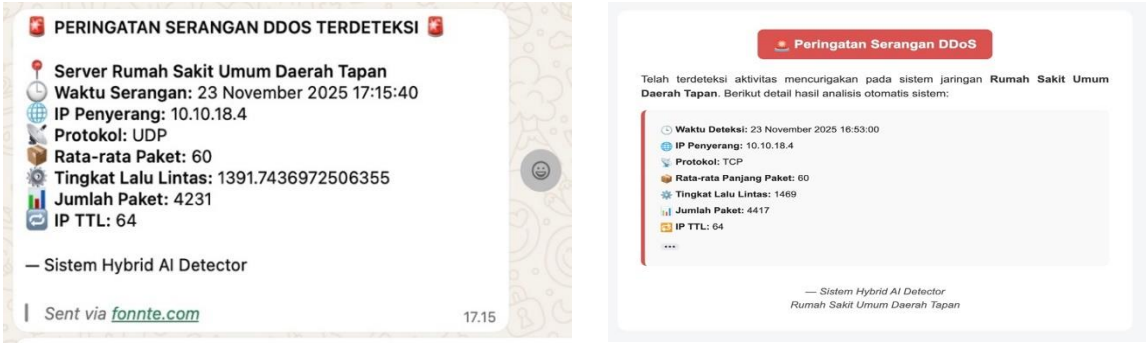
Gambar 8. Hasil Sistem Deteksi dan Pencegahan Sistem dari Blue Teaming

Gambar 8 menyajikan keluaran sistem deteksi berbasis *Naive Bayes* dalam mengidentifikasi serangan pada *server* dan *router*. Tampilan antarmuka menunjukkan status koneksi, jenis serangan terdeteksi, serta tingkat keyakinan klasifikasi. Data klasifikasi yang dihasilkan memiliki akurasi tinggi berdasarkan pengujian terhadap dataset serangan sintetis, seperti Gambar 9.



Gambar 9. Hasil Sistem Deteksi dan Pencegahan Sistem dari Blue Teaming

Gambar 9 menampilkan tahapan pencegahan otomatis yang dijalankan sistem setelah serangan berhasil diklasifikasikan. *Firewall* menerima perintah untuk memblokir alamat *Internet Protocol* (IP) sumber yang terindikasi melakukan serangan. *Server* secara mandiri mengaktifkan mekanisme *rate limiting* guna menstabilkan beban trafik. *Router* turut memperbarui daftar hitam berbasis aturan dari sistem deteksi. Keseluruhan proses berlangsung tanpa campur tangan administrator secara langsung. Setelah itu sistem akan mengirimkan pesan notifikasi seperti Gamar 10.



(a) Pesan WhatsApp (b) Pesan Email

Gambar 10. Notifikasi Pesan Otomatis

Gambar 10 menampilkan pesan peringatan dan pemblokiran yang dikirimkan ke *WhatsApp* dan *Email*. Sistem menyampaikan informasi serangan dan detail penyerang kepada pihak terkait. Notifikasi yang sama dikirimkan melalui *email* untuk memastikan dokumentasi dan tindak lanjut.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem deteksi serangan *Distributed Denial of Service* (DDoS) menggunakan algoritma *Naïve Bayes* yang dikombinasikan dengan strategi *Hybrid Teaming*. Sistem

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

mampu mengklasifikasikan aktivitas jaringan dengan tingkat *accuracy*, *percision*, *recall*, dan *F1-score* mencapai 100% berdasarkan data pelatihan dan pengujian yang digunakan. Implementasi pada *server* dan *router MikroTik* menunjukkan kemampuan sistem dalam mendeteksi serangan *flooding* secara *real-time* serta melakukan respons otomatis berupa pemblokiran alamat IP penyerang dan pengiriman notifikasi melalui *WhatsApp* dan *Email*. Pendekatan *Hybrid Teaming* memberikan keunggulan dalam pengujian menyeluruh melalui simulasi peran *Red Team*, *Blue Team*, dan *Purple Team* sehingga meningkatkan efektivitas analisis ketahanan jaringan. Hasil penelitian ini menunjukkan bahwa kombinasi metode klasifikasi dan strategi kolaboratif dapat menjadi solusi yang efektif dan adaptif dalam menghadapi ancaman serangan siber pada infrastruktur jaringan.

REFERENCES

[1] I. Rahmadaniar, D. A. A. Tondang, B. S. Fernando, and A. Setiawan, "Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS," *Journal of Internet and Software Engineering*, vol. 1, no. 3, p. 10, Jun. 2024, doi: 10.47134/pjise.v1i3.2564.

[2] Y. I. Mahendra and R. E. Putra, "Penerapan Algoritma Gradient Boosted Decision Tree (GBDT) untuk Klasifikasi Serangan DDoS," *Journal of Informatics and Computer Science*, vol. 6, no. 1, 2024, doi: 10.26740/jinacs.v6n01.p158-166.

[3] A. R. Syujak, K. Diantoro, A. Soderi, and P. A. Sucipto, "Integrasi deep packet inspection dengan intrusion detection system (ids) untuk identifikasi serangan ddos dalam jaringan skala besar," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1971–1975, 2024, doi: 10.33395/jmp.v13i2.14324.

[4] K. Ruswandi, M. R. Z. Pohan, K. V. Halim, and S. N. Neyman, "Strategi Pencegahan Efektif terhadap Serangan DDoS Slowloris menggunakan Kali Linux dan Linux Mint," *Journal of Technology and System Information*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2645.

[5] S. M. S. Munawarah and E. A. Winanto, "Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN)," *Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)*, vol. 4, no. 1, pp. 982–991, 2024, doi: 10.33998/jakakom.2024.4.1.1710.

[6] A. Steshenko, "Automating Correlation Between Attacks and Detection in Purple Team Exercises," 2023. [Online]. Available: http://www.usn.no

[7] L. G. Hedley, M. S. Bennett, J. Love, J. Houpt, S. Brown, and A. Eidels, "The relationship between teaming behaviours and joint capacity of hybrid human-machine teams," in *Proceedings of the annual meeting of the cognitive science society*, 2023.

[8] I. H. Sarker, H. Janicke, N. Mohammad, P. Watters, and S. Nepal, "AI Potentiality and Awareness: A Position Paper from the Perspective of Human-AI Teaming in Cybersecurity," Sep. 2023, [Online]. Available: http://arxiv.org/abs/2310.12162

[9] C. Wang *et al.*, "Leveraging Reinforcement Learning in Red Teaming for Advanced Ransomware Attack Simulations," Jun. 2024, [Online]. Available: http://arxiv.org/abs/2406.17576

[10] B. Kotwani, M. R. Sawant, and D. S. Chopra, "Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 07, no. 12, pp. 1–11, Dec. 2023, doi: 10.55041/ijsrem27675.

[11] A. Beutel, K. Xiao, J. Heidecke, and L. Weng, "Diverse and Effective Red Teaming with Auto-generated Rewards and Multi-step Reinforcement Learning," *arXiv preprint arXiv:2412.18693*, 2024.

[12] A. Z. Fazilat *et al.*, "AI-based cleft lip and palate surgical information is preferred by both plastic surgeons and patients in a blind comparison," *The Cleft Palate Craniofacial Journal*, vol. 62, no. 9, pp. 1542–1548, 2025, doi: 10.1177/10556656241266368.

[13] M. Al-Azzawi, D. Doan, T. Sipola, J. Hautamäki, and T. Kokkonen, "Red Teaming with Artificial Intelligence-Driven Cyberattacks: A Scoping Review," *arXiv preprint arXiv:2503.19626*, 2025.

[14] D. Novianto, Y. S. Japriadi, L. Tommy, and S. Sujono, "Implementasi Virtual Private Network Menggunakan Sstp Untuk Keamanan Akses Ke Network Attached Storage Server," *JUSIM (Jurnal Sistem Informasi Musirawas)*, vol. 10, no. 1, pp. 1–13, 2025.

[15] F. Bianchi, E. Bassetti, and A. Spognardi, "Scalable and automated Evaluation of Blue Team cyber posture in Cyber Ranges," in *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*, 2024, pp. 1539–1541.

[16] S. Wang, Y. Li, and F. Chen, "Optimizing blue team strategies with reinforcement learning for enhanced ransomware defense simulations," *Authorea Preprints*, 2024.

[17] S. Wang, Y. Li, and F. Chen, "Optimizing blue team strategies with reinforcement learning for enhanced ransomware defense simulations," *Authorea Preprints*, 2024.

[18] F. Bianchi, E. Bassetti, and A. Spognardi, "Scalable and automated Evaluation of Blue Team cyber posture in Cyber Ranges," in *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*, 2024, pp. 1539–1541.

[19] A. J. Titus and A. H. Russell, "The Promise and Peril of Artificial Intelligence--Violet Teaming Offers a Balanced Path Forward," *arXiv preprint arXiv:2308.14253*, 2023.

[20] Y. Ge and Q. Zhu, "Mega-pt: A meta-game framework for agile penetration testing," in *International Conference on Decision and Game Theory for Security*, Springer, 2024, pp. 24–44, doi: 10.1007/978-3-031-74835-6_2.

[21] L. Svotwa, A. Ganga, and T. Kachote, *Security Engineering with AI for Purple Teaming in Southern Africa*. 2025. doi: 10.13140/RG.2.2.16382.29762.

[22] J. K. Muchina, J. Njihia, and A. Wausi, "The Role of Shared Information Systems Knowledge, Information Systems Resources, and Information System Function Performance," *Electronic Journal of Knowledge Management*, vol. 23, no. 2, pp. 149–165, 2025, doi: 10.34190/ejkm.23.2.3740.

[23] F. Putra, "Penerapan Teknologi Machine Learning dalam Deteksi Dini Penyakit Pada Tanaman Pangan," *Jurnal Kolaborasi Sains dan Ilmu Terapan*, vol. 3, no. 1, pp. 1–5, 2024, doi: 10.69688/juksit.v3i1.50.

Journal of Information System Research (JOSH)
Volume 7, No. 3, April 2026, pp 784−796
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i3.9323

[24] R. V. Rahadyan and R. A. Widyanto, "Literatur Riview: Implementasi Machine Learning pada E Learning System," in *Prosiding University Research Colloquium*, 2023, pp. 723–729.
[25] A. S. Sitio and F. A. Sianturi, "Penerapan Algoritma Machine Learning dalam Analisis Pola Perilaku Penggunaan Internet," *Dike*, vol. 2, no. 2, pp. 46–51, 2024, doi: 10.69688/dike.v2i2.102.
[26] P. Triya, N. Suarna, and N. D. Nuris, "Penerapan Machine Learning Dalam Melakukan Prediksi Harga Saham Pt. Bank Mandiri (Persero) Tbk Dengan Algoritma Linear Regression," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 1, pp. 1207–1214, 2024, doi: 10.36040/jati.v8i1.8958.
[27] B. Ramadhani, R. R. Suryono, and K. Kunci, "Komparasi Algoritma Naïve Bayes dan Logistic Regression Untuk Analisis Sentimen Metaverse," *vol*, vol. 8, pp. 714–725, 2024.
[28] K. B. P. Y. Perkasa and F. E. Purwiantono, "Sistem Rekomendasi Jurusan Menggunakan Algoritma Naïve Bayes Gaussian Berbasis Web," *J-INTECH (Journal of Information and Technology)*, vol. 11, no. 2, pp. 361–370, 2023.
[29] P. G. Aryanti and I. Santoso, "Analisis Sentimen Pada Twitter Terhadap Mobil Listrik Menggunakan Algoritma Naive Bayes," *IKRA-ITH Informatika: Jurnal Komputer Dan Informatika*, vol. 7, no. 2, pp. 133–137, 2023.
[30] W. A. Firmansyach, U. Hayati, and Y. A. Wijaya, "Analisa Terjadinya Overfitting Dan Underfitting Pada Algoritma Naive Bayes Dan Decision Tree Dengan Teknik Cross Validation," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 1, pp. 262–269, 2023, doi: 10.36040/jati.v7i1.6329.
[31] J. Castro, "Using Red and Purple Teaming to Reduce Cyber Risk," Aug. 2024.
[32] M. Feffer, A. Sinha, W. H. Deng, Z. C. Lipton, and H. Heidari, "Red-Teaming for generative AI: Silver bullet or security theater?," in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2024, pp. 421–437.
[33] E. Karhunen, "Purple teaming in system hacking," *Computer science*, 2025.
[34] N. Khoirunnisaa, K. N. N. Kesuma, S. Setiawan, and A. Y. P. Yusuf, "Klasifikasi Teks Ulasan Aplikasi Netflix Pada Google Play Store Menggunakan Algoritma Naive Bayes dan SVM," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 7, no. 1, pp. 64–73, 2024, doi: 10.36080/skanika.v7i1.3138.
[35] G. Honestya, S. Defit, and G. W. Nurcahyo, "Penerapan Naive Bayes untuk Memilih Produk Berdasarkan Jenis Kulit di Toko Kosmetik," *Jurnal KomtekInfo*, pp. 274–280, 2024.
[36] Y. Naufal, R. Putro, A. Afriansyah, and R. Bagaskara, "Penggunaan Algoritma Gaussian Naïve Bayes & Decision Tree Untuk Klasifikasi Tingkat Kemenangan Pada Game Mobile Legends," *JUKI : Jurnal Komputer dan Informatika*, vol. 6, 2024.
[37] Fenilinas Adi Artanto, "Analisis Sentimen Opini Publik terhadap Fenomena Bunuh Diri Mahasiswa di Twitter Menggunakan Algoritma Naive Bayes," *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, vol. 4, no. 1, pp. 70–77, Apr. 2024, doi: 10.54259/satesi.v4i1.2908.
[38] E. N. Cahyo, E. Susanti, and R. Y. Ariyana, "Model Machine Learning Untuk Klasifikasi Kesegaran Daging Menggunakan Arsitektur Transfer Learning Xception," *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, vol. 11, no. 2, pp. 371–376, 2023, doi: 10.26418/justin.v11i2.57517.