LINIER
LITERATUR INFORMATIKA & KOMPUTER
e-ISSN: 3063-2218
DOI : 10.33096/linier.v3i2.3640
Literatur Informatika & Komputer
Vol 3, No 2 (2026), pp 234-240

Perancangan Deteksi Serangan Syn Flooding Menggunakan Metode Naïve Bayes

Fitradi Bambang Kutana[a], Erick Irawadi Alwi[b], Andi Widya Mufila Gaffar[c]
Universitas Muslim Indonesia, Makassar, Indonesia
[a]13020200140@umi.ac.id; [b]erick.alwi@umi.ac.id; [c]widya.mufila@umi.ac.id

Received: 08-04-2026 | Revised: 02-06-2026 | Accepted: 26-06-2026 | Published: 29-06-2026

Abstrak

Serangan *Distributed Denial of Service* (DDoS), khususnya SYN Flooding, merupakan salah satu ancaman serius dalam keamanan jaringan komputer yang memanfaatkan kelemahan proses three-way handshake pada protokol TCP. Serangan ini menyebabkan server mengalami kelebihan beban akibat banyaknya koneksi setengah terbuka sehingga mengganggu ketersediaan layanan. Penelitian ini bertujuan untuk merancang sistem deteksi serangan SYN Flooding menggunakan metode Naive Bayes sebagai algoritma klasifikasi berbasis probabilitas. Metode penelitian meliputi pengumpulan data trafik jaringan normal dan serangan, preprocessing data melalui pembersihan dan ekstraksi fitur, serta pembagian dataset menjadi data latih dan data uji. Fitur yang digunakan antara lain jumlah paket SYN, durasi koneksi, dan status koneksi. Model Naive Bayes kemudian dibangun dan dievaluasi menggunakan confusion matrix dengan parameter akurasi, precision, recall, dan F1-score. Hasil penelitian menunjukkan bahwa metode Naive Bayes mampu mengklasifikasikan trafik jaringan dengan baik serta mendeteksi serangan SYN Flooding secara akurat dan efisien. Selain itu, metode ini memiliki keunggulan dalam hal kesederhanaan dan kecepatan komputasi sehingga cocok diterapkan pada sistem deteksi intrusi jaringan. Dengan demikian, penelitian ini memberikan kontribusi dalam pengembangan sistem keamanan jaringan yang adaptif dan efektif dalam menghadapi ancaman serangan siber.

Kata kunci: SYN Flooding, DoS, Naive Bayes, Keamanan Jaringan, Serangan.

Pendahuluan

Penggunaan jaringan komputer semakin meningkat seiring dengan perkembangan terkonologi informasi yang semakin pesat. Jaringan komputer tidak hanya digunakan untuk kepentingan bisnis,tetapi juga digunakan untuk kepentingan pribadi seperti internet banking dan media sosial. Namun,semakin banyak penggunaan jaringan komputer, semakin banyaka pula ancaman keamanan yang mengintai. Oleh karena itu,keamanan jaringan menjadi suatu hal yang sangat penting untuk menjaga kerahasiaan,integritas serta ketersediaan data [1]. Serangan Denial of Service (DoS) merupakan salah satu jenis serangan yang bertujuan untuk mengganggu ketersediaan layanan pada suatu sistem atau server [2]. Serangan ini bekerja dengan cara membanjiri server dengan sejumlah besar permintaan dari satu sumber sehingga kapasitas sumber daya server menjadi penuh. Akibatnya, server tidak mampu menangani permintaan yang masuk secara normal dan menyebabkan layanan tidak dapat diakses atau tidak berjalan sebagaimana mestinya [3].

Syn flood adalah salah satu serangan *Denial of service (DoS)* yang memanfaatkan mekanisme TCP *Three way handshake* sehingga menyulitkan untuk membedakan dengan koneksi TCP legal karena memiliki karakteristik yang sama dengan koneksi TCP legal [4], [5]. Serangan *Syn Flood* muncul ketika klien tidak merespon *SYN/ACK* dari server sehingga layanan berhenti sampai waktunya habis [4], [6]. Pada tipe serangan ini klien tidak pernah merespon karena alamat asalnya dipalsukan. Sasaran penyerangan adalah mengirim paket *SYN* kepada server dengan lebih cepat daripada waktu yang diperlukan server untuk berhenti menunggu respon ACK dari klien sehingga menyebabkan server begitu sibuk untuk menunggu klien yang tidak menjawab *SYN/ACK server.* Setelah proses tersebut dilalui maka transferan data akan dimulai [7].

Dalam beberapa tahun terakhir, *Syn Flood* masih menjadi salah satu jenis serangan jaringan yang paling agresif dan sering digunakan oleh penyerang, terutama dalam lingkungan jaringan modern seperti SDN dan *cloud computing* [8]. Serangan ini tidak hanya berdampak pada penurunan performa jaringan, tetapi juga dapat menyebabkan kerugian finansial dan gangguan operasional pada sistem yang bergantung pada layanan jaringan secara real-time. Selain itu, meningkatnya skala jaringan dan penggunaan perangkat yang terhubung secara luas menyebabkan potensi serangan menjadi semakin besar, termasuk kemungkinan penggunaan botnet untuk melancarkan serangan secara masif (Distributed DoS). Hal ini memperparah kondisi karena sistem keamanan

tradisional seperti firewall sering kali tidak mampu membedakan antara trafik normal dan trafik serangan secara akurat [9], [10], [11].

Seiring dengan meningkatnya kompleksitas jaringan komputer dan tingginya ancaman keamanan siber, diperlukan metode deteksi yang mampu mengidentifikasi serangan secara cepat dan akurat. Salah satu pendekatan yang banyak digunakan dalam sistem deteksi intrusi adalah metode berbasis *machine learning*, khususnya algoritma Naive Bayes. Metode ini dikenal karena kesederhanaannya, efisiensi komputasi, serta kemampuannya dalam melakukan klasifikasi berdasarkan probabilitas data yang diamati. Naive Bayes merupakan algoritma klasifikasi yang didasarkan pada Teorema Bayes dengan asumsi bahwa setiap fitur bersifat independen satu sama lain [12]. Dalam konteks keamanan jaringan, metode ini dapat digunakan untuk mengklasifikasikan trafik jaringan ke dalam kategori normal atau serangan berdasarkan pola tertentu yang terdeteksi pada data [13]. Keunggulan utama dari Naive Bayes adalah kemampuannya dalam menangani dataset berukuran besar serta memberikan hasil klasifikasi yang cukup akurat dengan waktu komputasi yang relatif cepat [14]. Dalam beberapa penelitian nasional terbaru, metode Naive Bayes telah banyak diterapkan dalam berbagai bidang keamanan siber, termasuk deteksi serangan jaringan. Penerapan algoritma ini pada sistem deteksi intrusi menunjukkan bahwa Naive Bayes mampu mengidentifikasi pola serangan dengan tingkat akurasi yang tinggi, terutama pada data yang memiliki karakteristik statistik yang jelas. Selain itu, metode ini juga dinilai efektif dalam memproses data trafik jaringan yang kompleks dan dinamis. Terkait dengan serangan *SYN Flooding***,** penggunaan Naive Bayes menjadi solusi yang cukup menjanjikan karena serangan ini memiliki pola trafik tertentu yang dapat dianalisis secara probabilistik. *SYN Flooding* biasanya ditandai dengan tingginya jumlah paket SYN yang tidak diikuti oleh penyelesaian koneksi (ACK), sehingga menghasilkan banyak koneksi setengah terbuka [15]. Pola ini dapat dijadikan sebagai fitur dalam proses klasifikasi menggunakan Naive Bayes [16].

Beberapa penelitian nasional menunjukkan bahwa penggunaan Naive Bayes dalam mendeteksi serangan jaringan, termasuk *SYN Flooding*, mampu menghasilkan performa yang baik dengan tingkat akurasi yang tinggi. Selain itu, metode ini juga relatif mudah diimplementasikan dan tidak memerlukan sumber daya komputasi yang besar, sehingga cocok digunakan dalam sistem keamanan jaringan skala kecil hingga menengah [17]. Dengan demikian, penggunaan metode Naive Bayes dalam mendeteksi serangan SYN Flooding menjadi salah satu pendekatan yang efektif dan efisien dalam meningkatkan keamanan jaringan. Oleh karena itu, penelitian ini mengkaji penerapan Naive Bayes sebagai metode klasifikasi dalam sistem deteksi serangan SYN Flooding guna menghasilkan sistem yang mampu mendeteksi serangan secara cepat, akurat, dan adaptif terhadap perubahan pola trafik jaringan.

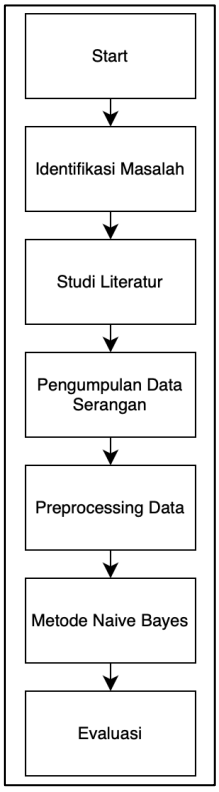
Metode

A. Tahapan Penelitian

Penelitian dilakukan melalui beberapa langkah penelitian yang dapat dilihat pada Gambar 1.

1. Identifikasi Masalah
   Tahap awal penelitian dilakukan dengan mengidentifikasi permasalahan yang terjadi pada jaringan komputer, khususnya terkait serangan *Denial of Service* (DoS) jenis *SYN Flooding*. Pada tahap ini dianalisis bagaimana serangan tersebut bekerja, dampaknya terhadap sistem, serta kelemahan metode deteksi yang sudah ada.
2. Studi Literatur
   Tahap ini dilakukan dengan mengkaji Konsep dasar jaringan komputer dan keamanan jaringan, Karakteristik serangan *SYN Flooding,* Metode deteksi intrusi berbasis machine learning, Penerapan algoritma Naive Bayes dalam klasifikasi data
3. Pengumpulan Data Serangan
   Data yang digunakan berupa data trafik jaringan normal dan data trafik serangan *Syn Flooding*
4. Processing Data
   Data yang telah dikumpulkan kemudian diproses terlebih dahulu sebelum digunakan,seperti membersihkan data (data cleaning) menghapus data yang tidak lengkap atau noise. Transformasi data mengubah data ke format yang sesuai. Ekstraksi fitur mengambil atribut penting seperti jumlah paket SYN,durasi koneksi dan ukuran paket.

5. Metode Naive Bayes
   Menentukan variabel input(fitur) dan output (label:normal atau attack). Menghitung probabilitas prior dan likehood. Membangun model klasifikasi menggunakan data training serta menguji model menggunakan data testing.
6. Evaluasi
   Tahap evaluasi dilakukan untuk mengukur kinerja model yang telah dibangun. Evaluasi dilakukan dengan menggunakan confusion matrix dengan parameter: Accuracy (tingkat ketetapan model) Precision (ketetapan prediksi positif) Recall (kemampuan mendeteksi serangan) F1-score (keseimbangan antara precision dan recall).



Gambar 1. Tahapan Penelitian

B. *Syn Flooding*
Serangan *SYN Flood* merupakan salah satu bentuk gangguan pada ketersediaan layanan (*Denial of Service*) yang menargetkan celah pada prosedur inisiasi koneksi TCP [18], [19]. Penyerang membanjiri target dengan permintaan koneksi yang tidak tuntas, sehingga menghabiskan kapasitas memori server dan memutus akses bagi pengguna yang sah [20].

Gambar 2. Ilustrasi Syn Flooding

C. Naive Bayes

Metode Naive Bayes merupakan algoritma klasifikasi dalam pembelajaran mesin yang berlandaskan pada Teorema Bayes dengan asumsi kemandirian antar variabel yang sangat kuat. Teknik ini bekerja dengan menghitung peluang probabilitas dari setiap kategori berdasarkan fitur yang ada, di mana setiap fitur dianggap memberikan kontribusi yang independen tanpa adanya ketergantungan satu sama lain [21]. Meskipun memiliki asumsi yang sangat sederhana, Naive Bayes sangat efektif dalam menangani kumpulan data besar serta sering digunakan dalam analisis teks dan penyaringan informasi karena efisiensi komputasinya yang tinggi [22], [23].

D. Confusion Matrix

Confusion Matrix merupakan alat evaluasi kinerja yang menyajikan perbandingan antara hasil prediksi model klasifikasi dengan data aktual dalam bentuk tabel pemetaan. Melalui matriks ini, performa sistem diukur berdasarkan empat parameter utama, yaitu *True Positive, True Negative, False Positive, dan False Negative*, yang memungkinkan identifikasi jenis kesalahan klasifikasi secara mendalam. Tidak hanya terbatas pada akurasi semata, tabel ini menjadi dasar perhitungan metrik evaluasi penting lainnya seperti presisi, sensitivitas (*recall*), dan F1-score, sehingga memberikan gambaran yang lebih menyeluruh mengenai efektivitas model dalam mengenali setiap kelas target [24]. Adapun rumus akurasi, presisi, recall sebagai berikut [25].

$$Accuracy = \frac{TposPos + TnonNon + TNegNeg}{Total} \quad (1)$$

$$Precision = \frac{TPosPos}{TPosPos + NonFP + NegFP} \quad (2)$$

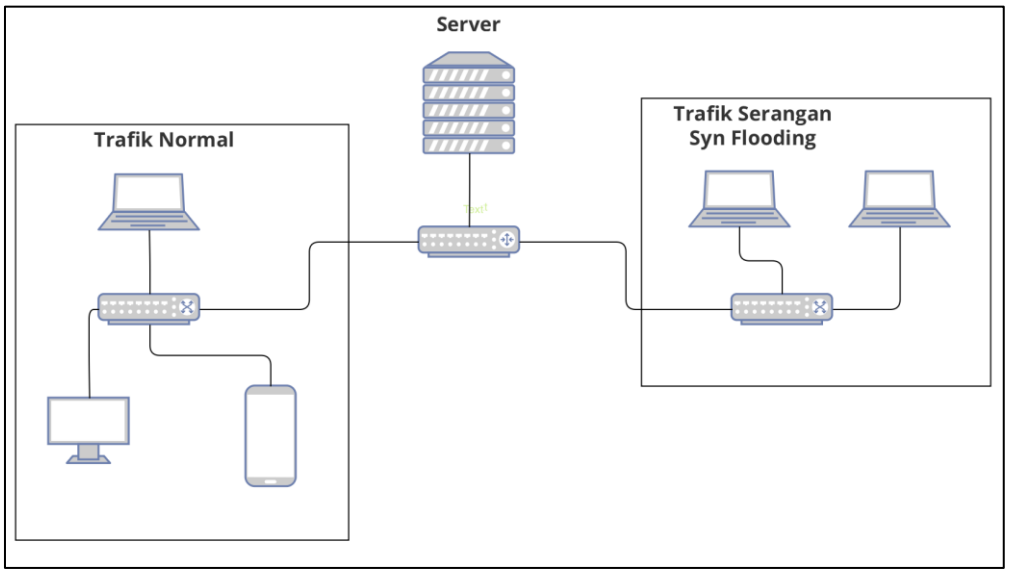
$$Recall = \frac{TPosPos}{TPosPos + PFNon + PFNeg} \quad (3)$$

$$Total = TPosPos + PFNon + PFNeg + NonFP + TNonNon + NonFNeg + NegFP + NegFNon + TNegNeg \quad (4)$$

Perancangan

A. Desain Topologi Jaringan

Adapun perancangan topologi jaringan dapat dilihat pada Gambar 2.



Gambar 2. Topologi Jaringan

Topologi tersebut menunjukkan perbandingan antara kondisi trafik jaringan normal dan saat terjadi serangan SYN Flooding pada sebuah server. Pada kondisi normal, berbagai perangkat seperti laptop, komputer, dan smartphone mengirimkan permintaan ke server melalui jaringan secara wajar dan terkontrol, sehingga server mampu merespons setiap permintaan dengan baik tanpa mengalami gangguan.

Namun, pada kondisi serangan SYN Flooding, sejumlah perangkat atau penyerang mengirimkan permintaan koneksi secara berlebihan dan tidak lengkap (hanya mengirimkan sinyal SYN tanpa menyelesaikan proses handshake). Hal ini menyebabkan server dipenuhi oleh koneksi setengah terbuka sehingga sumber daya menjadi terbebani. Akibatnya, kinerja server menurun dan bahkan dapat gagal melayani permintaan dari pengguna yang sah, yang berujung pada kondisi penolakan layanan (Denial of Service).

B. Skenario Penelitian

Adapun langkah penelitian sebagai berikut:

1. Menyiapkan dua perangkat dalam jaringan, dimana satu berperan sebagai klien dan perangkat lainnya sebagai server.
2. Menempatkan *packet sniffer* di antara klien dan server untuk melakukan monitoring serta merekam seluruh aktivitas lalu lintas jaringan yang terjadi di antara keduanya.
3. Klien melakukan aktivitas koneksi normal dengan menjalankan *script* yang secara berkala mengakses server melalui koneksi TCP pada protokol HTTP serta melakukan proses pengunduhan data.
4. Pada waktu yang bersamaan, klien juga mensimulasikan serangan *SYN flood* ke server untuk menghasilkan trafik serangan.
5. Data hasil tangkapan kemudian dipilah dengan menghapus informasi yang tidak relevan dari dataset.
6. Dataset yang telah melalui tahap *preprocessing* dan berbentuk file ASCII selanjutnya disimpan ke dalam database.
7. Dilakukan kembali proses pembersihan data untuk memastikan hanya informasi penting yang digunakan dalam analisis.
8. Dataset hasil *preprocessing* kembali diinput ke dalam database sebagai data yang siap digunakan.
9. Pengguna menyiapkan data latih sebagai dasar dalam proses analisis atau pemodelan.
10. Pengguna menentukan data uji beserta parameter yang diperlukan untuk proses deteksi.
11. Setiap koneksi pada data uji dianalisis untuk menghitung tingkat kemungkinan terjadinya serangan *SYN flood* dengan mengacu pada data latih yang telah tersedia.
12. Hasil perhitungan probabilitas tersebut digunakan untuk menentukan apakah suatu koneksi termasuk serangan *SYN flood* atau bukan, berdasarkan nilai kemungkinan tertinggi.

Pemodelan

A. Pengumpulan dan Pra-pemrosesan Data (Traffic Scraping)

Dalam tahap ini, dataset lalu lintas jaringan dikumpulkan dan diproses untuk mendeteksi anomali yang mengarah pada serangan SYN Flooding. Data yang diperoleh melalui proses *scraping* atau *packet sniffing* mencakup fitur-fitur kritikal seperti alamat IP sumber, jumlah paket SYN yang masuk dalam interval waktu tertentu, status koneksi (*half-open*), serta durasi *handshake*. Analisis awal menunjukkan adanya pola pembeda yang jelas: aktivitas normal ditandai dengan rasio paket SYN dan ACK yang seimbang, sedangkan indikasi serangan terlihat pada lonjakan drastis paket SYN dari alamat IP yang tidak valid atau tersebar, yang secara langsung berkorelasi dengan peningkatan beban kerja memori pada server target.

B. Pembagian Data

Untuk memastikan model deteksi memiliki kemampuan generalisasi yang baik, seluruh dataset lalu lintas jaringan dibagi menjadi dua bagian dengan proporsi 70% untuk data latih (*training set*) dan 30% untuk data uji (*testing set*). Penggunaan rasio 70:30 ini bertujuan agar algoritma Naïve Bayes dapat mempelajari karakteristik statistik dari trafik normal maupun trafik serangan secara mendalam. Data latih digunakan untuk membentuk pola hubungan antar fitur keamanan, sementara data uji berfungsi untuk memvalidasi akurasi model dalam mengidentifikasi serangan baru yang belum pernah dikenali sebelumnya (data *unseen*).

C. Implementasi Klasifikasi Naïve Bayes

Pemodelan Naïve Bayes diterapkan untuk mengklasifikasikan status keamanan jaringan ke dalam kategori: "Normal", "Waspada", atau "Serangan (SYN Flood)". Algoritma ini bekerja dengan menghitung probabilitas bersyarat berdasarkan fitur-fitur trafik, seperti rata-rata (*mean*) jumlah permintaan koneksi

setengah terbuka dan variansi (*variance*) waktu tunggu paket ACK. Hasil pemodelan menunjukkan bahwa pada kondisi serangan, nilai rata-rata jumlah paket SYN meningkat secara signifikan dengan variansi yang cenderung rendah, menandakan adanya pola serangan yang masif dan seragam. Dengan menghitung *prior probabilities* dari distribusi data, model dapat secara cepat menentukan status jaringan, sehingga memungkinkan sistem pertahanan untuk melakukan mitigasi sebelum sumber daya server habis terkuras.

D. Evaluasi Model

Tahap terakhir dalam perancangan ini adalah evaluasi performa model menggunakan *Confusion Matrix* untuk mengukur efektivitas algoritma Naïve Bayes dalam mendeteksi serangan. Berdasarkan hasil pengujian pada data uji (*testing set*), kinerja model dinilai melalui tiga metrik utama: Akurasi, *Recall*, dan F1-Score. Akurasi memberikan gambaran umum mengenai persentase prediksi benar model terhadap keseluruhan trafik. Sementara itu, *Recall* (sensitivitas) menjadi parameter krusial untuk melihat sejauh mana model mampu mengidentifikasi seluruh paket serangan *SYN Flood* tanpa ada yang terlewat (*false negative*). Terakhir, F1-Score digunakan sebagai penyeimbang antara presisi dan recall untuk memastikan bahwa model tetap stabil dalam membedakan antara trafik normal dan anomali, sehingga sistem deteksi yang dihasilkan memiliki tingkat kepercayaan yang tinggi dalam menjaga ketersediaan sumber daya server.

Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa metode Naive Bayes mampu diterapkan secara efektif dalam sistem deteksi serangan SYN Flooding pada jaringan komputer. Melalui tahapan pengumpulan data, preprocessing, ekstraksi fitur, hingga proses klasifikasi, model yang dibangun dapat membedakan antara trafik normal dan trafik serangan berdasarkan pola probabilistik yang terbentuk.

Hasil pengujian menunjukkan bahwa Naive Bayes memiliki tingkat akurasi yang cukup tinggi serta efisiensi waktu komputasi yang baik, sehingga cocok digunakan untuk sistem deteksi intrusi secara real-time maupun pada jaringan skala kecil hingga menengah. Selain itu, karakteristik serangan SYN Flooding yang memiliki pola tertentu, seperti tingginya jumlah paket SYN tanpa penyelesaian handshake, dapat dikenali dengan baik oleh model.

Dengan demikian, penerapan metode Naive Bayes dapat menjadi solusi yang sederhana, cepat, dan efektif dalam meningkatkan keamanan jaringan, khususnya dalam mendeteksi serangan SYN Flooding. Namun, untuk pengembangan selanjutnya, disarankan untuk mengombinasikan metode ini dengan algoritma lain atau menggunakan dataset yang lebih kompleks agar meningkatkan akurasi dan ketahanan sistem terhadap berbagai jenis serangan yang lebih beragam.

Daftar Pustaka

[1] A. B. Pratomo, “Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik RouterOS,” *Bulletin of Network Engineer and Informatics*, vol. 1, no. 2, p. 51, Oct. 2023, doi: 10.59688/bufnets.v1i2.10.

[2] A. R. Aulia, E. I. Alwi, and A. W. M. Gaffar, “Perancangan Sistem Keamanan Jaringan Intrusion Prevention System Menggunakan Suricata Dan IPTables,” *LINIER: Literatur Informatika dan Komputer*, vol. 1, no. 3, pp. 235–240, Dec. 2024, doi: 10.33096/linier.v1i3.2500.

[3] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Na\"\ive Bayes,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 1, pp. 172–180, 2022.

[4] W. M. Eddy, “SYN Flood Attack,” in *Encyclopedia of Cryptography, Security and Privacy*, Cham: Springer Nature Switzerland, 2025, pp. 2564–2566. doi: 10.1007/978-3-030-71522-9_276.

[5] K. Hussain, S. J. Hussain, N. Jhanjhi, and M. Humayun, “SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET,” in *2019 International Conference on Computer and Information Sciences (ICCIS)*, IEEE, Apr. 2019, pp. 1–4. doi: 10.1109/ICCISci.2019.8716416.

[6] T. Das, O. A. Hamdan, S. Sengupta, and E. Arslan, “Flood Control: TCP-SYN Flood Detection for Software-Defined Networks using OpenFlow Port Statistics,” in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, Jul. 2022, pp. 1–8. doi: 10.1109/CSR54599.2022.9850339.

[7] S. M. Syifa Munawarah, Kurniabudi, and Eko Arip 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, Apr. 2024, doi: 10.33998/jakakom.2024.4.1.1710.

[8] S. Kumar and S. Gupta, "SDN TCP-SYN Dataset: A dataset for TCP-SYN flood DDoS attack detection in software-defined networks," *Data Brief*, vol. 59, p. 111314, Apr. 2025, doi: 10.1016/j.dib.2025.111314.

[9] C.-H. Yang, J.-P. Wu, F.-Y. Lee, T.-Y. Lin, and M.-H. Tsai, "Detection and Mitigation of SYN Flooding Attacks through SYN/ACK Packets and Black/White Lists," *Sensors*, vol. 23, no. 8, p. 3817, Apr. 2023, doi: 10.3390/s23083817.

[10] I. N. B. Arya Wirianda, R. B. Huwae, and A. H. Jatmika, "Pengujian Efektivitas Intrusion Detection Systems (IDS) Snort,Suricata, dan Zeek terhadap Serangan SYN Flood tection System Snort, Suricata, dan Zeek dalam Mendeteksi Serangan SYN Flood pada Windows Server 2022," *Jurnal Bumigora Information Technology (BITe)*, vol. 7, no. 2, pp. 95–108, Dec. 2025, doi: 10.30812/bite.v7i2.5226.

[11] R. G. Gunawan, Erik Suanda Handika, and Edi Ismanto, "Pendekatan Machine Learning Dengan Menggunakan Algoritma Xgboost (Extreme Gradient Boosting) Untuk Peningkatan Kinerja Klasifikasi Serangan Syn," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 3, pp. 453–463, Dec. 2022, doi: 10.37859/coscitech.v3i3.4356.

[12] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Na\"\ive Bayes," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 1, pp. 172–180, 2022.

[13] I. Bagus *et al.*, "Implementasi Algoritma Naive Bayes Classifier (NBC) Dan Information Gain Untuk Mendeteksi DDoS," *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, 2022, [Online]. Available: https://api.semanticscholar.org/CorpusID:254666381

[14] E. S. J. Atmadji, Y. Wabula, H. T. Karsanti, and K. Kristopher, "The Use of Naive Bayes Classifier in Sentiment Analysis at Indonesia's Super Priority Tourism Destinations Based on User Reviews," *Jurnal Sosioteknologi*, vol. 24, no. 2, pp. 226–239, Jul. 2025, doi: 10.5614/sostek.itbj.2025.24.2.7.

[15] Adam Zukhruf, Bagus Fatkhurrozi, and Andriyatna Agung Kurniawan, "Comparative Study Of Distributed Denial of Service (DDOS) Attack Detection In Computer Networks," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1033–1039, Oct. 2023, doi: 10.52436/1.jutif.2023.4.5.756.

[16] D. Firdaus, F. Fahira, and R. Rianti, "Deteksi Anomali dan Serangan Low Rate DDOS Dalam Lalu Lintas Jaringan Menggunakan Naive Bayes," *Naratif : Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, vol. 5, no. 2, pp. 140–148, Dec. 2023, doi: 10.53580/naratif.v5i2.208.

[17] I. Saputri, P. Arsi, and K. N. Isnaini, "Effectiveness Hyperparameter Tuning On Random Forest, Linear Discrimant Analysis, Logistic Regression and Naive Bayes Algorithms For Detecting DOS Network Attacks," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 1, pp. 87–104, Feb. 2025, doi: 10.52436/1.jutif.2025.6.1.4175.

[18] M. F. E. Erlangga, N. Fahriani, and A. H. Tantri, "Deteksi Serangan Syn Flood Pada Server Menggunakan Metode Algoritma K-Nearest Neightbor," in *SEMASTER: Seminar Nasional Teknologi Informasi & Ilmu Komputer*, 2023, pp. 68–72.

[19] A. Dwi Azahra and K. Monika Dian Pertiwi, "Deteksi Serangan DoS pada IoT Berbasis MQTT Menggunakan XGB dan PSO," *Jurnal Algoritma*, vol. 22, no. 2, Dec. 2025, doi: 10.33364/algoritma/v.22-2.2623.

[20] G. Putra, F. Indrajid, K. F. Andika, K. K. Bramanda, I. G. A. J. Saskara, and I. M. E. Listartha, "Analisis Hasil DoS SYN Flood Attack Pada Web Server," *Format J. Ilm. Tek. Inform*, vol. 12, no. 1, p. 1, 2023.

[21] A. A. Aqsa, I. Irawati, and L. Syafie, "Perbandingan Metode Naïve Bayes dan SVM dalam Analisis Sentimen Netizen Twitter Terhadap Isu Kemenkeu," *Buletin Sistem Informasi dan Teknologi Islam*, vol. 4, no. 4, pp. 327–338, Dec. 2023, doi: 10.33096/busiti.v4i4.1824.

[22] W. I. D. Mining, "Data mining: Concepts and techniques," *Morgan Kaufinann*, vol. 10, no. 559–569, p. 4, 2006.

[23] M. Munir, I. Ardiansyah, J. D. Santoso, A. Mustopa, and S. Mulyatun, "Detection and Mitigation of Distributed Denial of Service Attack On Network Architecture Software Defined Networking Using The Naive Bayes Algorithm," *Journal of Information System Management (JOISM)*, vol. 3, no. 2, pp. 51–55, Jan. 2022, doi: 10.24076/joism.2022v3i2.656.

[24] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Inf. Process. Manag.*, vol. 45, no. 4, pp. 427–437, Jul. 2009, doi: 10.1016/j.ipm.2009.03.002.

[25] R. Nurhidayat and K. E. Dewi, "Penerapan Algoritma K-Nearest Neighbor dan Fitur Ekstraksi N-Gram Dalam Analisis Sentimen Berbasis Aspek," *Komputa : Jurnal Ilmiah Komputer dan Informatika*, vol. 12, no. 1, pp. 91–100, May 2023, doi: 10.34010/komputa.v12i1.9458.