Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

OPTIMASI GRID SEARCH PADA SISTEM DETEKSI INTRUSI JARINGAN MENGGUNAKAN SUPPORT VECTOR MACHINE

Radhiyatammardhiyyah [1], Muhammad Andi Aziz [2], Azhar [3]
1,2,3) Teknik Informatika, Teknologi Informasi dan Komputer, Politeknik Negeri Lhokseumawe, Indonesia

Article Info

Article history:

Received: 15 Juli 2026
Revised: 03 Agustus 2026
Accepted: 05 Agustus 2026

ABSTRACT

Abstrak

Ancaman serangan digital yang terus meningkat mendorong kebutuhan akan sistem deteksi intrusi jaringan yang akurat dan efisien. Sistem ini berperan dalam memantau lalu lintas jaringan serta mengidentifikasi aktivitas mencurigakan sebelum berdampak pada infrastruktur. Penelitian ini bertujuan untuk mengevaluasi kinerja metode Support Vector Machine dalam mengklasifikasikan lalu lintas jaringan ke dalam tiga kategori, yaitu Normal, Exploits, dan Generic, menggunakan dataset UNSW-NB15. Tahapan penelitian meliputi preprocessing data, encoding fitur kategorikal, standardisasi fitur numerik, serta pembagian data latih dan data uji. Untuk mengatasi ketidakseimbangan data, dilakukan proses sampling pada setiap kelas. Model dilatih menggunakan kernel Radial Basis Function dengan parameter terbaik yang diperoleh melalui proses optimasi. Evaluasi dilakukan menggunakan metrik akurasi, precision, recall, dan F1-score. Hasil pengujian menunjukkan bahwa model mampu mencapai akurasi sebesar 95% dengan performa klasifikasi yang baik pada seluruh kategori. Berdasarkan hasil tersebut, metode Support Vector Machine efektif digunakan untuk mendukung sistem deteksi intrusi jaringan dalam mengidentifikasi berbagai jenis serangan secara akurat.

Kata Kunci: Deteksi Intrusi, Support Vector Machine, UNSW-NB15, Klasifikasi Trafik Jaringan, Keamanan Jaringan

Abstract

The increasing threat of cyberattacks has highlighted the need for accurate and efficient network intrusion detection systems. These systems play a crucial role in monitoring network traffic, detecting anomalies, and identifying potential attacks before they impact infrastructure. This study aims to evaluate the performance of the Support Vector Machine method in classifying network traffic into three main categories: Normal, Exploits, and Generic, using the UNSW-NB15 dataset. The research process includes data preprocessing, categorical feature encoding, numerical feature standardization, and data splitting into training and testing sets. To address data imbalance, a sampling technique is applied to each class. The model is trained using a Radial Basis Function kernel with optimized parameters. Performance evaluation is conducted using accuracy, precision, recall, and F1-score metrics. The results show that the model achieves an accuracy of 95% with strong classification performance across all categories. These findings indicate that the Support Vector Machine method is effective for supporting intrusion detection systems in accurately identifying various types of network attacks.

Keywords: Intrusion Detection System, Support Vector Machine, UNSW-NB15, Network Traffic Classification, Network Security

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Corresponding Author:
E-mail : radhiyah.td@pnl.ac.id

1. PENDAHULUAN

Ancaman serangan siber semakin meningkat dan menjadi isu serius bagi organisasi maupun individu. Serangan ini mencakup berbagai bentuk, seperti hacking, phishing, malware, denial-of-service (DoS), hingga backdoors yang bertujuan merusak, mengubah, atau mencuri data penting [1]. Kegagalan dalam menjaga keamanan sistem dapat mengganggu infrastruktur digital dan menimbulkan kerugian besar. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2022 mencatat lebih dari 973 juta anomali lalu lintas jaringan di Indonesia, yang menunjukkan eskalasi signifikan dari ancaman serangan siber [2]. Kondisi ini menegaskan pentingnya pengembangan sistem deteksi serangan yang lebih cerdas dan efektif.

Salah satu solusi yang banyak digunakan adalah Intrusion Detection System (IDS). IDS berfungsi untuk memantau lalu lintas jaringan dan mengidentifikasi aktivitas mencurigakan atau berbahaya [3]. Seiring perkembangan teknologi, IDS semakin sering dikombinasikan dengan metode machine learning untuk meningkatkan keakuratannya [4]. Berbagai algoritma telah diuji dalam penelitian IDS, mulai dari Support Vector Machine (SVM), Random Forest, Neural Network, hingga Multi-Layer Perceptron (MLP). Yin dkk. (2022) melaporkan akurasi 84,24% menggunakan MLP dengan seleksi fitur hibrid [5]. Putro (2024) menguji SVM dengan kernel polynomial dan mencatat akurasi 89,43% [6], sementara Putra (2024) menunjukkan bahwa Neural Network mampu mencapai akurasi 92% [7]. Temuan-temuan tersebut menunjukkan bahwa meskipun IDS berbasis machine learning telah menunjukkan hasil yang baik, sebagian besar model masih menghasilkan akurasi di bawah 95%, sehingga diperlukan upaya optimasi lebih lanjut.

SVM merupakan algoritma supervised learning yang bekerja dengan mencari hyperplane optimal untuk memisahkan data antar kelas [8]. Algoritma ini memiliki sejumlah keunggulan, seperti kemampuan menangani data berdimensi tinggi dan tidak

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

linear [9], menghasilkan margin klasifikasi maksimum yang stabil [10], serta lebih tahan terhadap overfitting melalui pengaturan parameter seperti C dan gamma [11]. Meskipun secara alami dirancang untuk klasifikasi dua kelas, SVM dapat diterapkan dalam kasus multiclass menggunakan pendekatan One-vs-Rest (OvR), di mana setiap model biner dilatih untuk membedakan satu kelas dengan seluruh kelas lainnya [12].

Penelitian ini menggunakan dataset UNSW-NB15 yang dikembangkan oleh Australian Centre for Cyber Security (ACCS) pada tahun 2015. Dataset ini berisi lebih dari 2 juta network flow berlabel dengan 49 fitur yang mencakup informasi protokol, statistik, serta perilaku koneksi [13]. UNSW-NB15 dianggap relevan untuk penelitian IDS modern karena mencakup berbagai serangan terkini, termasuk Exploits dan Generic. Pada penelitian ini, SVM dikembangkan untuk mendeteksi tiga kategori utama lalu lintas jaringan, yaitu Normal, Exploits, dan Generic.

Kebaruan penelitian ini terletak pada penerapan pendekatan multi-classification berbasis SVM dengan optimasi parameter pada dataset UNSW-NB15. Dengan membatasi fokus pada tiga kategori serangan yang paling sering muncul, penelitian ini bertujuan menghasilkan model IDS yang lebih akurat dan konsisten. Selain itu, penelitian ini juga mengintegrasikan model ke dalam sistem berbasis web sehingga dapat dimanfaatkan oleh administrator jaringan untuk mendeteksi serangan secara lebih efisien dan praktis.

2. METODE PENELITIAN

2.1 Dataset

Data yang digunakan dalam penelitian ini terdiri dari data sekunder, yaitu dataset UNSW-NB15 yang diambil dari Australian Centre for Cyber Security. UNSW-NB15 merupakan dataset acuan yang biasa dipakai untuk membuat dan menilai sistem deteksi intrusi jaringan. Dataset ini mencakup sembilan jenis serangan, yaitu DoS, Worms, Backdoors, Exploits, Fuzzers, Generic, Shellcode, Analysis, dan Reconnaissance, namun dalam penelitian ini hanya tiga kategori yang digunakan, yaitu Normal, Exploits, dan Generic. Jumlah total aktivitas pada dataset UNSW-NB15 mencapai 2. 540. 044 entri, yang terdiri dari 175. 341 entri untuk data pelatihan dan 82. 332 entri untuk data pengujian. Dataset ini telah disusun dalam format tabel hasil dari ekstraksi paket jaringan mentah yang siap digunakan dalam proses klasifikasi.

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

2.2 Preprocessing Data

Preprocessing data bertujuan untuk membersihkan dan menyiapkan dataset agar sesuai digunakan oleh algoritma klasifikasi. Pertama, dilakukan penghapusan kolom yang tidak relevan (misalnya kolom yang tidak dapat diperoleh secara real-time, kolom dengan data sangat jarang, atau kolom redundan), agar fitur yang tersisa konsisten dengan kondisi implementasi — hal ini sejalan dengan pentingnya feature selection dalam mengurangi noise dan dimensi data [14].

Selanjutnya, label kelas difokuskan hanya pada kategori Normal, Generic, dan Exploits karena distribusi data pada kelas tersebut paling dominan, sehingga menghasilkan 129.393 catatan dengan sebaran kelas relatif seimbang. Penyaringan kelas ini penting untuk mengatasi masalah ketidakseimbangan data, yang diketahui dapat menurunkan performa model [15].

Fitur kategorikal seperti proto dan state kemudian diubah ke bentuk numerik menggunakan Label Encoding, dengan penambahan label unknown untuk menangani kategori baru saat inferensi real-time. Transformasi ini diperlukan karena algoritma pembelajaran mesin memerlukan representasi numerik [16].

Untuk fitur numerik, dilakukan standarisasi menggunakan StandardScaler agar setiap fitur memiliki rata-rata 0 dan standar deviasi 1. Normalisasi semacam ini sangat penting karena perbedaan skala antar-fitur dapat memengaruhi hasil klasifikasi, dan penelitian menunjukkan pemilihan teknik scaling berpengaruh signifikan terhadap performa [17]

Terakhir, dataset dibagi menjadi 80% untuk pelatihan dan 20% untuk pengujian menggunakan Stratified Split, sehingga proporsi setiap kelas tetap terjaga dalam kedua subset. Teknik stratifikasi ini direkomendasikan untuk mencegah bias distribusi data antar subset [18].

2.3 Support Vetor Machine

Support Vector Machine (SVM) adalah algoritma pembelajaran mesin yang digunakan untuk tugas klasifikasi maupun regresi. Metode ini diperkenalkan oleh Boser, Guyon, dan Vapnik pada tahun 1992 dan dikenal efektif dalam memisahkan data ke dalam kelas yang berbeda melalui pencarian hyperplane dengan margin terbesar [19]. Prinsip utama SVM adalah menentukan bidang pemisah (hyperplane) optimal yang dapat

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

memaksimalkan jarak antar kelas dalam ruang fitur [20]. Secara matematis, batas luar kelas +1 dapat ditentukan dengan:

$$(w \cdot xi)+b \geq 1 \quad (1)$$

Sedangkan persamaan hyperplane dituliskan sebagai:

$$(w \cdot xi)+b=0 \quad (2)$$

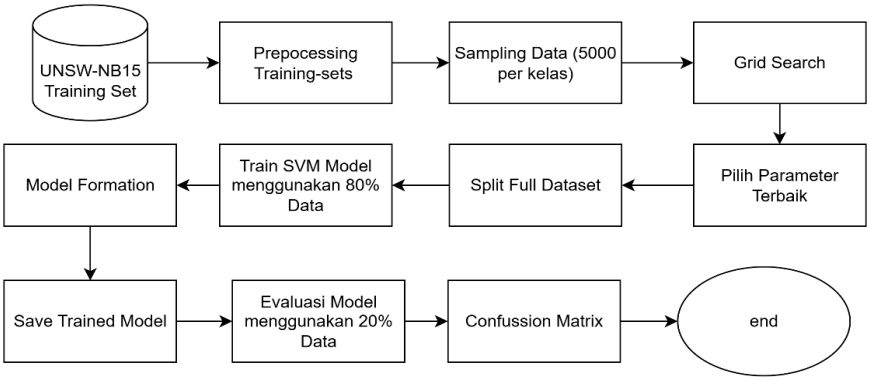
w : Bobot dari sebuah atribut

Xi : Atribut ke-i

b : Bias

Pada penelitian ini, SVM digunakan untuk mengklasifikasikan lalu lintas jaringan ke dalam tiga kategori, yaitu Normal, Generic, dan Exploits. Proses pembentukan model meliputi beberapa tahapan, dimulai dari Preprocessing data, sampling data untuk setiap kelas, pencarian parameter terbaik melalui Grid Search, hingga evaluasi menggunakan confusion matrix.

Alur pelatihan dan evaluasi model SVM ditunjukkan pada Gambar 1. Dataset UNSW-NB15 yang telah melalui tahap Preprocessing kemudian diproses melalui sampling agar distribusi kelas lebih seimbang. Selanjutnya dilakukan pemilihan parameter terbaik menggunakan Grid Search sebelum model dibentuk. Setelah model terbentuk, dataset dibagi menjadi data pelatihan (80%) dan data pengujian (20%). Hasil evaluasi dari confusion matrix digunakan untuk mengukur performa model, dan model yang terbaik disimpan untuk kebutuhan implementasi pada sistem deteksi intrusi jaringan.



Gambar 1 Topologi Jaringan

2.4 Evaluasi Model

Evaluasi model digunakan untuk mengukur performa algoritma *Support Vector Machine* (SVM) dalam mengklasifikasikan data. Metode yang dipakai adalah *Confusion matrix*, yang menyajikan distribusi prediksi benar dan salah pada setiap kelas. Dari

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

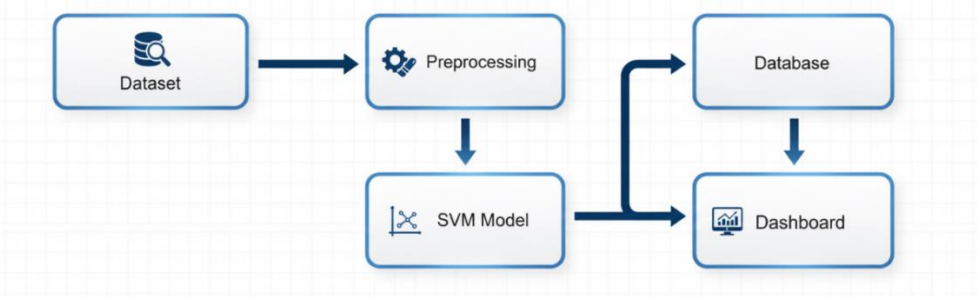
Confusion matrix dapat dihitung beberapa metrik penting:

a. *Accuracy*, persentase prediksi benar dibandingkan dengan seluruh data uji.
b. *Precision*, tingkat ketepatan prediksi positif, proporsi prediksi positif yang benar-benar positif.
c. *Recall*, tingkat keberhasilan model dalam menemukan seluruh instance positif yang terdapat di data.
d. *F1-score*, rata-rata harmonis antara *Precision* dan *Recall*, memberikan penilaian seimbang ketika distribusi kelas tidak merata.

Penggunaan *Confusion matrix* beserta metrik turunannya merupakan pendekatan standar dalam penelitian sistem deteksi intrusi jaringan (IDS), karena mampu memberikan gambaran detail mengenai performa model pada setiap kelas serangan [21][22].

2.5 Arsitektur Sistem

Arsitektur sistem penelitian ini dirancang untuk mengintegrasikan model klasifikasi SVM dengan sistem monitoring berbasis web. Alur arsitektur ditunjukkan pada Gambar 2



Gambar 2 *Arsitektur Sistem*

Arsitektur dimulai dari dataset sebagai sumber data utama. Dataset kemudian melalui tahap Preprocessing, meliputi pembersihan, encoding, dan standardisasi fitur sebelum dipakai dalam proses pelatihan maupun pengujian. Data hasil Preprocessing selanjutnya digunakan untuk membentuk model SVM, yang berfungsi sebagai inti dari sistem deteksi intrusi.

Hasil prediksi model disimpan ke dalam Database untuk pencatatan dan analisis lebih lanjut. Database kemudian terhubung ke *dashboard*, yang memungkinkan administrator jaringan memantau aktivitas serta mendeteksi serangan secara real-time. Dengan rancangan ini, sistem IDS tidak hanya melakukan klasifikasi serangan, tetapi juga menyajikan informasi yang mudah diakses melalui antarmuka web [23].

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

2.6 Teknik Pengujian

Pada skenario pertama, seluruh client menjalankan speedtest bersamaan untuk mengetahui kapasitas bandwidth dasar (4 Mbps) sebelum dan sesudah penerapan RED. Skenario kedua, semua client mengunduh file ISO besar (Kali Linux dan Debian netinst) secara serentak guna memaksimalkan trafik masuk dan menilai kinerja jaringan pada beban tinggi berdasarkan *throughput, delay, jitter*, dan *packet loss*. Skenario ketiga menguji aktivitas upload file ke Google Drive untuk menilai efektivitas RED dalam mengelola antrian data keluar. Pada skenario keempat, tiap client melakukan aktivitas berbeda: browsing, download ISO, dan streaming YouTube (480p–720p). Kondisi ini merepresentasikan campuran trafik ringan, sedang, dan berat, termasuk trafik sensitif terhadap delay.

Skenario kelima melibatkan seluruh client menonton YouTube pada kualitas standar untuk menguji kestabilan RED dalam menangani trafik multimedia. Sedangkan skenario keenam menguji streaming YouTube beresolusi 4K secara bersamaan, menghasilkan trafik konstan dengan kebutuhan bandwidth tinggi. Fokus utamanya adalah *delay* dan *jitter* untuk mengevaluasi stabilitas QoS pada kondisi padat. Hasil dari keenam skenario dibandingkan dengan standar QoS untuk memperoleh gambaran menyeluruh mengenai efektivitas RED dalam mengelola lalu lintas data pada berbagai kondisi jaringan.

3 HASIL DAN PEMBAHASAN

3.1 Hasil *Preprocessing* Data

Tahap *Preprocessing* dilakukan pada dataset UNSW-NB15 yang awalnya berjumlah 175.341 records dengan 49 fitur, diperoleh 129.393 records dan 27 fitur setelah proses *feature selection* dan penyaringan kelas. Data hanya difokuskan pada tiga kelas utama, yaitu Normal, Generic, dan Exploits.

Fitur kategorikal telah ditransformasikan menjadi numerik menggunakan Label Encoding, sedangkan fitur numerik diNormalisasi dengan StandardScaler. Dataset kemudian dibagi menjadi 80% data latih (103.514 catatan) dan 20% data uji (25.879 catatan) dengan *Stratified Split* untuk menjaga proporsi distribusi kelas. Ringkasan hasil Preprocessing dapat dilihat pada Tabel 1.

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Tabel 1 Hasil *Preprocessing* Dataset

Tahap	Jumlah Data	Jumlah Fitur	Keterangan
Dataset awal	175.341	49	UNSW-NB15 train-set
Setelah *feature selection*	175.341	27	Hapus kolom tidak relevan
Setelah filter kelas	129.393	27	*Normal*, *Generic*, *Exploits*
Split train/test	103.514 / 25.879	26 + label	*Stratified* 80:20

3.2 Penentuan Paarameter Terbaik

Setelah Preprocessing, tahap berikutnya adalah optimasi parameter *Support Vector Machine* (SVM) menggunakan metode *Grid Search* dengan validasi silang 5-fold. Proses ini dilakukan dengan mengevaluasi kombinasi nilai C = [1, 10, 100], gamma = [0.1, 1, 10], dan kernel RBF, yang dipilih karena efektif dalam menangani data non-linear pada permasalahan deteksi intrusi [24].

Untuk mengurangi beban komputasi, tuning parameter dilakukan pada subset data sebanyak 5.000 sampel per kelas (total 15.000). Hasil *Grid Search* menunjukkan kombinasi terbaik pada C = 100, gamma = 0.1, dan kernel = RBF, dengan akurasi validasi silang sebesar 94,29%.

Kombinasi ini kemudian digunakan dalam pelatihan akhir dengan seluruh data latih, karena memberikan performa paling optimal sekaligus menjaga kemampuan generalisasi model terhadap data baru.

3.3 Evaluasi Model SVM

Model *Support Vector Machine* (SVM) dilatih menggunakan parameter terbaik hasil Grid Search, yaitu C = 100 dan γ = 0.1 dengan kernel RBF, yang dikenal efektif dalam menangani data non-linear [25]. Proses pelatihan dilakukan dengan pendekatan One-vs-Rest (OvR) untuk menyelesaikan klasifikasi multi-kelas (Normal, Generic, Exploits. Kemudian evaluasi dilakukan menggunakan classification report dan confusion matrix. Hasil classification report dapat dilihat pada Gambar 3.

Classification report dengan model terbaik:

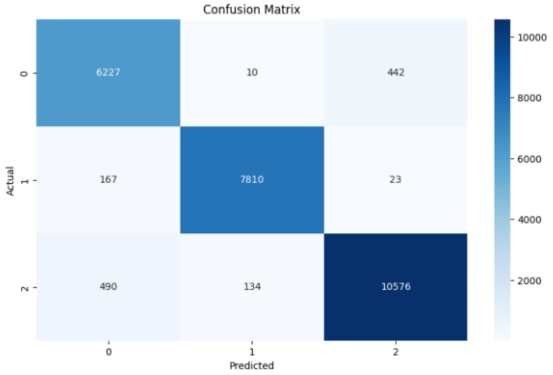
	precision	recall	f1-score	support
Exploits	0.90	0.93	0.92	6679
Generic	0.98	0.98	0.98	8000
Normal	0.96	0.94	0.95	11200
accuracy			0.95	25879
macro avg	0.95	0.95	0.95	25879
weighted avg	0.95	0.95	0.95	25879

Gambar 3 Classification report Model SVM

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Model berhasil mencapai akurasi 95%, dengan performa yang stabil pada semua kelas. Pada kelas Exploits, nilai Precision tercatat 0.90 dan Recall 0.93; pada kelas Generic, Precision dan Recall sama-sama 0.98; sedangkan pada kelas Normal, Precision 0.96 dan Recall 0.94. Rata-rata makro dan tertimbang untuk Precision, Recall, serta F1-score semuanya berada pada nilai 0.95.

Confusion matrix yang ditampilkan pada Gambar 4 memperlihatkan distribusi prediksi model terhadap data uji. Model mampu mengklasifikasikan sebagian besar data dengan benar, dengan jumlah kesalahan prediksi relatif kecil.



Gambar 4 Confusion matrix Model SVM

Secara keseluruhan, hasil ini menunjukkan bahwa model SVM dengan kernel RBF dan parameter optimal mampu memberikan performa yang baik dalam mendeteksi serangan jaringan, sekaligus menjaga keseimbangan akurasi pada ketiga kelas yang diuji.

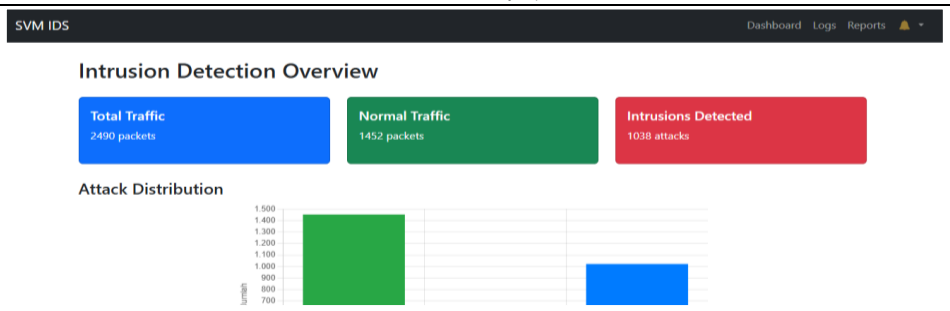
3.4 Implementasi Sistem

Sistem *Network Intrusion Detection System* (NIDS) berbasis *Support Vector Machine* (SVM) ini diimplementasikan dalam bentuk aplikasi web menggunakan framework Flask. Antarmuka sistem terdiri atas tiga halaman utama, yaitu Dashboard, Logs, dan Reports.

a. Tampilan Dashboard

Halaman utama sistem dapat dilihat pada Gambar 5. Dashboard menampilkan ringkasan data berupa Total Traffic, Normal Traffic, dan Intrusions Detected. Selain itu, terdapat grafik Attack Distribution yang memperlihatkan jumlah kategori serangan yang telah terdeteksi oleh sistem, seperti Normal, Generic, dan Exploits. Fitur ini membantu administrator memahami pola serangan secara visual.

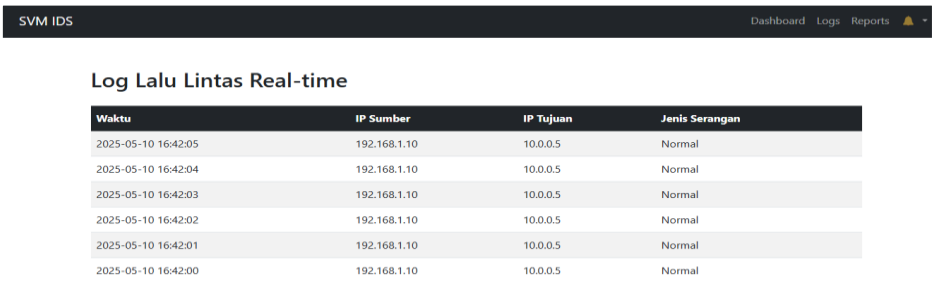
Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno



Gambar 5 Tampilan Dashboard

b. Tampilan Logs

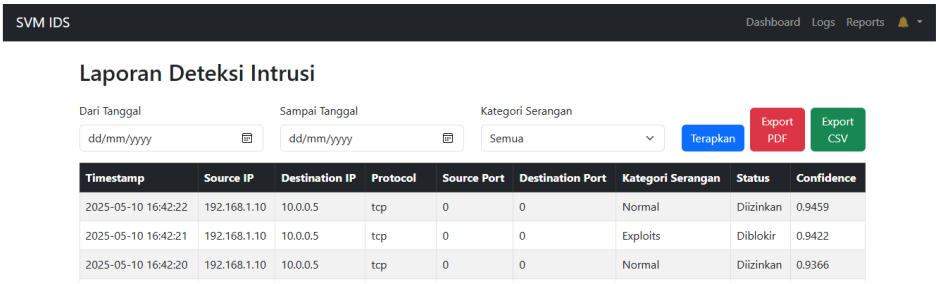
Halaman Logs pada Gambar 6. menampilkan hasil klasifikasi lalu lintas jaringan secara real-time. Informasi yang disajikan meliputi timestamp, IP sumber, IP tujuan, serta jenis serangan hasil klasifikasi model SVM. Dengan adanya log ini, administrator dapat memantau aktivitas jaringan dan mendeteksi serangan secara cepat.



Gambar 6 Tampilan Logs

c. Tampilan Reports

Halaman Reports (Gambar 7) menyajikan data historis deteksi intrusi dalam format tabel yang lebih rinci. Informasi yang ditampilkan meliputi timestamp, IP sumber dan tujuan, protokol, port, kategori serangan, status aksi sistem (diizinkan/diblokir), serta confidence score. Fitur filter berdasarkan tanggal dan kategori serangan disediakan, serta ekspor laporan ke dalam PDF dan CSV untuk kebutuhan dokumentasi.



Gambar 7 Tampilan Reports

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Secara keseluruhan, sistem yang dibangun mampu melakukan deteksi intrusi secara real-time, menyimpan data log, menampilkan notifikasi, menyajikan visualisasi serangan, serta menyediakan laporan yang dapat digunakan administrator untuk analisis keamanan jaringan.

4 SIMPULAN

Berdasarkan hasil penelitian, metode Support Vector Machine (SVM) dengan pendekatan multi-kelas One-vs-Rest (OvR) terbukti efektif dalam mengklasifikasikan lalu lintas jaringan menjadi Normal, Exploits, dan Generic pada dataset UNSW-NB15. Model terbaik dengan kernel RBF dan parameter C = 100, gamma = 0,1 mampu mencapai akurasi 95%, dengan Precision, Recall, dan F1-score yang seimbang pada ketiga kelas. Pada kelas Exploits, Precision sebesar 0,90 dan Recall 0,93 menunjukkan bahwa model cukup baik mendeteksi serangan, meskipun masih ada sebagian kecil alarm palsu dan serangan yang terlewat. Kelas Generic mencatat performa hampir sempurna dengan Precision dan Recall sama-sama 0,98, yang menandakan bahwa model sangat konsisten dalam mengenali serangan ini. Sedangkan pada kelas Normal, Precision 0,96 dan Recall 0,94 memperlihatkan kemampuan model dalam membedakan trafik Normal dari trafik berbahaya dengan tingkat kesalahan yang sangat kecil. Selain itu, nilai macro average dan weighted average yang keduanya mencapai 0,95 membuktikan bahwa performa model merata di semua kelas tanpa bias signifikan. Hal ini menguatkan kesimpulan bahwa algoritma SVM dengan kernel RBF tidak hanya akurat, tetapi juga konsisten dan seimbang, sehingga layak digunakan sebagai dasar dalam membangun Intrusion Detection System (IDS) untuk meningkatkan keamanan jaringan terhadap ancaman siber.

REFERENCES

[1]. M. Al Amin, "Artificial Intelligence and Machine Learning Algorithms Are Used to Detect and Prevent Cyber Threats as Well as Their Potential Impact on the Future of Cybersecurity Practices," International Journal of Computer Science & Information Technology, vol. 17, no. 1, pp. 1–16, Feb. 2025, doi: 10.5121/ijcsit.2025.17101.

[2]. Id-SIRTII/CC, “Laporan Hasil Monitoring Keamanan Siber Nasional – Laporan Bulanan Desember 2022.” [Online]. Available: https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html. Accessed: Nov. 18, 2024.

[3]. E. T. Fatima and Jurgen, "AI-Driven Intrusion Detection: Applying NLP to Unstructured Network Traffic Data," ResearchGate, 2025. [Online]. Available:https://www.researchgate.net/publication/389694974_AIDriven_Intrusion_Detection_Applying_NLP_to_Unstructured_Network_Traffic_Data. Accessed: Nov. 18, 2024.

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

[4]. E. Oluwagbade, "Enhancing Resource Allocation in Biopharmaceutical Multi-Project Management Using AI," ResearchGate, 2025. [Online]. Available:https://www.researchgate.net/publication/389518623_Enhancing_Resource_Allocation_in_Biopharmaceutical_Multi-Project_Management_Using_AI.

[5]. Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, and J. Kwak, "IGRF-RFE: A Hybrid Feature Selection Method for MLP-Based Network Intrusion Detection on UNSW-NB15 Dataset," Journal of Big Data, vol. 10, no. 1, Art. no. 15, 2023, doi: 10.1186/s40537-023-00694-8.

[6]. I. H. Putro, "Performance Comparison of SVM Kernels for Intrusion Detection System Using UNSW-NB15 Dataset," Jurnal Teknik Elektro, vol. 17, no. 2, pp. 55–61, Sep. 2024, doi: 10.9744/jte.17.2.55-61.

[7]. Z. P. Putra, "Evaluating the Performance of Classification Algorithms on the UNSW-NB15 Dataset for Network Intrusion Detection," Jurnal Ilmiah FIFO, vol. 16, no. 1, pp. 84–95, Jun. 2024, doi: 10.22441/fifo.2024.v16i1.009.

[8]. P. Zhao, X. Wang, Q. Zhao, Q. Xu, Y. Sun, and X. Ning, "Non-Destructive Detection of External Defects in Potatoes Using Hyperspectral Imaging and Machine Learning," MDPI, vol. 15, no. 6, p. 573, 2025, doi: https://doi.org/10.3390/agriculture15060573.

[9]. Z. Mokadem, M. Djerioui, B. Attallah, and Y. Brik, "A Comparison of Machine Learning Algorithms for Predicting Alzheimer's Disease Using Neuropsychological Data," Science, Engineering and Technology, vol. 5, no. 1, pp. 177–191, Apr. 2025, doi: 10.54327/set2025/v5.i1.182.

[10]. Amna, Wahyuddin S., I G. I. Sudipa, T. A. E. Putra, A. J. Wahidin, W. A. Syukrilla, A. K. Wardhani, N. Heryana, T. Indriyani, and L. W. Santoso, Data Mining. Padang, Indonesia: PT Global Eksekutif Teknologi, 2023.

[11]. A. D. Goldie, J. Cohen, S. Whiteson, and J. N. Foerster, "Do Symbolic or Black-Box Representations Generalise Better in Learned Optimisation?," in Proc. Int. Conf. Learn. Represent. (ICLR), 2025, pp. 1–24.

[12]. S. N. and K. M., "An Improved Multiclass Classification of Acute Lymphocytic Leukemia Using Enhanced Glowworm Swarm Optimization," Scientific Reports, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-98823-1.

[13]. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," in Proc. 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

[14]. G. Chandrashekar and F. Sahin, "A Survey on Feature Selection Methods," Computers & Electrical Engineering, vol. 40, no. 1, pp. 16–28, Jan. 2014, doi: 10.1016/j.compeleceng.2013.11.024.

[15]. E. Jafarigol and T. B. Trafalis, "A Review of Machine Learning Techniques in Imbalanced Data and Future Trends," arXiv:2310.07917, 2023, doi: 10.48550/arXiv.2310.07917.

[16]. M. Kuhn and K. Johnson, Applied Predictive Modeling. New York, NY, USA: Springer, 2013, doi: 10.1007/978-1-4614-6849-3.

[17]. A. K. Jain, R. P. W. Duin, and J. Mao, "Statistical Pattern Recognition: A Review," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 4–37, Jan. 2000, doi: 10.1109/34.824819.

[18]. R. Kohavi, "A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection," in Proc. 14th Int. Joint Conf. Artif. Intell. (IJCAI), Montreal, QC, Canada, vol. 2, Aug. 1995, pp. 1137–1143.

[19]. M. Sun, "Support Vector Machine Models for Classification," in Encyclopedia of Business Analytics and Optimization, J. Wang, Ed. Hershey, PA, USA: IGI Global, 2014, pp. 2395–2409, doi: 10.4018/978-1-4666-5202-6.ch215.

[20]. U. Ahmed et al., "Signature-based Intrusion Detection Using Machine Learning and Deep Learning Approaches Empowered with Fuzzy Clustering," Scientific Reports, vol. 15, no. 1, Art. no. 1726, 2025, doi: 10.1038/s41598-025-85866-7.

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 2, Agustus 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

[21]. S. Kumar and D. N. K. Pathak, "Evaluation of Machine Learning Algorithms for Intrusion Detection Utilizing UNSW-NB15 Dataset," Journal of Pharmaceutical Negative Results, vol. 13, no. S08, pp. 4819–4832, 2022, doi: 10.47750/pnr.2022.13.S08.630.

[22]. I. Sumaiya Thaseen and C. Aswani Kumar, "Intrusion Detection Model Using Fusion of Chi-Square Feature Selection and Multi-Class SVM," Journal of King Saud University – Computer and Information Sciences, vol. 29, no. 4, pp. 462–472, 2017, doi: 10.1016/j.jksuci.2015.12.004.

[23]. A. Shivani, R. Sreelakshmi, A. Bhavani, J. Ramdas, and A. Jithender, "Detection and Mitigation of Web Attacks with End-To-End Deep Learning," Journal of Computational and Allied Intelligence, vol. 3, no. 3, pp. 56–80, 2025, doi: 10.69996/jcai.2025017.

[24]. A. A. Alsadhan, N. Al Roken, S. Ansari, B. Khan, S. H. Abdulhussain, and A. J. Hussain, "Kernel-Based Machine Learning Intrusion Detection Systems for ICMPv6 DDoS Detection," Results in Engineering, vol. 28, Art. no. 106940, 2025, doi: 10.1016/j.rineng.2025.106940.

[25]. M. A. Hamzah and S. H. Othman, "Performance Evaluation of Support Vector Machine Kernels in Intrusion Detection System for Wireless Sensor Network," International Journal of Innovative Computing, vol. 12, no. 1, pp. 9–15, 2021, doi: 10.11113/ijic.v12n1.334.