Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

Implementasi One-Class Support Vector Machine untuk Deteksi Serangan Jaringan Kampus

Asep Sapaatullah[1], Rahmat[2], Mochammad Darip[3,*]

[1] Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Bina Bangsa, Kota Serang - Banten, Indonesia
[2] Fakultas Informatika, Program Studi Manajemen Informatika, Akademi Manajemen Informatika Dan Komputer, Kota Serang - Banten, Indonesia
[3] Fakultas Ilmu Komputer, Program Studi Ilmu Komputer, Universitas Bina Bangsa, Kota Serang - Banten, Indonesia
Email: [1]asepsapaatullah.binabangsa@gmail.com, [2]rahmat042@gmail.com,
(* : darif.uniba@gmail.com)

Abstrak- Keamanan jaringan pada lingkungan kampus menghadapi tantangan yang semakin kompleks seiring meningkatnya penggunaan internet, sistem akademik digital, serta banyaknya perangkat yang terhubung ke jaringan. Permasalahan utama yang sering terjadi adalah keterbatasan sistem keamanan konvensional dalam mendeteksi serangan jaringan baru atau serangan yang bersifat anomali. Sistem tradisional umumnya hanya mampu mengenali serangan berdasarkan pola yang telah diketahui, sehingga kurang efektif terhadap serangan yang belum terdefinisi. Oleh karena itu, penelitian ini menawarkan solusi berupa penerapan metode Support Vector Machine (SVM) untuk mendeteksi serangan jaringan secara otomatis. Metode penelitian meliputi pengumpulan data trafik jaringan kampus, tahap pra-pemrosesan data berupa data cleaning, normalisasi, dan seleksi fitur, pelatihan model SVM, serta evaluasi performa menggunakan confusion matrix dan ROC curve. Hasil penelitian menunjukkan bahwa model SVM mampu mengklasifikasikan trafik normal dan trafik serangan dengan tingkat akurasi yang sangat baik, adapun tingkat akurasinya sebesar 100%, precision 100%, recall 100%, serta nilai AUC-nya sebesar 1.000. Model yang dibangun berhasil mengklasifikasikan 22 flow data yang terdiri dari 15 trafik normal dan 7 trafik serangan tanpa kesalahan klasifikasi. Dengan demikian, penerapan SVM terbukti efektif sebagai metode deteksi intrusi dalam meningkatkan keamanan jaringan kampus secara adaptif dan efisien.

Kata Kunci: Keamanan Jaringan; Deteksi Intrusi; Support Vector Machine; Machine Learning.

Abstract- Network security in campus environments faces increasingly complex challenges with the increasing use of the internet, digital academic systems, and the large number of devices connected to the network. The main problem that often occurs is the limitations of conventional security systems in detecting new network attacks or anomalous attacks. Traditional systems are generally only able to recognize attacks based on known patterns, making them less effective against undefined attacks. Therefore, this study offers a solution in the form of implementing the Support Vector Machine (SVM) method to detect network attacks automatically. The research method includes collecting campus network traffic data, data pre-processing stages such as data cleaning, normalization, and feature selection, training the SVM model, and evaluating its performance using a confusion matrix and ROC curve. The results show that the SVM model is able to classify normal traffic and attack traffic with a very good level of accuracy, with an accuracy level of 100%, precision of 100%, recall of 100%, and an AUC value of 1,000. The model successfully classified 22 data flows consisting of 15 normal traffic and 7 attack traffic without any classification errors. Thus, the application of SVM is proven to be effective as an intrusion detection method in improving campus network security adaptively and efficiently.

Keywords: Network Security, Intrusion Detection, Support Vector Machine, Machine Learning

1. PENDAHULUAN

Perkembangan teknologi informasi telah meningkatkan ketergantungan perguruan tinggi terhadap jaringan komputer dalam mendukung kegiatan akademik, administrasi, dan layanan digital. Jaringan kampus menjadi infrastruktur utama yang harus dijaga keamanannya karena berperan dalam penyimpanan dan pertukaran data penting. Tingginya aktivitas jaringan juga meningkatkan risiko terjadinya gangguan keamanan yang dapat mempengaruhi stabilitas sistem secara keseluruhan [1], [2]. Berdasarkan laporan keamanan siber global tahun 2024, terjadi peningkatan serangan *Distributed Denial of Service* (DDoS) sebesar lebih dari 30% dibandingkan tahun sebelumnya. Lingkungan perguruan tinggi menjadi salah satu target utama karena sifat jaringan yang terbuka dan heterogeny [3]. Secara khusus, jaringan kampus memiliki karakteristik terbuka dengan jumlah pengguna dan perangkat yang beragam. Kondisi ini menjadikan jaringan kampus rentan terhadap berbagai serangan siber seperti *malware, port scanning*, dan *denial of service*. Sistem keamanan konvensional umumnya masih bergantung pada *signature-based detection* sehingga kurang efektif dalam mendeteksi serangan baru atau serangan anomali yang belum memiliki pola tetap [4], [5].

Sebagai solusi, pendekatan berbasis *machine learning* dapat digunakan untuk meningkatkan kemampuan deteksi serangan jaringan. *Support Vector Machine* (SVM) merupakan salah satu algoritma yang banyak digunakan dalam sistem deteksi intrusi karena kemampuannya menangani data berdimensi tinggi dan menghasilkan model klasifikasi yang optimal. SVM mampu mengenali pola trafik jaringan normal dan mendeteksi penyimpangan yang mengindikasikan adanya serangan [6], [7] .

Penelitian ini bertujuan untuk menerapkan metode *Support Vector Machine* dalam mendeteksi serangan jaringan pada lingkungan kampus berdasarkan data trafik jaringan. Sistem yang dikembangkan diharapkan mampu mengklasifikasikan trafik jaringan secara otomatis sehingga dapat membantu administrator jaringan dalam meningkatkan keamanan dan respons terhadap ancaman [8], [9]. Manfaat penelitian ini adalah memberikan kontribusi dalam pengembangan sistem keamanan jaringan kampus yang lebih adaptif serta menjadi referensi akademik dalam penerapan machine learning pada

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

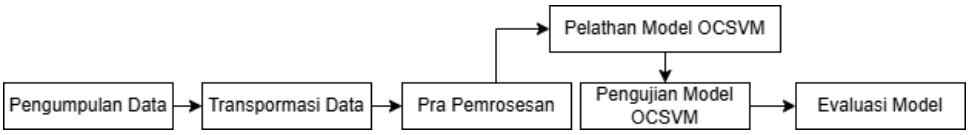
bidang deteksi intrusi. Selain itu, penelitian ini diharapkan dapat mendukung pengambilan keputusan dalam pengelolaan keamanan jaringan kampus [10].

Beberapa penelitian sebelumnya menunjukkan bahwa SVM memiliki performa yang baik dalam mendeteksi serangan jaringan dengan tingkat akurasi tinggi. Dan sebagian besar penelitian masih menggunakan dataset publik seperti NSL-KDD atau CICIDS dan belum banyak yang diterapkan langsung pada lingkungan jaringan kampus, seperti menguji performa model pada data trafik nyata [11], [12]. Hal ini menunjukkan bahwa evaluasi performa SVM pada data trafik nyata jaringan kampus masih belum banyak dilakukan. Oleh karena itu, penelitian ini memiliki perbedaan pada penggunaan data trafik jaringan kampus serta penerapan *One-Class* SVM yang sesuai untuk kondisi keterbatasan data serangan. Pengembangan selanjutnya dapat dilakukan dengan memperluas dataset, menerapkan sistem real-time, serta mengombinasikan SVM dengan metode lain untuk meningkatkan akurasi deteksi [13] , [14].

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode eksperimental dengan menerapkan algoritma *Support Vector Machine* untuk mendeteksi serangan jaringan berdasarkan data trafik jaringan kampus. Seluruh proses pengolahan data, pelatihan model, dan evaluasi dilakukan menggunakan bahasa pemrograman Python dengan bantuan *library machine learning* [15]. Data yang digunakan berupa data trafik jaringan kampus dalam format CSV yang mencakup informasi alamat IP sumber, alamat IP tujuan, protokol jaringan, ukuran paket, dan waktu pengiriman paket. Data ini digunakan untuk menganalisis pola trafik jaringan normal dan anomali [11], [16].

Tahap pra-pemrosesan data meliputi data cleaning untuk menghapus data kosong dan duplikat, normalisasi data menggunakan StandardScaler, serta seleksi fitur yang relevan seperti jumlah paket, rata-rata ukuran paket, dan total byte. Tahapan ini bertujuan untuk meningkatkan kualitas data dan performa model klasifikasi [6], [15]. Model yang digunakan adalah *One-Class Support Vector Machine* yang dilatih menggunakan data trafik normal. Model ini membentuk representasi pola normal jaringan dan mendeteksi penyimpangan sebagai serangan. Implementasi model dilakukan menggunakan *library scikit-learn* [7], [12]. Evaluasi performa model dilakukan menggunakan *confusion matrix* dan metrik evaluasi seperti *accuracy, precision, recall, F1-score*, serta *ROC Curve* dan *AUC* untuk menilai kemampuan model dalam mendeteksi serangan jaringan [9], [17]. Gambar 1 di bawah ini merupakan Langkah-langkah penelitian yang dilakukan.



Gambar 1. Diagram Alur Penelitian

2.1 Arsitektur dan Cara Kerja Sistem

Sistem deteksi serangan jaringan yang dikembangkan pada penelitian ini dirancang dalam suatu alur pemrosesan data yang terstruktur dan terintegrasi. Tahapan diawali dengan pengumpulan data trafik jaringan kampus yang disimpan dalam format CSV sebagai sumber data utama. Data tersebut kemudian dimuat ke dalam sistem melalui aplikasi berbasis Streamlit untuk dilakukan pemrosesan lebih lanjut. Pada tahap berikutnya, sistem secara otomatis melakukan pra-pemrosesan data yang mencakup pembersihan data (data cleaning), normalisasi menggunakan StandardScaler, serta seleksi fitur yang relevan untuk meningkatkan kualitas input model. Selanjutnya, model One-Class Support Vector Machine dilatih menggunakan data latih untuk membentuk representasi pola trafik normal jaringan. Model yang telah terbentuk kemudian digunakan untuk mengklasifikasikan data uji guna mengidentifikasi aktivitas yang menyimpang sebagai indikasi serangan. Hasil klasifikasi dan evaluasi performa model, termasuk metrik akurasi dan visualisasi confusion matrix, ditampilkan secara interaktif melalui antarmuka Streamlit sehingga memudahkan proses analisis dan interpretasi hasil.

2.2 Dataset Trafik Jaringan Kampus

Dataset yang digunakan dalam penelitian ini diperoleh dari hasil pemantauan lalu lintas jaringan kampus. Data mentah tersebut tersimpan dalam format CSV dan terdiri dari beberapa atribut utama, yaitu timestamp yang menunjukkan waktu terjadinya paket jaringan, *src_ip* sebagai alamat IP sumber, *dst_ip* sebagai alamat IP tujuan, *protocol* yang merepresentasikan jenis protokol jaringan yang digunakan, serta *packet_size* yang menunjukkan ukuran paket dalam satuan byte. Data ini merepresentasikan aktivitas jaringan secara rinci pada level paket *(packet-level traffic*), sehingga memungkinkan analisis lebih lanjut terhadap pola komunikasi jaringan sebelum dilakukan proses transformasi dan agregasi data. Visualisasi struktur data mentah tersebut ditunjukkan pada Gambar 2.

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

Unnamed: 0	timestamp	src_ip	dst_ip	protocol	packet_size
0	2025-01-01 08:00:01	192.168.1.10	10.10.10.2	TCP	1200
1	2025-01-01 08:00:02	192.168.1.10	10.10.10.3	TCP	1300
2	2025-01-01 08:00:03	192.168.1.11	10.10.10.4	UDP	300
3	2025-01-01 08:00:04	192.168.1.12	10.10.10.5	TCP	1400
4	2025-01-01 08:00:05	192.168.1.10	10.10.10.6	TCP	1500
5	2025-01-01 08:00:06	192.168.1.13	10.10.10.7	ICMP	60
6	2025-01-01 08:00:07	192.168.1.11	10.10.10.8	UDP	280
7	2025-01-01 08:00:08	192.168.1.14	10.10.10.9	TCP	1600
8	2025-01-01 08:00:09	192.168.1.10	10.10.10.10	TCP	1700
9	2025-01-01 08:00:10	192.168.1.15	10.10.10.11	UDP	320
10	2025-01-01 08:00:11	192.168.1.16	10.10.10.12	TCP	1800
11	2025-01-01 08:00:12	192.168.1.10	10.10.10.13	TCP	1900
12	2025-01-01 08:01:01	172.16.0.5	10.10.10.20	TCP	60
13	2025-01-01 08:01:02	172.16.0.5	10.10.10.21	TCP	60
14	2025-01-01 08:01:03	172.16.0.5	10.10.10.22	TCP	60
15	2025-01-01 08:01:04	172.16.0.5	10.10.10.23	TCP	60
16	2025-01-01 08:01:05	172.16.0.5	10.10.10.24	TCP	60
17	2025-01-01 08:02:01	10.20.30.1	10.10.10.30	TCP	2200
18	2025-01-01 08:02:02	10.20.30.2	10.10.10.30	TCP	2300
19	2025-01-01 08:02:03	10.20.30.3	10.10.10.30	TCP	2400
20	2025-01-01 08:02:04	10.20.30.4	10.10.10.30	TCP	2500
21	2025-01-01 08:02:05	10.20.30.5	10.10.10.30	TCP	2600
22	2025-01-01 08:02:06	10.20.30.6	10.10.10.30	TCP	2700
23	2025-01-01 08:03:01	192.168.50.10	10.10.10.40	TCP	900
24	2025-01-01 08:03:02	192.168.50.10	10.10.10.40	TCP	920
25	2025-01-01 08:03:03	192.168.50.10	10.10.10.40	TCP	940
26	2025-01-01 08:03:04	192.168.50.10	10.10.10.40	TCP	960
27	2025-01-01 08:03:05	192.168.50.10	10.10.10.40	TCP	980
28	2025-01-01 08:04:01	10.5.5.5	10.10.10.50	UDP	1800
29	2025-01-01 08:04:02	10.5.5.5	10.10.10.51	UDP	1850
30	2025-01-01 08:04:03	10.5.5.5	10.10.10.52	UDP	1900
31	2025-01-01 08:04:04	10.5.5.5	10.10.10.53	UDP	1950
32	2025-01-01 08:05:01	192.168.200.1	10.10.10.60	ICMP	64
33	2025-01-01 08:05:02	192.168.200.1	10.10.10.60	ICMP	64
34	2025-01-01 08:05:03	192.168.200.1	10.10.10.60	ICMP	64
35	2025-01-01 08:05:04	192.168.200.1	10.10.10.60	ICMP	64
36	2025-01-01 08:05:05	192.168.200.1	10.10.10.60	ICMP	64
37	2025-01-01 08:06:01	192.168.1.20	10.10.10.70	TCP	1400
38	2025-01-01 08:06:02	192.168.1.21	10.10.10.71	UDP	310
39	2025-01-01 08:06:03	192.168.1.22	10.10.10.72	TCP	1350
40	2025-01-01 08:06:04	192.168.1.23	10.10.10.73	ICMP	64
41	2025-01-01 08:06:05	192.168.1.24	10.10.10.74	TCP	1500

Gambar 2. DataSet Trafik Jaringan Kampus

2.2 Transpormasi Data

Algoritma *Support Vector Machine* tidak dapat secara langsung memproses data mentah berbasis paket, sehingga diperlukan tahap transformasi data untuk membentuk dataset berbasis aliran trafik *(flow-based data)*. Proses agregasi ini dilakukan secara otomatis menggunakan *library pandas* untuk merangkum informasi pada level paket menjadi representasi statistik per aliran komunikasi. Transformasi diawali dengan pengelompokan seluruh paket jaringan berdasarkan alamat IP sumber *(src_ip)* sehingga setiap kelompok merepresentasikan satu aliran trafik. Selanjutnya, dilakukan perhitungan fitur statistik untuk setiap aliran, yang meliputi jumlah paket yang dikirim *(packet_count),* rata-rata ukuran paket *(avg_packet_size),* total *byte* yang ditransmisikan *(total_bytes),* serta jumlah protokol unik yang

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

digunakan oleh setiap IP sumber *(unique_protocol)*. Hasil proses agregasi ini menghasilkan dataset baru yang lebih terstruktur dan representatif sebagai input bagi model *Support Vector Machine*. Dataset hasil transformasi tersebut (Gambar 2) kemudian digunakan dalam proses pelatihan dan pengujian model serta ditampilkan melalui antarmuka *Streamlit* pada bagian hasil deteksi [18].

Unnamed: 0	src_ip	packet_count	avg_packet_size	total_bytes	unique_protocol	anomaly_score	prediction
0	10.20.30.1	1	2200	2200	1	0,011680837	Normal
1	10.20.30.2	1	2300	2300	1	0,011965801	Normal
2	10.20.30.3	1	2400	2400	1	0,011167448	Normal
3	10.20.30.4	1	2500	2500	1	0,009076004	Normal
4	10.20.30.5	1	2600	2600	1	0,005524587	Normal
5	10.20.30.6	1	2700	2700	1	0,000397898	Normal
6	10.5.5.5	4	1875	7500	1	-9,22292E-05	Attack
7	172.16.0.5	5	60	30	1	-0,00035799	Attack
8	192.168.1.10	5	1520	500	1	-0,000124528	Attack
9	192.168.1.11	2	290	580	1	0,025086945	Normal
10	192.168.1.12	1	1400	1400	1	-9,22265E-05	Attack
11	192.168.1.13	1	60	60	1	0,000559872	Normal
12	192.168.1.14	1	1600	1600	1	0,001300182	Normal
13	192.168.1.15	1	320	320	1	0,011007759	Normal
14	192.168.1.16	1	1800	1800	1	0,004741199	Normal
15	192.168.1.20	1	1400	1400	1	-9,22265E-05	Attack
16	192.168.1.21	1	310	310	1	0,010795177	Normal
17	192.168.1.22	1	1350	1350	1	-3,57403E-05	Attack
18	192.168.1.23	1	64	64	1	0,000802204	Normal
19	192.168.1.24	1	1500	1500	1	0,000291975	Normal
20	192.168.200.1	5	64	320	1	6,49073E-05	Normal
21	192.168.50.10	5	940	4700	1	0,000255044	Attack

Gambar 2. Hasil Agregasi DataSet Trafik Jaringan Kampus

1. Pra Pemrosesan Data
   Setelah dataset hasil agregasi terbentuk, dilakukan tahap pra-pemrosesan data untuk memastikan kualitas dan kesiapan data sebelum digunakan dalam proses pelatihan model. Tahap pertama adalah *data cleaning*, di mana sistem secara otomatis menghapus nilai kosong (*missing values*) dan data duplikat, serta memastikan seluruh fitur numerik memiliki format yang valid dan konsisten. Selanjutnya, dilakukan proses normalisasi menggunakan metode *StandardScaler* untuk menyamakan skala seluruh fitur numerik agar tidak terjadi dominasi fitur tertentu dalam proses pembelajaran model. Tahap ini penting karena *algoritma Support Vector Machine* sangat sensitif terhadap perbedaan skala data. Setelah normalisasi, dilakukan seleksi fitur dengan memilih atribut yang relevan untuk proses klasifikasi, yaitu *packet_count, avg_packet_size, total_bytes,* dan *unique_protocol*. Rangkaian tahapan pra-pemrosesan ini bertujuan untuk meningkatkan stabilitas model serta mengoptimalkan performa deteksi serangan jaringan.
2. Metode Support Vector Machine.
   Support Vector Machine digunakan sebagai metode klasifikasi untuk membedakan trafik normal dan trafik serangan. SVM bekerja dengan mencari *hyperplane* optimal yang memaksimalkan jarak antar kelas [19]. Fungsi keputusan SVM dapat dituliskan sebagai:
   $$f(x) = w \cdot x + b \qquad (1)$$
   Dalam penelitian ini, model SVM diimplementasikan menggunakan *library scikit-learn* sehingga seluruh proses optimasi dan komputasi dilakukan otomatis oleh system.
3. Implementasi Sistem Menggunakan Streamlite
   Implementasi sistem pada penelitian ini dilakukan menggunakan framework Streamlit karena kemampuannya dalam membangun aplikasi analisis data yang interaktif dan terintegrasi secara efisien. Streamlit digunakan sebagai antarmuka untuk mengunggah dataset dalam format CSV, menampilkan data awal beserta hasil pra-pemrosesan, serta menjalankan proses pelatihan model *Support Vector Machine*. Selain itu, *framework* ini juga digunakan untuk menampilkan hasil evaluasi performa model secara visual, seperti confusion matrix dan grafik *ROC*, sehingga memudahkan proses interpretasi hasil analisis. Penggunaan Streamlit memastikan bahwa seluruh proses komputasi dilakukan secara otomatis dengan memanfaatkan *library Python*, sehingga mengurangi potensi kesalahan perhitungan manual dan meningkatkan *reproducibility* penelitian [20].
4. Metode Evaluasi dan Confusion Matrix
   Evaluasi performa model dilakukan menggunakan *confusion matrix* sebagai alat untuk mengukur kemampuan klasifikasi dalam membedakan antara trafik normal dan trafik serangan. Confusion matrix merepresentasikan hasil prediksi model dalam empat kategori utama, yaitu *True Positive (TP)* yang menunjukkan jumlah trafik serangan yang berhasil terdeteksi sebagai serangan, *True Negative (TN)* yang menunjukkan jumlah trafik normal yang terklasifikasi

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

dengan benar sebagai normal, *False Positive (FP)* yang merepresentasikan trafik normal yang keliru diklasifikasikan sebagai serangan, serta *False Negative (FN)* yang menunjukkan jumlah trafik serangan yang tidak berhasil terdeteksi oleh model. Melalui komponen-komponen tersebut, dapat dianalisis tingkat ketepatan dan kesalahan klasifikasi yang dihasilkan oleh model secara menyeluruh.

5. Validasi Kinerja
   Evaluasi model dilakukan menggunakan empat metrik validasi utama sebagai berikut:
   1) Accuracy Accuracy mengukur tingkat ketepatan keseluruhan model dalam melakukan klasifikasi

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (2)$$

   2) Precision Precision mengukur tingkat ketepatan prediksi serangan yang dilakukan oleh system

$$Precision = TP / (TP + FP) \quad (3)$$

   3) Recall Recall mengukur kemampuan sistem dalam mendeteksi seluruh serangan yang ada

$$Recall = TP / (TP + FN) \quad (4)$$

   4) F1-Score F1-Score merupakan rata-rata harmonis antara precision dan recall

$$F1 - Score = 2 \times (Precision \times Recall) / (Precision + Recall) \quad (5)$$

   Seluruh metrik ini dihitung secara otomatis menggunakan library scikit-learn dan ditampilkan melalui antarmuka Streamlit

3. HASIL DAN PEMBAHASAN

3.1 HASIL

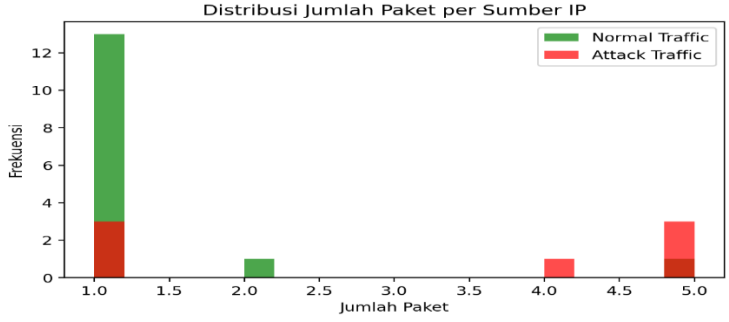
1. Hasil Analisis Visual Statistik Trafik Jaringan

Untuk mendukung analisis visual pada grafik,dilakukan perhitungan statistik deskriptif terhadap data trafik jaringan yang dianalisis.Ringkasan statistik ditampilkan pada Tabel 1.

Tabel 1. Ringkasan Statistik Trafik Jaringan

No	Parameter	Nilai
1	Total flow	22
2	Rata-rata paket	1,91
3	Total bytes	45.504

Berdasarkan Tabel 1, total *flow* menunjukkan bahwa terdapat 22 sumber IP yang dianalisis dalam penelitian ini. Nilai rata-rata paket sebesar 1,91 mengindikasikan bahwa secara umum jumlah paket yang dikirim oleh setiap sumber IP relatif rendah, namun terdapat beberapa sumber IP dengan jumlah paket lebih tinggi yang berpotensi sebagai trafik serangan. Total bytes menunjukkan besarnya volume data yang ditransmisikan selama proses pengamatan.
Gambar 1, menunjukkan distribusi jumlah paket yang dikirim oleh setiap sumber IP pada trafik jaringan kampus. Grafik membedakan antara trafik normal dan trafik serangan. Terlihat bahwa trafik normal cenderung memiliki jumlah paket yang lebih rendah dan stabil, sedangkan trafik serangan menunjukkan jumlah paket yang lebih tinggi pada beberapa sumber IP. Pola ini mengindikasikan adanya aktivitas anomali yang dapat digunakan sebagai dasar dalam proses klasifikasi menggunakan metode *Support Vector Machine (SVM).*



Gambar 3. Distribusi Jumlah Paket Per Sumber IP

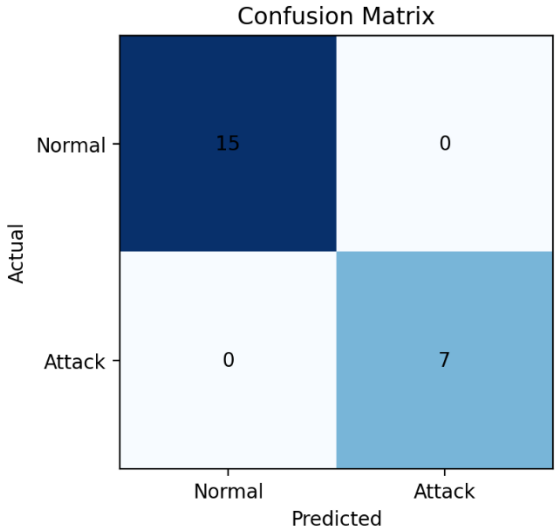
Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

2. Hasil Evaluasi Performa Berdasarkan Confusion Matrix

Tabel 2. Performance Statistik Trafik Jaringan

No	Parameter Evaluasi	Nilai
1	True positive (TP)	7
2	True negative (TN)	15
3	False positive (FP)	0
4	False negative (FN)	0
5	Akurasi	100%

Berdasarkan Table 2, *model One-Class Support Vector Machine* (*OCSVM)* berhasil mengklasifikasikan seluruh data dengan benar. Sebanyak 7 data serangan terdeteksi sebagai serangan *(True Positive),* dan 15 data trafik normal diklasifikasikan dengan tepat sebagai normal *(True Negative).* Tidak ditemukan kesalahan klasifikasi, baik *False Positive* maupun *False Negative*, sehingga model mencapai tingkat akurasi sebesar 100%. Dan meskipun hasil menunjukkan akurasi 100%, hal ini dikarenakan jumlah dataset yang relatif kecil memungkinkan terjadinya *overfitting*. Oleh karena itu, penelitian selanjutnya perlu dilakukan pada dataset yang lebih besar untuk menguji generalisasi model.
Untuk mengevaluasi *performa model*, digunakan *confusion matrix* yang membandingkan antara label aktual dan hasil prediksi model [21]. *Confusion matrix* ditampilkan pada Gambar 4. Berdasarkan confusion matrix tersebut, model berhasil mengklasifikasikan seluruh data dengan benar. Sebanyak 15 data trafik normal terprediksi sebagai normal dan 7 data serangan terdeteksi dengan tepat sebagai serangan. Tidak ditemukan kesalahan klasifikasi, baik *false positive* maupun *false negative,* yang menunjukkan bahwa model memiliki tingkat akurasi yang sangat tinggi pada data pengujian.



Gambar 4. Confusion Matrix Model One-Class SVM

3. Hasil Deteksi Lalu Lintas Jaringan

Untuk memberikan gambaran kuantitatif terhadap hasil prediksi model, dilakukan perhitungan jumlah trafik normal dan trafik serangan yang terdeteksi. Ringkasan hasil klasifikasi ditampilkan pada Tabel 3.

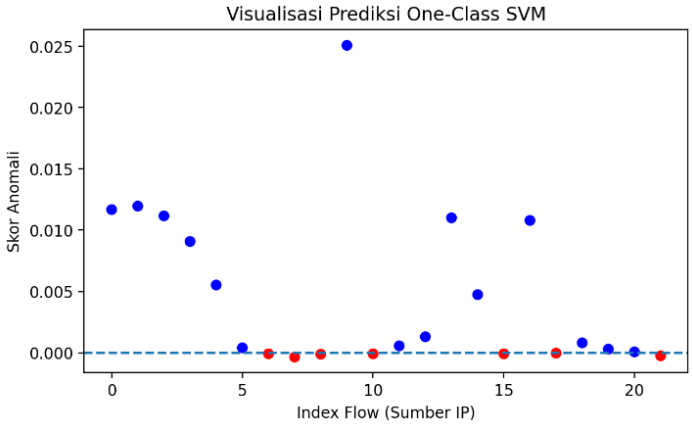
Tabel 3. Hasil Deteksi Lalu Lintas Jaringan

No	Parameter	Nilai
1	Total flow	22
2	Normal	15
3	Serangan	7

Berdasarkan Tabel 3, dari total 22 flow IP yang dianalisis, sebanyak 15 flow diklasifikasikan sebagai trafik normal, sedangkan 7 flow lainnya terdeteksi sebagai serangan. Hasil ini menunjukkan bahwa model *One-Class SVM* mampu mengidentifikasi sejumlah aktivitas jaringan yang menyimpang dari pola normal.
Gambar 5 menunjukkan hasil prediksi deteksi serangan jaringan menggunakan metode *One-Class Support Vector Machine* (OCSVM). Grafik tersebut menampilkan skor anomali dari setiap flow IP yang dianalisis, di mana sumbu

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

horizontal merepresentasikan *indeks flow (sumber IP*) dan sumbu vertikal menunjukkan nilai skor anomali. Pada grafik tersebut, garis ambang batas *(threshold)* digunakan untuk membedakan antara trafik normal dan trafik anomali. Flow IP yang memiliki skor anomali berada di atas ambang batas diklasifikasikan sebagai serangan, sedangkan *flow* IP dengan skor di bawah ambang batas dikategorikan sebagai trafik normal.



Gambar 5. Grafik Prediksi One-Class SVM

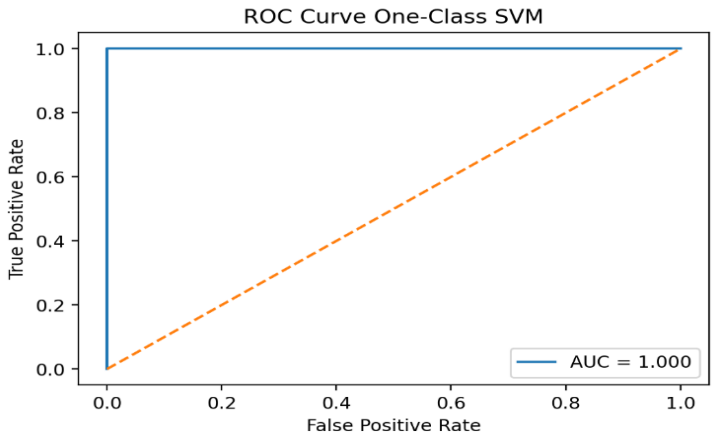
Hasil visualisasi menunjukkan bahwa sebagian besar *flow IP* berada pada kategori normal, namun terdapat beberapa *flow IP* yang terdeteksi sebagai serangan, yang mengindikasikan adanya aktivitas anomali pada lalu lintas jaringan.

4. Hasil Evaluasi Performa Berdasarkan ROC Curve

Tabel 4. Hasil Evaluasi Performa ROC Curve

No	Parameter	Nilai
1	True positive rate (TPR)	1.000
2	False positive rate (FPR)	0.000
3	Area under Curve (AUC)	1.000

Berdasarkan Tabel 4, nilai *True Positive Rate (TPR)* sebesar 1.000 menunjukkan bahwa seluruh data serangan berhasil terdeteksi oleh model. Nilai *False Positive Rate (FPR)* sebesar 0.000 menunjukkan tidak adanya kesalahan dalam mendeteksi trafik normal sebagai serangan. Nilai *Area Under Curve (AUC)* sebesar 1.000 mengindikasikan bahwa *model One-Class SVM* memiliki performa yang sangat baik dalam membedakan antara trafik normal dan trafik serangan.
Selain *confusion matrix,* evaluasi performa model juga dilakukan menggunakan *Receiver Operating Characteristic* (ROC) Curve. ROC Curve menggambarkan hubungan antara *True Positive Rate (TPR)* dan *False Positive Rate (FPR)* dari model klasifikasi. Berdasarkan Gambar 6, nilai *Area Under Curve (AUC)* yang diperoleh adalah sebesar 1.000. Nilai AUC yang mendekati 1 menunjukkan bahwa model memiliki kemampuan yang sangat baik dalam membedakan antara trafik normal dan trafik serangan. Dengan demikian, dapat disimpulkan bahwa model One-Class SVM memiliki performa yang sangat optimal dalam mendeteksi anomali pada lalu lintas jaringan yang dianalisis.



Gambar 6. Grafik Hasil Analisis ROC Curve One Class SVM

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

Berdasarkan Gambar 6, kurva *ROC* menunjukkan bahwa model memiliki kemampuan diskriminasi yang sempurna antara kelas normal dan serangan. Kurva berada di sudut kiri atas grafik, yang menandakan nilai sensitivitas tinggi dan tingkat kesalahan sangat rendah.

3.2 PEMBAHASAN

Hasil penelitian menunjukkan bahwa model *One-Class Support Vector Machine* mampu mendeteksi serangan jaringan pada lingkungan kampus dengan performa yang sangat baik. Data trafik jaringan yang telah melalui tahap pra-pemrosesan berhasil digunakan untuk membentuk pola trafik normal, sehingga penyimpangan dapat terdeteksi sebagai anomali [7], [11].

Hasil klasifikasi menunjukkan bahwa model mampu membedakan trafik normal dan trafik serangan secara akurat. Fitur jumlah paket dan total byte memberikan kontribusi signifikan dalam mendeteksi aktivitas jaringan yang tidak normal. Hal ini menunjukkan bahwa pemilihan fitur yang tepat sangat memengaruhi keberhasilan model klasifikasi [6], [12].

Evaluasi menggunakan confusion matrix menunjukkan bahwa seluruh data uji berhasil diklasifikasikan dengan benar tanpa kesalahan *false positive* maupun *false negative*. Kondisi ini menunjukkan tingkat ketepatan model yang sangat tinggi dalam mendeteksi serangan tanpa mengganggu trafik normal yang sah [9] , [15].Nilai *accuracy, precision*, dan *recall* yang tinggi menunjukkan bahwa model memiliki performa yang konsisten dan andal. Konsistensi ini penting dalam sistem keamanan jaringan karena kesalahan deteksi dapat menimbulkan gangguan operasional atau risiko keamanan yang lebih besar [10], [17]. Hasil evaluasi *ROC Curve* menunjukkan nilai *Area Under Curve (AUC)* yang mendekati satu, yang menandakan bahwa model memiliki kemampuan pemisahan kelas yang sangat baik. Hal ini memperkuat bahwa *One-Class SVM* merupakan metode yang efektif untuk deteksi anomali pada trafik jaringan kampus [12], [14].

Secara keseluruhan, hasil penelitian membuktikan bahwa metode *Support Vector Machine* mampu memberikan solusi yang efektif dalam mendeteksi serangan jaringan kampus. Integrasi sistem ke dalam aplikasi berbasis Streamlit juga memudahkan analisis dan visualisasi hasil, sehingga sistem berpotensi diterapkan sebagai pendukung keamanan jaringan kampus secara nyata [8], [16].

4. KESIMPULAN

Penelitian ini bertujuan untuk menerapkan metode *Support Vector Machine* dalam mendeteksi serangan jaringan pada lingkungan kampus berdasarkan data trafik jaringan. Berdasarkan proses penelitian yang telah dilakukan, dapat disimpulkan bahwa pendekatan machine learning menggunakan *Support Vector Machine,* khususnya *One-Class Support Vector Machine,* mampu digunakan secara efektif sebagai metode pendukung sistem deteksi serangan jaringan. Model yang dikembangkan mampu mengenali pola trafik jaringan normal dan mengidentifikasi penyimpangan sebagai indikasi serangan jaringan. Hal ini menunjukkan bahwa tujuan penelitian untuk membangun sistem deteksi serangan berbasis data trafik jaringan kampus dapat tercapai tanpa bergantung pada metode deteksi konvensional berbasis *signature.* Penerapan tahapan pra-pemrosesan data serta integrasi sistem ke dalam aplikasi berbasis *Streamlit* memungkinkan proses deteksi dan evaluasi berjalan secara otomatis dan mudah digunakan. Untuk pengembangan selanjutnya, penelitian ini dapat diperluas dengan penggunaan data trafik jaringan dalam skala yang lebih besar, penerapan pemantauan secara real-time, serta penggabungan metode lain guna meningkatkan kemampuan deteksi terhadap serangan yang lebih kompleks. Penelitian ini memberikan kontribusi pada penerapan *One-Class Support Vector Machine* pada data trafik nyata jaringan kampus, yang masih jarang dilakukan pada penelitian sebelumnya yang umumnya menggunakan dataset publik. Selain itu, penelitian ini menunjukkan bahwa transformasi *data packet-level* ke *flow-based feature* dapat meningkatkan efektivitas deteksi anomali. Berdasarkan hasil penelitian, model *One-Class Support Vector Machine* berhasil mendeteksi serangan jaringan dengan tingkat akurasi 100%, *precision* 100%, *recall* 100%, dan nilai *AUC* sebesar 1.000. Dari 22 *flow* data yang dianalisis, 15 diklasifikasikan sebagai trafik normal dan 7 sebagai serangan tanpa kesalahan klasifikasi. Hasil ini menunjukkan bahwa pendekatan SVM efektif dalam mendukung sistem deteksi intrusi pada jaringan kampus. Namun demikian, pengujian pada dataset yang lebih besar dan implementasi secara real-time masih diperlukan untuk memastikan robustitas sistem.

REFERENCES

[1] "Towards An Efficient Internet of Things Intrusion Detection by Using Support Vector Machine, Baghdad Science Journal, 2024.", doi: 11067.

[2] Y. Irawan, R. Pramitasari, W. M. Ashari, and A. N. H. Yansyah, "Support Vector Machine Classification Algorithm for Detecting DDoS Attacks on Network Traffic," *Journal of Applied Informatics and Computing*, vol. 9, no. 4, pp. 1945–1954, 2025.

[3] R. W. A. Yahya, "Mendeteksi Dan Pencegahan Serangan Distributed Denial Of Service (Ddos) Pada Jaringan Kampus Menggunakan Algoritma K-Nearest Neighbors," s1, Universitas Lancang Kuning, 2024. Accessed: Mar. 01, 2026. [Online]. Available: https://repository.unilak.ac.id/5285

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

[4] H. Haeruddin, E. Erick, and H. W. Aripradono, "Perbandingan Support Vector Machine, Random Forest Classifier, dan K-Nearest Neighbour dalam Pendeteksian Anomali pada Jaringan DDos," *Jurnal Teknologi Informasi dan Multimedia*, vol. 7, no. 1, pp. 23–33, 2025.

[5] K. M. Abuali, L. Nissirat, and A. Al-Samawi, "Advancing network security with AI: SVM-based deep learning for intrusion detection," *Sensors*, vol. 23, no. 21, p. 8959, 2023.

[6] T. Tan, H. Sama, G. Wijaya, and O. E. Aboagye, "Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning:(Metode SVM dan ANN)," *Jurnal Teknologi dan Informasi*, vol. 13, no. 2, pp. 152–164, 2023.

[7] S. Jumpathong, K. Kriengket, P. Boonkwan, and T. Supnithi, "Anomaly Detection in Lexical Definitions via One-Class Classification Techniques," in *2021 16th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)*, IEEE, 2021, pp. 1–6. Accessed: Jan. 27, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9678166/

[8] A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," *Discov Artif Intell*, vol. 5, no. 1, p. 314, Nov. 2025, doi: 10.1007/s44163-025-00578-1.

[9] "[8] A Systematic Review on Intrusion Detection System,... - Google Scholar." Accessed: Jan. 27, 2026. [Online]. Available: https://scholar.google.com/scholar?hl=id&as_sdt=0%2C5&q=%5B8%5D%09A+Systematic+Review+on+Intrusion+Detection+System%2C+OJSScience%2C+2024.&btnG=

[10] P. Bountzis, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "A deep one-class classifier for network anomaly detection using autoencoders and one-class support vector machines," *Frontiers in Computer Science*, vol. 7, p. 1646679, 2025.

[11] A. Zahoor, W. Abbasi, M. Z. Babar, and A. Aljohani, "Robust iot security using isolation forest and one class svm algorithms," *Scientific Reports*, vol. 15, no. 1, p. 36586, 2025.

[12] W. Khreich, B. Khosravifar, A. Hamou-Lhadj, and C. Talhi, "An anomaly detection system based on variable N-gram features and one-class SVM," *Information and Software Technology*, vol. 91, pp. 186–197, 2017.

[13] S. Golande, S. Vaidya, A. Pardeshi, V. Katkade, and V. Pawar, "An Efficient Network Intrusion Detection and Classification System using Machine Learning," *International Journal of Advanced Research in Science, Communication and Technology*, 2024, Accessed: Jan. 27, 2026. [Online]. Available: https://www.researchgate.net/profile/Shashikant-Golande-2/publication/385671415_An_Efficient_Network_Intrusion_Detection_and_Classification_System_using_Machine_Learning/links/6730cc2a5852dd723cb56f3e/An-Efficient-Network-Intrusion-Detection-and-Classification-System-using-Machine-Learning.pdf

[14] K. A. Nugroho, T. Hariguna, and A. S. Barkah, "Optimizing Early Network Intrusion Detection: A Comparison of LSTM and LinearSVC with SMOTE on Imbalanced Data," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 6, pp. 5349–5370, 2025.

[15] A. Alsajri and A. Steiti, "Intrusion detection system based on machine learning algorithms:(SVM and genetic algorithm)," *Babylonian Journal of Machine Learning*, vol. 2024, pp. 15–29, 2024.

[16] A. T. Zy, A. T. Sasongko, and A. Z. Kamalia, "Penerapan Naïve Bayes Classifier, Support Vector Machine, dan Decision Tree untuk Meningkatkan Deteksi Ancaman Keamanan Jaringan," *Media Online*, vol. 4, no. 1, pp. 610–617, 2023.

[17] V. Timčenko and S. Gajin, "Machine learning based network anomaly detection for IoT environments," in *ICIST-2018 conference*, 2018. Accessed: Jan. 27, 2026. [Online]. Available: https://www.eventiotic.com/eventiotic/files/Papers/URL/e5bb6a65-0030-4acf-815e-37c58cdc0bda.pdf

[18] S. Auliana, B. R. S. Permana, M. Darip, and S. C. Roy, "FuelGuard: Fuel Consumption Anomaly Detection and Visual Verification in Logistics Using Isolation Forest, CBIR, and OCR," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 6, pp. 6017–6030, 2025, doi: 10.52436/1.jutif.2025.6.6.5276.

[19] R. Guido, S. Ferrisi, D. Lofaro, and D. Conforti, "An Overview on the Advancements of Support Vector Machine Models in Healthcare Applications: A Review," *Information*, vol. 15, no. 4, p. 235, Apr. 2024, doi: 10.3390/info15040235.

[20] "(3) Streamlit: Transforming Data Analysis Scripts into Powerful Web Applications." Accessed: Mar. 01, 2026. [Online]. Available: https://www.academia.edu/128116333/Streamlit_Transforming_Data_Analysis_Scripts_into_Powerful_Web_Applications

[21] W. Rizki and M. Darip, "Penggunaan Algoritma Support Vector Machine Untuk mendeteksi Anomali Aktivitas Pengguna Pada Sistem Informasi Keuangan PT. Digidokat Indonesia," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 3, Art. no. 3, May 2025, doi: 10.36040/jati.v9i3.13385.

Bulletin of Information Technology (BIT)
Vol 7, No 1, Maret 2026, Hal. 40 - 49
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2602
https://journal.fkpt.org/index.php/BIT

[22] A. Karim and A. Ernawati, "Uncovering Smartphone Brand Strategies through Specification-Based Clustering and Classification," Buletin Ilmiah Informatika Teknologi, vol. 4, no. 1, pp. 24–32, Oct. 2025, doi: 10.58369/biit.v2i3.167.