LINIER
LITERATUR INFORMATIKA & KOMPUTER
e-ISSN: 3063-2218
DOI : 10.33096/linier.v2i2.3105
Literatur Informatika & Komputer
Vol 2, No 2 (2025), pp 147-159

Analisis Perbandingan Serangan UDP *Flooding* dan SYN *Flooding* Menggunakan Metode *Support Vector Machine*

A. Muh. Syafei Emil Ma'arif[a], Farniwati Fattah[b], Herdianti Darwis[c], Tazkirah Amaliah[d]
Universitas Muslim Indonesia, Makassar, Indonesia
Email: [a]Andimuhsyafei06@gmail.com; [b]farniwatifattah@umi.ac.id; [c]herdiantidarwis@umi.ac.id; [d]tazkirahamaliah.iclabs@umi.ac.id;

Received: 18-08-2024 | Revised: 12-05-2025 | Accepted: 11-06-2025 | Published: 29-06-2025

Abstrak

Dalam upaya untuk meningkatkan Keamanan jaringan komputer di Laboratorium Fakultas Ilmu Komputer UMI, seperti halnya serangan UDP *Flooding* dan SYN *Flooding* paket data yang datang sangat banyak dan menumpuk yang bisa saja terjadi kapan saja maka sangat dibutuhkan analisa. Serangan DOS adalah jenis serangan terhadap sebuah komputer atau *server* dengan cara menghabiskan sumber daya yang dimiliki sehingga tidak dapat berfungsi secara optimal. Sehingga secara tidak langsung menghalangi pengguna lain untuk memperoleh akses layanan dari komputer atau *server* tersebut. Penelitian ini melakukan klasifikasi serangan pada data-data yang diuji dengan menggunakan metode klasifikasi SVM (Support Vector Machines). Data yang diklasifikasi dari serangan DoS yaitu UDP *Flooding* dan SYN *Flooding* dengan mencatat aktivitas data traffic jaringan menggunakan tools *Wireshark*, Hasil penelitian ini Klasifikasi serangan dengan metode SVM menghasilkan tingkat akurasi yang sangat tinggi dalam waktu perekaman data selama 5 menit mendapatkan data record sebanyak 10.000 data yang sudah di seleksi untuk masing-masing serangan dengan rata-rata class yang diprediksi semuanya menghasilkan akurasi sebesar 100%.

Kata kunci: Laboratorium Fakultas Ilmu Komputer, Serangan DOS, UDP *Flooding,* SYN *Flooding,* Metode *Support Vector Machine*

Pendahuluan

Keamanan jaringan komputer sangat dibutuhkan pada saat perkembangan teknologi komunikasi dan jaringan yang cukup pesat ini. Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan keamanan informasi yang diterapkan pada komputer [1]. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan. Hal ini mengakibatkan semua komputer yang terhubung ke jaringan komputer sangat rentan terhadap serangan atau kegiatan yang bersifat merugikan yang dilakukan oleh orang lain yang bertujuan untuk mengambil data, memanipulasi data, bahkan merusak data-data berharga untuk tujuan tertentu [2].

Salah satu contoh serangan terhadap keamanan jaringan yang populer saat ini yaitu serangan *Denial of Service* (DOS). Serangan DOS adalah jenis serangan terhadap sebuah komputer atau *server* dengan cara menghabiskan sumber daya yang dimiliki sehingga tidak dapat berfungsi secara optimal [3]. Sehingga DOS secara tidak langsung menghalangi pengguna lain untuk memperoleh akses layanan dari komputer atau *server* tersebut. Perusahaan keamanan siber Kapersky merilis laporan statistik serangan siber terbaru. Dalam laporan tersebut, Kapersky menjelaskan statistik serangan DOS pada kuartal kedua tahun 2019 tipe serangan DOS yaitu SYN *Flooding* masih mendominasi dengan presentase 82,43%. Selanjutnya disusul tipe serangan UDP *Flood* dengan presentase 10,94% [4].

Serangan DOS merupakan serangan yang bertujuan untuk mempengaruhi trafik jaringan sehingga jaringan tersebut tidak dapat digunakan oleh pengguna yang berhak atau sah. Serangan DOS dilakukan dengan cara membanjiri IP *address* jaringan target dengan *request* sehingga sistem menjadi *crash*, *hang* atau turun kinerjanya karena beban CPU tinggi [5]. Selain itu, tipe serangan DOS adalah *Ping of Death*, SYN *Attack*, *Land Attack*, UDP *Flood*, dan *Smurf Attack*. Adapun metode yang sering digunakan untuk mendeteksi serangan *Denial of Service* (DOS) dalam beberapa tahun terakhir ini adalah metode *Machine Learning* atau *Deep Learning* [6]. SYN *attack* adalah salah satu jenis serangan DOS yang mengimplementasi protokol TCP/IP dengan mengirimkan paket-paket SYN *request* kedalam *port-port* pada *router* sasaran dengan maksud menyerap seluruh sumber daya yang ada pada *server* sehingga *server* menjadi terlalu sibuk dan tidak dapat mengontrol lalu lintas jaringan dengan baik. Bahkan dapat berakibat macetnya sistem (*hang*) [7]. Penerapan

metode-metode *data mining* untuk mendeteksi serangan dapat menjadi solusi dari permasalahan peningkatan jumlah data yang besar karena memiliki keunggulan dapat memproses *system logs* data dalam jumlah yang besar [8].

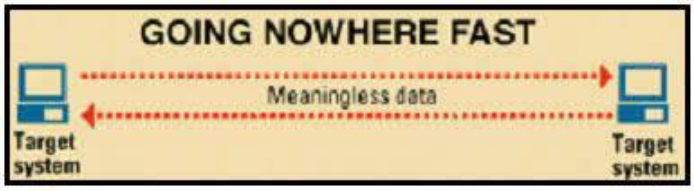
Metode *Support Vector Machine* (SVM) adalah metode *data mining* yang baik untuk mengklasifikasikan pola-pola paket jaringan sehingga menghasilkan klasifikasi trafik jaringan sesuai dengan *Destination Network* dan *Protocol* [9].

Berdasarkan uraian latar belakang, maka penulis melakukan penelitian dengan judul "Analisis Perbandingan Serangan UDP *Flooding* dan SYN *Flooding* menggunakan metode *Support Vector Machine*" dilakukan untuk mengetahui klasifikasi serangan.

Metode

A. UDP *Flooding*

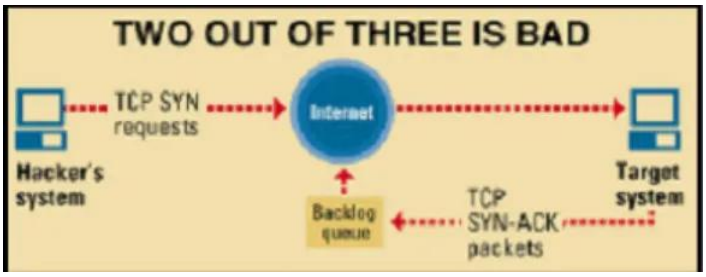
Pengiriman data UDP secara berlebihan kedalam suatu jaringan, pengiriman UDP *flood* ini akan membentuk suatu jalur hubungan dengan suatu servis UDP dari *host* tujuan. UDP *Flood* ini akan mengirimkan karakter yang akan mengetes jaringan korban. Sehingga terjadi aliran data yang tidak perlu dalam jaringan korban tersebut [10].



Gambar 1. Mekanisme serangan UDP *Flooding*

B. SYN *Flooding*

SYN *Flooding* terjadi bila suatu *host* hanya mengirimkan paket SYN TCP saja secara kontinyu tanpa mengirimkan paket ACK sebagai konfirmasinya. Hal ini akan menyebabkan *host* tujuan akan terus menunggu paket tersebut dengan menyimpannya kedalam *backlog*. Meskipun besaran paketnya kecil, tetapi apabila pengiriman SYN tersebut terus menerus akan memperbesar *backlog*. Hal yang terjadi apabila *backlog* sudah besar akan mengakibatkan *host* tujuan akan otomatis menolak semua paket SYN yang datang, sehingga *host* tersebut tidak bisa dikoneksi oleh *host* yang lain [11].



Gambar 2. Mekanisme serangan SYN *Flooding*

C. Support Vector Machine

Support Vector Machine (SVM) adalah salah satu metode pada *machine learning* yang sering digunakan untuk mengklasifikasikan data [12]. SVM memiliki konsep dasarnya merupakan gabungan dari teori komputasi, seperti *hyperplane*, kernel, dan konsep pendukung lainnya. Prinsip dasar SVM adalah klasifikasi *linear*, kemudian dikembangkan agar dapat bekerja pada *problem* non-*linear* dengan konsep *kernel trick* pada data berdimensi tinggi. SVM bersifat *Supervised Learning* ataupun dapat dikontrol data *training* dan *testing* untuk mendapatkan keakuratan klasifikasi. Konsep kerja dari SVM ketika pertama kali digunakan/dikembangkan oleh Boser, Guyon, Vapnik pada tahun 1992 hanya dapat menangani klasifikasi data yang memiliki 2 kelas tapi seiring waktu SVM telah dikembangkan dalam klasifikasi data yang memiliki lebih dari 2 kelas dengan *Pattern Recognition* pada ruang kerja berdimensi tinggi. Proses

klasifikasi pada SVM adalah menentukan *hyperplane* terbaik untuk pemisah dua kelas data, data yang paling dekat dengan *hyperplane* disebut *support vector*. Untuk mendapatkan *hyperplane* terbaik dengan cara menentukan *max margin*. *Margin* adalah jarak antara *hyperplane* dengan *support vector* [13].

D. Confusion Matrix

Untuk menguji hasil klasifikasi pada sistem yang dibangun, diperlukan suatu metode perhitungan untuk evaluasi kinerja [14]. Tahap yang di perlukan untuk evaluasi kinerja yaitu dengan menghitung nilai presisi, *recall*, dan nilai-nilai ukuran f1. Akurasi adalah cara sistem mengklasifikasikan benar dengan data benar dan salah, dan ukuran-f1 adalah untuk menilai kinerja keseluruhan sistem dengan menghitung nilai akurasi dan re*call* :

Tabel 1. *Confusion matrix*

		Nilai Aktual	
		Tabel sub kepala	Tabel sub kepala
Nilai Prediksi	*Positive*	TP	FP
	Negative	TN	FN

Keterangan:

TP (*True Positive*) = Prediksi positif dan nilai sebenarnya positif
TN (*True Negative*) = Prediksi negatif dan nilai sebenarnya negatif
FP (*False Positive*) = Prediksi positif dan nilai sebenarnya negative
FN (*False Negative*) = Prediksi negatif dan nilai sebenarnya positif

Rumus dari akurasi *confusion matrix* dapat dilihat pada persamaan 1, 2, 3 [15]:

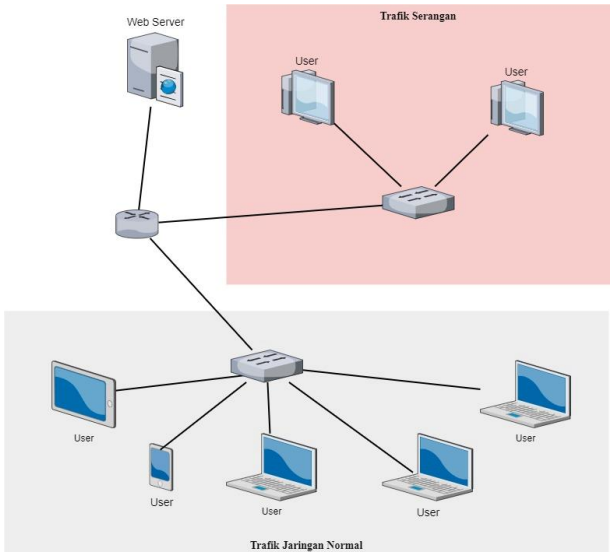
$$Precision = \frac{TP}{TP+FP} \times 100\% \text{ [16]} \quad (1)$$

$$Accuracy = \frac{TP+TN}{TP+FP+TN+TN} \times 100\% \text{ [17]} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \times 100\% \text{ [18]} \quad (3)$$

Perancangan

A. Desain Topologi Jaringan

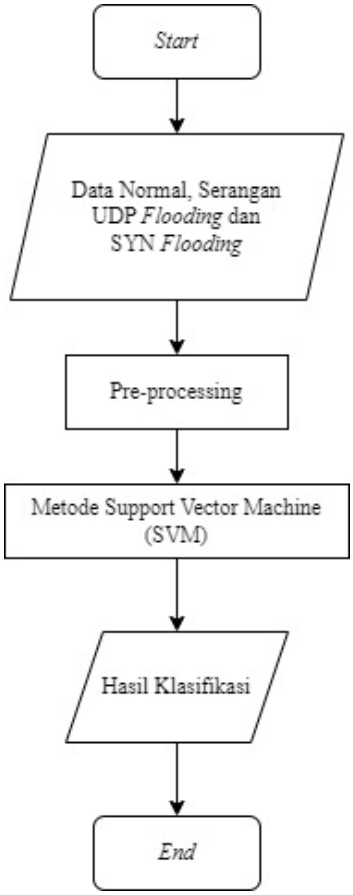


Gambar 3. Desain Topologi Jaringan

Model topologi jaringan pada penelitian ini dimana ada 2 data trafik jaringan yaitu trafik serangan dan trafik jaringan normal, di trafik serangan akan dilakukan serangan UDP *Flooding* dan SYN *Flooding*

dari komputer 2 ke komputer 1 yang akan dilakukan perekaman data serangan untuk mendapatkan hasil *traffic* jaringan dan jumlah paket yang dihasilkan penyerangan, di trafik jaringan normal juga akan dilakukan perekaman data normal yang akan dibuatkan model klasifikasi data pada metode SVM [19].

B. Desain Klasifikasi Data



Gambar 4. Desain Klasifikasi Data

Gambar 4. mekanisme klasifikasi data yang berisi paket-paket serangan UDP *Flooding* dan SYN *Flooding* yang nantinya akan di*capture* oleh *wireshark* (trafik jaringan) untuk mendapatkan protokol jaringan yang akan diolah sesuai atribut yang telah ditentukan, setelah data diperoleh maka akan dilakukan tahap Pre-*processing*, data diolah dan disimpan didalam database *Microsoft Excel* yang kemudian di konversi menjadi sebuah dataset yang akan digunakan untuk membentuk sebuah model klasifikasi yang akan digunakan dalam mengklasifikasi data dimana akan dilakukan pengujian terhadap model tersebut dengan menggunakan SVM untuk mengetahui hasil klasifikasi serangan terhadap dataset yang dibuat.

Pemodelan

Dalam penelitian ini, di samping mengumpulkan dan menganalisis data serangan yang terdeteksi menggunakan Wireshark, penting untuk mencatat bahwa terdapat pula penggunaan data pembanding yang mencerminkan lalu lintas jaringan yang normal, bukan serangan. Data pembanding ini dimanfaatkan untuk melatih model SVM (*Support Vector Machine*) yang digunakan dalam upaya pendeteksian serangan *flood* [20]. Melibatkan data pembanding memungkinkan penelitian ini memberikan wawasan yang lebih holistik mengenai perbedaan karakteristik antara serangan dan lalu lintas jaringan yang normal. Dan berikut adalah data yang bukan merupakan data serangan.

	Time	Source	Destination	Protocol	Length	Info	Seq	Win	Len	Src
0	0.920053	172.125.1.137	172.125.0.68	TCP	60	0 > 1102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
1	0.920053	172.125.1.137	172.125.0.68	TCP	60	0 > 1104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
2	0.920053	172.125.1.137	172.125.0.68	TCP	60	0 > 1107 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
3	0.920053	172.125.1.137	172.125.0.68	TCP	60	0 > 1108 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
4	0.920102	172.125.1.137	172.125.0.68	TCP	60	0 > 1103 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
...	...	...	...	...	...	...	...	...	...	...
9995	1.126845	172.125.1.137	172.125.0.68	TCP	60	0 > 11093 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
9996	1.126854	172.125.1.137	172.125.0.68	TCP	60	0 > 11094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
9997	1.126864	172.125.1.137	172.125.0.68	TCP	60	0 > 11095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
9998	1.126895	172.125.1.137	172.125.0.68	TCP	60	0 > 11097 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0
9999	1.126896	172.125.1.137	172.125.0.68	TCP	60	0 > 11096 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0

Gambar 5. Tampilan data Serangan SYN *Flooding*

	Time	Source	Destination	Protocol	Length	Info	Seq	Win	Len	Src	Dst
0	0.000000	172.125.1.137	172.125.0.68	TCP	60	0 > 6478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	6478
1	0.000065	172.125.1.137	172.125.0.68	TCP	60	0 > 6479 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	6479
2	0.000134	172.125.1.137	172.125.0.68	TCP	60	0 > 6480 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	6480
3	0.000206	172.125.1.137	172.125.0.68	TCP	60	0 > 6481 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	6481
4	0.000270	172.125.1.137	172.125.0.68	TCP	60	0 > 6482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	6482
...	...	...	...	...	...	...	...	...	...	...	...
9995	1.014262	172.125.1.137	172.125.0.68	TCP	60	0 > 16409 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	16409
9996	1.014343	172.125.1.137	172.125.0.68	TCP	60	0 > 16410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	16410
9997	1.014405	172.125.1.137	172.125.0.68	TCP	60	0 > 16411 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	16411
9998	1.014474	172.125.1.137	172.125.0.68	TCP	60	0 > 16412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	16412
9999	1.014545	172.125.1.137	172.125.0.68	TCP	60	0 > 16413 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	0	16413

Gambar 6. Tampilan data Serangan UDP *Flooding*

	Time	Source	Destination	Protocol	Length	Info	Seq	Win	Len	MSS	Src	Dst
0	0.131954	162.247.241.14	172.126.0.20	TCP	66	443 > 63142 [ACK] Seq=1 Ack=1 Win=8 Len=0 TS...	1	8	0	NaN	443	63142
1	0.132146	172.126.0.20	162.247.241.14	TCP	66	[TCP ACKed unseen segment] 63142 > 443 [ACK]...	1	2048	0	NaN	63142	443
2	0.158286	18.64.18.119	172.126.0.20	TCP	66	443 > 60859 [ACK] Seq=1 Ack=33 Win=142 Len=0...	1	142	0	NaN	443	60859
3	0.657625	172.126.0.20	18.64.18.119	TCP	66	60859 > 443 [ACK] Seq=33 Ack=29 Win=2047 Len...	33	2047	0	NaN	60859	443
4	1.540110	162.247.241.14	172.126.0.20	TCP	66	443 > 62881 [ACK] Seq=1 Ack=1 Win=8 Len=0 TS...	1	8	0	NaN	443	62881
...	...	...	...	...	...	...	...	...	...	...	...	...
16940	1748.189946	172.126.0.20	17.36.202.137	TCP	54	54466 > 443 [ACK] Seq=518 Ack=5439 Win=25670...	518	256704	0	NaN	54466	443
16941	1748.191181	172.126.0.20	17.36.202.137	TCP	54	54466 > 443 [ACK] Seq=518 Ack=5781 Win=25632...	518	256320	0	NaN	54466	443
16942	1748.226937	172.126.0.20	17.36.202.137	TCP	54	[TCP Window Update] 54466 > 443 [ACK] Seq=51...	518	262144	0	NaN	54466	443
16943	1748.317692	17.32.194.2	172.126.0.20	TCP	1514	443 > 54455 [PSH, ACK] Seq=11062 Ack=1175 Wi...	11062	133120	1448	NaN	443	54455
16944	1748.317779	172.126.0.20	17.32.194.2	TCP	66	54455 > 443 [ACK] Seq=1175 Ack=12510 Win=422...	1175	4224	0	NaN	54455	443

Gambar 7. Tampilan data normal

A. Pelabelan Data

Dalam konteks penelitian ini, untuk mempersiapkan data yang digunakan dalam pelatihan model SVM, diperlukan label yang menandakan apakah data tersebut merupakan serangan atau data normal. Untuk melakukan hal ini, dilakukan penambahan kolom label pada DataFrame yang mengandung data tersebut.

Setiap data yang terkait dengan serangan akan diberi label 1, sedangkan data yang mewakili lalu lintas jaringan normal akan diberi label 0. Penambahan label ini akan membedakan antara kedua jenis data dalam proses pelatihan model SVM. Dan berikut adalah tampilan ketika data telah digabung menjadi 2 dataset yang akan dibuatkan masing-masing sebuah model.

	Time	Source	Destination	Protocol	Length	Info	Seq	Win	Len	MSS	Src	Dst	attack
0	0.131954	162.247.241.14	172.126.0.20	TCP	66	443 > 63142 [ACK] Seq=1 Ack=1 Win=8 Len=0 TS...	1	8	0	NaN	443	63142	0
1	0.132146	172.126.0.20	162.247.241.14	TCP	66	[TCP ACKed unseen segment] 63142 > 443 [ACK]...	1	2048	0	NaN	63142	443	0
2	0.158286	18.64.18.119	172.126.0.20	TCP	66	443 > 60859 [ACK] Seq=1 Ack=33 Win=142 Len=0...	1	142	0	NaN	443	60859	0
3	0.657625	172.126.0.20	18.64.18.119	TCP	66	60859 > 443 [ACK] Seq=33 Ack=29 Win=2047 Len...	33	2047	0	NaN	60859	443	0
4	1.540110	162.247.241.14	172.126.0.20	TCP	66	443 > 62881 [ACK] Seq=1 Ack=1 Win=8 Len=0 TS...	1	8	0	NaN	443	62881	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...
9995	1.126845	172.125.1.137	172.125.0.68	TCP	60	0 > 11093 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	11093	1
9996	1.126854	172.125.1.137	172.125.0.68	TCP	60	0 > 11094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	11094	1
9997	1.126864	172.125.1.137	172.125.0.68	TCP	60	0 > 11095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	11095	1
9998	1.126895	172.125.1.137	172.125.0.68	TCP	60	0 > 11097 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	11097	1
9999	1.126896	172.125.1.137	172.125.0.68	TCP	60	0 > 11096 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	11096	1

Gambar 8. Tampilan dataset SYN

	Time	Source	Destination	Protocol	Length	Info	Seq	Win	Len	MSS	Src	Dst	attack
0	2.897145	157.240.208.54	172.125.0.2	TCP	66	443 > 56772 [ACK] Seq=1 Ack=71 Win=279 Len=0...	1	279	0	NaN	443	56772	0
1	3.174981	172.125.0.2	157.240.208.54	TCP	66	56772 > 443 [ACK] Seq=71 Ack=73 Win=2046 Len...	71	2046	0	NaN	56772	443	0
2	3.821955	172.125.0.2	142.251.12.19	TCP	54	60385 > 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0	1	2048	0	NaN	60385	443	0
3	3.872044	142.251.12.19	172.125.0.2	TCP	66	[TCP ACKed unseen segment] 443 > 60385 [ACK]...	1	295	0	NaN	443	60385	0
4	6.136700	157.240.208.16	172.125.0.2	TCP	66	443 > 56647 [ACK] Seq=1 Ack=33 Win=280 Len=0...	1	280	0	NaN	443	56647	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...
9995	1.014262	172.125.1.137	172.125.0.68	TCP	60	0 > 16409 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	16409	1
9996	1.014343	172.125.1.137	172.125.0.68	TCP	60	0 > 16410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	16410	1
9997	1.014405	172.125.1.137	172.125.0.68	TCP	60	0 > 16411 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	16411	1
9998	1.014474	172.125.1.137	172.125.0.68	TCP	60	0 > 16412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	16412	1
9999	1.014545	172.125.1.137	172.125.0.68	TCP	60	0 > 16413 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	1	0	0	NaN	0	16413	1

Gambar 9. Tampilan data UDP

B. Pembersihan Data

Dalam tahap pembersihan data untuk penelitian ini, beberapa langkah telah diambil untuk menghapus kolom-kolom yang dianggap tidak memiliki fitur yang signifikan untuk model SVM yang akan dikembangkan. Pertama, dataset dilakukan pengacakan dengan menggunakan metode 'sample' dari modul pandas. Pengacakan ini bertujuan untuk mengacak urutan data dalam dataset agar tidak ada bias atau urutan tertentu yang mempengaruhi pelatihan model [21].

Selanjutnya, dilakukan penghapusan beberapa kolom yang dianggap minim fitur yang relevan untuk model SVM. Kolom-kolom yang dihapus adalah '*Source*', '*Destination*', 'Info', 'MSS', dan '*Protocol*' [22]. Dengan menghapus kolom-kolom ini, penelitian ini fokus pada fitur-fitur lain yang dianggap lebih penting dalam deteksi serangan *flood* menggunakan SVM. Dan berikut adalah hasil dataset yang telah dibersihkan dan dapat diproses untuk pemodelan SVM.

	Time	Length	Seq	Win	Len	Src	Dst	attack
0	1399.563400	66	518	2816	0	53036	443	0
1	1462.031131	66	18809	425	0	443	63312	0
2	718.428321	66	1727	279	0	443	60407	0
3	1153.606361	54	609	2048	0	60563	443	0
4	0.991262	60	1	0	0	0	3803	1
...	...	...	...	...	...	...	...	...
26940	1413.970526	1514	1	64768	1448	443	53100	0
26941	854.670792	66	6607	73472	0	443	49800	0
26942	1.039951	60	1	0	0	0	6355	1
26943	361.245552	66	499	131072	0	65057	443	0
26944	1.007783	60	1	0	0	0	4693	1

Gambar 10. Tampilan dataset SYN yang telah dibersihkan

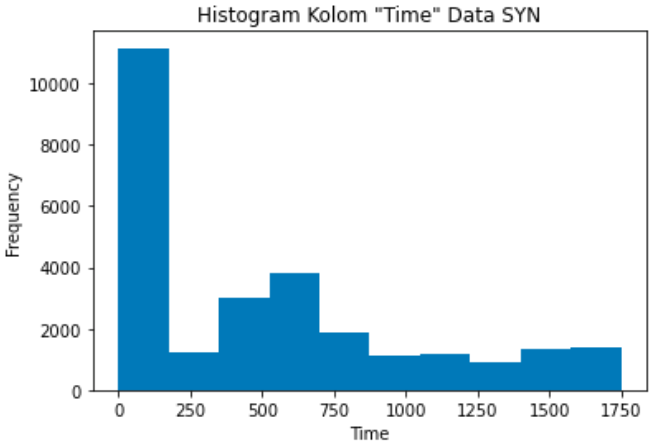
	Time	Length	Seq	Win	Len	Src	Dst	attack
0	0.855126	60	1	0	0	0	14858	1
1	74.328664	66	1022	10112	0	60765	443	0
2	93.308886	66	1022	7232	0	60765	443	0
3	53.969701	78	1022	4352	0	60765	443	0
4	0.735224	60	1	0	0	0	13694	1
...	...	...	...	...	...	...	...	...
20305	82.356081	66	1022	4416	0	60774	443	0
20306	0.614691	60	1	0	0	0	12524	1
20307	76.165218	66	1022	2944	0	60765	443	0
20308	88.826230	66	1	64768	0	443	60931	0
20309	0.346881	60	1	0	0	0	9892	1

Gambar 11. Tampilan dataset UDP yang telah dibersihkan

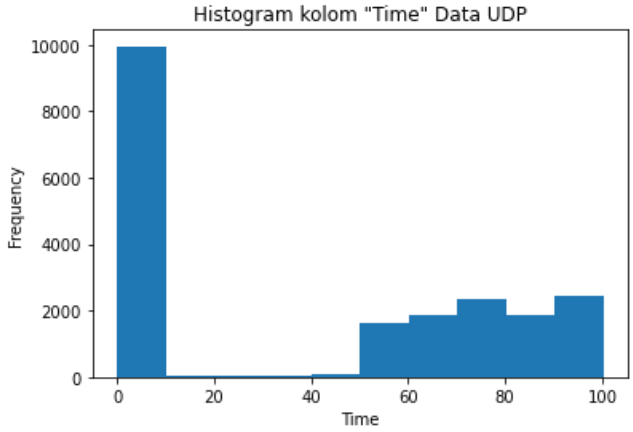
C. Eksplorasi Analisis Data

1. *Histogram* Kolom "*Time*"

Grafik histogram ini dapat memberikan gambaran visual tentang bagaimana data waktu dalam dataset terdistribusi. Hal ini dapat membantu peneliti dalam memahami pola atau kecenderungan waktu yang terkandung dalam dataset dan melihat apakah terdapat konsentrasi tertentu atau perubahan signifikan dalam rentang waktu tertentu [23].



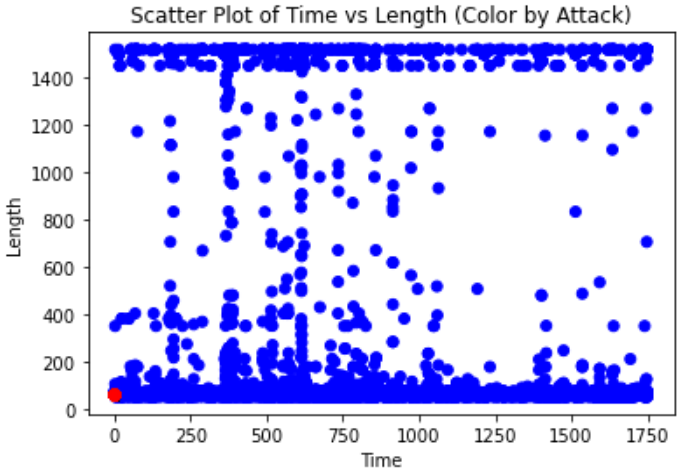
Gambar 12. Data SYN



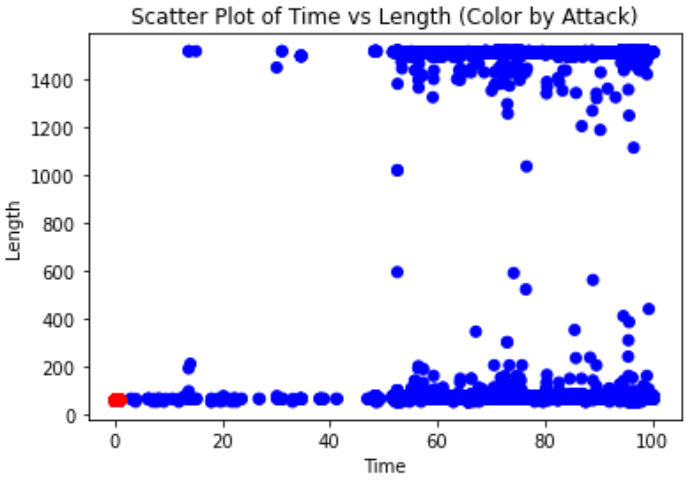
Gambar 13. Data UDP

2. Scatterplot kolom “Time” dan “Length”

Grafik *scatter plot* ini membantu visualisasi hubungan antara waktu dan panjang dalam dataset, serta memberikan pemahaman tentang bagaimana serangan dan data normal terdistribusi dalam konteks variabel tersebut. Hal ini dapat membantu peneliti dalam memperoleh wawasan mengenai pola, korelasi, atau perbedaan yang ada antara serangan dan data normal dalam hal waktu dan Panjang [24].



Gambar 14. Data SYN



Gambar 15. Data UDP

D. Pemodelan SVM

1. *Train & Test Splitting*

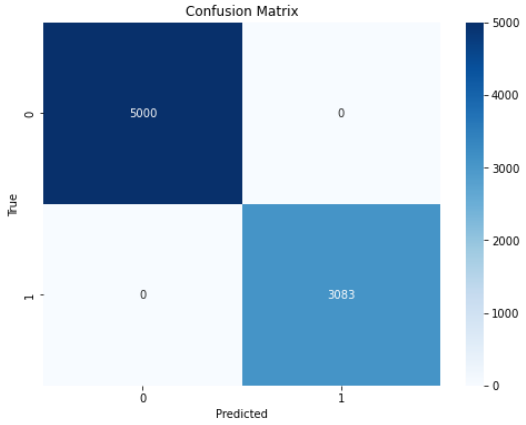
Salah satu tahap penting dalam pengembangan model SVM adalah membagi data menjadi subset pelatihan (*train*) dan subset pengujian (*test*) [25]. Hal ini dilakukan untuk mengukur kinerja model pada data yang tidak pernah dilihat sebelumnya dan memastikan bahwa model dapat generalisasi dengan baik. Pada tahap *Train & Test Splitting*, data yang telah dipersiapkan akan dibagi menjadi dua subset menggunakan metode *splitting*. Biasanya, sebagian besar data akan dialokasikan untuk subset pelatihan, sedangkan sebagian kecil akan dialokasikan untuk subset pengujian. Rasio pemisahan dapat bervariasi tergantung pada ukuran data dan kebutuhan spesifik penelitian.

Tujuan dari pembagian data ini adalah untuk melatih model SVM menggunakan subset pelatihan dan mengukur kinerja model pada subset pengujian yang merupakan representasi data baru. Dengan

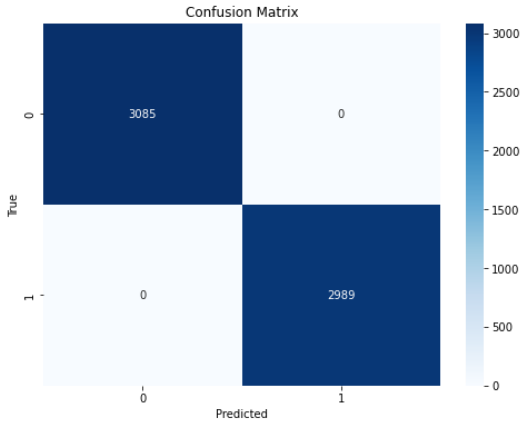
melakukan evaluasi pada subset pengujian, kita dapat mengukur sejauh mana model mampu menggeneralisasi pola dan perilaku dari data yang belum pernah dilihat sebelumnya.

2. *Confusion Matrix*

Confusion matrix adalah sebuah metode evaluasi yang umum digunakan dalam pemodelan klasifikasi untuk menggambarkan performa model dalam memprediksi kelas-kelas yang berbeda [26].



Gambar 16. Model SYN



Gambar 17. Model UDP

3. *Classification Report*

Classification report adalah sebuah laporan yang memberikan ringkasan tentang performa model klasifikasi berdasarkan hasil prediksinya. Laporan ini menyajikan beberapa metrik evaluasi yang umum digunakan, seperti akurasi (*accuracy*), presisi (*precision*), recall (*recall*), dan skor F1 (F1 *score*) [27].

	precision	recall	f1-score	support
0	1.00	1.00	1.00	5000
1	1.00	1.00	1.00	3083
accuracy			1.00	8083
macro avg	1.00	1.00	1.00	8083
weighted avg	1.00	1.00	1.00	8083

Gambar 18. Model SYN

	precision	recall	f1-score	support
0	1.00	1.00	1.00	3085
1	1.00	1.00	1.00	2989
accuracy			1.00	6074
macro avg	1.00	1.00	1.00	6074
weighted avg	1.00	1.00	1.00	6074

Gambar 19. Model UDP

4. *Cross Validation*

Cross-validation merupakan sebuah metode evaluasi yang umum digunakan untuk mengukur kinerja model secara objektif. Metode ini membagi dataset menjadi beberapa subset atau *"fold"* yang saling tumpang tindih. Dalam proses *cross-validation*, subset yang dipilih secara bergantian menjadi subset pengujian, sedangkan subset lainnya digunakan sebagai subset pelatihan. Dengan demikian, setiap subset akan berfungsi sebagai data pelatihan maupun pengujian pada suatu titik tertentu. Hal ini dilakukan untuk memastikan bahwa model dinilai berdasarkan kinerjanya pada berbagai kombinasi data.

Tujuan utama dari *cross-validation* adalah untuk memperoleh estimasi kinerja model yang lebih stabil dan mengurangi risiko *overfitting* atau *underfitting*. Dengan melakukan evaluasi pada beberapa subset, cross-validation dapat memberikan gambaran yang lebih umum tentang kemampuan model dalam menggeneralisasi pola dan perilaku data baru. Dan berikut adalah hasil skor cross-validation dari kedua model yang telah di training.

```
Cross-Validation Scores:
[1. 1. 1. 1. 1. 1.]
Average Score: 1.0
```

Gambar 20. Model SYN

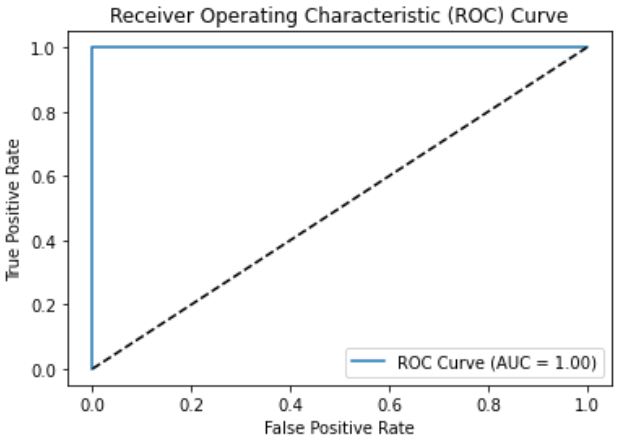
```
Cross-Validation Scores:
[1. 1. 1. 1. 1. 1.]
Average Score: 1.0
```

Gambar 21. Model UDP

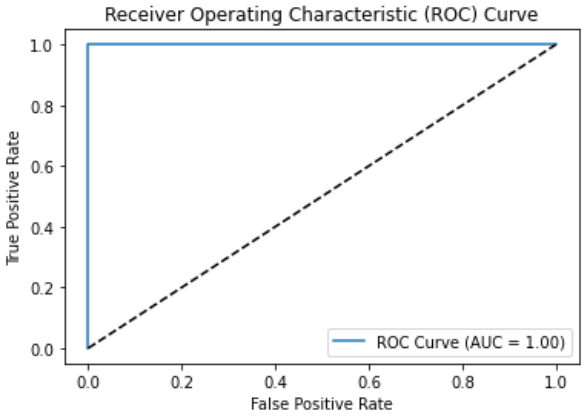
5. Kurva ROC

Kurva ROC (*Receiver Operating Characteristic*) adalah salah satu metode evaluasi yang digunakan dalam pemodelan klasifikasi untuk mengukur performa model dalam membedakan antara kelas positif dan negatif. Grafik Kurva ROC menggambarkan hubungan antara *False Positive Rate* (FPR) dan *True Positive Rate* (TPR) pada berbagai nilai *threshold*.

Dalam pembuatan Kurva ROC, model klasifikasi diuji dengan menggunakan berbagai threshold untuk mengklasifikasikan data. Setiap nilai *threshold* menghasilkan pasangan nilai FPR dan TPR yang berbeda. FPR mengukur sejauh mana model memprediksi keliru kelas negatif sebagai positif, sedangkan TPR mengukur sejauh mana model dapat mendeteksi dengan benar kasus positif.



Gambar 22. Model SYN



Gambar 23. Model UDP

Kesimpulan

Sesuai hasil penelitian analisis perbandingan serangan SYN *Flooding* dan UDP *Flooding* metode SVM maka di simpulkan sebagai berikut: Pada pengembangan model deteksi serangan flood menggunakan metode SVM, proses pengekstraksian data membantu dalam mempersiapkan data dengan memisahkan dan menyimpan informasi yang relevan dari kolom 'Info'. Hal ini memungkinkan analisis lebih lanjut dan memudahkan pemrosesan data sesuai dengan kebutuhan penelitian. Dalam pembersihan data, penghapusan kolom-kolom yang dianggap tidak memiliki fitur yang berarti seperti '*Source*', '*Destination*', 'Info', 'MSS', dan '*Protocol*' untuk pemodelan SVM dilakukan. Hal ini memfokuskan penelitian pada fitur-fitur yang dianggap lebih penting dalam deteksi serangan flood menggunakan SVM.

Confusion matrix memberikan informasi tentang performa model dalam memprediksi kelas-kelas yang berbeda. Dalam kasus yang diberikan, confusion matrix menunjukkan bahwa model memiliki tingkat akurasi yang tinggi dengan jumlah *False Positive* (FP) dan *False Negative* (FN) yang nol. Kurva ROC memberikan gambaran visual tentang kemampuan model dalam membedakan antara kelas positif dan negatif. Dalam contoh yang diberikan, nilai AUC-ROC adalah 1.00, menunjukkan bahwa model memiliki performa yang sangat baik dalam membedakan kelas-kelas dalam dataset.

Laporan evaluasi klasifikasi menyajikan metrik-metrik seperti *precision, recall*, dan *f1-score* untuk setiap kelas, serta nilai akurasi dan metrik evaluasi rata-rata. Dalam laporan tersebut, semua metrik evaluasi mencapai nilai maksimal, menunjukkan bahwa model memiliki performa yang sangat baik dan mampu mengklasifikasikan dengan benar data dalam kedua kelas. Dalam keseluruhan, hasil penelitian ini menunjukkan bahwa model SVM yang dikembangkan mampu memprediksi serangan flood dengan tingkat akurasi yang tinggi dan mampu mengklasifikasikan dengan benar antara data serangan dan data normal. Hasil ini memberikan dukungan bagi penggunaan metode SVM dalam deteksi serangan *flood* serta memberikan

wawasan yang penting untuk pengembangan lebih lanjut dalam bidang keamanan jaringan.

Bagi Peneliti selanjutnya, hasil penelitian ini bias digunakan sebagai bahan perbandingan, referensi untuk penelitian dan sebagai bahan pertimbangan untuk lebih memperdalam penelitian selanjutnya dengan menggunakan metode yang lain.

Daftar Pustaka

[1] P. L. L. Belluano and B. L. E. Panggabean, "The development of Web-based information system using quick UDP internet connection," *Ilk. J. Ilm.*, 2022, doi: 10.33096/ilkom.v14i3.1134.314-322.

[2] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[3] M. I. Suriansyah, I. Mulyana, and J. B. Sanger, "Compute functional analysis leveraging the IAAS private cloud computing service model in packstack development," 2021, *academia.edu*. doi: 10.33096/ilkom.v13i1.693.9-17.

[4] B. P. Firdaus and I. M. Suartana, "Implementasi Keamanan Jaringan Intrusion Detection/Prevention System Menggunakan Pfsense," 2020.

[5] H. Azis, P. Purnawansyah, and N. Alfiyyah, "Multiclass Classification on Nominal Value of Rupiah Banknotes Based on Image Processing," *Ilk. J. Ilm.*, 2024, doi: 10.33096/ilkom.v16i1.1784.87-99.

[6] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 1, pp. 43–52, 2021, doi: 10.30812/matrik.v21i1.1078.

[7] M. Fakhmi and L. M. Gultom, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis)," *Semin. Nas. Ind. dan Teknol.*, pp. 260–277, 2021.

[8] R. N. Wibowo, P. Sukarno, and E. M. Jadied, "Pendeteksian Serangan DoS Menggunakan Multiclassfier Pada NSL-KDD Dataset," 2018, *core.ac.uk*.

[9] M. Surahman, L. A. Abdillah, and Ferdiansyah, "Penerapan Metode SVM-Based Machine Learning Untuk Menganalisa Pengguna Data Trafik Internet (Studi Kasus Jaringan Internet Wlan Mahasiswa Bina Darma)," pp. 196–206, 2020.

[10] A. H. Hambali and S. Nurmiati, "Implementasi Intrusion Detection System (IDS) Pada Keamanan PC Server Terhadap Serangan Flooding Data," *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 28, no. 1, pp. 35–43, 2018, doi: 10.37277/stch.v28i1.267.

[11] K. Ramadhani, M. Yusuf, H. E. Wahanani, and J. T. Informatika, "Anomali Perubahan Traffic Jaringan Berbasis Cusum," 2013.

[12] D. Kurnia, "Analisis Pertahanan Website pada Protokol TCP dan UDP dari Serangan DDoS," 2019, *academia.edu*.

[13] Y. W. Sitorus, P. Sukarno, and S. Mandala, "Analisis Deteksi Malware Android menggunakan metode Support Vector Machine & Random Forest," *e-Proceeding Eng.*, vol. 8, no. 6, pp. 12500–12518, 2021.

[14] M. F. Fibrianda and A. Bhawiyuga, "Analisis perbandingan akurasi deteksi serangan pada jaringan komputer dengan metode naïve bayes dan support vector machine (SVM)," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, 2018.

[15] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, 2022.

[16] H. Darwis, R. Puspitasari, and D. Widyawati, "Comparative Analysis of Anxiety Disorder Classification Using Algorithm Naïve Bayes, Decision Tree and K-NN," *2025 19th Int. Conf. Ubiquitous Inf. Manag. Commun. IMCOM 2025*, 2025, doi: 10.1109/IMCOM64595.2025.10857485.

[17] D. Probst, "Aiming beyond slight increases in accuracy," *Nat. Rev. Chem.*, 2023, doi: 10.1038/s41570-023-00480-3.

[18] K. Roth, L. Pemula, and J. Zepeda, "Towards total recall in industrial anomaly detection," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2022, doi: 10.1109/CVPR52688.2022.01392.

[19] V. Paradigm, "Visual Paradigm Online," 2020.

[20] H. Darwis, R. Puspitasari, and W. Astuti, "A Deep Learning Approach for Improving Waste Classification Accuracy with ResNet50 Feature Extraction," *2025 19th Int. Conf. Ubiquitous Inf. Manag. Commun. IMCOM 2025*, 2025, doi: 10.1109/IMCOM64595.2025.10857536.

[21] H. Darwis, A. N. P. Pagala, and S. Anraeni, "Analysis of Public Sentiment about Childfree in Indonesia using Support Vector Machine Methods," *2025 19th Int. Conf. Ubiquitous Inf. Manag. Commun. IMCOM 2025*, 2025, doi: 10.1109/IMCOM64595.2025.10857551.

[22] A. R. Manga, A. N. Handayani, and H. W. Herwanto, "Analysis of the Ensemble Method Classifier's

Performance on Handwritten Arabic Characters Dataset," 2023, *researchgate.net*. doi: 10.33096/ilkom.v15i1.1357.186-192.

[23] P. Purnawansyah, A. P. Wibawa, and ..., "Comparative Study of Herbal Leaves Classification using Hybrid of GLCM-SVM and GLCM-CNN," *Ilk. J. ...*, 2023, doi: 10.33096/ilkom.v15i2.1759.382-389.

[24] F. Umar, H. Darwis, and P. Purnawansyah, "Fourier Descriptor on Lontara Scripts Handwriting Recognition," *Ilk. J. Ilm.*, 2023, doi: 10.33096/ilkom.v15i1.1040.193-200.

[25] W. Astuti, A. P. Wibawa, and H. Haviluddin, "DIET Classifier Model Analysis for Words Prediction in Academic Chatbot," *Ilk. J. Ilm.*, 2024, doi: 10.33096/ilkom.v16i1.1598.59-67.

[26] R. Mukarramah, D. Atmajaya, and L. B. Ilmawan, "Performance comparison of support vector machine (SVM) with linear kernel and polynomial kernel for multiclass sentiment analysis on twitter," 2021, *academia.edu*. doi: 10.33096/ilkom.v13i2.851.168-174.

[27] I. As'ad, M. A. Asis, H. M. Pakka, R. Mursalim, and Y. M. Noor, "K-Nearest Neighbors Analysis for Public Sentiment towards Implementation of Booster Vaccines in Indonesia," *Ilk. J. Ilm.*, vol. 15, no. 2, pp. 365–372, 2023, doi: 10.33096/ilkom.v15i2.1561.365-372.