JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Deteksi Serangan ICMP Flood Menggunakan Metode Random Forest Dan Support Vector Machine Dan Seleksi Fitur Forward Selection Pada Jaringan Internet Of Things (IoT)

Harid*, Kurniabudi, Abdul Harris

Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Dinamika Bangsa, Jambi, Indonesia
Email: [1,*]haridjambi@gmail.com, [2]kbudiz@yahoo.com, [3]abdulharris@unama.ac.id
Email Penulis Korespondensi: kbudiz@yahoo.com
Submitted **24-04-2025;** Accepted **23-07-2025;** Published **14-08-2025**

Abstrak

Perangkat IoT telah memainkan peran penting dalam mendorong serangan DDoS, dan merupakan ancaman pada jaringan IoT. Salah satunya yaitu serangan ICMP Flood. Untuk mengatasi serangan pada IoT salah satunya menggunakan Intrusion Detection System (IDS). Namun disisi lain IDS memiliki tantangan dalam menangani kompleksitas data berdimensi tinggi. Salah satu solusi yang disarankan untuk mengatasi masalah dimensi data adalah pemanfaatan teknik seleksi fitur. Teknik seleksi fitur Forward Selection digunakan untuk mengeliminasi fitur yang tidak relevan. Penelitian ini melakukan komparasi performa algoritma Random Forest dan SVM. Untuk keperluan eksperimen, penelitian ini menggunakan dataset CICIoT2023, yang mewakili trafik IoT. Penggunaan Forward Selection mendapatkan 11 fitur terpilih yang akan digunakan pada proses machine learning menggunakan metode Random Forest dan SVM. Seleksi fitur mempengaruhi waktu komputasi atau waktu proses, dikarenakan semakin sedikit fitur yang digunakan maka mampu mengurangi beban kerja sistem dalam melakukan proses klasifikasi. Hasil pengujian memperlihatkan penggunaan seleksi fitur meningkatkan kinerja random forest dengan accuracy sebesar 100%. Sedangkan untuk model SVM mendapatkan akurasi yang lebih baik dengan menggunakan seleksi fitur dengan accuracy tertinggi sebesar 99.4508% pada pengujian supplied test set.

Kata Kunci: Serangan DDoS; ICMP Flood; Machine Learning; Random Forest; SVM; Seleksi Fitur; Forward Selection

Abstract

IoT devices have played an important role in driving DDoS attacks, and are a threat to IoT networks. One of them is the ICMP Flood attack. To overcome attacks on IoT, one of them uses an Intrusion Detection System (IDS). However, on the other hand, IDS has challenges in handling the complexity of high-dimensional data. One of the suggested solutions to overcome the problem of data dimensions is the use of feature selection techniques. The Forward Selection feature selection technique is used to eliminate irrelevant features. This study compares the performance of the Random Forest and SVM algorithms. For experimental purposes, this study used the CICIoT2023 dataset, which represents IoT traffic. The use of Forward Selection obtained 11 selected features that will be used in the machine learning process using the Random Forest and SVM methods. Feature selection affects the computation time or processing time, because the fewer features used, the more the system's workload in carrying out the classification process. The test results show that the use of feature selection improves the performance of random forest with an accuracy of 100%. Meanwhile, the SVM model gets better accuracy by using feature selection with the highest accuracy of 99.4508% in the supplied test set test..

Keywords: DDoS Attack; ICMP Flood; Machine Learning; Random Forest; SVM; Feature Selection; Forward Selection

1. PENDAHULUAN

Internet of Things (IoT) telah muncul sebagai teknologi inovatif di mana jaringan perangkat fisik yang sering disebut sebagai benda atau objek pintar saling terhubung dalam skala global [1]. Penggunaan *Internet of Things* (IoT) semakin marak dan kini menjadi fitur umum dalam kehidupan sehari-hari [2]. *Internet of Things* (IoT) secara umum mencakup penggabungan perangkat berwujud yang mampu beroperasi, digerakkan, dan berkomunikasi secara mandiri untuk meningkatkan dan memfasilitasi penyediaan layanan baru di berbagai domain [3].

Terlepas dari evolusi *Internet of Things* (IoT) yang cepat, IoT tetap menjadi target yang menarik dan rentan bagi pengguna dan penyerang yang berniat jahat karena langkah-langkah keamanannya yang rendah dan kebutuhan daya komputasi yang tinggi di tingkat perangkat [4]. Belakangan ini, ada tren yang di mana perangkat IoT telah memainkan peran penting dalam mendorong serangan DDoS. Hal ini tetap menjadi ancaman yang belum berkurang [5].

Distributed Denial-of-Service (DDoS) adalah metode serangan yang membanjiri server dan sistem jaringan dengan membanjiri mereka dengan jumlah paket atau permintaan yang berlebihan, sehingga menyebabkan mereka tidak berfungsi atau *crash*. Berbagai bentuk serangan DDoS salah satunya yaitu *ICMP Flood* [6]. *Internet Control Message Protocol (ICMP)* terutama digunakan untuk tujuan diagnostik, pelaporan kesalahan atau menanyakan server mana pun. Dalam serangan *ICMP flood*, penyerang membanjiri sumber daya yang dituju dengan paket *ICMP echo request* (*ping*), serta paket ICMP yang besar dan jenis ICMP lainnya, untuk memenuhi dan menghambat infrastruktur jaringan korban [7],[8].

Oleh karena itu, dibutuhkan suatu sistem yang dapat digunakan untuk melindungi jaringan. *Intrusion Detection System* (IDS) merupakan salah satu sistem untuk memantau dan menganalisis jaringan dan sistem komputer untuk mengetahui adanya potensi akses yang tidak sah atau kerentanan [9]. *Intrusion Detection System* (IDS) digunakan sebagai teknologi untuk mengidentifikasi dan mengenali serangan siber. *Intrusion Detection System* (IDS) umumnya menggunakan pengklasifikasi *machine learning* untuk mengkategorikan berbagai jenis serangan [1]. Seperti penelitian [10], menggunakan metode KNN, SVM, dan *Random Forest* serta pada dataset CIC_IDS_2017 mendapatkan tingkat akurasi yaitu 95%, 92%, dan 96.66% ketika diberikan parameter yang optimal. Kemudian penelitian [11], menggunakan

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

metode algoritma C5.0 untuk mendeteksi DDoS dengan tingkat akurasi yang cukup tinggi sebesar 98.38%. Selanjutnya pada penelitian [12], menggunakan kombinasi antara 3 jenis seleksi fitur yaitu *filter*, *wrapper*, dan *embedded* dengan metode KNN, SVM, ANN, dan NB dengan akurasi tertinggi diraih metode KNN dengan akurasi 98.30% dengan menggunakan jenis seleksi fitur *wrapper* dengan 6 fitur terpilih. Sedangkan pada penelitian [13], menggunakan metode *Naïve Bayes*, *Random Forest*, DT, MLP, dan KNN di mana metode *Random Forest* (RF) mendapatkan akurasi tertinggi yaitu 98.9%.

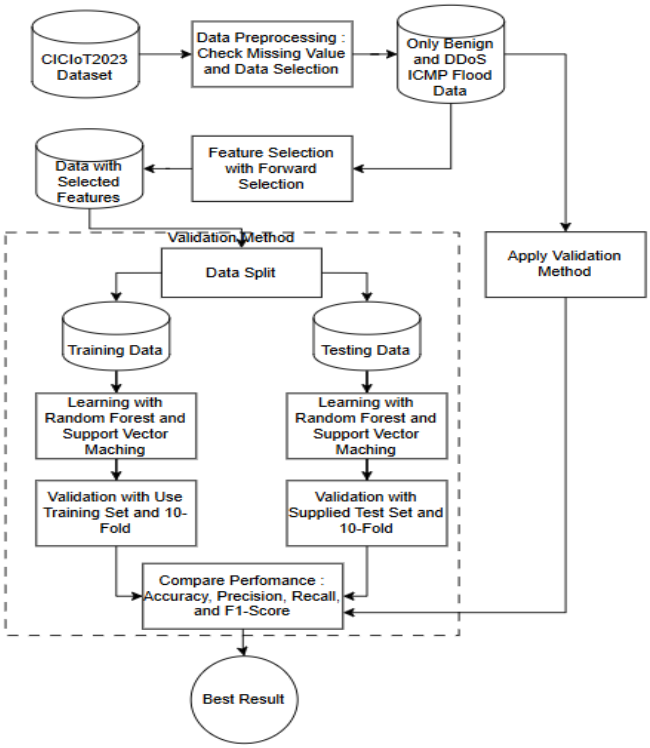
Di sisi lain, kemajuan teknologi, protokol dan strategi serangan pada jaringan data telah memunculkan kompleksitas baru dalam penelitian *Intrusion Detection System*. Jaringan mengalami arus lalu lintas yang besar, sehingga menghasilkan data yang rumit dengan dimensi data yang sangat tinggi. Salah satu solusi yang disarankan untuk mengatasi masalah dimensi data adalah pemanfaatan teknik seleksi fitur [14]. Teknik seleksi fitur melibatkan eliminasi variabel yang membantu dalam meningkatkan pemahaman data, mengurangi kebutuhan komputasi, mengatasi tantangan yang ditimbulkan oleh data berdimensi tinggi, dan pada akhirnya meningkatkan kemampuan prediksi model [15]. *Forward Selection* (FS) merupakan salah satu seleksi fitur metode *wrapper*. *Forward Selection* (FS) dipilih karena efektivitasnya yang telah terbukti dalam mengidentifikasi subset fitur yang optimal [12].

Berdasarkan penelitian sebelumnya, penulis menyarankan untuk menggunakan pendekatan *hybrid* dari metode seleksi fitur dan algoritma klasifikasi untuk mengembangkan sistem deteksi dengan performa yang optimal. Dari sekian banyak algoritma klasifikasi yang telah dikembangkan, algoritma *Random Forest* menggunakan pendekatan acak untuk membangun ensemble kolektif pohon keputusan [16]. Salah satu manfaat menggunakan *RF* adalah kemampuannya untuk memproses dataset dengan jumlah fitur yang banyak secara efektif sekaligus mengurangi risiko *overfitting*. *RF* juga telah menunjukkan keefektifannya dalam mengidentifikasi anomali dalam jaringan komputer [17]. *Support Vector Machine* (SVM) adalah model serbaguna yang menggunakan teknik analisis klasifikasi dan regresi untuk mendefinisikan dan menganalisis pola yang diamati dalam data [12]. SVM menonjol dari algoritma klasifikasi lainnya karena penekanannya pada memaksimalkan margin [18]. Pada penelitian ini metode *RF* dan *SVM* yang digabungkan dengan *Forward Selection* sebagai seleksi fitur digunakan untuk mendapatkan akurasi yang lebih optimal dalam mendeteksi serangan.

2. METODOLOGI PENELITIAN

2.1 Rancangan Eksperimen

Penelitian ini memiliki penekanan besar pada tahap eksperimen untuk mengetahui pengaruh *Forward Selection* dalam meningkatkan nilai evaluasi kinerja klasifikasi machine learning. Eksperimen ini melibatkan analisis menyeluruh terhadap beberapa komponen, termasuk penggunaan teknik seleksi fitur, alokasi set data untuk pelatihan dan pengujian, serta desain dan pengaturan metode pembelajaran mesin dan variabel terkait. Untuk memastikan hasil yang optimal untuk penelitian ini, serangkaian langkah penting yang terstruktur dirancang untuk mengembangkan model yang sesuai dan menghindari penyimpangan dari tujuan yang diinginkan. Tahapan eksperimen pada penelitian ini disajikan gambar 1.



Gambar 1. Rancangan Eksperimen

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Berdasarkan gambar 1, dapat dijelaskan tahapan eksperimen sebagai berikut :

a. *Data Preprocessing*. Pada tahap ini, proses data cleaning akan dilakukan untuk meminimalkan data yang tidak konsisten atau tidak relevan sebelum klasifikasi model menggunakan tools weka. Hal ini mencakup check missing values pada data dan penghapusan jenis label selain *BenignTraffic* dan *DDoS-ICMP Flood*.
b. *Feature Selection*. Pada tahap ini dilakukan proses seleksi fitur untuk memilih fitur yang paling relevan untuk digunakan dalam deteksi serangan menggunakan *RF* dan *SVM*. Teknik seleksi fitur yang digunakan adalah *Forward Selection*.
c. *Data Split*. Pada tahap ini, *dataset* akan dipisahkan menjadi dua *subset*, dengan alokasi 80% *training* dan 20% *testing*. Tabel 1 dan tabel 2 menyajikan *dataset* untuk *training* dan untuk *testing*.

Tabel 1. Jumlah Label Pada *Data Training* (80%)

No	Jenis Serangan	Jumlah
1.	*BenignTraffic*	8455
2.	*DDoS-ICMP_Flood*	55635
	Total	64090

Tabel 2. Jumlah Label Pada *Data Testing* (20%)

No	Jenis Serangan	Jumlah
1.	*BenignTraffic*	2153
2.	*DDoS-ICMP_Flood*	13869
	Total	16022

d. Klasifikasi menggunakan tools weka dengan metode algoritma *RF* dan *SVM*. Pelatihan model menggunakan use training set dan 10-fold cross validation dan pengujian model menggunakan supplied test set.
e. Setelah tahap klasifikasi dan validasi selesai, akan dilakukan penilaian komparatif untuk mengevaluasi kinerja algoritma random forest dan SVM. Penilaian performa dilakukan menggunakan confusion matrix untuk menghitung metrik accuracy, precision, recall, dan f1-score.

2.2 *Dataset*

Pada penelitian ini akan menggunakan *dataset* data publik yaitu CIC_IoT_2023 dari *kaggle* yang dapat diakses pada laman https://www.kaggle.com/datasets/madhavmalhotra/unb-cic-iot-dataset. *Dataset* ini berisi total 46.686.579 entri *data*, dengan berbagai macam 33 jenis serangan yang tercatat di dalamnya [19]. Trafik serangan pada dataset ini dikategorikan ke dalam tujuh kelompok yang berbeda, seperti *DDoS, DoS, Reconnaissance, Web-based, Brute Force, Spoofing,* dan *Mirai* [20].

2.3 *Forward Selection*

Selanjutnya yaitu menggunakan seleksi fitur *forward selection*. Seleksi fitur melibatkan proses pemilihan subset fitur dari set asli berdasarkan kriteria tertentu, dengan tujuan untuk mengidentifikasi fitur yang paling relevan dalam kumpulan data. Hal ini terlibat dalam kompresi skala pemrosesan data dengan menghilangkan fitur yang berlebihan dan tidak relevan [21]. Adapun persamaan dari *forward selection* yang ditunjukkan pada persamaan 1.

$$K + (K-1) + \cdots + (K-k+1) = \frac{K(K+1) - (K-k)(K-k+1)}{2} = \frac{k(2K-k+1)}{2} \quad (1)$$

Persamaan di atas menggambarkan bahwa kompleksitas algoritma meningkat secara kuadratik dengan jumlah fitur yang dipilih yang dilambangkan sebagai k. Ketika memilih subset dari k fitur, fitur berikutnya, fk+1 yang belum termasuk dalam subset Sk dipilih dengan cara yang memaksimalkan performa set yang dihasilkan. Pada setiap iterasi, algoritma hanya mempertimbangkan K-k fitur, dengan K mewakili jumlah total fitur [22].

2.4 *Random Forest*

Random forest terdiri dari banyak *decision tree* [16]. Proses klasifikasi dalam *random forest* dimulai dengan memecah data sampel awal ke dalam beberapa *decision tree*. Salah satu manfaat menggunakan *random forest* adalah kemampuannya untuk memproses dataset dengan jumlah fitur yang banyak secara efektif sekaligus mengurangi risiko *overfitting* [17]. Adapun persamaan dari *random forest* yang ditunjukkan pada persamaan 2.

$$mg(X,Y) = av_b P(T_1(X) = Y) - \max_{j \neq Y} av_b (T_1(X) = j) \quad (2)$$

Diberikan pengklasifikasi ensemble T1(X), T2(X), T3(X) dengan data latih acak yang diperoleh dari vektor X dan Y. *Margin* digunakan untuk mengevaluasi nilai rata-rata *voting* dari X dan Y. Semakin besar nilai *margin*, semakin akurat klasifikasi tersebut.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

2.5 *Support Vector Machine* (SVM)

Support Vector Machine (SVM) adalah model serbaguna yang menggunakan teknik analisis klasifikasi dan regresi untuk mendefinisikan dan menganalisis pola yang diamati dalam data [12]. Konsep dasar SVM berpusat pada pengoptimalan pemisahan antara dua kelas dengan memaksimalkan jarak margin [23]. Adapun persamaan dari SVM yang ditunjukkan pada persamaan 3.

$$W.X + b = +1 \text{ dan } W.X + b = -1 \quad (3)$$

Persamaan untuk dua kelas, dilambangkan sebagai +1 dan -1, berada di margin dengan vektor pendukung yang ditempatkan sesuai dengan yang ditunjukkan. Vektor W mewakili vektor normal ke *hyperplane*. yaitu arah tegak lurus terhadap *hyperplane*. Parameter b dalam persamaan mewakili offset atau jarak hyperplane dari titik asal sepanjang vektor normal w.

3. HASIL DAN PEMBAHASAN

Bagian ini memberikan analisis dari hasil tentang eksperimen yang telah dilakukan, meliputi hasil klasifikasi model tanpa fitur, proses seleksi fitur, hasil klasifikasi model setelah seleksi fitur, dan penilaian performa model *random forest* dan SVM dalam mendeteksi serangan *DDoS ICMP Flood*. Dalam penelitian ini, tiga pendekatan mode klasifikasi yang berbeda akan diterapkan pada *dataset*, menggunakan *use training set* dan menerapkan *10-Fold Cross Validation* untuk *data training*, serta menggunakan *supplied test set* yang disediakan untuk *data testing*. Penelitian ini akan menggunakan satu set data CSV tunggal, yaitu *ICMP Part 79*, yang diekstraksi dari kumpulan data CIC IoT 2023 untuk analisis.

3.1 Klasifikasi *Random Forest* Tanpa Seleksi Fitur

Proses ini menyajikan hasil deteksi serangan melalui pemanfaatan metode *random forest*. Klasifikasi algoritma *random forest* akan menggunakan semua fitur yang tersedia pada *dataset*. Proses pelatihan model melibatkan penggunaan *use training set* dan menerapkan metode *10-fold cross validation*, sedangkan pengujian model menggunakan *supplied test set* yang telah disediakan. Hasil klasifikasi dari model *random forest* tanpa seleksi fitur disajikan pada tabel 3.

Tabel 3. Hasil Klasifikasi *Random Forest* Tanpa Seleksi Fitur

Mode Klasifikasi	*Accuracy*	*Precision*	*Recall*	*F1-Score*
Use Training Set	100%	1.000	1.000	1.000
10-Fold Cross Validation	99.9984%	1.000	1.000	1.000
Supplied Test Set	100%	1.000	1.000	1.000

Hasil dari teknik klasifikasi *random forest*, yang melibatkan 3 prosedur klasifikasi terpisah dan tidak menyertakan seleksi fitur, disajikan pada tabel 3. Hasil eksperimen menunjukkan bahwa *accuracy* tertinggi sebesar 100% dicapai oleh metode *random forest* dengan mode klasifikasi *use training set* dan *supplied test set*. Klasifikasi *10-fold cross validation* menghasilkan nilai terendah dibandingkan dengan klasifikasi *use training set* dan *supplied test set*, mencapai *accuracy* 99,9984%. Pada setiap klasifikasi, nilai *precision*, *recall*, dan *f1-score* masing-masing mencapai nilai sempurna yaitu 1.000.

3.2 Klasifikasi SVM Tanpa Seleksi Fitur

Proses ini menyajikan hasil deteksi serangan yang dicapai melalui pemanfaatan metode *Support Vector Machine* (SVM). Klasifikasi *Support Vector Machine* (SVM) akan menggunakan semua fitur yang tersedia pada *dataset*. Proses pelatihan model melibatkan penggunaan *use training set* dan teknik *10-fold cross validation*, sementara pengujian model memerlukan penggunaan *supplied test set* yang disediakan. Tabel 4 menyajikan hasil kategorisasi model *Support Vector Machine* (SVM) tanpa adanya seleksi fitur.

Tabel 4. Hasil Klasifikasi SVM Tanpa Seleksi Fitur

Mode Klasifikasi	*Accuracy*	*Precision*	*Recall*	*F1-Score*
Use Training Set	98.0995%	0.981	0.981	0.981
10-Fold Cross Validation	98.0668%	0.980	0.981	0.980
Supplied Test Set	98.1151%	0.981	0.981	0.981

Tabel 4 menyajikan hasil klasifikasi SVM yang dihasilkan dari tiga proses klasifikasi, di mana tidak ada seleksi fitur yang digunakan. Hasil eksperimen menunjukkan bahwa *accuracy* tertinggi sebesar 98,1151% dalam klasifikasi *supplied test set* yang disediakan dicapai oleh model SVM. Klasifikasi *10-fold cross validation* menunjukkan nilai terendah dibandingkan dengan klasifikasi *use training set* dan *supplied test set*, mencapai *accuracy* 98,0668%. Klasifikasi *use training set* dan *supplied test set* mencapai nilai tertinggi untuk *precision*, *recall*, dan *f1-score*, dengan nilai masing-masing 0.981, 0.981, dan 0.981.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

3.3 Seleksi Fitur *Forward Selection*

Pada penelitian ini, penulis menggunakan metode seleksi fitur *forward selection* menggunakan metode *search method BestFirst Direction Forward* serta *Attribute Elevator CfsSubsetEval*. *Forward Selection* (FS) dipilih karena efektivitasnya yang telah terbukti dalam mengidentifikasi subset fitur yang optimal [12]. Dalam eksperimen, implementasi teknik seleksi fitur menggunakan perangkat lunak Weka 3.8.1. Pada *forward selection*, performa sistem dievaluasi dengan penambahan fitur baru setiap proses iterasi. Satu-satunya fitur yang dimasukkan dalam pemilihan untuk fungsi objek adalah fitur yang menunjukkan performa tertinggi. Berikut ini adalah spesifikasi perintah pemilihan fitur di Weka.

Started weka.attributeSelection.CfsSubsetEval
Command: weka.attributeSelection.CfsSubsetEval -s "weka.attributeSelection.BestFirst -P 1 -D 1 -N 5" -P 1 -E 1
Filter command: weka.filters.supervised.attribute.AttributeSelection -E "weka.attributeSelection.CfsSubsetEval -P 1 -E 1" -S "weka.attributeSelection.BestFirst -P 1 -D 1 -N 5"
Meta-classifier command: weka.classifiers.meta.AttributeSelectedClassifier -E "weka.attributeSelection.CfsSubsetEval -P 1 -E 1" -S "weka.attributeSelection.BestFirst -P 1 -D 1 -N 5" -W weka.classifiers.trees.J48 -- -C 0.25 -M 2
Finished weka.attributeSelection.CfsSubsetEval weka.attributeSelection.BestFirst

Hasil seleksi fitur *forward selection* disajikan pada tabel 5.

Tabel 5. Hasil Seleksi Fitur *Forward Selection*

Teknik Seleksi	Total	Fitur Terpilih
Forward Selection (CfsSubsetEval + BestFirst Direction Forward)	11	*flow_duration, Protocol Type, fin_count, urg_count,* TCP, ICMP, *Tot size,* IAT, *Number, Magnitue, Weight*.

3.4 Klasifikasi *Random Forest* Menggunakan Seleksi Fitur

Proses ini menyajikan hasil deteksi serangan menggunakan metode *random forest*. Klasifikasi model *random forest* akan menggunakan fitur yang terpilih dari seleksi fitur *forward selection* setiap *dataset*. Setelah proses seleksi akan dilakukan pelatihan model menggunakan *use training set* dan *10-fold cross validation*. Pengujian model menggunakan *supplied test set*. Tabel 6 menyajikan hasil klasifikasi model *random forest* menggunakan seleksi fitur

Tabel 6. Hasil Klasifikasi *Random Forest* Menggunakan Seleksi Fitur

Mode Klasifikasi	*Accuracy*	*Precision*	*Recall*	*F1-Score*
Use Training Set	100%	1.000	1.000	1.000
10-Fold Cross Validation	100%	1.000	1.000	1.000
Supplied Test Set	100%	1.000	1.000	1.000

Tabel 6 menyajikan hasil klasifikasi *random forest* menggunakan seleksi fitur dengan 3 (tiga) proses klasifikasi. Hasil menunjukkan *random forest* mendapatkan *accuracy* tertinggi 100% yang didapatkan pada setiap klasifikasi. Klasifikasi *10-fold cross validation* mendapatkan kenaikan nilai accuracy menjadi 100% dibandingkan pada klasifikasi tanpa fitur yang mendapatkan *accuracy* 99.9984%. Untuk nilai *precision*, *recall*, dan *f1-score* mendapatkan nilai 1.000 pada setiap klasifikasi.

3.5 Klasifikasi SVM Menggunakan Seleksi Fitur

Proses ini menyajikan hasil deteksi serangan menggunakan metode SVM. Klasifikasi model SVM akan menggunakan fitur yang terpilih dari seleksi fitur *forward selection*. Setelah proses seleksi akan dilakukan pelatihan model menggunakan *use training set* dan *10-fold cross validation*. Pengujian model menggunakan supplied test set. Tabel 7 menyajikan hasil klasifikasi model SVM menggunakan seleksi fitur.

Tabel 7. Hasil Klasifikasi SVM Menggunakan Seleksi Fitur

Mode Klasifikasi	*Accuracy*	*Precision*	*Recall*	*F1-Score*
Use Training Set	98.9452%	0.989	0.989	0.989
10-Fold Cross Validation	99.2011%	0.992	0.992	0.992
Supplied Test Set	99.4508%	0.994	0.995	0.995

Pada tabel 7 disajikan hasil klasifikasi SVM menggunakan seleksi fitur dengan 3 (tiga) proses klasifikasi. Hasil menunjukkan SVM mendapatkan *accuracy* tertinggi 99.4508% yang didapatkan pada klasifikasi *supplied test set*. Semua mode klasifikasi mendapatkan kenaikan *accuracy* yang sebelumnya 98.0995% untuk *training set,* 98.0668% untuk *10-Fold Cross Validation,* dan 98.1151% untuk *supplied test set* menjadi 98.9452% untuk *training set,* 99.2011% untuk *10-Fold Cross Validation,* dan 99.4508% untuk *supplied test set*. Untuk nilai *precision*, *recall*, dan *f1-score* mendapatkan nilai tertinggi masing-masing 0.994, 0.995, dan 0.995 yang diraih pada klasifikasi *use training set* dan *supplied test set*.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Nilai *precision*, *recall*, dan *f1-score* juga mendapatkan kenaikan dibandingkan dengan hasil yang didapatkan tanpa seleksi fitur.

3.6 Komparasi Performa *Random Forest* dan SVM

Selanjutnya, efisiensi algoritma dalam mengidentifikasi serangan *DDoS ICMP Flood* dinilai. Penilaian ini melibatkan analisis komparatif algoritma *random forest* dan *Support Vector Machine* (SVM) dalam hal performa. Tujuan dari analisis ini adalah untuk menentukan metode yang paling efektif dalam mendeteksi serangan *DDoS ICMP Flood* berdasarkan keakuratan hasil yang diperoleh. Untuk menilai kinerja, nilai *accuracy*, *precision*, *recall*, *f-measure/f1-score*, dan waktu performa model digunakan untuk proses komparasi. Tabel 8 memberikan komparasi tingkat *accuracy* dari *random forest* dan SVM dalam melakukan prediksi.

Tabel 8. Komparasi *Accuracy Random Forest* dan SVM

Algoritma Klasifikasi	Mode Klasifikasi	*Accuracy*
Pengujian 1 *Random Forest*	*Use Training Set*	100%
	10-Fold Cross Validation	99.9984%
	Supplied Test Set	100%
Pengujian 2 *Random Forest + Forward Selection*	*Use Training Set*	100%
	10-Fold Cross Validation	100%
	Supplied Test Set	100%
Pengujian 3 SVM	*Use Training Set*	98.0995%
	10-Fold Cross Validation	98.0668%
	Supplied Test Set	98.1151%
Pengujian 4 SVM + *Forward Selection*	*Use Training Set*	98.9452%
	10-Fold Cross Validation	99.2011%
	Supplied Test Set	99.4508%

Pada tabel 8 disajikan 4 hasil pengujian *random forest* dan SVM tanpa dan menggunakan seleksi fitur dengan 3 (tiga) proses klasifikasi. Hasil menunjukkan pengujian 2 yaitu *random forest* menggunakan *forward selection* mendapatkan *accuracy* tertinggi 100% yang didapatkan pada setiap klasifikasi. Klasifikasi *10-fold cross validation* mendapatkan kenaikan nilai accuracy menjadi 100% dibandingkan pada klasifikasi tanpa fitur yang mendapatkan *accuracy* 99.9984%. Untuk nilai *precision*, *recall*, dan *f1-score* mendapatkan nilai 1.000 pada setiap klasifikasi. Selanjutnya pada tabel 9 menyajikan komparasi *precision random forest* dan SVM.

Tabel 9. Komparasi *Precision Random Forest* dan SVM

Algoritma Klasifikasi	Mode Klasifikasi	*Precision*
Pengujian 1 *Random Forest*	*Use Training Set*	1.000
	10-Fold Cross Validation	1.000
	Supplied Test Set	1.000
Pengujian 2 *Random Forest + Forward Selection*	*Use Training Set*	1.000
	10-Fold Cross Validation	1.000
	Supplied Test Set	1.000
Pengujian 3 SVM	*Use Training Set*	0.981
	10-Fold Cross Validation	0.980
	Supplied Test Set	0.981
Pengujian 4 SVM + *Forward Selection*	*Use Training Set*	0.989
	10-Fold Cross Validation	0.992
	Supplied Test Set	0.994

Tabel 9 menampilkan hasil dari pengujian *random forest* dan SVM pada kondisi fitur yang tidak terseleksi dan terseleksi dengan menggunakan tiga proses klasifikasi. Hasil menunjukkan bahwa pada pengujian 1 dan 2, khususnya metode *random forest* tanpa dan dengan seleksi fitur mendapatkan *precision* sebesar 1.000 yang dicapai pada setiap klasifikasi. Selanjutnya, perbandingan antara nilai *recall* dari *random forest* dan SVM disajikan pada tabel 10.

Tabel 10. Komparasi *Recall Random Forest* dan SVM

Algoritma Klasifikasi	Mode Klasifikasi	*Recall*
Pengujian 1 *Random Forest*	*Use Training Set*	1.000
	10-Fold Cross Validation	1.000
	Supplied Test Set	1.000
Pengujian 2 *Random Forest + Forward Selection*	*Use Training Set*	1.000
	10-Fold Cross Validation	1.000
	Supplied Test Set	1.000
Pengujian 3	*Use Training Set*	0.981

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 4, Agustus 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i4.8554
Hal 454-461
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

SVM	*10-Fold Cross Validation*	0.981
	Supplied Test Set	0.981
Pengujian 4 SVM + *Forward Selection*	*Use Training Set*	0.989
	10-Fold Cross Validation	0.992
	Supplied Test Set	0.995

Tabel 10 menampilkan hasil pengujian dari empat model *random forest* dan SVM, baik dengan dan tanpa seleksi fitur, menggunakan tiga prosedur klasifikasi. Hasil menunjukkan bahwa pada pengujian 1 dan pengujian 2, di mana *random forest* digunakan dengan dan tanpa seleksi fitur, mendapatkan nilai *recall* 1.000 yang dicapai pada setiap klasifikasi. Selain itu, tabel 11 mengilustrasikan perbandingan *F-Measure/F1-Score* antara *random forest* dan SVM.

Tabel 11. Komparasi *F1-Score Random Forest* dan SVM

Algoritma Klasifikasi	Mode Klasifikasi	*F1-Score*
Pengujian 1 *Random Forest*	*Use Training Set*	1.000
	10-Fold Cross Validation	1.000
	Supplied Test Set	1.000
Pengujian 2 *Random Forest + Forward Selection*	*Use Training Set*	1.000
	10-Fold Cross Validation	1.000
	Supplied Test Set	1.000
Pengujian 3 SVM	*Use Training Set*	0.981
	10-Fold Cross Validation	0.981
	Supplied Test Set	0.981
Pengujian 4 SVM + *Forward Selection*	*Use Training Set*	0.989
	10-Fold Cross Validation	0.992
	Supplied Test Set	0.995

Tabel 11 menunjukkan hasil pengujian untuk empat model *random forest* dan SVM, baik dengan maupun tanpa seleksi fitur, menggunakan tiga proses klasifikasi. Hasil menunjukkan bahwa pengujian 1 dan pengujian 2, khususnya metode *random forest* tanpa dan dengan seleksi fitur, mencapai nilai *f1-score* sebesar 1.000 di setiap klasifikasi. Kemudian, Tabel 12 menyajikan perbandingan waktu performa antara model *random forest* dan SVM.

Tabel 12. Komparasi Waktu Performa Model *Random Forest* dan SVM

Algoritma Klasifikasi	Mode Klasifikasi	Tanpa Seleksi Fitur	Seleksi Fitur
Random Forest	*Use Training Set*	8.05 detik	4.46 detik
	10-*Fold Cross Validation*	7.81 detik	4.49 detik
	Supplied Test Set	7.02 detik	5.94 detik
SVM	*Use Training Set*	5.79 detik	4.24 detik
	10-*Fold Cross Validation*	5.78 detik	5.5 detik
	Supplied Test Set	5.64 detik	2.95 detik

Pada tabel 12 disajikan waktu performa model *random forest* dan SVM tanpa dan menggunakan seleksi fitur dengan 3 (tiga) proses klasifikasi. Hasil menunjukkan bahwa algoritma *random forest* memiliki waktu proses sedikit lebih lama dibandingkan dengan model *support vector machine*. Pemanfaatan seleksi fitur dapat mengurangi waktu pemrosesan karena berkurangnya jumlah fitur yang diklasifikasikan.

4. KESIMPULAN

Penelitian ini berhasil menerapkan metode *Random Forest* dan *Support Vector Machine* (SVM) dalam deteksi serangan *ICMP Flood*. Tindakan ini dilaksanakan untuk menggunakan kemampuan klasifikasi data yang efektif dari kedua algoritma tersebut, dengan tujuan meningkatkan *accuracy* dan keandalan sistem dalam mendeteksi serta mencegah serangan *ICMP Flood* yang dapat mengancam keamanan jaringan IoT. Pemanfaatan *Forward Selection* dalam proses seleksi fitur menghasilkan 11 fitur yang terpilih untuk digunakan dalam implementasi *machine learning* dengan menggunakan metode *Random Forest* dan *Support Vector Machine* (SVM). Hasil pengujian menggunakan metode seleksi fitur *Forward Selection* menunjukkan bahwa terdapat peningkatan *accuracy* dalam klasifikasi model *Random Forest* dan SVM. Dari hasil pengujian diperlihatkan pula bahwa banyaknya fitur memiliki dampak signifikan terhadap waktu komputasi atau waktu proses. Hal ini disebabkan oleh fakta bahwa semakin sedikit fitur yang digunakan maka mampu mengurangi beban kerja sistem dalam melakukan proses klasifikasi. Berdasarkan hasil implementasi algoritma *Random Forest* dan SVM dalam mendeteksi serangan *ICMP Flood* menunjukkan bahwa metode klasifikasi *Random Forest* memiliki performa optimal yang lebih baik daripada metode klasifikasi SVM. Dari 4 pengujian yang dilakukan, pengujian 2 dengan penerapan seleksi fitur menunjukkan hasil yang paling optimal karena model *Random Forest* berhasil mencapai akurasi 100% pada setiap mode klasifikasi. Pada model SVM, akurasi yang lebih tinggi dapat dicapai dengan melakukan

seleksi fitur, dimana akurasi tertinggi yang diperoleh adalah sebesar 99.4508% saat diuji menggunakan *supplied test set* yang disediakan.

REFERENCES

[1] M. Roopak, G. Y. Tian, and Chambers Jonathon, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," in 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas: IEEE, 2020, pp. 562–567. doi: 10.1109/CCWC47524.2020.9031206.

[2] S. S. Bhunia and M. Gurusamy, "Dynamic Attack Detection and Mitigation in IoT using SDN," in 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne: IEEE, 2017. doi: 10.1109/ATNAC.2017.8215418.

[3] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating IoT Device based DDoS Attacks using Blockchain," in CRYBLOCK 2018 - Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018: The 16th Annual International Conference on Mobile Systems, Applications, and Services, Association for Computing Machinery, Inc, Jun. 2018, pp. 71–76. doi: 10.1145/3211933.3211946.

[4] J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, "A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN," IEEE Internet Things J, vol. 9, no. 5, pp. 3612–3630, Mar. 2022, doi: 10.1109/JIOT.2021.3098029.

[5] D. K. Sharma et al., "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks," Ad Hoc Networks, vol. 121, Oct. 2021, doi: 10.1016/j.adhoc.2021.102603.

[6] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 6, no. 1, pp. 172–180, 2022, [Online]. Available: http://j-ptiik.ub.ac.id

[7] Harshita, "Detection and Prevention of ICMP Flood DDOS Attack," International Journal of New Technology and Research (IJNTR), vol. 3, no. 3, pp. 63–69, 2017, [Online]. Available: www.ijntr.org

[8] V. Chauhan and P. Saini, "ICMP flood attacks: A vulnerability analysis," in Advances in Intelligent Systems and Computing, Springer Verlag, 2018, pp. 261–268. doi: 10.1007/978-981-10-8536-9_26.

[9] E. Hodo et al., "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System," in International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet: [IEEE], 2016. doi: 10.1109/ISNCC.2016.7746067.

[10] M. Aamir and S. M. Ali Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 4, pp. 436–446, May 2021, doi: 10.1016/j.jksuci.2019.02.003.

[11] E. O. Nasution and A. Basuki, "Implementasi Algoritme C5.0 Untuk Klasifikasi Serangan DDoS," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 5, no. 1, pp. 389–395, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[12] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," Sustainability (Switzerland), vol. 12, no. 3, pp. 1–16, Feb. 2020, doi: 10.3390/su12031035.

[13] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," Computer Networks, vol. 158, pp. 35–45, Jul. 2019, doi: 10.1016/j.comnet.2019.04.027.

[14] K. Kurniabudi, A. Harris, and V. Veronica, "Komparasi Performa Tree-Based Classifier Untuk Deteksi Anomali Pada Data Berdimensi Tinggi dan Tidak Seimbang," JURNAL MEDIA INFORMATIKA BUDIDARMA, vol. 6, no. 1, p. 370, Jan. 2022, doi: 10.30865/mib.v6i1.3473.

[15] K. Kurniabudi, A. Harris, and A. E. Mintaria, "Komparasi Information Gain, Gain Ratio, CFs-Bestfirst dan CFs-PSO Search Terhadap Performa Deteksi Anomali," JURNAL MEDIA INFORMATIKA BUDIDARMA, vol. 5, no. 1, p. 332, Jan. 2021, doi: 10.30865/mib.v5i1.2258.

[16] Y. Chen, J. Hou, Q. Li, and H. Long, "DDoS Attack Detection Based on Random Forest," in International Conference on Progress in Informatics and Computing (PIC), Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 328–334. doi: 10.1109/PIC50277.2020.9350788.

[17] L. Ikhwanul Uzlah, R. Adi Saputra, and Isnawaty, "DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST," Jurnal Mahasiswa Teknik Informatika, vol. 8, no. 3, pp. 2787–2793, Jun. 2024, doi: https://doi.org/10.36040/jati.v8i3.8891.

[18] S. Sivaranjani, S. Ananya, J. Aravinth, and R. Karthika, "Diabetes Prediction using Machine Learning Algorithms with Feature Selection and Dimensionality Reduction," in 7th International Conference on Advanced Computing and Communication Systems (ICACCS)), Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 141–146. doi: 10.1109/ICACCS51430.2021.9441935.

[19] S. M. Tseng, Y. Q. Wang, and Y. C. Wang, "Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset," Future Internet, vol. 16, no. 8, pp. 1–25, Aug. 2024, doi: 10.3390/fi16080284.

[20] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," Sensors, vol. 23, no. 13, pp. 1–26, Jul. 2023, doi: 10.3390/s23135941.

[21] J. Cai, J. Luo, S. Wang, and S. Yang, "Feature selection in machine learning: A new perspective," Neurocomputing, vol. 300, pp. 70–79, Jul. 2018, doi: 10.1016/j.neucom.2017.11.077.

[22] F. Kamalov, S. Elnaffarr, A. Cherukuri, and A. Jonnalagadda, "Forward feature selection: empirical analysis," Journal of Intelligent Systems and Internet of Things, vol. 11, no. 1, pp. 44–54, 2024, doi: 10.54216/JISIoT.110105.

[23] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," in Amity International Conference on Artificial Intelligence (AICAI), Institute of Electrical and Electronics Engineers, 2019, pp. 870–875. doi: https://doi.org/10.1109/AICAI.2019.8701238.