Bridge: Jurnal Publikasi Sistem Informasi dan Telekomunikasi
Volume 4, Nomor 3, Agustus 2026
e-ISSN: 3046-725X; p-ISSN: 3046-7268, Hal. 192-204
DOI: https://doi.org/10.62951/bridge.v4i3.1011
Tersedia: https://journal.aptii.or.id/index.php/Bridge

Analisis dan Mitigasi Serangan *Distributed Denial of Service (DDoS)* Menggunakan Metode *Machine Learning* Berbasis Deteksi Anomali

Wulan Andryani[1*], Iwan Suhardi[2], Abd. Muis Mappalotteng[3]
[1-3]Jurusan Teknik Informatika dan Komputer, Fakultas Teknik, Universitas Negeri Makassar, Indonesia
**Penulis Korespondensi: wulanandryani0@gmail.com*

Abstract. *Distributed Denial of Service (DDoS) attacks, particularly Volumetric DDoS, pose a serious threat to network infrastructure by disrupting service availability through traffic flooding. Signature-based defense approaches are often less effective in detecting new and adaptive attack patterns. This study aims to implement a Random Forest algorithm based on anomaly detection and evaluate the effectiveness of automated mitigation in a Software-Defined Networking (SDN) architecture in real time. The study employed a quantitative experiment based on network simulation. The model was trained using the CICIDS2017 dataset with stratified random sampling of 300,000 data rows. Network traffic features were normalized using Min-Max Scaler to optimize classification performance. The validated model was exported in pickle (.pkl) format and integrated into the Ryu Controller as a hybrid defense mechanism combined with a volumetric threshold. The simulation was conducted using the Mininet emulator with a single-switch topology and an ICMP Flood/Ping Flood attack scenario. The results showed that Random Forest achieved an accuracy of 99.80% during test data evaluation. Real-time testing in the SDN environment achieved a mitigation success rate of 99.79%, reducing attack traffic from 22,358 packets to only 48 packets reaching the target through automatic injection of DROP rules based on OFPFlowMod messages. The integration of machine learning and SDN effectively provides protection against Volumetric DDoS attacks with minimal mitigation response delay.*

Keywords: *Anomaly Detection; Attack Mitigation; DDoS Attacks; Machine Learning; Network Security.*

Abstrak. Serangan Distributed Denial of Service (DDoS), khususnya Volumetric DDoS, merupakan ancaman serius terhadap infrastruktur jaringan karena dapat mengganggu ketersediaan layanan melalui banjir trafik. Pendekatan pertahanan berbasis signature sering kurang efektif dalam mengenali pola serangan baru dan adaptif. Penelitian ini bertujuan mengimplementasikan algoritma Random Forest berbasis deteksi anomali serta mengevaluasi efektivitas mitigasi otomatis pada arsitektur Software-Defined Networking (SDN) secara real-time. Penelitian menggunakan eksperimen kuantitatif berbasis simulasi jaringan. Model dilatih menggunakan dataset CICIDS2017 dengan stratified random sampling sebanyak 300.000 baris data. Fitur trafik jaringan dinormalisasi menggunakan Min-Max Scaler untuk mengoptimalkan klasifikasi. Model tervalidasi diekspor dalam format pickle (.pkl) dan diintegrasikan ke Ryu Controller sebagai pertahanan hibrida bersama mekanisme volumetric threshold. Simulasi dilakukan pada emulator Mininet dengan topologi single-switch menggunakan skenario ICMP Flood/Ping Flood. Hasil menunjukkan Random Forest mencapai akurasi 99,80% pada pengujian data. Pengujian real-time pada SDN menghasilkan tingkat keberhasilan mitigasi 99,79%, dengan trafik serangan berkurang dari 22.358 paket menjadi 48 paket yang mencapai target melalui injeksi aturan DROP otomatis berbasis pesan OFPFlowMod. Integrasi machine learning dan SDN terbukti efektif memberikan perlindungan terhadap Volumetric DDoS dengan respons mitigasi minimal.

Kata Kunci: Deteksi Anomali; Keamanan Jaringan; Mitigasi Serangan; Pembelajaran Mesin; Serangan *DDoS.*

1. LATAR BELAKANG

Kemajuan teknologi informasi dan komunikasi telah memberikan dampak besar bagi kehidupan manusia dalam berbagai aspek, seperti bisnis, pendidikan, kesehatan, dan pemerintahan. Dengan berkembangnya infrastruktur jaringan internet, akses terhadap informasi dan layanan daring menjadi semakin mudah. Namun, di balik berbagai manfaat tersebut, ancaman keamanan siber juga semakin meningkat. Salah satu ancaman terbesar dalam dunia siber adalah *serangan Distributed Denial of Service* (DDoS) (Makbull Rizki, 2022). Serangan ini bertujuan untuk melumpuhkan layanan dengan membanjiri lalu lintas jaringan

Naskah Masuk: 30 Juni 2026; Revisi: 25 Juli 2026; Diterima: 27 Agustus 2026; Terbit: 31 Agustus 2026

menggunakan sejumlah besar permintaan palsu sehingga sumber daya sistem menjadi terbebani dan tidak dapat diakses oleh pengguna yang sah

DDoS merupakan bentuk serangan yang berkembang pesat seiring dengan meningkatnya jumlah perangkat yang terhubung ke internet. Perangkat yang telah dikompromikan oleh peretas, dikenal sebagai botnet, digunakan untuk meluncurkan serangan secara simultan ke target tertentu (Salsabilah et al., 2024). Serangan ini dapat menargetkan berbagai sektor, termasuk pemerintahan, perbankan, *e-commerce*, dan layanan *cloud computing*. Dalam beberapa kasus, serangan DDoS telah menyebabkan kerugian finansial yang besar serta menurunkan kepercayaan pengguna terhadap layanan yang disediakan. Berdasarkan laporan Cloudflare Threat Report (2024) frekuensi dan kompleksitas serangan DDoS meningkat secara signifikan dalam beberapa tahun terakhir. Serangan DDoS modern tidak hanya mengandalkan peningkatan volume lalu lintas, tetapi juga mengeksploitasi kelemahan dalam protokol jaringan dan sistem aplikasi. Hal ini membuat metode deteksi berbasis tanda tangan (*signature-based detection*) menjadi kurang efektif dalam menangani serangan yang terus berkembang dan beradaptasi. Pendekatan tradisional dalam mendeteksi serangan DDoS sering kali menggunakan firewall, sistem pencegahan intrusi (*Intrusion Prevention System*), dan mekanisme pemfilteran lalu lintas. Namun, metode-metode ini memiliki keterbatasan dalam mengenali pola serangan baru yang belum pernah terjadi sebelumnya. Oleh karena itu, dibutuhkan pendekatan yang lebih canggih dan adaptif untuk mendeteksi dan mengatasi serangan DDoS.

Teknologi kecerdasan buatan, khususnya *machine learning*, menawarkan solusi yang lebih efisien dalam mendeteksi anomali dalam lalu lintas jaringan. Dengan menggunakan teknik *machine learning*, sistem dapat mengidentifikasi pola lalu lintas yang mencurigakan berdasarkan data historis. Pendekatan ini memungkinkan sistem untuk mendeteksi serangan secara dini tanpa bergantung pada tanda tangan serangan yang sudah dikenal. Beberapa algoritma *machine learning* yang umum digunakan dalam deteksi DDoS mencakup *Random Forest*, *Support Vector Machine (SVM)*, *Neural Networks*, dan pendekatan berbasis *deep learning* seperti *Convolutional Neural Networks (CNN)* dan *Recurrent Neural Networks (RNN)*.

Selain itu, metode deteksi berbasis anomali memainkan peran penting dalam mengidentifikasi serangan DDoS yang tidak terdeteksi oleh metode berbasis tanda tangan. Teknik ini bekerja dengan membandingkan pola lalu lintas jaringan yang sedang terjadi dengan pola normal yang telah dipelajari sebelumnya. Jika terdapat penyimpangan yang signifikan, sistem akan mengklasifikasikannya sebagai anomali dan mengeluarkan peringatan. Dengan

demikian, metode deteksi berbasis anomali dapat mendeteksi serangan baru yang belum pernah terjadi sebelumnya dan mengurangi kemungkinan serangan yang berhasil melewati sistem keamanan tradisional.

Selain deteksi, langkah mitigasi juga merupakan aspek krusial dalam menangani serangan DDoS. Setelah serangan terdeteksi, diperlukan strategi mitigasi yang cepat dan efektif untuk mengurangi dampaknya. Beberapa teknik mitigasi yang umum digunakan meliputi pemfilteran paket, redistribusi lalu lintas, dan penggunaan layanan *content delivery network (CDN)* untuk menyebarkan beban lalu lintas. Selain itu, penerapan sistem otomatis yang dapat menyesuaikan kebijakan keamanan berdasarkan kondisi jaringan saat ini juga menjadi langkah penting dalam mengatasi serangan DDoS.

Dalam penelitian ini, akan dikembangkan model deteksi serangan DDoS berbasis *machine learning* dengan pendekatan deteksi anomali. Model ini bertujuan untuk meningkatkan akurasi dalam mendeteksi serangan, mengurangi tingkat *false positive*, serta mengoptimalkan strategi mitigasi agar serangan dapat ditangani secara lebih efisien. Dengan adanya sistem deteksi dan mitigasi yang lebih canggih, diharapkan dapat meningkatkan keamanan infrastruktur jaringan serta mengurangi dampak serangan DDoS terhadap layanan daring.

Penelitian ini berfokus pada pemanfaatan tunggal algoritma *Random Forest* yang diintegrasikan ke dalam arsitektur hibrida bersama kontroler Ryu. Pemilihan algoritma *Random Forest* didasarkan pada kemampuan performanya yang stabil dan efisien dalam melakukan klasifikasi biner maupun multikelas pada lalu lintas data jaringan berskala besar. Evaluasi terhadap efektivitas model dilakukan dengan menggunakan metrik seperti akurasi, presisi, recall, dan *F1-score*. Selain itu, dataset yang digunakan dalam penelitian ini akan berasal dari sumber publik maupun hasil simulasi serangan yang dilakukan di lingkungan laboratorium.

Dengan semakin kompleksnya serangan DDoS, kebutuhan akan sistem keamanan yang adaptif dan berbasis kecerdasan buatan menjadi semakin mendesak. Oleh karena itu, penelitian ini berfokus pada implementasi dan evaluasi algoritma *Random Forest* berbasis deteksi anomali pada arsitektur *Software-Defined Networking* (SDN). Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan teknologi keamanan jaringan serta menjadi referensi bagi akademisi dan praktisi dalam meningkatkan pertahanan terhadap ancaman siber.

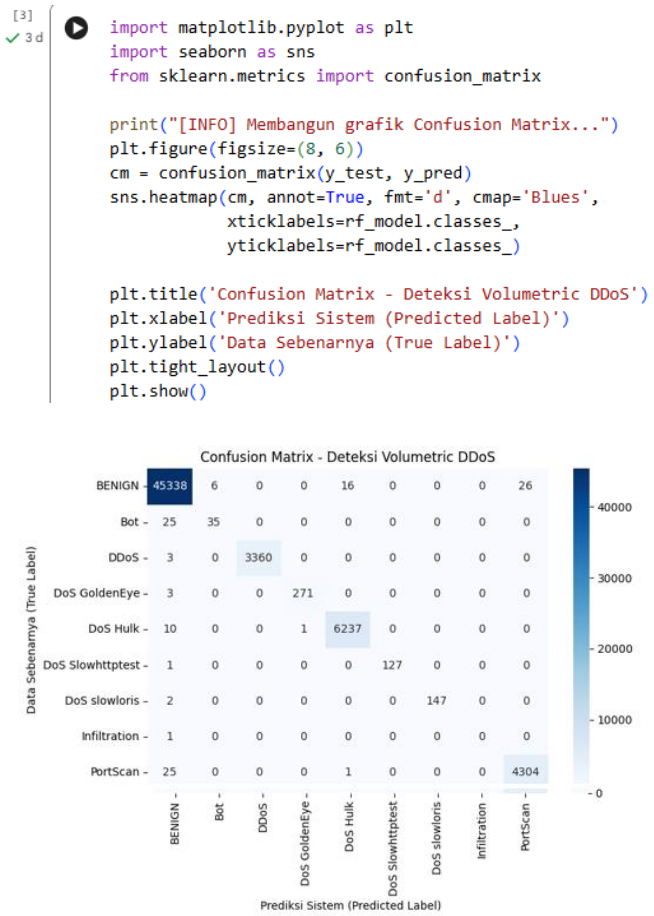
2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan desain eksperimen laboratorium berbasis simulasi jaringan yang dilaksanakan di Laboratorium Keamanan Jaringan, Program Studi Teknik Komputer, Universitas Negeri Makassar, pada Januari–Juni 2026. Sistem dikembangkan pada arsitektur *Software-Defined Networking* (SDN) menggunakan emulator Mininet, Ryu Controller, Open vSwitch, OpenFlow 1.3, dan Python. Dataset CICIDS2017 digunakan sebagai sumber data utama untuk membangun model deteksi anomali berbasis *Random Forest*. Pada tahap prapemrosesan, dataset direduksi secara proporsional menggunakan *stratified random sampling* menjadi 300.000 baris data, kemudian nilai *Infinity* dikonversi menjadi *NaN* dan data yang tidak lengkap dieliminasi, dilanjutkan dengan pemisahan fitur dan target serta normalisasi menggunakan *Min-Max Scaler* pada rentang 0–1. Data yang telah diproses dibagi menjadi 80% data pelatihan dan 20% data pengujian, sedangkan kestabilan model dievaluasi menggunakan *5-fold cross-validation*. Kinerja klasifikasi dinilai menggunakan *confusion matrix* dengan parameter *accuracy, precision, recall,* dan *F1-score*. Model *Random Forest* yang telah tervalidasi kemudian diserialisasi dalam format .pkl bersama parameter normalisasi dan diintegrasikan ke dalam Ryu Controller menggunakan arsitektur *Hybrid Threshold + Random Forest*, dengan *volumetric threshold* sebagai *fast-path* dan model *machine learning* sebagai *slow-path*. Pemantauan statistik trafik dilakukan setiap 3 detik dengan batas trafik normal ≤100 *packets per second* (PPS) dan batas anomali kritis ≥500 PPS. Pengujian dinamis dilakukan pada Mininet dengan menyimulasikan serangan *Volumetric DDoS* berupa ICMP/*Ping Flood*, sedangkan efektivitas mitigasi dievaluasi berdasarkan jumlah paket yang berhasil diblokir melalui aturan *DROP*, persentase keberhasilan mitigasi, paket yang lolos, ketersediaan koneksi pengguna sah, serta waktu respons Ryu Controller dalam mengeksekusi pesan OFPFlowMod.

3. HASIL DAN PEMBAHASAN

Pengujian dilakukan pada lingkungan simulasi *Software-Defined Networking* (SDN) menggunakan Mininet dan Ryu Controller. Hasil penelitian dibagi menjadi dua tahap utama, yaitu evaluasi model *Random Forest* pada dataset CICIDS2017 dan pengujian mitigasi serangan *Volumetric DDoS* secara *real-time*. Setelah proses *stratified random sampling*, pembersihan data, dan normalisasi menggunakan *Min-Max Scaler*, dataset yang digunakan terdiri atas 239.753 data latih dan 59.939 data uji. Model *Random Forest* dengan 50 pohon keputusan (*n_estimators* = 50) menghasilkan akurasi global sebesar 99,80%. Pada kelas utama, yaitu trafik normal (*BENIGN*) dan DDoS, nilai *precision, recall,* dan *F1-score* mencapai sekitar

1,00. Dari 45.386 sampel *BENIGN*, sebanyak 45.338 berhasil diklasifikasikan dengan benar, sedangkan pada 3.363 sampel DDoS, sebanyak 3.360 berhasil dideteksi dan hanya tiga sampel menjadi *false negative*. Performa model terhadap kelas minoritas lebih rendah; kelas *Bot* memiliki *recall* 0,58 dengan 25 dari 60 sampel tidak terdeteksi, sedangkan satu sampel *Infiltration* gagal dikenali. Kondisi ini menghasilkan *macro average F1-score* sebesar 0,85, meskipun *weighted average F1-score* mencapai 1,00 akibat dominasi kelas mayoritas.



Gambar 1. *Confusion Matrix* Pengujian Model *Random Forest.*

Gambar *confusion matrix* perlu dipertahankan karena menunjukkan bahwa akurasi global yang tinggi terutama berasal dari performa model pada kelas mayoritas sekaligus memperlihatkan keterbatasan klasifikasi pada kelas minoritas. Dengan demikian, gambar ini lebih informatif untuk artikel dibandingkan tangkapan layar proses prapemrosesan atau pelatihan model.

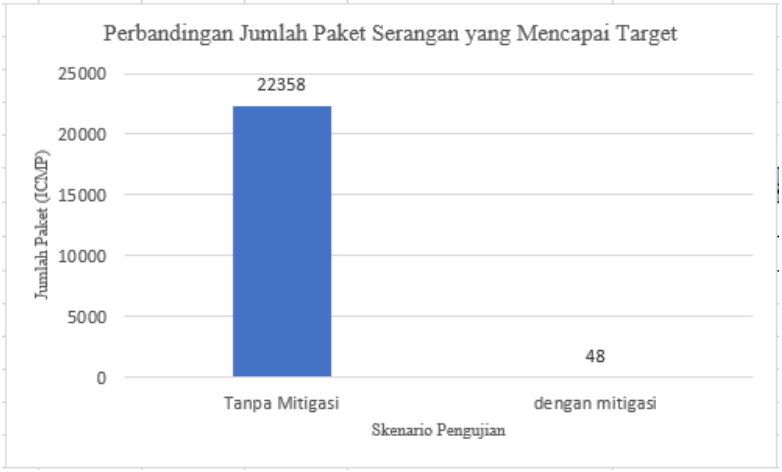
Model yang telah tervalidasi kemudian diintegrasikan ke dalam Ryu Controller sebagai bagian dari arsitektur *Hybrid Threshold + Random Forest*. Pengujian dinamis dilakukan menggunakan serangan *ICMP Flood* dari host h1 (10.0.0.1) menuju host target h2 (10.0.0.2). Saat serangan berlangsung, sistem mencatat lonjakan trafik hingga beberapa ribu paket per

detik dan secara otomatis menerapkan *DROP rule* melalui pesan OFPFlowMod. Dari 22.358 paket ICMP yang dikirimkan penyerang, sebanyak 22.310 paket (99,79%) berhasil diblokir dan hanya 48 paket (0,21%) yang mencapai target pada fase awal sebelum aturan mitigasi diterapkan sepenuhnya. Setelah mitigasi aktif, trafik kembali berada pada kondisi normal tanpa terjadi *crash* atau gangguan layanan.

Tabel 1. Ringkasan Hasil Mitigasi Serangan DDoS.

Status trafik	Jumlah paket	Persentase	Hasil
Berhasil dimitigasi (*DROP*)	22.310	99,79%	Paket serangan diblokir melalui OFPFlowMod
Lolos pada fase awal	48	0,21%	Paket lolos sebelum aturan mitigasi aktif sepenuhnya
Total paket serangan	22.358	100,00%	Total trafik ICMP Flood

Hasil tersebut menunjukkan penurunan jumlah paket serangan yang mencapai target dari 22.358 paket menjadi hanya 48 paket setelah mitigasi diterapkan.



Gambar 2. Perbandingan Jumlah Paket Serangan yang Mencapai Target Sebelum dan Setelah Mitigasi.

Gambar perbandingan ini sebaiknya dipertahankan karena menyajikan hasil utama mitigasi secara langsung dan mudah dipahami, yaitu penurunan trafik serangan dari 22.358 menjadi 48 paket.

Pengujian lanjutan menunjukkan bahwa mitigasi bersifat selektif. Host penyerang h1 mengalami 100% *packet loss* ketika mencoba mengakses kembali h2, sedangkan pengguna legal h3 tetap dapat berkomunikasi dengan h2 dengan 0% *packet loss* dan rata-rata *round-trip time* sebesar 11,446 ms. Hasil tersebut menunjukkan bahwa aturan *DROP* mengisolasi sumber serangan tanpa memutus koneksi pengguna sah.

Dari aspek responsivitas, Ryu Controller melakukan pemantauan statistik trafik pada interval 3 detik. Setelah ambang batas anomali teridentifikasi, proses inferensi *Random Forest*

dan pemicu instruksi mitigasi OFPFlowMod membutuhkan waktu sekitar 15–45 ms. Meskipun demikian, sistem masih menggunakan *threshold* statis sebesar 100 dan 500 PPS serta durasi pemblokiran tetap selama 15 detik. Evaluasi juga masih terbatas pada lingkungan Mininet dan satu skenario serangan utama berupa *ICMP/Ping Flood*, sehingga hasil belum dapat digeneralisasikan langsung pada infrastruktur fisik maupun jenis serangan seperti UDP Flood, SYN Flood, dan serangan lapisan aplikasi.

Pembahasan

Penelitian ini menghasilkan akurasi global model *Random Forest* sebesar 99,80% setelah pelatihan menggunakan dataset CICIDS2017. Dari 59.939 data uji, performa klasifikasi sangat baik pada trafik *BENIGN* dan DDoS, dengan nilai *precision*, *recall*, dan *F1-score* yang dibulatkan menjadi 1,00. Pada kelas DDoS, 3.360 dari 3.363 sampel berhasil diklasifikasikan dengan benar dan hanya tiga sampel menjadi *false negative*. Hasil tersebut menunjukkan kemampuan diskriminasi yang tinggi terhadap pola trafik utama yang menjadi sasaran penelitian. Performa ini sejalan dengan kecenderungan hasil penelitian berbasis *Random Forest* pada deteksi DDoS. Ekawijana et al. (2024) memperoleh akurasi 98% pada deteksi DDoS di jaringan SDN menggunakan *Random Forest*, sedangkan Ferdiansyah et al. (2024) mendapatkan akurasi 97%, lebih tinggi dibandingkan *Naive Bayes* dan *LinearSVC*. Sari et al. (2025) juga mendapatkan akurasi *Random Forest* sebesar 99,95% pada CICDDoS2019.

Hasil penelitian nasional lain memperkuat pemilihan *Random Forest* sebagai algoritma klasifikasi trafik DDoS. Bhaskara et al. (2022) menggabungkan *Random Forest* dengan *correlation-based feature selection* dan memperoleh *precision* rata-rata 99,784%. Penelitian tersebut juga menunjukkan perbedaan performa yang besar antara model dengan dan tanpa seleksi fitur, sehingga konfigurasi fitur dan parameter model dapat memberi pengaruh substansial terhadap hasil klasifikasi. Prayogi et al. (2024), menggunakan CICIDS2017 seperti penelitian ini, memperoleh *precision* 97,8%, *recall* 98,2%, dan *F1-score* 98,0% dengan memasukkan karakteristik perilaku trafik seperti *inter-arrival time*, ukuran segmen rata-rata, dan jumlah paket per detik. Hasil penelitian ini yang mencapai akurasi 99,80% berada pada rentang performa tinggi yang juga ditemukan pada kedua penelitian tersebut.

Temuan serupa terdapat pada penelitian internasional. Sawah et al. (2025) mengevaluasi beberapa algoritma pada DDoS-SDN dan melaporkan *Random Forest* sebagai model terbaik dengan akurasi 99,99% setelah penerapan *feature selection*, *grid search*, dan *5-fold cross-validation*. Liu et al. (2023) juga mendapatkan *Random Forest* sebagai klasifikator terbaik dibandingkan SVM, k-NN, *Decision Tree*, dan XGBoost setelah pembersihan data, normalisasi, dan optimasi fitur. Mahar et al. (2026) mengembangkan model hibrida RF-

XGBoost pada *testbed* SDN berbasis Ryu dan Open vSwitch dengan akurasi 99,36%. Rentang hasil tersebut memperlihatkan bahwa akurasi 99,80% pada penelitian ini dapat dikategorikan kompetitif dibandingkan penelitian terbaru, meskipun perbandingan langsung tetap harus mempertimbangkan perbedaan dataset, distribusi kelas, fitur, topologi jaringan, dan konfigurasi pengujian (Liu et al., 2023; Mahar et al., 2026; Sawah et al., 2025).

Tahap prapemrosesan turut menentukan stabilitas model. Penelitian ini menggunakan *stratified random sampling* untuk mereduksi dataset menjadi 300.000 baris secara proporsional, mengubah nilai *Infinity* menjadi *NaN*, mengeliminasi data tidak lengkap, serta menerapkan *MinMaxScaler* pada rentang 0–1. Pendekatan tersebut sesuai dengan penelitian Liu et al. (2023), yang melakukan pembersihan dan normalisasi sebelum seleksi fitur dan klasifikasi. Sawah et al. (2025) bahkan menunjukkan bahwa kombinasi eliminasi fitur dan optimasi hiperparameter meningkatkan performa RF hingga 99,99%. Bhaskara et al. (2022) juga mendapatkan peningkatan besar ketika CFS diterapkan pada *Random Forest*. Temuan tersebut menunjukkan bahwa akurasi tinggi tidak hanya ditentukan oleh algoritma, tetapi juga oleh kualitas data masukan dan representasi fitur (Bhaskara et al., 2022; Liu et al., 2023; Sawah et al., 2025).

Walaupun akurasi global penelitian ini mencapai 99,80%, evaluasi *confusion matrix* memperlihatkan performa yang tidak seragam pada seluruh kelas. Kelas *Bot* hanya mencapai *recall* 0,58; dari 60 sampel, 25 diklasifikasikan sebagai *BENIGN*. Model juga tidak mampu mengenali satu sampel *Infiltration*. Kondisi ini menurunkan *macro average F1-score* menjadi 0,85, sementara *weighted average F1-score* tetap mencapai 1,00 karena dominasi kelas mayoritas. Temuan ini penting karena akurasi global yang sangat tinggi dapat menyembunyikan kelemahan pada kelas dengan jumlah sampel kecil. Fathima et al. (2023) menggunakan beberapa dataset, termasuk CSE-CICIDS2017 dan CSE-CICIDS2018, untuk mengurangi ketergantungan evaluasi pada satu distribusi data. Butt et al. (2024) juga mengevaluasi model menggunakan *precision*, *recall*, *F1-score*, *specificity*, *confusion matrix*, ROC, dan AUC, bukan hanya akurasi. Evaluasi semacam ini lebih tepat untuk dataset keamanan siber dengan distribusi kelas tidak seimbang (Butt et al., 2024; Fathima et al., 2023).

Keberhasilan tinggi pada kelas DDoS tetap memiliki nilai teknis yang kuat karena serangan tersebut merupakan fokus utama penelitian. Dari 3.363 sampel DDoS, hanya tiga yang gagal dideteksi. Nilai *false negative* yang sangat kecil penting pada sistem pertahanan jaringan karena *false negative* berarti trafik serangan dapat dilewatkan sebagai trafik normal. Sangodoyin et al. (2021) juga mendapatkan performa tinggi dari algoritma pembelajaran mesin dalam klasifikasi serangan DDoS pada SDN, dengan model CART mencapai akurasi sekitar

98% serta kecepatan prediksi tinggi. Wang et al. (2022) menunjukkan bahwa karakteristik perubahan aliran jaringan yang relatif sederhana pun dapat digunakan untuk mendeteksi *flooding DDoS* secara efektif dengan model *supervised learning*. Hasil tersebut mendukung penggunaan karakteristik trafik berbasis aliran dan laju paket sebagai indikator serangan pada penelitian ini (Sangodoyin et al., 2021; Wang et al., 2022).

Kontribusi berikutnya terletak pada integrasi model klasifikasi dengan Ryu Controller untuk melakukan deteksi sekaligus mitigasi. Ketika h1 mengirimkan 22.358 paket ICMP menuju h2, sistem berhasil menjatuhkan 22.310 paket (99,79%), sedangkan 48 paket (0,21%) lolos sebelum aturan pemblokiran aktif sepenuhnya. Integrasi deteksi berbasis pembelajaran mesin dengan SDN memiliki keuntungan karena keputusan keamanan dapat diterjemahkan langsung menjadi aturan *flow* pada *data plane*. Alwabisi et al. (2022) juga menggabungkan pembelajaran mesin dan SDN untuk mendeteksi serta memitigasi DDoS, sementara El Sayed et al. (2022) mengembangkan pendekatan anomali berbasis *flow* dan mengevaluasinya pada CICIDS2017, CICIDS2018, dan InSDN. Kedua penelitian tersebut menunjukkan bahwa kemampuan pemrograman SDN dapat digunakan untuk menghubungkan hasil klasifikasi dengan respons jaringan secara otomatis (Alwabisi et al., 2022; El Sayed et al., 2022).

Penggunaan arsitektur *Hybrid Threshold + Random Forest* pada penelitian ini memberi dua jalur keputusan. Trafik dengan laju sangat tinggi dapat ditangani menggunakan *volumetric threshold*, sedangkan trafik yang membutuhkan inspeksi lebih lanjut diproses oleh model *Random Forest*. Desain ini relevan untuk mengurangi kebutuhan inferensi model pada setiap aliran dan mempercepat respons terhadap lonjakan trafik yang jelas abnormal. Mehmood et al. (2025) menunjukkan bahwa optimasi model dan pemilihan fitur dapat menghasilkan deteksi sangat tinggi pada InSDN dan CICDDoS2019, dengan nilai *true positive* mendekati 100%. Butt et al. (2024) juga mengembangkan mekanisme seleksi fitur dinamis dan memperoleh akurasi sekitar 99% dengan RF dan k-NN. Hasil tersebut menunjukkan arah pengembangan sistem DDoS yang tidak lagi hanya mengejar algoritma klasifikasi, tetapi mengoptimalkan aliran komputasi, fitur, dan mekanisme pengambilan keputusan (Butt et al., 2024; Mehmood et al., 2025).

Mitigasi yang dihasilkan juga bersifat selektif. Setelah aturan *DROP* diterapkan, h1 sebagai sumber serangan mengalami 100% *packet loss*, sedangkan h3 sebagai pengguna legal tetap dapat berkomunikasi dengan target h2 dengan 0% *packet loss* dan rata-rata *round-trip time* 11,446 ms. Hasil ini menunjukkan bahwa pemblokiran tidak diterapkan secara global terhadap target atau seluruh jalur jaringan, tetapi diarahkan pada sumber trafik yang dianggap berbahaya. Karakteristik tersebut penting pada pertahanan SDN karena deteksi yang

menghasilkan *false positive* dapat memutus akses pengguna sah. Ekawijana et al. (2024) dan Ferdiansyah et al. (2024) sama-sama menempatkan *precision* dan ketepatan klasifikasi trafik normal sebagai parameter yang perlu diperhatikan, bukan hanya kemampuan mendeteksi trafik serangan.

Sistem memonitor statistik aliran setiap 3 detik, sedangkan setelah ambang anomali tercapai, inferensi model dan pemicu pesan OFPFlowMod membutuhkan sekitar 15–45 ms. Kedua nilai tersebut perlu dibedakan ketika menginterpretasikan responsivitas sistem. Waktu 15–45 ms menggambarkan komputasi dan aktuasi setelah trafik diperiksa, bukan keseluruhan waktu dari awal serangan sampai deteksi. Latensi deteksi terburuk masih dipengaruhi interval pengambilan statistik. Wang et al. (2022) menekankan kebutuhan model yang ringan dan fitur yang mudah diperoleh untuk mempercepat deteksi *flooding attack*. El Sayed et al. (2022) juga mengevaluasi dampak sistem deteksi terhadap *throughput* dan latensi *end-to-end*, sehingga evaluasi performa sistem keamanan tidak hanya terbatas pada skor klasifikasi (El Sayed et al., 2022; Wang et al., 2022).

Masih terdapat keterbatasan pada penggunaan *threshold* statis, yaitu 100 PPS sebagai batas bawah dan 500 PPS sebagai batas atas, serta durasi aturan *DROP* selama 15 detik. Nilai statis efektif pada topologi dan pola trafik yang digunakan dalam penelitian, tetapi belum tentu optimal ketika karakteristik trafik normal berubah. Trafik sah dengan intensitas tinggi dapat melewati batas yang sama, sementara serangan berkecepatan rendah dapat berada di bawah *threshold*. Butt et al. (2024) mengarah pada seleksi fitur yang lebih dinamis, sedangkan Mahar et al. (2026) menggabungkan RF dan XGBoost dengan fitur spesifik SDN yang dikumpulkan melalui statistik *flow* dan *port*. Pendekatan adaptif semacam ini dapat digunakan untuk pengembangan berikutnya, misalnya melalui *dynamic threshold*, *adaptive timeout*, atau model yang memperbarui keputusan berdasarkan pola trafik periode sebelumnya.

Keterbatasan lain berasal dari lingkungan Mininet dan skenario serangan yang hanya difokuskan pada *ICMP/Ping Flood*. Sistem belum diuji terhadap UDP Flood, SYN Flood, *low-rate DDoS*, atau serangan lapisan aplikasi. Sari et al. (2025) juga menyatakan bahwa penggunaan satu dataset dan simulasi *offline* membatasi generalisasi hasil ke jaringan riil. Mahar et al. (2026) menggunakan data yang dikonstruksi langsung dari *testbed* SDN berbasis Ryu dan Open vSwitch, sementara Wang et al. (2022) melakukan pengujian menggunakan simulasi sekaligus *real testbed*. Pengujian berikutnya pada *hardware switch* OpenFlow, beberapa topologi, variasi jumlah host, serta beberapa jenis serangan diperlukan untuk menentukan apakah keberhasilan mitigasi 99,79% tetap konsisten ketika kondisi jaringan semakin kompleks (Mahar et al., 2026; Sari et al., 2025; Wang et al., 2022).

Secara keseluruhan, hasil penelitian memperlihatkan dua capaian yang saling melengkapi. Pertama, model *Random Forest* memberikan performa klasifikasi yang tinggi pada trafik *BENIGN* dan *Volumetric DDoS*, dengan akurasi global 99,80%. Kedua, integrasi model ke Ryu Controller memungkinkan keputusan deteksi diterjemahkan menjadi mitigasi otomatis dengan keberhasilan 99,79% tanpa memutus akses pengguna legal. Hasil ini konsisten dengan perkembangan penelitian 2021–2026 yang menunjukkan performa tinggi algoritma berbasis *ensemble learning* pada deteksi DDoS. Perbedaan performa pada *Bot* dan *Infiltration*, penggunaan *threshold* statis, interval pemantauan 3 detik, serta pengujian yang masih terbatas pada Mininet dan ICMP Flood menjadi batas utama sebelum sistem dapat dinilai siap untuk implementasi jaringan produksi.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, implementasi, dan pengujian sistem deteksi dan mitigasi serangan *Volumetric DDoS* pada arsitektur *Software-Defined Networking* (SDN), algoritma *Random Forest* yang dilatih menggunakan dataset CICIDS2017 mampu mencapai akurasi sebesar 99,80% dalam membedakan trafik normal (*benign*) dan trafik serangan, dengan dukungan pemilihan fitur berbasis *flow* serta tahap *preprocessing* menggunakan *MinMaxScaler*. Integrasi model ke dalam *Ryu Controller* melalui arsitektur hibrida dan protokol *OpenFlow* juga mampu menjalankan mitigasi secara otomatis dengan mengirimkan instruksi *OFPFlowMod* untuk melakukan *drop* paket pada lapisan *data plane*. Pada simulasi *ICMP Flood/Ping Flood* di Mininet, sistem mencapai keberhasilan mitigasi sebesar 99,79%, dengan hanya 0,21% paket yang sempat lolos pada tahap awal inferensi tanpa mengganggu ketersediaan layanan pada *host* target. Meskipun demikian, performa tinggi tersebut masih terbatas pada karakteristik dataset CICIDS2017 dan lingkungan simulasi yang digunakan. Pengembangan selanjutnya disarankan melakukan pengujian pada perangkat *switch* fisik yang mendukung *OpenFlow*, menerapkan mekanisme *adaptive timeout* agar durasi pemblokiran dapat disesuaikan dengan intensitas serangan, serta menggunakan metode *oversampling* atau *class weight adjustment* untuk meningkatkan kemampuan deteksi pada kelas minoritas seperti *Bot* dan *Infiltration*.

DAFTAR REFERENSI

Alwabisi, S., Ouni, R., & Saleem, K. (2022). Using machine learning and software-defined networking to detect and mitigate DDoS attacks in fiber-optic networks. *Electronics, 11*(23), 4065. https://doi.org/10.3390/electronics11234065

Bhaskara, I. M. W., Suputra, I. P. G. H., Widiartha, I. M., Kadyanan, I. G. A. G. A., Putra, I. G. N. A. C., & Dwidasmara, I. B. G. (2022). Klasifikasi serangan Distributed Denial of Service (DDoS) menggunakan Random Forest dengan CFS. *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), 11*(2), 215–222. https://doi.org/10.24843/JLK.2022.v11.i02.p01

Butt, H. A., Al Harthy, K. S., Shah, M. A., Hussain, M., Amin, R., & Rehman, M. U. (2024). Enhanced DDoS detection using advanced machine learning and ensemble techniques in software defined networking. *Computers, Materials & Continua, 81*(2), 3003–3031. https://doi.org/10.32604/cmc.2024.057185

Ekawijana, A., Bakhrun, A., & Kurniawan, M. T. (2024). Deteksi serangan DDOS pada jaringan SDN dengan metode Random Forest. *Jurnal Media Informatika Budidarma, 8*(1), 685–694. https://doi.org/10.30865/mib.v8i1.6928

El Sayed, M. S., Le-Khac, N.-A., Azer, M. A., & Jurcut, A. D. (2022). A flow-based anomaly detection approach with feature selection method against DDoS attacks in SDNs. *IEEE Transactions on Cognitive Communications and Networking, 8*(4), 1862–1880. https://doi.org/10.1109/TCCN.2022.3186331

Fathima, A., Devi, G. S., & Faizaanuddin, M. (2023). Improving distributed denial of service attack detection using supervised machine learning. *Measurement: Sensors, 30*, 100911. https://doi.org/10.1016/j.measen.2023.100911

Ferdiansyah, Antoni, D., Valdo, M., Mikko, Mukmin, C., & Ependi, U. (2024). Machine learning models for DDoS detection in software-defined networking: A comparative analysis. *Journal of Information Systems and Informatics, 6*(3), 1790–1803. https://doi.org/10.51519/journalisi.v6i3.864

Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., & Shan, Y. (2023). A DDoS detection method based on feature engineering and machine learning in software-defined networks. *Sensors, 23*(13), 6176. https://doi.org/10.3390/s23136176

Mahar, I. A., Aziz, K., Chakrabarti, P., Ahmed, N., Ladan, M., & Javed, Y. (2026). A hybrid machine learning approach for detecting DDoS attacks in software-defined networks. *Scientific Reports, 16*, 6533. https://doi.org/10.1038/s41598-026-35458-w

Mehmood, S., Amin, R., Mustafa, J., Hussain, M., Alsubaei, F. S., & Zakaria, M. D. (2025). Distributed Denial of Services (DDoS) attack detection in SDN using optimizer-equipped CNN-MLP. *PLOS ONE, 20*(1), e0312425. https://doi.org/10.1371/journal.pone.0312425

Prayogi, A., Pane, M. A. S., Dian, R., Siregar, R. M., Sugianto, R. A., & Simbolon, H. F. S. (2024). Penggunaan Random Forest dan analisis perilaku untuk prediksi serangan DDoS dalam lingkungan cloud computing. *Techno.Com, 23*(3), 668–678. https://doi.org/10.62411/tc.v23i3.11317

Salsabilah, S. P., Mita, A. Al, Zachwan Irsyad, M., & Sakti, E. M. S. (2024). *Implementasi Penggunaan Kali linux dengan Teknik Ddos dalam Uji coba Keamanan Website*. *25*(1), 98–106.

Sangodoyin, A. O., Akinsolu, M. O., Pillai, P., & Grout, V. (2021). Detection and classification of DDoS flooding attacks on software-defined networks: A case study for the application of machine learning. *IEEE Access, 9*, 122495–122508. https://doi.org/10.1109/ACCESS.2021.3109490

Sari, L., Faiz, M. N., & Muhammad, A. W. (2025). Perbandingan pendekatan machine learning dalam deteksi serangan DDoS jaringan komputer. *Infotekmesin, 16*(1), 153–159. https://doi.org/10.35970/infotekmesin.v16i1.2556

Sawah, M. S., Elmannai, H., El-Bary, A. A., Lotfy, K., & Sheta, O. E. (2025). Distributed denial of service (DDoS) classification based on random forest model with backward elimination algorithm and grid search algorithm. *Scientific Reports, 15*, 19063. https://doi.org/10.1038/s41598-025-03868-x

Wang, S., Balarezo, J. F., Chavez, K. G., Al-Hourani, A., Kandeepan, S., Asghar, M. R., & Russello, G. (2022). Detecting flooding DDoS attacks in software defined networks using supervised learning techniques. *Engineering Science and Technology, an International Journal, 35*, 101176. https://doi.org/10.1016/j.jestch.2022.101176