InComTech: Jurnal Telekomunikasi dan Komputer
vol.16, no.2, Agustus 2026, 95-110
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Optimasi Deteksi DDoS Berbasis Hybrid CNN-LSTM dengan Recursive Feature Elimination pada Software-Defined Networking

Wayan Praka*, Erik Iman Heri Ujianto, Rianto, Andri Yudha Pratama

Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
Jl. Siliwangi, Jombor, Sleman, Daerah Istimewa Yogyakarta, Indonesia
*Email Penulis Koresponden: wayanpraka123@gmail.com

***Abstrak*:**
Software-Defined Networking (SDN) merupakan arsitektur jaringan yang menawarkan fleksibilitas tinggi melalui pemisahan control plane dan data plane, namun karakteristik tersebut menjadikan controller sebagai titik kritis yang rentan terhadap serangan *Distributed Denial of Service* (DDoS). Pendekatan menggunakan *deep learning* sudah dikembangkan dalam meningkatkan akurasi deteksi, tetapi sebagian besar masih menggunakan seluruh fitur pada dataset sehingga meningkatkan kompleksitas komputasi dan memperlambat proses deteksi. Penelitian ini mengusulkan metode *Hybrid CNN-LSTM* yang dioptimalkan dengan *Recursive Feature Elimination* (RFE) dalam meningkatkan efisiensi deteksi DDoS pada jaringan SDN. Dataset CIC-DDoS2019 dipakai untuk data eksperimen yang melalui tahapan pra-pemrosesan, seleksi fitur menggunakan RFE berbasis *Random Forest*, transformasi data menjadi input tiga dimensi untuk *Hybrid CNN-LSTM*, serta evaluasi menerapkan metrik *accuracy, precision, recall, F1-score*, waktu pelatihan, dan latensi inferensi. Hasil penelitian menggunakan RFE berhasil mereduksi jumlah fitur dari 77 menjadi 25 fitur tanpa menurunkan performa model. Model optimasi menghasilkan *accuracy* sebesar 92,08%, *precision* sebesar 89,71%, *recall* sebesar 92,08%, dan *F1-score* sebesar 90,43%, serta mampu menurunkan waktu pelatihan menjadi 41,11 detik dan latensi inferensi menjadi 0,00000274 detik per paket. Dibandingkan dengan *CNN, LSTM,* dan *Hybrid CNN-LSTM Baseline*, model optimasi menawarkan keseimbangan yang lebih baik antara tingkat akurasi klasifikasi dan efisiensi komputasi. Hasil penelitian menunjukkan bahwa integrasi RFE dengan *Hybrid CNN-LSTM* efektif menghasilkan model deteksi DDoS yang lebih ringan, cepat, dan akurat, sehingga berpotensi diterapkan pada sistem deteksi berbasis SDN yang membutuhkan respons secara real-time.

***Kata Kunci*:**
Software-Defined Networking;
Distributed Denial of Service;
Recursive Feature Elimination;
Hybrid CNN-LSTM;
Optimasi Deteksi Ddos;

Riwayat Artikel:
Diserahkan 09 April 2025
Direvisi 9 Agustus 2026
Diterima 11 Agustus 2026

DOI:
10.22441/incomtech.v16i2.38690

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer telah mendorong penerapan *Software Defined Networking* (SDN) sebagai arsitektur jaringan yang menerapkan pemisahan antara control plane dan data plane sehingga pengelolaan jaringan menjadi lebih fleksibel, skalabilitas, dan kemudahan pengelolaan jaringan. Meskipun menawarkan berbagai keunggulan, mekanisme kontrol yang terpusat pada SDN menjadikan controller sebagai *Single Point of Failure*, sehingga rentan terhadap berbagai ancaman keamanan, khususnya serangan *Distributed Denial of Service* (DDoS) [1]. Serangan DDoS memanfaatkan lonjakan trafik dalam jumlah besar untuk mengganggu ketersediaan layanan pada jaringan target sehingga menguras sumber daya *controller* dan mengganggu ketersediaan layanan jaringan [2]. Seiring berkembangnya teknik serangan, pelaku memanfaatkan jaringan *botnet* berskala besar yang menghasilkan pola lalu lintas menyerupai trafik normal sehingga semakin sulit dideteksi [3]. Kompleksitas tersebut juga diperparah oleh meluasnya target serangan ke lingkungan jaringan sensor nirkabel dan *Internet of Medical Things* (IoMT), yang memerlukan mekanisme deteksi intrusi dengan akurasi tinggi serta kemampuan merespons serangan secara cepat [4], [5].

Berbagai pendekatan telah dikembangkan untuk mendeteksi serangan DDoS pada lingkungan SDN. Metode sengan basis *machine learning* seperti *Decision Tree, Support Vector Machine* (SVM), *Random Forest*, hingga *Soft Voting Classifier* telah menunjukkan kemampuan yang baik dalam mengidentifikasi pola serangan [6], [7], [8], [9], [10]. Namun, metode tersebut masih bergantung pada proses ekstraksi fitur secara manual sehingga kurang optimal dalam menangkap pola lalu lintas jaringan yang semakin kompleks [11], [12]. Oleh karena itu, pendekatan *deep learning* mulai banyak diterapkan karena memungkinkan proses ekstraksi fitur berlangsung secara otomatis pada data berdimensi tinggi. Berbagai penelitian dengan memanfaatkan *Deep Q-Network*, jaringan saraf tiruan, serta *Long Short-Term Memory* (LSTM) dalam meningkatkan kemampuan deteksi serangan pada jaringan komputer [13], [14]. Khususnya, LSTM mampu mempelajari hubungan temporal terhadap data sekuensial secara efektif dalam membedakan trafik normal dan trafik serangan dibandingkan metode konvensional [15], [16].

Meskipun model *deep learning* mampu meningkatkan akurasi deteksi, penerapannya pada lingkungan SDN masih menghadapi tantangan berupa tingginya kompleksitas komputasi akibat besarnya dimensi pada dataset. Dataset CIC-DDoS2019, yang sering digunakan pada penelitian deteksi DDoS, yang terdiri dari puluhan atribut yang merepresentasikan karakteristik lalu lintas jaringan modern [9]. Penggunaan seluruh fitur secara langsung dapat menimbulkan *curse of dimensionality*, meningkatkan beban komputasi, memperpanjang waktu pelatihan, serta meningkatkan latensi proses deteksi [10]. Padahal, kecepatan deteksi merupakan aspek yang sangat penting pada SDN

karena sistem harus mampu merespons serangan secara *real-time* agar tidak mengganggu kinerja *controller* [11].

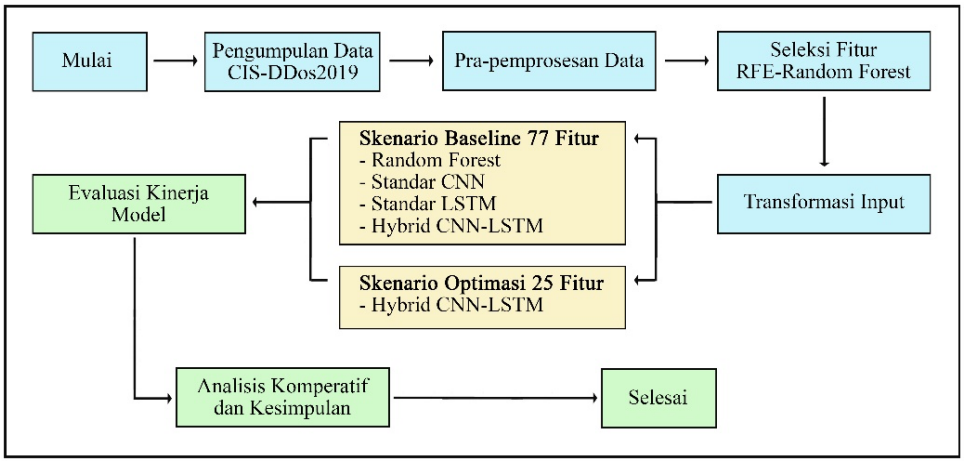
Berbagai penelitian telah mengusulkan teknik reduksi dimensi seperti *Principal Component Analysis* (PCA) dan *Information Gain* untuk mengurangi jumlah fitur [20], [21]. Namun, kedua pendekatan tersebut memiliki keterbatasan karena berpotensi mengurangi interpretabilitas fitur atau belum mampu memilih subset fitur yang relevan pada proses klasifikasi. Selain itu, *Recursive Feature Elimination* (RFE) memungkinkan melakukan eliminasi fitur secara bertahap berdasarkan tingkat kontribusinya sehingga menghasilkan subset fitur yang lebih representatif tanpa mengurangi kualitas model [22], [23]. Selain itu, penelitian terbaru menunjukkan bahwa integrasi *Convolutional Neural Network* (CNN) dan LSTM mampu menggabungkan keunggulan ekstraksi fitur spasial dan pemodelan ketergantungan temporal sehingga dapat memperoleh model deteksi yang lebih akurat dan efisien dibandingkan penggunaan LSTM secara tunggal [14]. Namun demikian, penelitian yang mengintegrasikan Hybrid CNN-LSTM dengan RFE untuk mengoptimalkan deteksi DDoS pada lingkungan SDN masih relatif terbatas, khususnya dalam mengevaluasi peningkatan efisiensi komputasi melalui pengurangan jumlah fitur tanpa menurunkan performa deteksi secara signifikan.

Berdasarkan celah penelitian tersebut, penelitian ini mengusulkan optimasi deteksi DDoS berbasis Hybrid CNN-LSTM dengan *Recursive Feature Elimination* (RFE) pada *Software-Defined Networking*. Tahap optimasi dilakukan melalui seleksi fitur menggunakan RFE untuk mereduksi 77 fitur menjadi 25 fitur yang paling relevan, sehingga mampu mengurangi kompleksitas data sekaligus mempertahankan informasi penting yang dibutuhkan dalam proses klasifikasi. Selanjutnya, fitur terpilih digunakan sebagai masukan bagi arsitektur Hybrid CNN-LSTM, di mana CNN berperan mengekstraksi karakteristik spasial, LSTM dimanfaatkan untuk memahami pola temporal serta ketergantungan waktu yang terdapat dalam data lalu lintas jaringan. Integrasi kedua metode tersebut diharapkan mampu menghasilkan model deteksi DDoS yang tidak sekadar mencapai tingkat akurasi klasifikasi yang tinggi, namun juga meningkatkan efisiensi komputasi melalui waktu pelatihan yang lebih singkat dan latensi inferensi yang lebih rendah. Dengan demikian, model yang diusulkan menjadi lebih sesuai untuk diimplementasikan pada lingkungan *Software-Defined Networking* (SDN) yang memerlukan mekanisme deteksi serangan secara cepat, akurat, dan responsif terhadap dinamika lalu lintas jaringan.

2. METODE

Penelitian ini terdiri atas tujuh tahapan sistematis untuk memperoleh model deteksi *Distributed Denial of Service* (DDoS) pada jaringan *Software-Defined Networking* (SDN). Tahapan penelitian meliputi pengumpulan dataset CIC-DDoS2019, pra-pemrosesan data melalui pembersihan, label encoding, normalisasi menggunakan MinMaxScaler, serta membagi data sebagai data pelatihan dan data pengujian. Selanjutnya, seleksi fitur diterapkan dengan menggunakan *Recursive Feature Elimination* (RFE) *dengan Random Forest* sebagai *estimator* untuk memperoleh fitur yang relevan. Fitur terpilih kemudian

diubah menjadi tensor 3 dimensi sebagai masukan Hybrid CNN-LSTM. Eksperimen dilakukan melalui dua skenario, yaitu *baseline* yang membandingkan Random Forest, CNN, LSTM, dan Hybrid CNN-LSTM menggunakan 77 fitur asli, serta skenario optimasi yang menerapkan Hybrid CNN-LSTM dengan 25 fitur hasil seleksi RFE. Evaluasi dilakukan berdasarkan *accuracy, precision, recall, F1-score,* waktu pelatihan, dan latensi inferensi. Hasil evaluasi kemudian dibandingkan untuk menganalisis pengaruh seleksi fitur terhadap performa dan efisiensi model. Alur penelitian optimasi DDos disajikan pada Gambar 1.



Gambar 1. Alur Penelitian Optimasi Detesi DDoS

Pengujian dilakukan dengan infrastruktur *hardware* yang mencakup RAM 16GB *dual-channel*, processor Intel Core i5-11400H 2.70GHz, serta GPU menggunakan NVIDIA GeForce GTX 1650 dengan VRAM 4GB guna mengakselerasi komputasi paralel pada model *deep learning*. Sementara itu, konfigurasi *software* yang diterapkan berbasis Windows 11, Python 3.9, dan *framework TensorFlow* 2.10 dengan Keras API. Untuk keperluan rekayasa data sekaligus penyaringan fitur, prosesnya dikerjakan pada *Visual Studio Code* dengan mengandalkan pustaka pendukung seperti *Scikit-learn, NumPy,* dan *Pandas*.

2.2. Dataset CIC-DDoS2019

Penelitian ini menggunakan data sekunder berupa dataset CIC-DDoS2019 yang diperoleh dari repositori publik *Kaggle*. Dataset tersebut dipilih karena menyediakan representasi yang beragam terhadap karakteristik ancaman *Distributed Denial of Service* (DDoS) pada jaringan modern, sehingga banyak digunakan sebagai acuan dalam penelitian deteksi intrusi. Dataset ini terdiri atas 431.371 sampel lalu lintas jaringan yang mencakup trafik normal (Benign) serta berbagai jenis serangan DDoS. Variasi serangan yang tersedia meliputi serangan berbasis *Distributed Reflection Denial of Service* (DrDoS), seperti *DrDoS_DNS, DrDoS_LDAP, DrDoS_NTP, DrDoS_SNMP, DrDoS_MSSQL, DrDoS_NetBIOS,* dan *DrDoS_UDP,* serta beberapa jenis serangan lainnya, yaitu *LDAP, MSSQL, UDP, UDPLag, NetBIOS, Portmap, Syn, TFTP, UDP-lag,* dan *WebDDoS*. Keberagaman kategori serangan tersebut menghasilkan dataset dengan

karakteristik multikelas dan dimensi fitur yang tinggi, sehingga mampu menggambarkan kondisi lalu lintas jaringan yang kompleks. Oleh karena itu, dataset CIC-DDoS2019 dinilai sesuai untuk mengevaluasi kemampuan model optimasi dalam mendeteksi berbagai pola serangan DDoS sekaligus menilai kinerja prediksi dan efisiensi pada komputasi [15].

2.3. Pra-pemrosesan Data

Tahap pra-pemrosesan data dilakukan untuk memperbaiki kualitas dataset agar lebih sesuai untuk digunakan dalam proses pelatihan model klasifikasi. Dataset CIC-DDoS2019 terlebih dahulu melalui proses pembersihan data melalui cara penghapusan nilai yang hilang dan nilai tak hingga yang berpotensi mengganggu proses pembelajaran model. Selanjutnya, atribut label ditransformasikan menjadi numerik menggunakan *Label Encoding* supaya bisa diproses oleh algoritma *machine learning* dan *deep learning*. Semua fitur numerik selanjutnya dinormalisasi dengan metode *MinMaxScaler* supaya memiliki rentang nilai yang seragam dan dapat mempercepat proses konvergensi model selama pelatihan. Kemudian dataset dibagi menjadi 80% data pelatihan dan 20% data pengujian menggunakan metode *train-test split* [16]. Tahapan ini dilakuan dengan tujuan untuk menghasilkan data bersih, terstandarisasi, dan bisa digunakan pada proses seleksi fitur serta melatih model deteksi DDoS.

2.4. Seleksi Fitur Menggunakan RFE

Seleksi fitur diterapkan dengan menggunakan metode *Recursive Feature Elimination* (RFE) untuk memangkas dimensi dataset sekaligus mempertahankan fitur-fitur yang memiliki kontribusi paling berpengaruh terhadap proses klasifikasi. RFE bekerja secara iteratif dengan mengevaluasi tingkat kepentingan setiap fitur berdasarkan model *estimator*, kemudian menghapus fitur yang memiliki kontribusi paling rendah hingga diperoleh jumlah fitur yang telah ditentukan. Pada penelitian ini, *Random Forest* digunakan sebagai *estimator* karena mampu menghitung *feature importance* setiap fitur secara efektif serta memiliki ketahanan yang baik terhadap *overfitting* [17]. Proses seleksi diawali dengan menggunakan seluruh 77 fitur pada dataset CIC-DDoS2019, kemudian RFE melakukan eliminasi secara bertahap hingga diperoleh 25 fitur terbaik yang digunakan sebagai masukan pada model Hybrid CNN-LSTM. Penggunaan RFE diharapkan dapat mengurangi kompleksitas komputasi, mempercepat proses pelatihan, serta meningkatkan efisiensi model tanpa mengurangi kemampuan dalam mendeteksi serangan DDoS.

2.5. Transformasi Data Input Hybrid CNN-LSTM

Sebelum proses pelatihan dilakukan, data hasil pra-pemrosesan dan seleksi fitur ditransformasikan ke dalam bentuk masukan yang sesuai dengan arsitektur Hybrid CNN-LSTM. Setiap baris data pada dataset CIC-DDoS2019 merepresentasikan satu *network flow* yang terdiri atas sekumpulan fitur statistik hasil ekstraksi menggunakan CICFlowMeter. Oleh karena itu, setiap *network flow*

diperlakukan sebagai satu sampel independen dan tidak dibentuk menjadi urutan dengan teknik sliding window. Data kemudian diubah menjadi tensor tiga dimensi dengan format jumlah sampel, time step, dan jumlah fitur, supaya bisa diproses oleh lapisan Conv1D dan LSTM. Selanjutnya nilai *time step* ditetapkan sebesar 1, yang menunjukkan bahwa setiap sampel hanya terdiri atas satu urutan observasi, sedangkan jumlah fitur disesuaikan dengan skenario pengujian, yaitu 77 fitur pada model baseline dan 25 fitur pada model optimasi setelah proses seleksi fitur menggunakan *Recursive Feature Elimination* (RFE). Transformasi ini memungkinkan model Hybrid CNN-LSTM memanfaatkan lapisan *Convolutional Neural Network* (CNN) untuk mengekstraksi pola antarfitur, pada lapisan *Long Short-Term Memory* (LSTM) mempelajari representasi data hasil dari sebelum proses klasifikasi dilakukan.

2.6. Aksitektur Hybrid CNN-LSTM

Model optimasi menggunakan arsitektur *Hybrid Convolutional Neural Network-Long Short-Term Memory* (CNN-LSTM) guna mengoptimalkan deteksi pada serangan *Distributed Denial of Service* (DDoS) dilingkungan *Software-Defined Networking* (SDN). Arsitektur ini menggabungkan kemampuan *Convolutional Neural Network* (CNN) dalam mengekstraksi pola lokal antarfitur dengan kemampuan *Long Short-Term Memory* (LSTM) guna menangkap karakteristik data sebagai dasar sebelum tahap klasifikasi diterapkan. Data masukan yang telah ditransformasikan ke dalam bentuk tensor tiga dimensi yang diproses oleh lapisan *Conv1D* untuk memperoleh representasi fitur yang lebih informatif. Selanjutnya, keluaran dari lapisan CNN diteruskan ke lapisan LSTM untuk membangun representasi yang lebih komprehensif. Untuk mengurangi risiko *overfitting*, digunakan lapisan *Dropout* sebelum data diteruskan ke lapisan *Dense* sebagai proses klasifikasi akhir [19].

2.6. Pelatihan Model

Pelatihan model dilakukan untuk mengevaluasi kinerja metode melalui dua skenario pengujian, yaitu skenario *baseline* dan skenario optimasi. Pada skenario *baseline*, dilakukan pelatihan terhadap empat model, yaitu *Random Forest, Convolutional Neural Network* (CNN), *Long Short-Term Memory* (LSTM), dan Hybrid CNN-LSTM menggunakan seluruh 77 fitur hasil pra-pemrosesan. Selanjutnya, pada skenario optimasi menerapkan metode *Recursive Feature Elimination* (RFE) guna mereduksi jumlah fitur menjadi 25 fitur, kemudian digunakan sebagai masukan bagi model Hybrid CNN-LSTM. Semua model dilatih menggunakan data pelatihan yang sudah dipisahkan pada tahap pra-pemrosesan menggunakan konfigurasi hiperparameter yang sama untuk model *deep learning*, sehingga perbedaan performa yang diperoleh lebih merefleksikan pengaruh arsitektur model dan penerapan seleksi fitur. Pendekatan ini memungkinkan evaluasi yang objektif terhadap kontribusi Hybrid CNN-LSTM dan RFE dalam meningkatkan akurasi deteksi sekaligus efisiensi komputasi pada lingkungan *Software-Defined Networking* (SDN) [16], [19].

2.7. Evaluasi Model

Evaluasi model dilakukan guna mengetahui kemampuan pada tiap model dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) dengan akurat dan efisien. Pada penelitian yang dilakukan, performa model dievaluasi dengan menggunakan *Confusion Matrix* untuk menghitung metrik *Accuracy, Precision, Recall,* dan *F1-score*. *Accuracy* dipakai untuk mengukur tingkat prediksi yang benar terhadap seluruh data pengujian, sedangkan *Precision* dipakai untuk mengukur tingkat ketepatan model dalam mengidentifikasi kelas serangan. *Recall* dipakai untuk mengukur kemampuan model dalam mendeteksi seluruh data serangan yang sebenarnya, Sementara itu, *F1-score* merupakan rata-rata gabungan antara *Precision* dan *Recall* yang mencerminkan keseimbangan kinerja model dalam melakukan klasifikasi. [15]. Selain mengevaluasi kinerja prediktif, penelitian ini juga mengukur efisiensi komputasi melalui waktu pelatihan dan latensi inferensi, mengingat tujuan utama penelitian adalah mengoptimalkan proses deteksi DDoS pada lingkungan *Software-Defined Networking* (SDN). Seluruh metrik evaluasi dihitung menggunakan data pengujian sehingga hasil yang diperoleh dapat menggambarkan kemampuan generalisasi masing-masing model.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Pra-pemprosesan Data

Pada tahap pra-pemrosesan, dataset CIC-DDoS2019 menghasilkan 345.096 sampel yang digunakan pada dua skenario pengujian, yaitu skenario *baseline* dengan 77 fitur asli dan skenario optimasi dengan 25 fitur hasil seleksi *Recursive Feature Elimination* (RFE), untuk mengevaluasi pengaruh reduksi fitur terhadap performa klasifikasi dan efisiensi komputasi. Pada skenario baseline, data memiliki bentuk tensor tiga dimensi 345096, 1, 77 sedangkan skenario usulan menghasilkan bentuk 345096, 1, 25. Reduksi fitur tersebut tidak mengubah jumlah sampel, tetapi hanya mengurangi dimensi atribut pada setiap *network flow*, sehingga diharapkan dapat menurunkan kompleksitas komputasi tanpa menghilangkan informasi penting untuk deteksi serangan DDoS. Karakteristik data hasil pra-pemrosesan pada kedua skenario ditampilkan pada Tabel 1.

Tabel 1. Karakteristik Data Hasil Pra-pemrosesan

Parameter	Baseline	Optimasi (RFE)
Jumlah Sampel	345.096	345.096
Jumlah Fitur	77	25
Time Step	1	1
Input Shape	345096, 1, 77	345096, 1, 25

3.2. Hasil Seleksi Fitur RFE

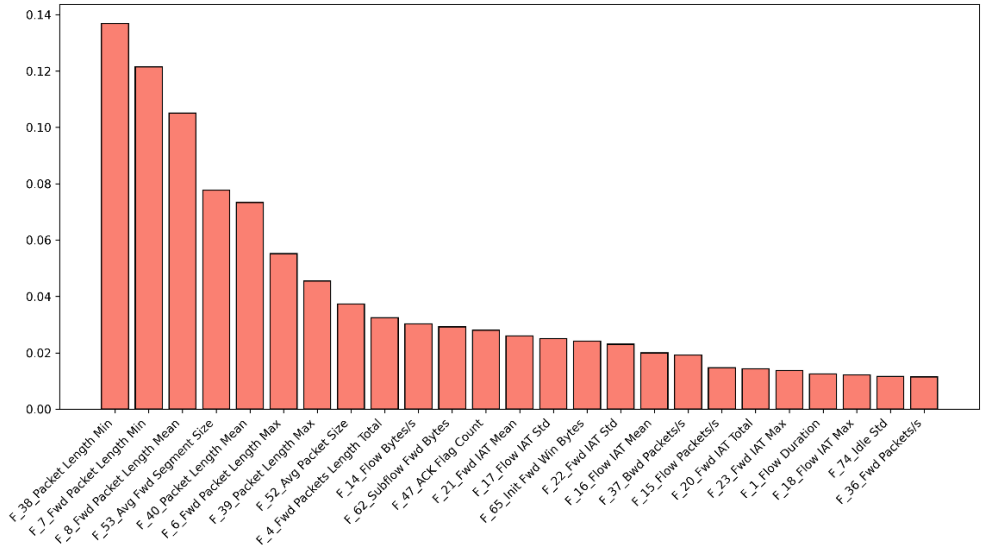
Pada tahap seleksi fitur dilakukan dengan *Recursive Feature Elimination* (RFE) menggunakan *Random Forest* sebagai estimator untuk mengidentifikasi fitur paling relevan terhadap proses klasifikasi. RFE secara iteratif mengeliminasi

fitur dengan tingkat kepentingan terendah hingga diperoleh 25 fitur dari total 77 fitur pada dataset CIC-DDoS2019, yang selanjutnya digunakan sebagai masukan model Hybrid CNN-LSTM. Hasil seleksi mempertahankan 32,47% fitur tanpa mengurangi jumlah sampel, sehingga diharapkan dapat menurunkan kompleksitas komputasi dan waktu pelatihan dengan tetap mempertahankan informasi penting untuk deteksi serangan *Distributed Denial of Service* (DDoS). Hasil Seleksi Fitur Menggunakan RFE ditampilkan pada Tabel 2.

Tabel 2. Hasil Seleksi Fitur Menggunakan RFE

Parameter	**Nilai**
Jumlah Fitur Awal	77
Jumlah Fitur Terpilih	25
Jumlah Fitur yang Dieliminasi	52
Persentase Fitur Terpilih	32,47%
Persentase Reduksi Fitur	67,53%

Hasil seleksi fitur dari 77 fitur dataset CIC-DDoS2019, RFE mempertahankan 25 fitur dengan tingkat kepentingan tertinggi, dengan *F_38_Packet Length Min, F_7_Fwd Packet Length Min, dan F_8_Fwd Packet Length Mean* sebagai fitur paling dominan. Fitur terkait *packet length, packet size, inter-arrival time*, dan statistik aliran juga menunjukkan tingkat kepentingan yang relatif tinggi. Hasil tersebut menunjukkan bahwa RFE mampu mempertahankan atribut yang representatif dalam membedakan lalu lintas normal maupun serangan DDoS, sekaligus mereduksi dimensi fitur tanpa menghilangkan informasi penting bagi model Hybrid CNN-LSTM yang ditampilkan pada Gambar 2.



Gambar 2. Hasil Seleksi 25 Fitur Terbaik Menggunakan RFE

3.3. Transformasi Data Input Hybrid CNN-LSTM

Hasil transformasi menunjukkan bahwa data hasil pra-pemrosesan dan seleksi fitur berhasil dikonversi ke dalam bentuk 3D tensor yang sesuai dengan arsitektur Hybrid CNN-LSTM. Pada skenario baseline, 77 fitur menghasilkan bentuk

masukan (345096, 1, 77), sedangkan hasil seleksi Recursive Feature Elimination (RFE) dengan 25 fitur membentuk tensor (345096, 1, 25). Transformasi ini mempertahankan jumlah sampel dan struktur data, namun mengurangi dimensi fitur yang diproses model. Format masukan tersebut memungkinkan lapisan Conv1D mengekstraksi pola antarfitur sebelum representasinya diproses oleh lapisan LSTM untuk menghasilkan klasifikasi. Hasil transformasi data ditampilkan pada Tabel 3.

Tabel 3. Hasil Transformasi Data Input Hybrid CNN-LSTM

Parameter	Baseline	Optimasi RFE
Jumlah Sampel	345.096	345.096
Time Step	1	1
Jumlah Fitur	77	25
Bentuk Input	(345096, 1, 77)	(345096, 1, 25)

3.4. Arsitektur Hybrid CNN-LSTM

Arsitektur Hybrid CNN-LSTM dirancang untuk mendeteksi serangan DDoS dengan mengombinasikan CNN dalam mengekstraksi pola lokal dan LSTM dalam membentuk representasi fitur tingkat tinggi. Model yang dioptimasi terdiri atas lima lapisan utama, yaitu *Input Layer, Conv1D, LSTM, Dropout,* dan *Dense*. Data berbentuk tensor tiga dimensi dengan dimensi masukan (1, 25) diproses melalui *Conv1D* menggunakan 32 filter dan *kernel size* 1 untuk mengekstraksi pola antarfitur, selanjutnya diproses oleh LSTM dengan 32-unit guna membentuk representasi fitur yang lebih komprehensif. Selanjutnya, *Dropout* dengan rate 0,2 digunakan untuk mengurangi risiko *overfitting*, sedangkan *Dense* dengan fungsi aktivasi *Softmax* menghasilkan 18 kelas klasifikasi. Arsitektur ini memiliki 9.746 parameter, sehingga relatif ringan dari sisi kompleksitas komputasi dan berpotensi meningkatkan efisiensi pelatihan serta inferensi tanpa mengurangi kemampuan deteksi DDoS pada lingkungan SDN. Arsitektur Hybrid CNN-LSTM ditampilkan pada Tabel 4.

Tabel 4. Arsitektur Hybrid CNN-LSTM

Layer	Konfigurasi	Output Shape	Jumlah Parameter
Input Layer	Input Shape (1, 25)	(None, 1, 25)	0
Conv1D	Filter = 32, Kernel = 1	(None, 1, 32)	832
LSTM	Unit = 32	(None, 32)	8.320
Dropout	Rate = 0.2	(None, 32)	0
Dense	Softmax, Unit = 18	(None, 18)	594
Total Parameter			9.746

Konfigurasi *hyperparameter* dirancang untuk menyeimbangkan akurasi deteksi dan efisiensi komputasi. Lapisan CNN menggunakan 32 filter, *kernel size* 1, dan aktivasi *ReLU* untuk mengekstraksi pola lokal antarfitur, sedangkan LSTM menggunakan 32-unit untuk membentuk representasi fitur sebelum klasifikasi. Model dilatih menggunakan *optimizer Adam, learning rate* sebesar 0,001, *batch size* sebesar 512, dan 20 *epoch*, serta *Sparse Categorical Crossentropy* sebagai fungsi *loss* untuk klasifikasi multikelas dengan label bilangan bulat. *Dropout*

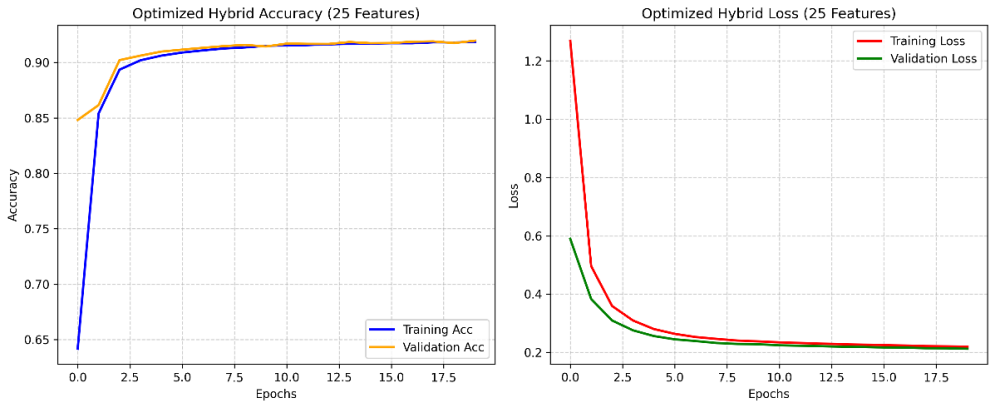
sebesar 0,2 dipakai untuk mengurangi risiko *overfitting*. Dengan 9.746 *trainable parameters*, konfigurasi ini menghasilkan arsitektur yang relatif ringan sehingga mendukung efisiensi pelatihan dan latensi inferensi yang rendah. Konfigurasi *hyperparameter* model ditampilkan pada Tabel 5.

Tabel 5. Konfigurasi Hyperparameter Model

Parameter	**Nilai**
Jumlah Filter CNN	32
Kernel Size	1
Unit LSTM	32
Fungsi Aktivasi CNN	ReLU
Fungsi Aktivasi Output	Softmax
Dropout	0.2
Optimizer	Adam
Learning Rate	0.001 *(Nilai default Keras)*
Batch Size	512
Epoch	20
Loss Function	Sparse Categorical Crossentropy
Total Trainable Parameter	9.746

3.5. Hasil Pelatihan Model

Proses pelatihan dilakukan untuk mengevaluasi kemampuan model dalam mengenali pola lalu lintas jaringan pada dataset CIC-DDoS2019. Pada model Hybrid CNN-LSTM yang dioptimasi, proses pelatihan berlangsung stabil dan mencapai konvergensi dalam 20 epoch. *Training accuracy* meningkat dari sekitar 64,2% pada epoch pertama menjadi 91,9% pada akhir pelatihan, sedangkan *validation accuracy* meningkat dari 84,8% menjadi 91,9%. Sejalan dengan peningkatan akurasi, *training loss* menurun dari 1,27 menjadi 0,22, sedangkan *validation loss* menurun dari 0,59 menjadi 0,22. Kedekatan kurva akurasi dan loss antara data pelatihan maupun validasi menunjukkan generalisasi yang baik tanpa indikasi *overfitting* maupun *underfitting*. Kurva mulai relatif stabil setelah *epoch* ke-10, yang mengonfirmasi bahwa model telah mempelajari pola lalu lintas secara efektif. Kurva akurasi dan loss ditampilkan pada Gambar 3.



Gambar 3. Kurva Akurasi dan Kurva Loss Selama Proses Pelatihan

3.6. Evaluasi Model Pembanding

Evaluasi model *baseline* dilakukan sebagai pembanding sebelum penerapan *Recursive Feature Elimination* (RFE). Seluruh model menggunakan 77 fitur hasil pra-pemrosesan dan dievaluasi pada data uji yang sama berdasarkan *accuracy, precision, recall, F1-score*, waktu pelatihan, dan latensi inferensi. Seluruh model mampu mendeteksi serangan *Distributed Denial of Service* (DDoS) dengan akurasi di atas 91%. *Random Forest* menghasilkan akurasi tertinggi (92,91%) dan waktu pelatihan tercepat (6,83 detik), tetapi kurang efektif dalam mempelajari pola spasial dan temporal dibandingkan arsitektur Hybrid CNN-LSTM. Sementara itu, model CNN, LSTM, dan Hybrid CNN-LSTM Baseline masing-masing memperoleh akurasi 91,33%, 91,39%, dan 91,71%. Setelah penerapan RFE, akurasi Hybrid CNN-LSTM meningkat menjadi 92,08%, disertai peningkatan *precision, recall,* dan *F1-score*, serta penurunan waktu pelatihan dari 41,76 menjadi 41,11 detik dan latensi inferensi dari 0,00000383 menjadi 0,00000274 detik per paket. Hasil ini mengindikasikan bahwa RFE mampu meningkatkan performa klasifikasi sekaligus meningkatkan efisiensi komputasi. Hasil pengujian ditampilkan pada Tabel 6.

Tabel 6. Hasil Evaluasi Model Pembanding

Model	Fitur	Accuracy	Precision	Recall	F1-Score	Durasi	Latensi s/paket
Random Forest	77	92,91%	92,86%	92,91%	92,85%	6,83 s	0,00000244
CNN	77	91,33%	88,46%	91,33%	89,24%	32,96 s	0,00000256
LSTM	77	91,39%	89,23%	91,39%	89,45%	50,20 s	0,00000488
Hybrid CNN-LSTM Baseline	77	91,71%	89,08%	91,71%	89,96%	41,76 s	0,00000383

Hybrid CNN-LSTM Optimasi	25	92,08%	89,71%	92,08%	90,43%	41,11 s	0,00000274

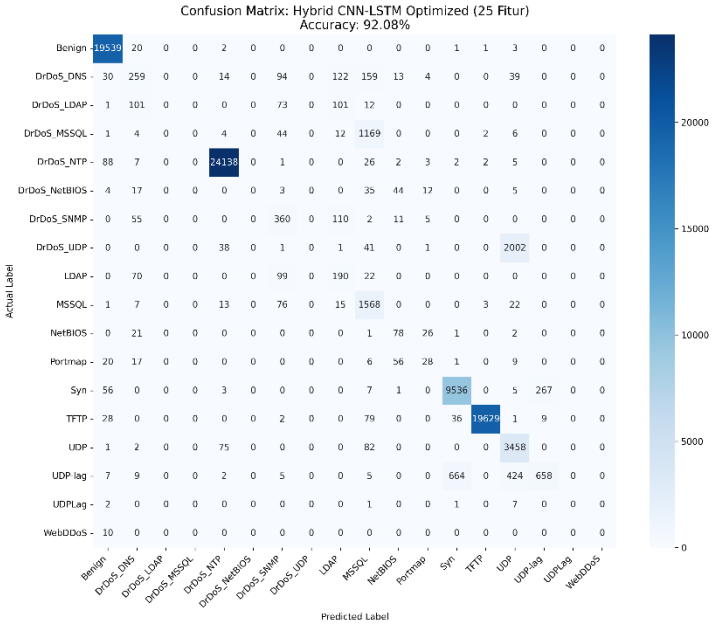
3.7. Evaluasi Model Hybrid CNN-LSTM dengan RFE

Penerapan model Hybrid CNN-LSTM yang dioptimalkan melalui *Recursive Feature Elimination* (RFE) mampu memberikan performa yang baik dalam mengidentifikasi serangan *Distributed Denial of Service* (DDoS) pada dataset CIC-DDoS2019. Berdasarkan hasil pengujian, model memperoleh *accuracy* sebesar 92,08%, dengan *precision* sebesar 89,71%, *recall* sebesar 92,08%, dan *F1-score* sebesar 90,43%. Hasil tersebut mengindikasikan bahwa proses reduksi fitur dari 77 fitur menjadi 25 fitur tidak menurunkan kemampuan klasifikasi, tetapi justru meningkatkan keseimbangan performa dibandingkan model *Hybrid CNN-LSTM Baseline*. Selain itu, model optimasi juga menunjukkan efisiensi komputasi yang lebih baik, ditandai dengan penurunan waktu pelatihan menjadi 41,11 detik serta latensi inferensi sebesar 0,00000274 detik per paket, sehingga lebih sesuai untuk kebutuhan deteksi serangan secara *real-time* pada lingkungan *Software-Defined Networking* (SDN). Peningkatan tersebut menunjukkan bahwa RFE berhasil mengurangi fitur-fitur yang kurang relevan sehingga model bisa memusatkan proses pembelajaran pada atribut yang memiliki kontribusi terbesar terhadap proses klasifikasi. Hasil evaluasi model yang dioptimasi ditampilkan pada Tabel 7.

Tabel 7. Hasil Evaluasi Hybrid CNN-LSTM dengan RFE

Metrik	**Nilai**
Jumlah Fitur	25
Accuracy	92,08%
Precision	89,71%
Recall	92,08%
F1-Score	90,43%
Training Time	41,11 s
Inference Latency	0,00000274 s/paket

Evaluasi pada *confusion matrix* menunjukkan bahwa model Hybrid CNN-LSTM yang dioptimalkan dengan RFE mampu mengklasifikasikan sebagian besar sampel dengan tepat, ditunjukkan oleh dominasi nilai pada diagonal utama. Kelas Benign, DrDoS_NTP, TFTP, SYN, dan UDP memiliki prediksi benar yang tinggi, menunjukkan bahwa model memiliki kemampuan yang baik dalam membedakan lalu lintas jaringan normal dari berbagai serangan DDoS. Kesalahan klasifikasi relatif terbatas dan terutama terjadi pada kelas dengan karakteristik lalu lintas serupa, seperti UDP, UDP-Lag, dan beberapa varian DrDoS. sehingga RFE mampu mempertahankan kualitas klasifikasi sekaligus meningkatkan efisiensi deteksi DDoS pada lingkungan *Software-Defined Networking* (SDN). *Confusion matrix* model teroptimasi ditampilkan pada Gambar 4.



Gambar 4. Confusion Matrix Model Hybrid CNN-LSTM dengan RFE

Classification Report menunjukkan bahwa model Hybrid CNN-LSTM teroptimasi dengan RFE memiliki kinerja baik pada kelas dengan jumlah sampel besar. Kelas Benign, DrDoS_NTP, SYN, dan TFTP memperoleh *precision, recall,* dan *F1-score* di atas 94%, dengan *F1-score* TFTP mencapai 99,59%. Sebaliknya, kelas DrDoS_LDAP, DrDoS_UDP, DrDoS_MSSQL, DrDoS_NetBIOS, UDPLag, dan WebDDoS memiliki *F1-score* 0%, yang menunjukkan model kesulitan dalam mengenali kelas dengan jumlah sampel terbatas akibat ketidakseimbangan data. Secara keseluruhan, model mencapai akurasi 92,08%, dengan *weighted average precision* sebesar 89,71%, *recall* sebesar 92,08%, dan *F1-score* sebesar 90,43%. Hasil tersebut mengonfirmasi bahwa model mampu mengklasifikasikan mayoritas data dengan baik, meskipun performa pada kelas minoritas masih perlu ditingkatkan melalui penyeimbangan data atau strategi pembelajaran yang lebih adaptif. *Classification Report* model teroptimasi ditampilkan pada Tabel 8.

Tabel 8. Classification Report Model Hybrid CNN-LSTM dengan RFE

Kelas Serangan	Precision	Recall	F1-Score	Support
Benign	98,74%	99,86%	99,30%	19.566
DrDoS_DNS	43,97%	35,29%	39,15%	734
DrDoS_LDAP	0,00%	0,00%	0,00%	288
DrDoS_MSSQL	0,00%	0,00%	0,00%	1.242
DrDoS_NTP	99,38%	99,44%	99,41%	24.274
DrDoS_NetBIOS	0,00%	0,00%	0,00%	120
DrDoS_SNMP	47,49%	66,30%	55,34%	543
DrDoS_UDP	0,00%	0,00%	0,00%	2.084
LDAP	34,48%	49,87%	40,77%	381
MSSQL	48,77%	91,96%	63,74%	1.705
NetBIOS	38,05%	60,47%	46,71%	129
Portmap	35,44%	20,44%	25,93%	137

Syn	93,11%	96,57%	94,81%	9.875
TFTP	99,96%	99,22%	99,59%	19.784
UDP	57,75%	95,58%	72,00%	3.618
UDP-lag	70,45%	37,09%	48,60%	1.774
UDPLag	0,00%	0,00%	0,00%	11
WebDDoS	0,00%	0,00%	0,00%	10
Accuracy	-	-	92,08%	86.275
Macro Average	42,64%	47,34%	43,63%	86.275
Weighted Average	89,71%	92,08%	90,43%	86.275

3.8. Analisis Efesiensi Komputasi

Penerapan Recursive Feature Elimination (RFE) tidak hanya berkontribusi terhadap peningkatan performa klasifikasi, tetapi juga peningkatan efisiensi komputasi Hybrid CNN-LSTM. Seleksi fitur dari 77 menjadi 25 fitur menurunkan waktu pelatihan dari 41,76 detik menjadi 41,11 detik atau sebesar 1,56%, serta mengurangi latensi inferensi dari 0,00000383 menjadi 0,00000274 detik per paket atau sebesar 28,46%. Meskipun peningkatan akurasi relatif kecil, dari 91,71% menjadi 92,08%, reduksi fitur mampu menurunkan beban komputasi tanpa mengurangi kualitas klasifikasi. Hasil ini menunjukkan bahwa RFE berhasil mempertahankan fitur yang relevan sehingga model menjadi lebih ringan serta sesuai untuk deteksi DDoS yang cepat dan efisien pada lingkungan *Software-Defined Networking* (SDN). Perbandingan efisiensi ditampilkan pada Tabel 9.

Tabel 9. Perbandingan Efisiensi Komputasi Hybrid CNN-LSTM

Parameter	**CNN-LSTM Baseline**	**CNN-LSTM + RFE**	**Perubahan**
Jumlah Fitur	77	25	- 67,53%
Accuracy	91,71%	92,08%	+ 0,37%
Precision	89,08%	89,71%	+ 0,63%
Recall	91,71%	92,08%	+ 0,37%
F1-Score	89,96%	90,43%	+ 0,47%
Durasi Pelatihan	41,76 s	41,11 s	+ 1,56%
Latensi Inferensi	0,00000383 s	0,00000274 s	+ 28,46%

4. KESIMPULAN

Penelitian ini berhasil mengembangkan model Hybrid CNN-LSTM yang dioptimalkan menggunakan *Recursive Feature Elimination* (RFE) untuk mendeteksi upaya serangan *Distributed Denial of Service* (DDoS) terhadap lingkungan *Software-Defined Networking* (SDN). Penggunaan RFE mampu mereduksi jumlah fitur dari 77 menjadi 25 fitur tanpa menurunkan performa klasifikasi, bahkan meningkatkan *accuracy* model dari 91,71% menjadi 92,08%, dengan *precision* sebesar 89,71%, recall sebesar 92,08%, dan F1-score sebesar 90,43%. Selain meningkatkan performa prediktif, model optimasi juga menunjukkan efisiensi komputasi yang lebih baik melalui penurunan waktu pelatihan menjadi 41,11 detik dan latensi inferensi menjadi 0,00000274 detik per paket, sehingga lebih sesuai untuk kebutuhan deteksi serangan secara *real-time* pada lingkungan SDN. Hasil perbandingan dengan model *Random Forest, CNN, LSTM,* dan *Hybrid CNN-LSTM Baseline* menunjukkan bahwa integrasi RFE

dengan arsitektur *Hybrid CNN-LSTM* mampu menghasilkan keseimbangan yang baik antara *accuracy* dan efisiensi komputasi. Meskipun demikian, hasil evaluasi per kelas menunjukkan bahwa performa model masih terbatas pada beberapa kelas dengan jumlah sampel yang sedikit atau distribusi data yang tidak seimbang. Pada penelitian selanjutnya dapat mengkaji penerapan teknik penyeimbangan data, seperti *class weighting*, *SMOTE*, atau *focal loss*, serta melakukan pengujian pada dataset lain untuk meningkatkan kemampuan generalisasi model dan performa deteksi pada kelas-kelas minoritas.

REFERENSI

[1] H. Ulfa, A. I. Basuki, G. M. Suranegara, and A. Fauzi, "Sistem Pengamanan Jaringan SDN dari Serangan DDoS Berbasis Multi Controller dan Load Balancer," Jan. 2024. doi: 10.32520/stmsi.v13i2.3802.

[2] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, and I. H. Hasbullah, "A deep learning approach to detect DDoS flooding attacks on SDN controller," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 38, no. 2, pp. 1245–1255, May 2025, doi: 10.11591/ijeecs.v38.i2.pp1245-1255.

[3] A. Sanmorino, L. Marnisah, and H. Di Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Engineering, Technology and Applied Science Research*, vol. 14, no. 5, pp. 16444–16449, 2024, doi: 10.48084/etasr.8362.

[4] F. Azhari, B. Hananto, and I. Ernawati, "Perbandingan Kinerja Algoritma Dalam Klasifikasi Serangan DDoS Berdasarkan Data CIC IoMT Dataset," *Informatik: Jurnal Ilmu Komputer*, vol. 21, no. 2, pp. 115–127, Aug. 2025, doi: 10.52958/iftk.v21i2.11467.

[5] Y. Yanti, T. Hidayat, N. Nurhanif, N. Safana, and P. N. P. Anggayoni, "Deteksi Serangan Distributed Deniel of Service Pada Jaringan Sensor Nirkabel Menggunakan Support Vector Machine," *G-Tech: Jurnal Teknologi Terapan*, vol. 8, no. 4, pp. 2687–2697, Oct. 2024, doi: 10.70609/gtech.v8i4.5428.

[6] T. Yuliswar, I. Elfitri, and O. W. Purbo, "Optimalisasi Sistem Deteksi Intrusi Menggunakan Machine Learning Untuk Deteksi Serangan Terdistribusi Pada Server," *JURNAL INOVTEK POLBENG*, vol. 10, no. 1, pp. 367–376, Mar. 2025, doi: 10.35314/vem9da98.

[7] Y. Irawan, R. Pramitasari, W. M. Ashari, and A. N. H. Yansyah, "Support Vector Machine Classification Algorithm for Detecting DDoS Attacks on Network Traffic," *Journal of Applied Informatics and Computing (JAIC)*, vol. 9, no. 4, pp. 1945–1954, 2025, doi: 10.30871/jaic.v9i4.10003.

[8] M. A. Fathurrahman and D. W. Prabowo, "Perbandingan Performa Algoritma Random Forest dan SVM Dalam Mendeteksi serangan DDoS di Jaringan Cloud," *Jurnal Riset Rekayasa Elektro*, vol. 7, no. 2, pp. 193–202, Dec. 2025, doi: 10.30595/jrre.v7i2.27866.

[9] D. Kiswanto, F. Ramadhani, N. M. Surbakti, and N. A. Nasution, "Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest," *Bulletin of Information Technology (BIT)*, vol. 6, no. 3, pp. 247–256, 2025, doi: 10.47065/bit.v5i2.2203.

[10] A. Ekawijana, A. Bakhrun, and M. T. Kurniawan, "Deteksi Serangan DDOS Pada Jaringan SDN dengan Metode Random Forest," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 8, no. 1, pp. 685–694, Jan. 2024, doi: 10.30865/mib.v8i1.6928.

[11] L. I. Uzlah, R. A. Saputra, and Isnawaty, "DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST," *Jurnal Mahasiswa Teknik Informatika (JATI)*, vol. 8, no. 3, pp. 2787–2793, 2024, doi: 10.36040/jati.v8i3.8891.

[12] S. Joses, S. Quinevera, R. Mardianto, D. Yulvida, and A. M. Shiddiqi, "Pendekatan Metode Ensemble Learning untuk Deteksi Serangan DDoS menggunakan Soft Voting Classifier,"

JEPIN (Jurnal Edukasi dan Penelitian Informatika), vol. 10, no. 1, pp. 79–87, 2024, doi: 10.26418/jp.v10i1.73241.

[13] R. Purba, W. S. Lestari, and M. Ulina, "Deteksi Serangan DDoS Mengunakan Deep Q-Network," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 1, pp. 648–658, Mar. 2022, [Online]. Available: http://jurnal.mdp.ac.id

[14] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 9, no. 3, pp. 373–379, Aug. 2020, doi: 10.32736/sisfokom.v9i3.945.

[15] Z. P. Putro and A. Desianty, "Classification of Cyber Attacks on Software-Defined Networking (SDN) Using Deep Learning LSTM and GRU," *Journal of Informatics and Communications Technology (JICT)*, vol. 7, no. 2, pp. 1–10, Dec. 2025, doi: 10.52661.

[16] M. R. Yusuf and Sumarlin, "Penerapan Deep Learning untuk Deteksi Anomali dalam Jaringan Keamanan Siber Menggunakan Recurrent Neural Networks (RNNs)," *Blend Sains Jurnal Teknik*, vol. 3, no. 4, pp. 460–470, May 2025, doi: 10.56211/blendsains.v3i4.800.

[17] D. Mualfah, R. Ardiansyah, and R. Gunawan, "Classification of DDoS attacks using the random forest method and class weight technique on the CICDDoS2019 dataset," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 6, no. 3, pp. 530–535, Dec. 2025, doi: 10.37859/coscitech.v6i3.10731.

[18] B. Ramadhan, D. Firdaus, and A. R. Rafi, "Teknik SMOTE Sebagai Solusi Imbalance Class dalam Model Deteksi Intrusi DDoS dengan Metode PCA-Random Forest," *MIND (Multimedia Artificial Intelligent Networking Database) Journal*, vol. 8, no. 1, pp. 52–64, 2023, doi: 10.26760/mindjournal.v8i1.52-64.

[19] H. A. Damanik and M. Anggraeni, "Analisis dan Mitigasi Kerentanan DDoS pada Infrastuktur Jaringan dengan Teknik Hierarchical Clustering dan Firewall IPTables," *Jurnal Pekommas*, vol. 10, no. 1, pp. 29–38, 2025, doi: 10.56873/jpkm.v9i1.5551.

[20] E. A. Winanto, Y. Novianto, S. Sharipuddin, I. S. Wijaya, and P. A. Jusia, "Peningkatan Performa Deteksi Serangan Menggunakan Metode PCA dan Random Forest," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 2, pp. 285–290, Apr. 2024, doi: 10.25126/jtiik.20241127678.

[21] E. Hariyanti, D. P. Hostiadi, Anggreni, Y. P. Atmojo, I. M. D. Susila, and I. Tangkawarow, "Analisis Perbandingan Metode Seleksi Fitur pada Model Klasifikasi Decission Tree untuk Deteksi Serangan di Jaringan Komputer," *JURNAL SISTEM DAN INFORMATIKA (JSI)*, vol. 18, no. 2, pp. 208–217, 2024, doi: 10.30864/jsi.v18i2.615.

[22] N. A. Maori and N. Azizah, "Penerapan Recursive Feature Elimination (RFE) pada Tree-Based Classifier untuk Identifikasi Risiko Diabetes," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 6, no. 2, pp. 465–471, 2024.

[23] A. M. Priyatno, W. F. R. Sudirman, R. J. Musridho, and F. Amalia, "Impurity-Based Important Features for feature selection in Recursive Feature Elimination for Stock Price Forecasting," *Jurnal Teknik Industri Terintegrasi (JUTIN)*, vol. 6, no. 4, pp. 1182–1194, 2023, doi: 10.31004/jutin.v6i4.17726.

[24] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.