Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN 3090-1154 (Media Online)
Volume 2, Tahun 2025

A Systematic Literature Review of Machine Learning Techniques for DDoS Detection: Accuracy, Efficiency, and Scalability Challenges

Muhamad Bunan Imtias[1], Khothibul Umam*[2], Hery Mustofa[3]
* Prodi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Walisongo, Semarang, Indonesia
2208096088@student.wakisongo.ac.id[1], khothibul_umam@walisongo.ac.id[2], herymustofa@walisongo.ac.id[3]
*Penulis Korespondensi

Abstrak

Serangan Distributed Denial of Service (DDoS) merupakan ancaman yang signifikan bagi jaringan modern dengan berupaya mengganggu layanan melalui banjir lalu lintas yang berlebihan. Seiring dengan perkembangan serangan ini, teknik deteksi konvensional sering kali gagal untuk beradaptasi. Artikel ini membahas efektivitas penggunaan *Machine Learning*(machine learning/ML) untuk deteksi DDoS, dengan menekankan keseimbangan antara presisi deteksi dan efisiensi komputasi. Tinjauan ini menganalisis berbagai model pembelajaran mesin, termasuk metode pembelajaran mendalam seperti Long Short-Term Memory (LSTM) dan Convolutional Neural Networks (CNNs), serta efektivitasnya dalam berbagai konteks jaringan, termasuk Software Defined Networks (SDN) dan Internet of Things (IoT). Meskipun model-model ini menunjukkan presisi yang sangat baik dalam mengidentifikasi pola serangan yang rumit, masalah terkait skalabilitas dan efektivitas deteksi secara real-time masih tetap menjadi tantangan. Artikel ini menyoroti algoritma *Machine Learning*yang efektif untuk deteksi DDoS dan mengkaji pertukaran yang terkait, memberikan wawasan untuk penelitian dan aplikasi praktis di masa depan.

Kata kunci: *Serangan DDoS, Efisiensi, IoT, Machine Learning, SDN.*

Abstract

Distributed Denial of Service (DDoS) present a substantial peril for contemporary networks by attempting to interrupt services through the inundation of excessive cartage. As these assaults progress, conventional detection techniques frequently fail to adapt. This paper examines the efficacy of machine learning (ML) for DDoS detection, emphasizing the equilibrium between detection precision and computing efficiency. The review analyzes multiple machines learning models, including deep learning methodologies that include Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNNs), and their efficacy in diverse network contexts including Software Defined Networks (SDN), and Internet of Things (IoT). Although these models exhibit excellent precision in identifying intricate assault patterns, issues about scalability and real-time detection efficacy persist. The paper emphasizes effective machine learning algorithms on DDoS detection and examines associated trade-offs, offering insights for research and practical applications in the future.

Keywords: *DDoS Attacks, Efficiency, IoT, Machine Learning, SDN*

I. PENDAHULUAN

Salah satu serangan dalam jaringan adalah DDoS (Distributed Denial of Service) yang merupakan ancaman serius bagi jaringan dan layanan modern [1]. Serangan ini membanjiri target dengan lalu lintas data yang ekstrem, membuatnya tidak dapat diakses oleh pengguna yang sah [2]. Peningkatan kecanggihan dan distribusi serangan ini menyebabkan tantangan besar bagi mekanisme keamanan konvensional [3]. Metode deteksi dan mitigasi tradisional sering kali kesulitan, terutama terkait dengan pengaturan jaringan yang rumit dan perubahan lanskap ancaman DDoS, yang dapat mengeksploitasi beberapa vektor secara bersamaan, termasuk protokol lapisan aplikasi dan jaringan [4][5].

Penelitian terkini menekankan perlunya teknik deteksi DDoS yang lebih canggih. Penelitian menunjukkan bahwa metodologi deteksi yang ada sering kali gagal membedakan secara akurat antara lalu lintas yang tidak berbahaya dan berbahaya selama serangan DDoS, terutama karena volume besar dan karakteristik dinamis dari serangan tersebut [6]. Munculnya *Machine Learning* dan kecerdasan buatan semakin diakui sebagai frontier yang menjanjikan dalam mendeteksi dan mencegah insiden DDoS, yang berpotensi meningkatkan adaptabilitas sistem keamanan yang bertanggung jawab untuk melindungi jaringan [7].

Tinjauan Literatur Sistematis (Systematic Literature Review/SLR) ini menyelidiki efektivitas metode *Machine Learning* untuk mengidentifikasi serangan DDoS, dengan fokus khusus pada pertukaran

antara akurasi (kemampuan untuk mengidentifikasi serangan dengan benar) dan efisiensi (sumber daya komputasi yang dibutuhkan untuk deteksi waktu nyata). Tinjauan ini menyintesis temuan dari berbagai studi, membandingkan berbagai model *Machine Learning* dan kinerjanya dalam berbagai lingkungan jaringan, termasuk Wireless Sensor Networks (WSN), Software-Defined Networks (SDN), dan Internet of Things (IoT).

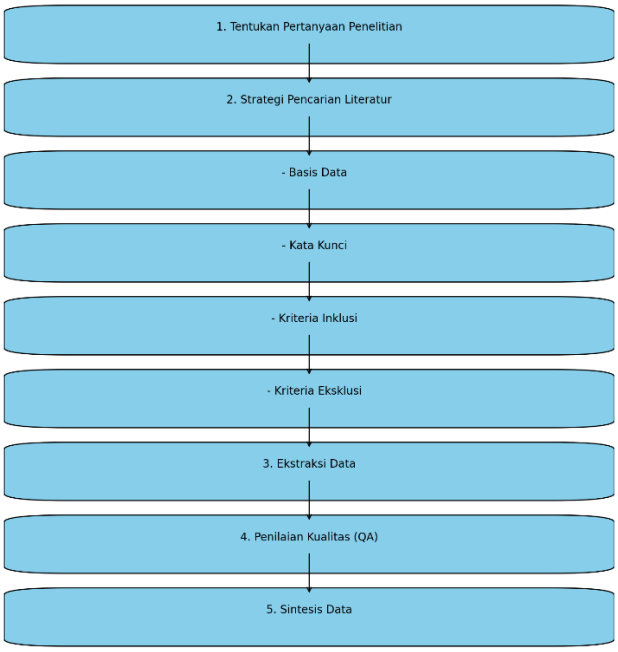
Tinjauan ini bertujuan untuk menjawab pertanyaan penelitian berikut:

- **RQ1:** Seberapa efektif metode *Machine Learning* dalam mengidentifikasi serangan Distributed Denial of Service (DDoS), terkait dengan akurasi dan efisiensi, dalam berbagai lingkungan jaringan?
- **RQ2:** Apa saja tantangan yang dihadapi metode *Machine Learning* dalam mendeteksi serangan DDoS, terutama terkait dengan skalabilitas dan pola serangan yang berkembang?
- **RQ3:** Apa saja metode *Machine Learning* yang paling menjanjikan untuk deteksi DDoS, berdasarkan literatur terkini?

Tinjauan ini bertujuan untuk memberikan wawasan mengenai tantangan, keterbatasan, dan kemungkinan kemajuan dalam deteksi DDoS dengan memeriksa model *Machine Learning* terbaru, yang pada akhirnya akan membantu penelitian di masa depan dan aplikasi di dunia nyata.

II. METODE PENELITIAN

Metode Untuk menjawab pertanyaan penelitian, kami melakukan Tinjauan Literatur Sistematis (Systematic Literature Review/SLR) dengan mengikuti metodologi yang terdefinisi dengan baik untuk memastikan pemeriksaan yang menyeluruh dan tidak bias terhadap studi-studi yang relevan [8]. Proses tinjauan secara umum dibagi menjadi beberapa tahap seperti skema pada **Gambar 1** yang akan diperinci pada penjelasan berikut.



Gambar 1. Metode Penelitian

2.1. Menentukan Pertanyaan Penelitian

Tahap awal untuk melakukan penelitian ini adalah dengan menentukan Research Question (RQ) yang sudah disebutkan pada bagian pendahuluan.

2.2. Strategi Pencarian Literatur

2.2.1. Basis Data

Kami mencari studi-studi relevan di basis data akademik terkenal, termasuk IEEE Xplore dan MDPI. Pencarian ini dilakukan dengan fokus pada artikel jurnal yang peer-reviewed, makalah konferensi, dan publikasi ilmiah lainnya dari lima tahun terakhir (2020–2025).

2.2.2. Kata Kunci

Pencarian mencakup istilah-istilah seperti "Systematic Literature Review," "DDoS detection," "machine learning," "distributed denial of service," "deep learning," dan "anomaly detection." Pencarian dikhususkan untuk artikel jurnal *open-source* seperti IEEE Access dan MDPI, serta beberapa jurnal lain yang sejenis.

2.2.3. Kriteria Inklusi

Studi dimasukkan jika mereka:

- Fokus pada metode berbasis *Machine Learning* untuk deteksi DDoS.
- Menyajikan hasil terkait akurasi dan efisiensi model deteksi.
- Mencakup berbagai lingkungan jaringan seperti SDN, IoT, dan WSN.

2.2.4. Kriteria Eksklusi

Artikel dikeluarkan jika mereka:

- Fokus pada metode mitigasi atau pencegahan DDoS yang tidak melibatkan pembelajaran mesin.
- Tidak diterbitkan di jurnal atau konferensi yang peer-reviewed.
- Tidak melaporkan hasil terkait metrik kinerja deteksi DDoS.

2.3. Ekstraksi Data

Kami mengekstrak informasi kunci dari artikel yang dipilih, termasuk:

- Model *Machine Learning* yang digunakan (misalnya, pembelajaran terawasi, pembelajaran tak terawasi, pembelajaran mendalam, model ensemble).
- Metrik evaluasi seperti akurasi, presisi, recall, skor F1, dan efisiensi komputasi (misalnya, waktu pemrosesan, penggunaan memori).
- Lingkungan jaringan tempat model diuji (misalnya, SDN, IoT, WSN).
- Temuan utama terkait kekuatan, keterbatasan, dan kemampuan beragam model dalam mendeteksi serangan DDoS.

2.4. Penilaian Kualitas (QA)

Penilaian kualitas dilakukan pada setiap studi untuk mengevaluasi ketelitian metodologis dan relevansinya terhadap pertanyaan penelitian. Artikel dinilai berdasarkan kriteria berikut:

- **QA 1:** Relevansi untuk deteksi DDoS menggunakan teknik pembelajaran mesin.
- **QA 2:** Ketelitian metodologis, termasuk kejelasan desain eksperimen dan kekuatan metrik evaluasi.
- **QA 3:** Kualitas data, termasuk ukuran dataset, keberagaman, dan penanganan ketidakseimbangan kelas.
- **QA 4:** Evaluasi hasil, termasuk penggunaan metrik kinerja yang signifikan secara statistik.
- **QA 5:** Kemampuan hasil untuk digeneralisasi ke skenario dunia nyata.
- **QA 6:** Inovasi dalam hal metode atau pendekatan baru. Kualitas setiap studi dinilai dengan (Y) untuk artikel yang memenuhi kriteria QA, dan (X) untuk artikel yang tidak memenuhi persyaratan.

2.5. Sintesis Data

Setelah data diekstraksi, kami menganalisis dan menyintesisnya untuk mengidentifikasi pola dan tema umum dalam penggunaan *Machine Learning* dalam konteks deteksi DDoS [9]. Sintesis ini fokus pada perbandingan akurasi dan efisiensi berbagai model pembelajaran mesin, serta kinerja model-model ini dalam berbagai lingkungan jaringan.

Pendekatan naratif digunakan untuk merangkum hasil dan menulis kesimpulan mengenai efektivitas metode deteksi DDoS berbasis pembelajaran mesin, dengan menjawab pertanyaan penelitian. Dengan menggunakan pendekatan sistematis ini, kami bertujuan untuk memberikan tinjauan yang luas dan tidak bias dalam hal *Machine Learning* untuk deteksi DDoS. Proses metodologis ini membantu memastikan bahwa temuan tinjauan didasarkan pada studi-studi berkualitas tinggi, memberikan wawasan berharga bagi komunitas akademik dan praktisi di bidang keamanan jaringan [10].

III. HASIL DAN PEMBAHASAN

Hasil dan Tinjauan literatur sistematis ini menghasilkan berbagai studi yang menggunakan teknik *Machine Learning* berbeda untuk mendeteksi serangan Distributed Denial of Service (DDoS). Studi-studi ini bervariasi dalam hal model *Machine Learning* yang digunakan, metrik evaluasi yang dilaporkan, dan lingkungan jaringan tempat sistem deteksi diterapkan. Berikut adalah temuan kunci dari studi-studi yang ditinjau:

3.1. Hasil Pencarian dan *Quality Assessment*

Dalam melakukan Tinjauan Literatur Sistematis (SLR), pencarian awal menggunakan kata kunci yang telah ditentukan menghasilkan total 57 artikel dari berbagai jurnal yang ditampilkan pada tabel 1.

Tabel 1. Hasil proses pencarian/*Search Process*

No.	Nama Jurnal	Indeks Jurnal	Jumlah
1.	IEEE Access	Q1	21
2.	Applied Sciences (Switzerland)	Q2	3
3.	Electronics (Switzerland)	Q2	5
4.	World Electric Vehicle Journal	Q2	1
5.	Energies	Q1	1
6.	Future Internet	Q2	3
7.	Revue d'Intelligence Artificielle	-	1
8.	Lecture Notes in Electrical Engineering	Q4	1
9.	Machine Learning and Knowledge Extraction	Q1	1
10.	Sensors	Q1	4
11.	IAES International Journal of Artificial Intelligence	Q2	1
12.	Internet of Things (Switzerland)	Q1	1
13.	International Conference on Emerging Smart Computing and Informatics	-	1
14.	Scientific Reports	Q1	1
15.	Repositor	-	1
16.	Mathematics	Q2	1
17.	Techno.COM	Sinta 4	1
18.	Algorithms	Q2	1
19.	Cyber Security and Applications	Q1	1
20.	International Journal of Computing and Digital Systems	Q3	1
21.	Journal of Cybersecurity and Privacy	Q1	1
22.	Lecture Notes in Electrical Engineering	Q4	1
23.	Security and Communication Networks	Q2 (2022)	1
24.	SSRN Electronic Journal	-	1
25.	Symmetry	Q2	1
26.	ABEC 4thInternational Annual Conference	-	1

Untuk menyaring kumpulan artikel ini, kriteria inklusi dan eksklusi diterapkan, menghasilkan 30 artikel yang sesuai dengan tujuan SLR. Selanjutnya, proses Penilaian Kualitas (QA) digunakan untuk mengevaluasi ketelitian metodologis dan relevansi artikel-artikel ini, memastikan kesesuaiannya untuk dimasukkan ke dalam tahap analisis berikutnya—hasil dari proses QA ini ditunjukkan dalam tabel 2.

Tabel 2. Hasil *Quality Assessment*

Ref.	Quality Assessment						
	QA 1	QA 2	QA 3	QA 4	QA 5	QA 6	Results
[11]	Y	Y	Y	Y	X	Y	✓
[12]	Y	Y	Y	Y	X	Y	✓
[13]	Y	Y	Y	Y	Y	Y	✓
[14]	Y	Y	Y	Y	X	Y	✓
[15]	Y	Y	Y	Y	X	Y	✓
[16]	Y	Y	X	X	X	Y	✗
[17]	Y	Y	X	Y	X	X	✓
[18]	Y	Y	Y	Y	Y	Y	✓
[19]	Y	Y	Y	Y	Y	Y	✓
[20]	Y	Y	Y	Y	Y	Y	✓
[21]	Y	Y	Y	Y	Y	Y	✓
[20]	Y	Y	Y	Y	Y	Y	✓
[22]	Y	Y	Y	Y	Y	Y	✓
[23]	Y	X	Y	X	Y	X	✗
[24]	Y	Y	Y	Y	Y	Y	✓
[25]	Y	Y	Y	Y	Y	Y	✓
[26]	Y	Y	Y	Y	Y	Y	✓
[27]	Y	Y	Y	Y	Y	Y	✓
[28]	Y	Y	Y	Y	Y	X	✓
[29]	Y	Y	Y	Y	Y	Y	✓

[30]	Y	Y	Y	Y	Y	X	✓
[31]	Y	Y	Y	Y	Y	Y	✓
[32]	Y	Y	Y	Y	Y	Y	✓
[33]	Y	Y	Y	Y	Y	X	✓
[34]	Y	Y	Y	Y	Y	Y	✓
[35]	Y	Y	Y	Y	Y	X	✓
[36]	Y	Y	Y	Y	Y	Y	✓
[37]	Y	Y	Y	Y	Y	Y	✓
[38]	Y	Y	Y	Y	Y	Y	✓
[39]	Y	Y	X	X	X	X	✗
[40]	Y	Y	Y	Y	Y	Y	✓

Deskripsi Simbol:

- (✓): Untuk jurnal atau data terkait penelitian yang memenuhi syarat. Terdapat cukup tantangan, pendekatan, dan informasi dalam data yang membuatnya layak untuk dipilih.
- (✗): Untuk jurnal atau data terkait penelitian yang tidak digunakan dalam penelitian karena data tersebut merupakan artikel yang ditulis oleh editor tamu yang menceritakan pengalaman, masalah, pendekatan, atau informasi yang tidak memadai untuk pemilihan data.

3.2. Analisis Data

Bagian ini akan menjawab pertanyaan penelitian (RQ) dan membahas hasil dari artikel-artikel yang ditinjau.

3.2.1. RQ1: Seberapa efektif teknik Machine Learning dalam mendeteksi serangan Distributed Denial of Service (DDoS), terkait dengan akurasi dan efisiensi, di berbagai lingkungan jaringan?

Teknik pembelajaran mesin, terutama metode pembelajaran mendalam seperti Convolutional Neural Networks (CNNs) dan Long Short-Term Memory (LSTM), telah menunjukkan efektivitas tinggi dalam mendeteksi serangan DDoS di berbagai lingkungan jaringan, termasuk Software Defined Networks (SDN), Internet of Things (IoT), SD-VANETs, dan sistem kontrol industri. Model-model ini secara konsisten mencapai akurasi tinggi, dengan beberapa studi melaporkan F1-score di atas 98%, serta tingkat presisi dan recall yang mendekati sempurna. Sebagai contoh, Al-Dulaimi et al. dalam penelitiannya menyatakan bahwa "Model Tree-CNN mencapai akurasi 96,02% pada UNSW-NB15, 99,99% pada CIC-IDS 2017, dan 99,96% pada CIC-IDS 2018" [38]. Demikian juga, ShieldRNN mengungguli model tradisional pada dataset CIC-IDS 2017 [37]. Namun, meskipun akurasi mereka mengesankan, model-model ini menghadapi tantangan dalam hal efisiensi komputasi, terutama saat diterapkan di lingkungan yang terbatas sumber daya. Model pembelajaran mendalam memerlukan daya pemrosesan dan memori yang tinggi untuk deteksi waktu nyata, yang dapat membatasi penerapannya pada jaringan berskala besar dengan lalu lintas tinggi. Sebaliknya, Random Forest dan XGBoost, yang lebih efisien secara komputasional, mungkin kesulitan menangani kompleksitas dan sifat dinamis pola serangan DDoS di lingkungan data besar dan berdimensi tinggi [23].

3.2.2. RQ2: Apa saja tantangan yang dihadapi oleh model Machine Learning dalam mendeteksi serangan DDoS, terutama dalam hal skalabilitas dan pola serangan yang berkembang?

Tantangan utama bagi model *Machine Learning* dalam mendeteksi serangan DDoS adalah skalabilitas dan sifat pola serangan yang terus berkembang.

1) Skalabilitas: Seiring dengan meningkatnya skala serangan DDoS, volume lalu lintas menjadi tantangan signifikan bagi model pembelajaran mesin. Dalam lingkungan seperti SDN dan IoT, model *Machine Learning* sering kesulitan untuk memproses lalu lintas volume tinggi secara waktu nyata. Jumlah data yang perlu dianalisis dengan cepat dapat membanjiri model tradisional, menyebabkan keterlambatan dalam deteksi. Misalnya, seiring meningkatnya volume lalu lintas, model-model tersebut mungkin mengalami kemacetan waktu pemrosesan, dan lonjakan penggunaan memori, terutama di jaringan besar [36]. Masalah skalabilitas ini sangat terlihat dalam lingkungan dinamis seperti SD-VANETs, di mana kendaraan bergerak terus-menerus dan topologi jaringan selalu berubah. Di sini, pemrosesan data waktu nyata menjadi sangat penting untuk deteksi serangan, namun model pembelajaran mendalam sering gagal menjaga efisiensi dalam kondisi tersebut.
2) Pola Serangan yang Berkembang: Tantangan signifikan lainnya adalah meningkatnya variasi dan kompleksitas serangan DDoS. Penyerang terus beradaptasi dengan metode mereka untuk menghindari sistem deteksi, sering menggunakan serangan berkecepatan rendah, pemalsuan IP, dan teknik

amplifikasi. Model *Machine Learning* tradisional yang dilatih pada data historis mungkin tidak mengenali vektor serangan baru ini, yang mengakibatkan false negatives. Ketidakseimbangan kelas dalam dataset DDoS, di mana lalu lintas yang tidak berbahaya jauh lebih banyak daripada lalu lintas serangan, juga membuat model cenderung mendeteksi lalu lintas normal daripada pola serangan yang jarang terjadi. Oleh karena itu, pelatihan ulang model secara terus-menerus diperlukan untuk mempertahankan kinerja terhadap serangan yang baru muncul. Namun, proses pelatihan ulang ini memperkenalkan beban komputasi dan keterbatasan sumber daya, yang dapat menghambat skalabilitas di jaringan besar waktu nyata [23][30].

3) Kemampuan Adaptasi Model: Seiring dengan semakin canggihnya teknik serangan, model perlu dapat beradaptasi. Sebagai contoh, model-model seperti ShieldRNN dan Tree-CNN lebih efektif karena mereka menggabungkan pembelajaran berbasis urutan dan ekstraksi fitur untuk beradaptasi dengan pola baru, namun kompleksitas mereka tetap menjadi keterbatasan di lingkungan berskala besar [13][38].

3.2.3. RQ3: Apa saja teknik Machine Learning yang paling menjanjikan untuk deteksi DDoS, berdasarkan literatur saat ini?

Berdasarkan literatur, teknik *Machine Learning* yang paling menjanjikan untuk deteksi DDoS meliputi model pembelajaran mendalam, model hibrida, dan teknik pembelajaran ensemble.

1) Model Pembelajaran Mendalam: Convolutional Neural Networks (CNNs) dan Long Short-Term Memory (LSTM) networks telah menunjukkan kinerja luar biasa dalam mendeteksi pola serangan yang kompleks. Model-model ini unggul di lingkungan yang memiliki lalu lintas jaringan berdimensi tinggi dan data dinamis, seperti yang terlihat di pengaturan IoT dan SDN. Sebagai contoh, model Tree-CNN menunjukkan akurasi dan ketahanan tinggi di berbagai dataset, terutama dalam mendeteksi jenis serangan yang canggih seperti serangan DDoS berbasis volumetrik dan protokol. Recurrent Neural Networks (RNN), khususnya yang digabungkan dengan LSTM, juga menunjukkan potensi besar dalam analisis data sekuensial, menangkap ketergantungan temporal dalam lalu lintas jaringan dan membuatnya sangat efektif untuk deteksi anomali berbasis waktu dalam serangan [18][27][32].
2) Model Hibrida: Menggabungkan teknik seperti Autoencoder dengan LSTM dan clustering dengan klasifikasi, telah terbukti efektif dalam deteksi anomali waktu nyata. Model-model ini menawarkan kemampuan deteksi yang tangguh dengan menangani pola serangan yang berkembang dengan efektif. Sebagai contoh, model hibrida AE-LSTM menunjukkan janji dalam mengatasi ketidakseimbangan kelas dan mendeteksi jenis serangan yang baru muncul [32].
3) Pembelajaran Ensemble: Metode ensemble, seperti Random Forest, SVM, dan XGBoost, merupakan pesaing kuat untuk deteksi DDoS karena mereka menggabungkan output dari beberapa pengklasifikasi, meningkatkan akurasi deteksi dan mengurangi false positives. Metode-metode ini terbukti efisien secara komputasional sambil tetap memberikan kinerja tinggi. Sebagai contoh, dalam sistem berbasis SDN, metode ensemble seperti Random Forest telah digunakan untuk menangani jaringan berskala besar sambil mempertahankan akurasi tinggi [33].
4) Federated Learning: Federated Learning muncul sebagai pendekatan yang menjanjikan untuk deteksi DDoS multi-domain, khususnya dalam skenario yang melibatkan masalah privasi data. Metode ini memungkinkan model dilatih di berbagai jaringan dan perangkat tanpa harus membagikan data dasar, sehingga mengakui masalah kesendirian sambil tetap memberikan deteksi yang efektif [11][34].
5) Generative Adversarial Networks (GANs): Generative Adversarial Networks (GANs) menunjukkan potensi dalam meningkatkan deteksi DDoS, terutama dalam lingkungan multi-domain di mana pola serangan sangat bervariasi. GANs dapat menghasilkan data serangan sintetis, membantu mengatasi ketidakseimbangan kelas dan meningkatkan ketahanan model terhadap jenis serangan baru [15][34].

IV. KESIMPULAN

Dari penelitian yang kami lakukan, dapat diambil kesimpulan sebagai berikut:

1. Efektivitas Metode Machine Learning dalam Deteksi DDoS (RQ1): Model pembelajaran mesin, khususnya CNN dan LSTM, terbukti sangat efektif dalam mendeteksi serangan DDoS dengan akurasi tinggi di berbagai lingkungan jaringan, termasuk SDN dan IoT. Meskipun demikian, meskipun model ini sangat akurat, mereka menghadapi tantangan dalam hal efisiensi komputasi dan memori, yang menghambat penerapan mereka pada jaringan berskala besar dengan lalu lintas tinggi.
2. Tantangan dalam Skalabilitas dan Pola Serangan yang Berkembang (RQ2): Skalabilitas menjadi tantangan utama ketika jumlah data dan kompleksitas serangan meningkat. Terutama di lingkungan dinamis seperti SDN dan IoT, model pembelajaran mesin mengalami kesulitan dalam menangani

volume besar lalu lintas yang diperlukan untuk deteksi waktu nyata. Selain itu, serangan DDoS yang terus berkembang, termasuk serangan berbasis rendah dan teknik amplifikasi, mempersulit kemampuan model dalam mendeteksi ancaman baru.

3. Metode Machine Learning yang Menjanjikan untuk Deteksi DDoS (RQ3): Teknik yang paling menjanjikan untuk deteksi DDoS termasuk pembelajaran mendalam (CNN, LSTM), model hibrida (seperti Autoencoder dengan LSTM), dan pembelajaran ensemble (seperti Random Forest dan XGBoost). Selain itu, pendekatan federated learning juga menunjukkan potensi besar untuk mengatasi masalah terkait privasi data dan skalabilitas, memungkinkan pelatihan model di beberapa domain tanpa berbagi data sensitif

REFERENSI

[1] M. A. Hossain and M. S. Islam, "Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity," *Meas. Sensors*, vol. 32, p. 101037, Apr. 2024, doi: 10.1016/j.measen.2024.101037.

[2] M. Shafi, A. H. Lashkari, V. Rodriguez, and R. Nevo, "Toward Generating a New Cloud-Based Distributed Denial of Service (DDoS) Dataset and Cloud Intrusion Traffic Characterization," *Information*, vol. 15, no. 4, p. 195, Mar. 2024, doi: 10.3390/info15040195.

[3] G. S. Rao and P. K. Subbarao, "A Novel Approach for Detection of DoS / DDoS Attack in Network Environment using Ensemble Machine Learning Model," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 9, pp. 244–253, 2023, doi: 10.17762/ijritcc.v11i9.8340.

[4] Y. Su, D. Xiong, K. Qian, and Y. Wang, "A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network," *Electronics*, vol. 13, no. 4, p. 807, Feb. 2024, doi: 10.3390/electronics13040807.

[5] S. Haider *et al.*, "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[6] P. Kumar *et al.*, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–15, Apr. 2022, doi: 10.1155/2022/5713092.

[7] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[8] E. Triandini, S. Jayanatha, A. Indrawan, G. Werla Putra, and B. Iswara, "Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia," *Indones. J. Inf. Syst.*, vol. 1, no. 2, p. 63, 2019, doi: 10.24002/ijis.v1i2.1916.

[9] S. Holge *et al.*, "The Impact of Age-Related Sensory Impairments (Hearing, Vision, and Taste) On Cognitive Function, Social Interaction, and Quality of Life in Older Adults," *Int. J. Geriatr. Gerontol.*, vol. 6, no. 1, Apr. 2023, doi: 10.29011/2577-0748.100055.

[10] Y. Suarghana, "Systematic Review of Machine Learning-Based DDoS Detection in SDN Networks : A PRISMA Approach," in *ABEC 4thInternational Annual Conference*, 2024, pp. 166–174.

[11] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "P4-HLDMC: A Novel Framework for DDoS and ARP Attack Detection and Mitigation in SD-IoT Networks Using Machine Learning, Stateful P4, and Distributed Multi-Controller Architecture," *Mathematics*, vol. 11, no. 16, p. 3552, 2023, doi: 10.3390/math11163552.

[12] R. Ahmad, R. Wazirali, Q. Bsoul, T. Abu-Ain, and W. Abu-Ain, "Feature-selection and mutual-clustering approaches to improve dos detection and maintain wsns' lifetime," *Sensors*, vol. 21, no. 14, 2021, doi: 10.3390/s21144821.

[13] C. S. Shieh, F. A. Ho, M. F. Horng, T. T. Nguyen, and P. Chakrabarti, "Open-Set Recognition in Unknown DDoS Attacks Detection With Reciprocal Points Learning," *IEEE Access*, vol. 12, no. March, pp. 56461–56476, 2024, doi: 10.1109/ACCESS.2024.3388149.

[14] D. Said, M. Bagaa, A. Oukaira, and A. Lakhssassi, "Quantum Entropy and Reinforcement Learning for Distributed Denial of Service Attack Detection in Smart Grid," *IEEE Access*, vol. 12, no. July, pp. 129858–129869, 2024, doi: 10.1109/ACCESS.2024.3441931.

[15] M. Zeeshan *et al.*, "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," *IEEE Access*, vol. 10, pp. 2269–2283, 2022, doi: 10.1109/ACCESS.2021.3137201.

[16] P. Rivas, J. Orduz, T. Das Jui, C. DeCusatis, and B. Khanal, "Quantum-Enhanced Representation Learning: A Quanvolutional Autoencoder Approach against DDoS Threats," *Mach. Learn. Knowl. Extr.*, vol. 6, no. 2, pp. 944–964, 2024, doi: 10.3390/make6020044.

[17] U. O. Obonna *et al.*, "Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms," *Futur. Internet*, vol. 15, no. 8, 2023, doi: 10.3390/fi15080280.

[18] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks - Current Research Solutions," *IEEE Access*, vol. 12, no. February, pp. 17982–18011, 2024, doi:

10.1109/ACCESS.2024.3360868.
[19] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.
[20] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," *IEEE Access*, vol. 11, no. March, pp. 28934–28954, 2023, doi: 10.1109/ACCESS.2023.3260256.
[21] S. A. D. AlSharman, O. Al-Khaleel, and M. Al-Ayyoub, "A Detailed Inspection of Machine Learning Based Intrusion Detection Systems for Software Defined Networks," *Internet of Things*, vol. 5, no. 4, pp. 756–784, 2024, doi: 10.3390/iot5040034.
[22] A. A. Alashhab *et al.*, "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," *IEEE Access*, vol. 12, no. April, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
[23] A. A. Alahmadi *et al.*, "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions," *Electron.*, vol. 12, no. 14, pp. 1–24, 2023, doi: 10.3390/electronics12143103.
[24] F. B. Saghezchi, G. Mantas, M. A. Violas, A. M. de Oliveira Duarte, and J. Rodriguez, "Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs," *Electron.*, vol. 11, no. 4, pp. 1–14, 2022, doi: 10.3390/electronics11040602.
[25] S. Ahmed *et al.*, "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron," *Futur. Internet*, vol. 15, no. 2, pp. 1–24, 2023, doi: 10.3390/fi15020076.
[26] Z. Liu, X. Yin, and Y. Hu, "CPSS LR-DDoS Detection and Defense in Edge Computing Utilizing DCNN Q-Learning," *IEEE Access*, vol. 8, no. 3, pp. 42120–42130, 2020, doi: 10.1109/ACCESS.2020.2976706.
[27] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Ben Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," *IEEE Access*, vol. 11, no. October, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
[28] J. Halladay *et al.*, "Detection and Characterization of DDoS Attacks Using Time-Based Features," *IEEE Access*, vol. 10, pp. 49794–49807, 2022, doi: 10.1109/ACCESS.2022.3173319.
[29] M. A. O. Rabah, H. Drid, Y. Medjadba, and M. Rahouti, "Detection and Mitigation of Distributed Denial of Service Attacks Using Ensemble Learning and Honeypots in a Novel SDN-UAV Network Architecture," *IEEE Access*, vol. 12, no. July, pp. 128929–128940, 2024, doi: 10.1109/ACCESS.2024.3443142.
[30] T. E. Ali, Y. W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," *Appl. Sci.*, vol. 13, no. 5, 2023, doi: 10.3390/app13053183.
[31] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," *Electron.*, vol. 9, no. 3, pp. 1–19, 2020, doi: 10.3390/electronics9030413.
[32] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810–146821, 2021, doi: 10.1109/ACCESS.2021.3123791.
[33] M. B. Bankó *et al.*, "Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges," *Algorithms*, vol. 18, no. 4, 2025, doi: 10.3390/a18040209.
[34] L. H. de Melo, G. de C. Bertoli, M. Nogueira, A. L. dos Santos, and L. A. P. Junior, "Anomaly-Flow: A Multi-domain Federated Generative Adversarial Network for Distributed Denial-of-Service Detection," *IEEE Access*, pp. 1–9, 2025, doi: 10.1109/MNET.2025.3567251.
[35] S. Shanmuga Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, "Machine Learning based DDOS Detection," *2020 Int. Conf. Emerg. Smart Comput. Informatics, ESCI 2020*, pp. 234–237, 2020, doi: 10.1109/ESCI48226.2020.9167642.
[36] U. Tariq, "Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs," *World Electr. Veh. J.*, vol. 15, no. 9, p. 395, 2024, doi: 10.3390/wevj15090395.
[37] F. Alasmary, S. Alraddadi, S. Al-Ahmadi, and J. Al-Muhtadi, "ShieldRNN: A Distributed Flow-Based DDoS Detection Solution for IoT Using Sequence Majority Voting," *IEEE Access*, vol. 10, no. June, pp. 88263–88275, 2022, doi: 10.1109/ACCESS.2022.3200477.
[38] R. T. A. Al-Dulaimi and A. K. Türkben, "A Hybrid Tree Convolutional Neural Network with Leader-Guided Spiral Optimization for Detecting Symmetric Patterns in Network Anomalies," *Symmetry (Basel).*, vol. 17, no. 3, 2025, doi: 10.3390/sym17030421.
[39] D. Akinleye and O. Godwin, "Optimizing SDN-Based DDoS Mitigation Using Machine Learning," 2024.
[40] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, "A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking," *Sensors*, vol. 23, no. 9, 2023, doi: 10.3390/s23094441.