terapan
ilmu pengetahuan

MDPI

Artikel

Teknik Pembelajaran Mesin untuk Mendeteksi Serangan DDoS di SDN: Tinjauan Sistematis

Tariq Emad Ali†, Yung Wey Chong *Bahasa Indonesia: ,† dan Selvakumar Manickam†

Pusat IPv6 Tingkat Lanjut Nasional, Universiti Sains Malaysia, Gelugor 11800, Penang, Malaysia
* Korespondensi: chong@usm.my
† Para penulis ini memberikan kontribusi yang sama terhadap karya ini.

Abstrak: Kemajuan terbaru dalam pendekatan keamanan telah meningkatkan kemampuan untuk mengidentifikasi dan mengurangi semua jenis ancaman atau serangan dalam infrastruktur jaringan apa pun, seperti jaringan yang ditentukan perangkat lunak (SDN), dan melindungi arsitektur keamanan internet dari berbagai ancaman atau serangan. Pembelajaran mesin (ML) dan pembelajaran mendalam (DL) adalah beberapa teknik paling populer untuk mencegah serangan penolakan layanan terdistribusi (DDoS) pada semua jenis jaringan. Tujuan dari tinjauan sistematis ini adalah untuk mengidentifikasi, mengevaluasi, dan membahas upaya baru pada strategi deteksi serangan DDoS berbasis ML/DL dalam jaringan SDN. Untuk mencapai tujuan kami, kami melakukan tinjauan sistematis di mana kami mencari publikasi yang menggunakan pendekatan ML/DL untuk mengidentifikasi serangan DDoS di jaringan SDN antara tahun 2018 dan awal November 2022. Untuk mencari literatur kontemporer, kami telah secara ekstensif menggunakan sejumlah perpustakaan digital (termasuk IEEE, ACM, Springer, dan perpustakaan digital lainnya) dan satu mesin pencari akademis (Google Scholar). Kami telah menganalisis studi yang relevan dan mengkategorikan hasil SLR ke dalam lima area: (i) Berbagai jenis deteksi serangan DDoS dalam pendekatan ML/DL; (ii) metodologi, kekuatan, dan kelemahan pendekatan ML/DL yang ada untuk deteksi serangan DDoS; (iii) kumpulan data dan kelas serangan yang dijadikan tolok ukur dalam kumpulan data yang digunakan dalam literatur yang ada; (iv) strategi praproses, nilai hiperparameter, pengaturan eksperimen, dan metrik kinerja yang digunakan dalam literatur yang ada; dan (v) kesenjangan penelitian saat ini dan arah masa depan yang menjanjikan.

Kata kunci:pembelajaran mesin; pembelajaran mendalam; penolakan layanan terdistribusi; kumpulan data

Kutipan: Ali, TE; Chong, Y.-W.; Manickam, S. Teknik Pembelajaran Mesin untuk Mendeteksi Serangan DDoS di SDN: Tinjauan Sistematis.*Ilmu Terapan***Tahun 2023**Bahasa Indonesia:*13*, 3183. https://doi.org/10.3390/app13053183

Editor Akademik: Luis Javier Garcia Villalba

Diterima: 19 Januari 2023
Direvisi: 23 Februari 2023
Disetujui: 26 Februari 2023
Diterbitkan: 2 Maret 2023

1. Pendahuluan

Dengan meningkatnya permintaan akan konten multimedia berkualitas tinggi, jaringan berbasis perangkat lunak (SDN) telah diusulkan sebagai masa depan arsitektur internet. Dalam paradigma jaringan ini, bidang kontrol (yang merupakan otak jaringan) dan bidang data (yang merupakan otot) dipisahkan [1]. Model SDN mencakup pengontrol SDN, serta API selatan dan utara. Arsitektur ini menyediakan jaringan yang dapat diprogram dan terpusat yang dapat menyediakan layanan secara dinamis [2]. OpenFlow (OF) adalah protokol standar dan terbuka yang digunakan dalam SDN yang menjelaskan bagaimana pengontrol terpusat mengonfigurasi dan mengatur lapisan kontrol dalam jaringan. Data dalam SDN disimpan dalam tabel Mac dan tabel perutean dan ditangani oleh berbagai protokol peralihan dan perutean yang canggih. Tabel-tabel ini digunakan untuk membuat bidang penerusan dalam jaringan tradisional [3].

Masyarakat saat ini sangat bergantung pada internet, yang sangat penting untuk transaksi ekonomi, pendidikan, dan komunikasi. Namun, seiring dengan banyaknya manfaatnya, internet telah mengalami peningkatan aktivitas kriminal, seperti peretasan, penyebaran informasi palsu, dan serangan penolakan layanan (DoS). Serangan DoS terjadi ketika layanan, sistem, atau jaringan yang sah dibuat tidak dapat diakses oleh pengguna yang dituju. Serangan DDoS, subkategori serangan DoS, melibatkan penyerang yang membobol beberapa sistem komputasi untuk mengganggu lalu lintas rutin target tertentu [4].

Bertahan terhadap serangan DoS dan DDoS lebih menantang di SDN daripada di jaringan tradisional. Jenis serangan ini telah menjadi ancaman signifikan bagi jaringan komputer, yang menyebabkan penurunan kinerja jaringan dengan menghabiskan sumber daya yang tersedia dan menonaktifkan layanan. Serangan DoS/DDoS yang efektif secara sengaja menghabiskan sumber daya dan mencegah host mengakses layanan yang ditargetkan. Di SDN, serangan DoS/DDoS dapat membanjiri bidang kontrol, bidang data, atau lebar pita bidang kontrol, yang berpotensi melumpuhkan seluruh jaringan. Serangan pada bidang data dapat menghabiskan semua RAM tabel aliran terbatas sakelar OpenFlow, yang mengakibatkan pembuangan paket dan ketidakmampuan untuk menginstal aturan aliran yang baru diterima. Serangan DoS/DDoS pada bidang data juga dapat melibatkan pembuatan sejumlah besar aliran baru yang tidak sesuai dengan entri tabel aliran. Paket-paket ini di-buffer oleh sakelar, dan jika buffer terisi penuh, seluruh paket dikirim ke pengontrol, bukan hanya header melalui pesan paket-masuk. Hal ini dapat menyebabkan keterlambatan dalam menginstal aturan aliran baru dan penggunaan lebar pita komunikasi yang lebih tinggi [5].

Perbedaan utama antara serangan DoS dan DDoS adalah bahwa DoS menggunakan banyak koneksi internet untuk melumpuhkan jaringan komputer korban, sedangkan serangan DDoS menggunakan jaringan perangkat yang dikendalikan oleh penyerang. Serangan DDoS lebih sulit dideteksi dan dilacak karena diluncurkan dari berbagai lokasi, dan volume serangan yang digunakan sangat besar. Serangan DDoS dilakukan secara berbeda dari serangan DoS, yang sering kali dilakukan melalui skrip atau alat DoS seperti Low-Orbit Ion Cannon. Jenis serangan DOS meliputi buffer overflows, ICMP floods, teardrop attacks, dan flooding attacks, sedangkan jenis serangan DDOS meliputi serangan volumetrik, serangan fragmentasi, serangan lapisan aplikasi, dan serangan protokol. Serangan DDoS lebih merusak daripada serangan DoS karena melibatkan beberapa sistem, sehingga lebih sulit bagi tim keamanan dan produk untuk menentukan sumber serangan [6].

Contoh-contoh yang disebutkan di atas menyoroti kebutuhan akan pendekatan yang andal untuk mengidentifikasi serangan DDoS. Serangan DDoS dapat dideteksi menggunakan berbagai pendekatan, termasuk analisis statistik, ML/DL, dll. Di antara pendekatan-pendekatan ini, pendekatan pembelajaran mendalam adalah yang paling efektif dalam mengidentifikasi serangan DDoS. Berikut ini adalah kekurangan dari pendekatan-pendekatan alternatif yang telah dipelajari hingga saat ini:

- Keterbatasan Metode Statistik: Keterbatasan berbagai pendekatan deteksi DDoS telah dipelajari, termasuk metode statistik dan pembelajaran mesin (ML). Metode statistik didasarkan pada informasi aliran jaringan masa lalu, yang mungkin tidak secara akurat menggambarkan lalu lintas jaringan saat ini karena aliran jaringan yang tidak bersahabat terus berkembang. Teknik-teknik tersebut sangat bergantung pada kriteria yang ditentukan pengguna, yang harus dapat berubah secara dinamis agar dapat mengikuti perubahan dalam jaringan. Teknik statistik seperti entropi dan korelasi memerlukan sejumlah besar upaya komputasi, sehingga tidak cocok untuk deteksi waktu nyata [7]. Metode ML bekerja secara efektif pada sejumlah kecil data dan menentukan sifat statistik serangan sebelum mengklasifikasikan atau menilai serangan tersebut. Namun, metode ini memerlukan pembaruan model rutin untuk mencerminkan perubahan dalam pola serangan, dan algoritme tertentu dapat memerlukan waktu yang sangat lama untuk diuji [8].
- Keterbatasan Machine Learning (ML): Bahkan ketika menerapkan prinsip ML pada data dalam jumlah yang sangat sedikit, ML dapat berfungsi dengan cukup efektif. ML terlebih dahulu menentukan sifat statistik serangan sebelum mengklasifikasikan atau menilainya. Selain itu, ML memerlukan pembaruan model rutin untuk mencerminkan perubahan pola serangan [9]. Teknik ML mengatasi masalah ini dengan menguraikannya menjadi submasalah yang dapat dikelola, mengatasi submasalah tersebut, dan kemudian memberikan solusi lengkap. Algoritma ML biasanya memerlukan waktu pelatihan yang singkat dan waktu pengujian yang jauh lebih lama [10].

Teknik DL dapat mengidentifikasi serangan DDoS secara efektif, karena data dapat diklasifikasikan dan fitur diekstraksi menggunakan algoritma DL, tidak seperti dalam ML yang perlu mengekstraksi fitur dalam algoritma yang berbeda sebelum memasukkannya ke dalam model. Dalam lingkungan keamanan saat ini, sistem deteksi yang dapat menangani ketidaktersediaan data merupakan suatu keharusan. Meskipun label untuk lalu lintas yang valid sering kali dapat diakses, label untuk lalu lintas berbahaya kurang umum. Metode DL mampu mengekstraksi informasi dari data yang tidak lengkap [11], dan sesuai untuk mengenali serangan dengan tingkat rendah. Untuk mengenali serangan dengan tingkat rendah,

data historis diperlukan, yang digunakan teknik DL untuk menemukan hubungan jangka panjang dari pola temporal [12]. Akibatnya, dalam keadaan di mana data tersebut tersedia, teknik DL dapat sangat membantu. Selama fase pelatihan, metode DL melakukan operasi matematika yang rumit di berbagai lapisan dan parameter tersembunyi [13]. Komputasi kuantum telah menunjukkan janji besar dalam berbagai bidang, termasuk kecerdasan buatan (AI), keamanan siber, dan penelitian medis. Komputasi kuantum dapat membantu AI untuk memecahkan masalah yang lebih rumit dengan mempercepat komputasi. Komputasi kuantum dapat digunakan dengan model SML dan DL untuk pelatihan cepat atau peningkatan lainnya. Dengan mengatasi masalah rumit yang membutuhkan kumpulan data besar dan sulit diproses, komputasi kuantum dapat meningkatkan kemampuan pembelajaran mendalam [14 Bahasa Indonesia:15].

Dibandingkan dengan studi tinjauan lain dalam literatur, Tabel1menggambarkan bahwa mayoritas studi ini belum memberikan evaluasi komprehensif mengenai teknik persiapan, manfaat, dan jenis serangan yang digunakan dalam kumpulan data yang dianalisis. Sebaliknya, studi sistematis kami menyajikan tinjauan ekstensif mengenai berbagai teknik pembelajaran mendalam untuk mendeteksi serangan DDoS. Melalui penelitian ini, kami telah mengidentifikasi kesenjangan dalam literatur, yaitu, bahwa evaluasi komprehensif metode pembelajaran mendalam untuk deteksi DDoS masih kurang. Studi kami berkontribusi untuk mengatasi kesenjangan ini dengan memberikan tinjauan dan analisis komprehensif mengenai kekuatan dan kelemahan berbagai pendekatan pembelajaran mendalam untuk mendeteksi serangan DDoS. Dengan demikian, tinjauan kami memberikan wawasan berharga mengenai keadaan terkini dalam deteksi serangan DDoS menggunakan teknik pembelajaran mendalam.

Tabel 1. Perbandingan berbagai makalah penelitian secara rinci (✓ = Ya; *Bahasa Indonesia:*=TIDAK).

Artikel Ulasan	**Ferrag dan kawan-kawan. [16][Bahasa Indonesia]**	**Aleesa dan lain-lain. [17][Bahasa Indonesia]**	**Gamage dan kawan-kawan. [18][Bahasa Indonesia]**	**Ahmad dan lain-lain. [19][Bahasa Indonesia]**	**Ahmad dan lain-lain. [20][Bahasa Indonesia]**	**Artikel ini**
Terfokus	Keamanan dunia maya	IDENTITAS	NID	IDENTITAS	Keamanan IoT	Serangan DDoS
deteksi intrusi						
Bahasa Inggris ML/DL	DL	D	DL	ML/DL	ML/DL	ML/DL
Studi sistematis	*Bahasa Indonesia:*	✓	D	✓		✓
Taksonomi	*Bahasa Indonesia:*				*Bahasa Indonesia:*	✓
Strategi praproses	*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	✓
Jenis serangan yang digunakan dalam literatur yang ada dari kumpulan data	*Bahasa Indonesia:*		*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	
Kekuatan	*Bahasa Indonesia:*	*Bahasa Indonesia:*	✓	*Bahasa Indonesia:*	*Bahasa Indonesia:*	✓
Kelemahan	*Bahasa Indonesia:*	*Bahasa Indonesia:*	✓			✓
Kesenjangan penelitian	*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	*Bahasa Indonesia:*	✓

Kami meninjau sistem deteksi serangan DDoS berdasarkan teknik DL dalam penelitian ini menggunakan protokol SLR, dan menawarkan temuan berikut:

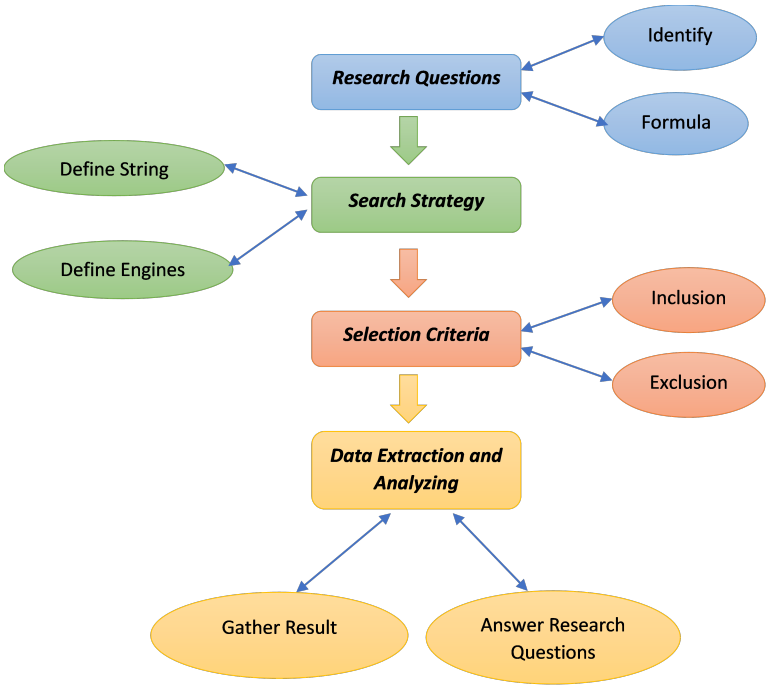
- Berdasarkan kriteria umum, teknologi deteksi serangan DDoS modern yang melibatkan algoritma pembelajaran mendalam telah diidentifikasi dan dikelompokkan.
- Metodologi, manfaat, dan kelemahan sistem ML/DL saat ini untuk mendeteksi serangan DDoS telah diuraikan.
- Berbagai jenis serangan dalam kumpulan data yang digunakan dalam studi terkini serta kumpulan data acuan DDoS yang dapat diakses telah dikompilasi.
- Inti tinjauan kami difokuskan pada teknik pra-pemrosesan data, penyesuaian hiperparameter, konfigurasi pengujian, dan ukuran kualitas yang digunakan oleh sistem ML/DL saat ini untuk mendeteksi serangan DDoS.
- Tujuan utama penelitian ini adalah untuk mengidentifikasi area untuk penelitian masa depan di bidang ini dan untuk menyoroti kesenjangan penelitian saat ini.

Sisa ulasan ini disusun sebagai berikut: protokol SLR dijelaskan di Bagian2; Bagian3 membahas metode ML/DL terkini yang telah digunakan dalam literatur untuk mendeteksi serangan DDoS; di Bagian4, metodologi, kelebihan, dan kekurangan dari berbagai penelitian dibahas; kumpulan data DDoS yang tersedia dan kelas serangan dalam kumpulan data yang umum digunakan dalam literatur dijelaskan di Bagian5; teknik praproses dan hiperparameter dijelaskan di Bagian6Bahasa Indonesia:

di Bagian7, kesenjangan penelitian dalam literatur saat ini ditunjukkan; akhirnya, di Bagian8, kesimpulan kami dijelaskan dan prospek masa depan dieksplorasi.

2. Protokol Tinjauan Literatur Sistematis (SLR)

Makalah ini menyajikan tinjauan pustaka sistematis (SLR) yang dilakukan antara tahun 2018 dan 2022 dengan fokus pada deteksi serangan DDoS menggunakan metode DL. Metode SLR yang digunakan dalam penelitian ini mematuhi rekomendasi yang dibuat dalam [21], menyediakan pendekatan komprehensif untuk memahami literatur tentang subjek tersebut. Tidak seperti makalah tinjauan sebelumnya, studi ini mencakup analisis teknik persiapan, keuntungan, dan berbagai jenis serangan yang digunakan dalam berbagai set data. Keluaran SLR adalah kumpulan publikasi penelitian yang disusun menurut taksonomi teknik DL yang digunakan. Dengan mengidentifikasi keterbatasan penelitian dalam kumpulan literatur, studi ini menawarkan opsi baru yang menarik untuk penelitian di masa mendatang. Secara keseluruhan, makalah ini menyajikan pendekatan yang ketat dan baru untuk tinjauan sistematis teknik deteksi serangan DDoS. Ringkasan protokol penelitian ditunjukkan pada Gambar1, dan dijelaskan secara rinci di bawah ini.



Gambar 1. Ikhtisar protokol survei.

2.1. Pertanyaan Penelitian

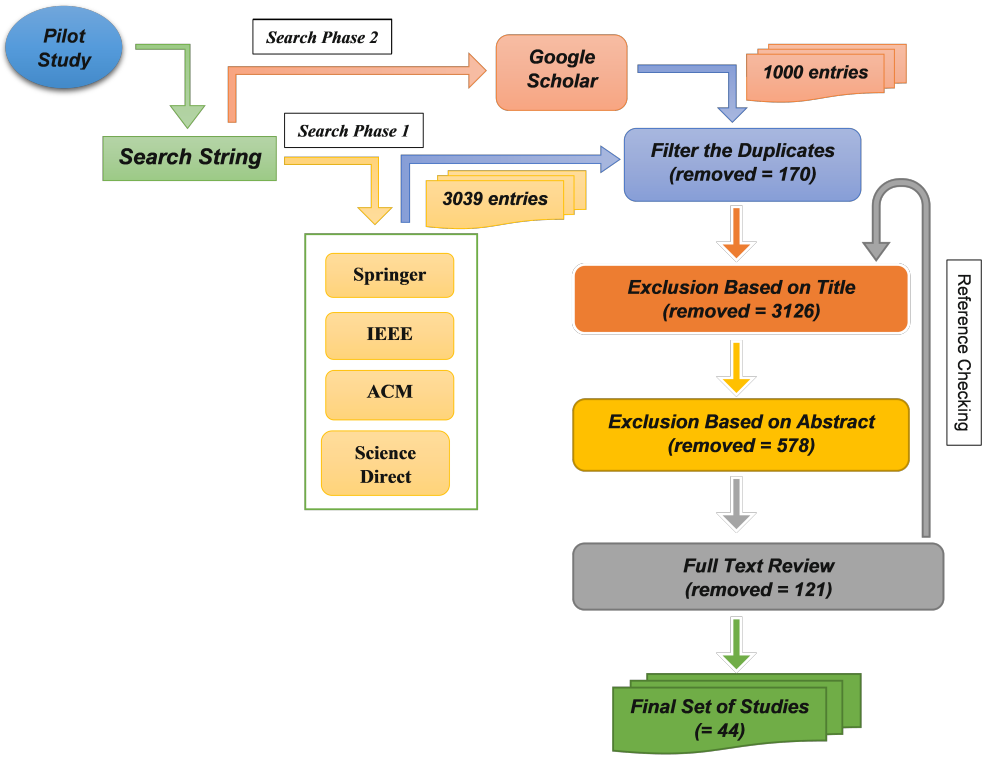
Tujuan utama dari tinjauan sistematis adalah untuk menjawab pertanyaan penelitian dengan menganalisis data yang diambil dari penelitian sebelumnya. Pertanyaan penelitian yang dibahas dalam karya ini meliputi:

- **Nomor RQ1:**Apa saja teknik DL terkini untuk mendeteksi serangan DDoS, dan bagaimana serangan tersebut dapat diklasifikasikan?
- **RQ2 adalah:**Apa saja metodologi, kelebihan, dan kekurangan metode DL saat ini untuk mendeteksi serangan DDoS?
- **RQ3:**Jenis serangan apa saja yang termasuk dalam kumpulan data yang digunakan dalam penelitian saat ini, dan kumpulan data DDoS acuan apa saja yang tersedia?
- **RQ4 adalah:**Teknik praproses, pengaturan hiperparameter, konfigurasi eksperimental, dan metrik kinerja apa yang digunakan oleh algoritma DL saat ini untuk mendeteksi serangan DDoS?
- **RQ5:**Apa saja kesenjangan penelitian dalam literatur yang diterbitkan?

2.2. Strategi Pencarian

Strategi pencarian yang efektif sangat penting untuk setiap survei sistematis. Dalam studi ini, serangkaian basis data yang dipilih dengan cermat digunakan untuk menggali literatur yang relevan. Dua fase pencarian dilakukan antara tahun 2018 dan 2022. Fase pertama mencari empat basis data: ACM, IEEE Explore, Springer, dan Science Direct. Fase kedua menambahkan Google Scholar untuk memastikan bahwa semua materi yang relevan disertakan. Untuk menyempurnakan rangkaian pencarian, penelitian percontohan dilakukan. Dari hasil pencarian, sepuluh artikel yang sangat dirujuk dan relevan dipilih.

Salah satu istilah pencarian yang digunakan di beberapa perpustakaan digital dengan sedikit perubahan adalah (deteksi serangan DDoS menggunakan pendekatan DL ATAU deteksi serangan DDoS menggunakan pendekatan ML ATAU Deteksi serangan DDoS menggunakan DL ATAU Deteksi serangan DDoS menggunakan ML). Dengan menggunakan "pilihan penyaringan", kami dapat meningkatkan hasil dari perpustakaan digital yang dipilih. Gambar2menunjukkan aliran berbagai fase protokol survei.



Gambar 2. Metode Tinjauan Literatur Sistematis.

2.3. Kriteria Pemilihan Studi

Tujuan utama dari proses seleksi penelitian adalah untuk mengidentifikasi literatur relevan yang membahas pertanyaan penelitian yang ditetapkan sambil mengecualikan materi yang tidak relevan. Untuk tujuan ini, kriteria inklusi dan eksklusi diterapkan; ini mencakup makalah penelitian yang dibangun berdasarkan studi relevan sebelumnya. Pada tahap 1, kami mengambil 1000 item pertama dari fase pencarian kedua dan menggabungkannya dengan 3039 entri dari fase pencarian pertama untuk membuat 4039 entri. Pada tahap 2, 170 entri duplikat dihilangkan. Setelah tahap 2, artikel dihapus sesuai dengan judulnya (3126), abstrak (581), dan teks lengkap (118). Pada akhirnya, (44) artikel penelitian dipilih. Studi yang tidak terkait dengan topik penelitian yang ditetapkan dihilangkan menggunakan kriteria inklusi dan eksklusi. Definisi berikut menjelaskan kriteria inklusi/eksklusi:

Kriteria inklusi:

• Semua publikasi yang menyajikan metode baru untuk deteksi serangan DDoS berbasis ML/DL
• Penelitian yang secara eksklusif memperhatikan teknik ML/DL
• Penelitian yang melibatkan topik terkait namun berbeda dalam elemen penting dimasukkan sebagai penelitian primer terpisah
• Penelitian yang menjawab pertanyaan penelitian
• Penelitian yang dibangun berdasarkan penelitian relevan sebelumnya
• Artikel yang dirilis antara tahun 2018 dan 2022.

Kriteria eksklusi:

• Artikel tidak ditulis dalam bahasa Inggris
• Penelitian yang tidak terkait dengan topik penelitian ini
• Meninjau makalah, editorial, diskusi, artikel data, komunikasi singkat, publikasi perangkat lunak, ensiklopedia, poster, abstrak, tutorial, karya yang sedang dalam proses, pidato utama, dan ceramah yang diundang
• Artikel yang tidak memberikan informasi yang cukup
• Duplikasi penelitian lain.

2.4. Pemeriksaan Referensi

Referensi dari (32) penelitian yang disimpan setelah pemindaian seluruh naskah dievaluasi untuk memastikan tidak ada karya penting yang terlewat. (76) makalah yang berkontribusi pada kesimpulan mereka kemudian dievaluasi lebih menyeluruh berdasarkan judul, abstrak, dan artikel lengkap menggunakan kriteria inklusi dan eksklusi yang sama seperti sebelumnya. Artikel berdasarkan judul (11), abstrak (51), dan seluruh artikel (12) dihapus pada putaran berikutnya. Dari makalah yang ditemukan melalui pemeriksaan referensi, (74) entri dihapus, sehingga hanya menghasilkan dua makalah tambahan.

2.5. Ekstraksi Data

Setelah memeriksa seluruh naskah, informasi yang relevan dikumpulkan berdasarkan pertanyaan penelitian kami. Informasi yang dikumpulkan dari setiap penelitian digunakan untuk melengkapi formulir yang telah disiapkan. Judul, teknik, kumpulan data yang digunakan, jumlah fitur, pengenalan kelas serangan dan asli, teknik praproses, konfigurasi pengujian untuk peningkatan model, metode evaluasi, kelebihan dan kekurangan model, dan ringkasan semuanya digunakan untuk mengevaluasi secara kritis kumpulan artikel akhir guna meringkas jawaban atas pertanyaan penelitian kami. Bidang yang digunakan untuk ekstraksi data dirinci dalam Tabel2.

Tabel 2. Bidang yang digunakan untuk ekstraksi data.

Bidang	Keterangan
Judul	Memberikan judul makalah penelitian
Pendekatan yang digunakan	Mencantumkan berbagai metode terkait ML/DL yang digunakan dalam artikel.
Kumpulan data	Mencantumkan berbagai kumpulan data yang digunakan dalam penelitian untuk analisis.
Jumlah fitur	Daftar fitur yang dipilih dari kumpulan data. Nama serangan yang digunakan dalam artikel Menjelaskan bagaimana data diproses terlebih dahulu sebelum model dilatih.
Identifikasi serangan dan klasifikasi yang sah	
Strategi praproses	
Pengaturan model dan pengoptimalan kinerja untuk eksperimen	Menjelaskan bagaimana eksperimen dilakukan dan mencantumkan nilai parameter model yang menghasilkan kinerja terbaik.
Metrik kinerja	Memberikan temuan saat menggunakan pengukuran yang berbeda untuk membandingkan satu model dengan model lainnya.
Kekuatan	Menjelaskan atribut positif model.
Kelemahan	Mencantumkan kekurangan model.
Ringkasan	Deskripsi singkat bidang-bidang yang disebutkan di atas

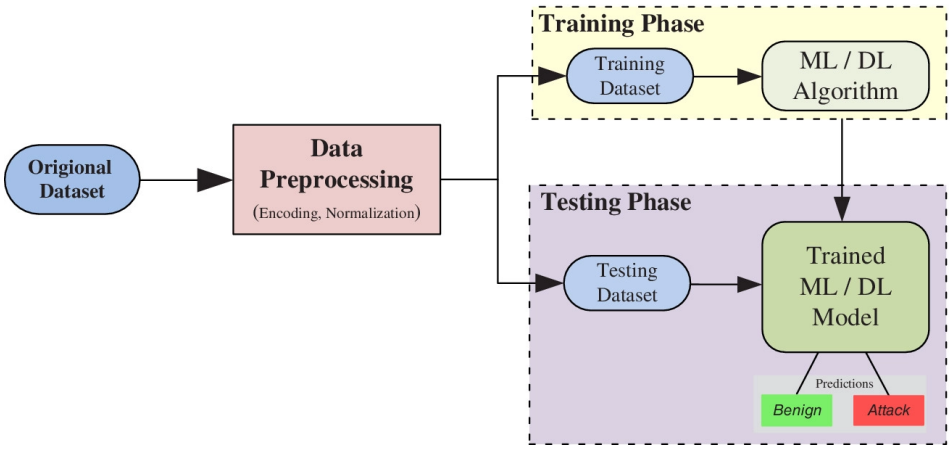
3. Teknik ML/DL Terbaru untuk Mendeteksi Serangan DDoS

Bidang ML merupakan subbidang kecerdasan buatan (AI) yang mencakup semua teknik dan algoritma yang memungkinkan komputer untuk belajar secara otomatis dari kumpulan data besar dengan menerapkan model matematika. Decision Tree (DT), K-Nearest Neighbor (KNN), Artificial Neural Network (ANN), Support Vector Machine (SVM), K-Means Clustering, Fast Learning Networks, Ensemble Methods, dan lainnya adalah metode ML paling populer yang digunakan untuk deteksi DDoS di SDN (kadang-kadang disebut Shallow Learning). Penjelasan singkat dari setiap kategori adalah sebagai berikut:

- **Pohon Keputusan (DT):**metode ML terbimbing fundamental yang memanfaatkan serangkaian aturan untuk mengklasifikasikan dan memprediksi data menggunakan regresi. Model ini terstruktur sebagai pohon dengan simpul, cabang, dan daun, di mana setiap simpul mewakili fitur atau karakteristik. Setiap daun pada cabang menunjukkan kemungkinan hasil atau label kelas, dan cabang itu sendiri menandakan keputusan atau aturan. Algoritme DT secara otomatis memilih atribut optimal untuk konstruksi pohon dan melakukan pemangkasan untuk menghilangkan cabang yang tidak perlu dan mencegah overfitting [22].
- **K-Tetangga Terdekat (KNN):**Algoritma K-Nearest Neighbor (KNN) adalah metode ML terbimbing sederhana yang menggunakan konsep “kesamaan fitur” untuk mengklasifikasikan sampel data tertentu. Dengan menentukan identitas sampel berdasarkan tetangganya dan seberapa jauh jaraknya dari mereka, KNN dapat secara efektif menentukan kelas sampel data. Nilai algoritma KNN*aku*parameter dapat memiliki dampak pada kinerjanya, dan memilih*aku*Nilai yang terlalu kecil atau terlalu besar dapat menyebabkan overfitting atau kategorisasi kasus sampel yang salah. Untuk meningkatkan tingkat deteksi serangan di kelas minoritas, peneliti menggunakan dataset benchmark terbaru, CSE-CIC-IDS2018, telah menerapkan Teknik Synthetic Minority Oversampling (SMOTE) untuk mengatasi masalah ketidakseimbangan dataset saat mengevaluasi kinerja berbagai algoritma ML, termasuk KNN [23].
- **Mesin Vektor Pendukung (SVM):**Support Vector Machine (SVM) adalah metode ML terbimbing yang menggunakan hyperplane pemisah margin maksimum dalam ruang fitur n-dimensi sebagai fondasinya. SVM dapat digunakan untuk memecahkan masalah linear dan non-linear, dengan menggunakan fungsi kernel untuk mengatasi masalah tersebut. Tujuan SVM adalah pertama-tama menerjemahkan vektor input berdimensi rendah ke dalam ruang fitur berdimensi tinggi menggunakan fungsi kernel, kemudian menggunakan vektor pendukung untuk membuat hyperplane marginal maksimum optimal yang berfungsi sebagai batas keputusan. Dengan mengidentifikasi kelas jinak dan berbahaya dengan benar, metode SVM dapat digunakan untuk mengidentifikasi serangan DDoS dengan efisiensi dan akurasi yang lebih baik [24].
- **Pengelompokan K-Rata-rata:**Tujuan di balik pengelompokan adalah untuk mengelompokkan kumpulan data yang sangat mirip untuk membagi data menjadi kelompok atau klaster yang bermakna. Salah satu teknik ML iteratif populer yang belajar tanpa pengawasan adalah pengelompokan K-Mean. Di sini,*Bahasa Inggris: K*menunjukkan jumlah total centroid (pusat klaster) dari suatu kumpulan data. Jarak biasanya diukur saat mengalokasikan titik data tertentu ke dalam klaster. Tujuan utamanya adalah untuk mengurangi jarak total antara setiap titik data dan centroid terkaitnya dalam klaster [25].
- **Jaringan Syaraf Tiruan (JST):**Fungsi sistem saraf manusia menjadi inspirasi bagi algoritma ML terbimbing yang dikenal sebagai ANN. Algoritma ini terdiri dari neuron (simpul), yang merupakan unit pemrosesan, dan koneksi yang menghubungkannya. Organisasi simpul-simpul ini mencakup lapisan masukan, beberapa level tersembunyi, dan lapisan keluaran. Algoritma backpropagation digunakan oleh ANN sebagai metode pembelajaran. Kapasitas pendekatan ANN untuk melakukan pemodelan nonlinier dengan belajar dari kumpulan data yang lebih besar merupakan manfaat utamanya. Namun, kesulitan mendasar dalam melatih model ANN adalah prosedur yang panjang yang diperlukan, karena kompleksitasnya dapat menghambat pembelajaran dan menghasilkan hasil yang kurang ideal [26].
- **Metode ansambel:**Gagasan utama di balik teknik ensemble adalah belajar dengan cara ensemble agar dapat memperoleh manfaat dari penggunaan beberapa classifier. Setiap classifier memiliki kelebihan dan kekurangannya sendiri; misalnya, mereka mungkin bagus dalam menemukan

jenis serangan tertentu dan buruk dalam mengenali jenis serangan lainnya. Dengan melatih beberapa pengklasifikasi, teknik ensemble dapat menggabungkan beberapa pengklasifikasi yang lemah untuk membuat satu pengklasifikasi yang lebih kuat, yang biasanya dipilih menggunakan mekanisme pemungutan suara [27].

DL adalah jenis ML yang digunakan dalam AI yang memiliki kemampuan untuk belajar dari data yang diawasi dan tidak terstruktur [28]. Model DL dikenal sebagai Deep Neural Networks atau Deep Neural Learning, karena teknologi ini menggunakan jaringan multi-lapis. Neuron menghubungkan level-level dan berperan dalam perhitungan matematika di balik proses pembelajaran [29]. Seperti yang terlihat pada Gambar3, tiga proses utama yang membentuk sebagian besar metode ML/DL adalah:**(Saya)**fase persiapan data,**(ii)**fase pelatihan, dan**(aku aku aku)**fase pengujian. Kumpulan data awalnya diproses terlebih dahulu untuk setiap solusi yang disarankan guna mengubahnya menjadi bentuk yang dapat digunakan oleh algoritme. Biasanya, fase ini melibatkan normalisasi dan pengodean. Kumpulan data mungkin perlu dibersihkan, yang dilakukan selama langkah ini jika perlu. Entri duplikat dan entri dengan data yang hilang dihapus. Kumpulan data pelatihan dan kumpulan data pengujian dibuat dengan membagi data yang telah diproses terlebih dahulu secara acak menjadi dua bagian. Biasanya, hampir semua (80%) dari ukuran kumpulan data awal biasanya terdiri dari kumpulan data pelatihan, dengan jumlah yang tersisa (20%) merupakan kumpulan data pengujian. Pada fase pelatihan berikutnya, algoritme ML atau DL diajarkan menggunakan kumpulan data pelatihan. Proporsi kumpulan data yang digunakan dan kompleksitas model yang dilatih memengaruhi berapa lama waktu yang dibutuhkan algoritme untuk belajar. Karena strukturnya yang rumit dan canggih, model DL sering kali memerlukan periode pelatihan yang lebih lama daripada model ML. Setelah pelatihan, model diuji menggunakan kumpulan data pengujian, dengan kinerja dinilai berdasarkan prediksi yang dibuat oleh model. Dalam kasus model deteksi DDoS, hal ini mengambil bentuk diklasifikasikannya kejadian lalu lintas jaringan sebagai kejadian jinak (normal) atau kejadian serangan.



Gambar 3. Metodologi untuk sistem deteksi DDoS berbasis pembelajaran mesin umum/pembelajaran mendalam.

Teknik DL dapat dibagi menjadi lima kelompok: pembelajaran hibrida, pembelajaran semi-supervised, pembelajaran contoh tersupervised, dan pembelajaran urutan tersupervised. Ringkasan singkat dari setiap kategori disediakan di bawah ini:

Pembelajaran instans yang diawasi: Supervised Instance l = Pembelajaran menggunakan aliran instance [18]. Untuk tujuan pelatihan, ia menggunakan contoh-contoh berlabel. Teknik yang paling populer di area ini adalah:

- **Jaringan Saraf Dalam (DNN):**struktur DL fundamental yang memungkinkan model untuk belajar di berbagai level. Struktur ini terdiri dari beberapa lapisan tersembunyi, beserta lapisan input dan output. DNN digunakan untuk mensimulasikan fungsi nonlinier yang kompleks. Penambahan lebih banyak lapisan tersembunyi meningkatkan level abstraksi model, memperluas potensinya. Untuk tujuan klasifikasi, lapisan output terdiri dari satu lapisan yang terhubung sepenuhnya dan pengklasifikasi softmax. Fungsi Rectified Linear Unit (ReLU) umumnya digunakan sebagai fungsi aktivasi untuk lapisan tersembunyi [30Bahasa Indonesia:31].

- **Jaringan Syaraf Konvolusional (CNN):**CNN merupakan struktur DL yang sangat cocok untuk data gambar dan sinyal. Semua CNN memiliki lapisan input, tumpukan lapisan konvolusional dan penggabungan untuk ekstraksi fitur, lapisan yang terhubung penuh, dan pengklasifikasi softmax dalam lapisan klasifikasi. CNN telah mencapai kemajuan besar dalam bidang visi komputer, dan dapat melakukan fungsi ekstraksi fitur dan klasifikasi yang diawasi untuk tugas deteksi DDoS [32].

Pembelajaran sekuensi yang diawasi:dalam pembelajaran urutan terbimbing, serangkaian aliran digunakan; ketika belajar dari sekumpulan masukan, bentuk model ini melacak status masukan sebelumnya dalam memorinya. Model yang paling populer dari jenis ini meliputi:

- **Jaringan Saraf Berulang (RNN):**RNN dikembangkan untuk meningkatkan kemampuan jaringan neural feed-forward tradisional dan data sekuens model. Unit input, hidden, dan output membentuk RNN, dengan unit hidden bertindak sebagai elemen memori. Untuk mencapai keputusan, setiap unit RNN mempertimbangkan input saat ini dan hasil input sebelumnya. RNN umumnya digunakan dalam berbagai bidang, seperti pemahaman semantik, prediksi tulisan tangan, pemrosesan suara, dan identifikasi aktivitas manusia [33]. RNN dapat digunakan untuk ekstraksi fitur dan kategorisasi terbimbing dalam deteksi DDoS. Namun, RNN hanya dapat mengelola urutan hingga panjang tertentu sebelum mengalami masalah memori jangka pendek [34].

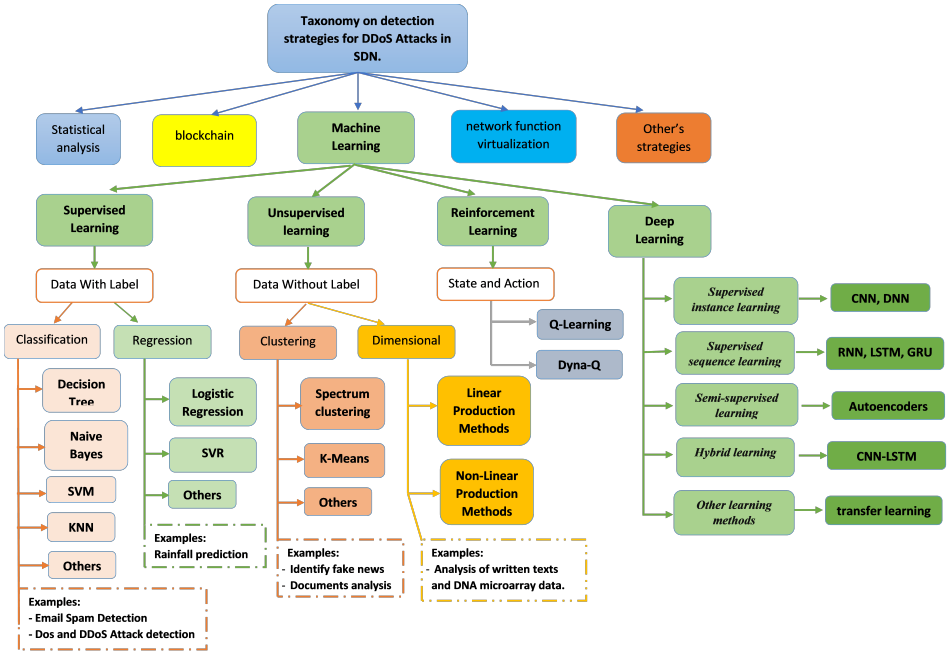
- **Memori Jangka Panjang dan Pendek (LSTM):**LSTM adalah struktur DL yang telah berhasil mengatasi tantangan RNN. Jaringan LSTM terdiri dari sel atau blok memori yang berbeda. Sel berikut menerima status tersembunyi dan status sel melalui tiga mekanisme yang dikenal sebagai gerbang, khususnya gerbang lupa, masukan, dan keluaran [35]. Blok memori dapat memilih data mana yang akan dipanggil kembali atau diabaikan. Gerbang lupa menghilangkan informasi dari masukan saat ini yang tidak lagi dibutuhkan LSTM [36]. Gerbang keluaran bertanggung jawab untuk mengekstrak data yang relevan dari masukan saat ini dan memprosesnya sebagai keluaran. Terakhir, gerbang masukan bertanggung jawab untuk menambahkan masukan ke status sel [37].

Pembelajaran semi-supervised: Pembelajaran semi-supervised melibatkan penggunaan data tak berlabel dalam tahap pra-pelatihan algoritma. Pendekatan ini melatih model menggunakan data berlabel dan tak berlabel. Dalam kasus ini, fitur diekstraksi menggunakan autoencoder dan klasifikasi dilakukan menggunakan berbagai model pembelajaran mesin deep atau shallow. AutoEncoding (AE) adalah metode deep-learning umum yang termasuk dalam keluarga jaringan saraf tak tersupervised. Dengan mempelajari fitur terbaik, AE bertujuan untuk mencocokkan output dengan input sedekat mungkin. Meskipun dimensi lapisan tersembunyi sering kali lebih kecil daripada dimensi lapisan input, autoencoder memiliki lapisan input dan output dengan dimensi yang sama. Operasi encoder-decoder simetris merupakan aspek utama AE. Stacked AE, Sparse AE, dan Variational AE adalah tiga versi AE yang berbeda [13].

Pembelajaran hibrida: Kombinasi dari dua metode lain, seperti pembelajaran mesin dangkal, pembelajaran mendalam terbimbing, atau pembelajaran mendalam tak terbimbing, dikenal sebagai metode pembelajaran hibrida. Para peneliti umumnya menggunakan CNN–LSTM [38–40]), LSTM–Bayes [41], RNN–AE [42], dan model hibrida lainnya.

Metode pembelajaran lainnya:kelompok ini mencakup pembelajaran transfer, di mana model yang telah dilatih dari repositori digunakan dalam teknik pembelajaran transfer [13]. Dalam kasus ini, peneliti menggunakan teknik pembelajaran mendalam untuk melatih model pada satu domain serangan sebelum menerapkannya ke domain serangan lain.

Bagian ini telah memberikan ringkasan menyeluruh tentang algoritma ML dan DL yang paling populer untuk sistem deteksi DDoS. Gambar4mengilustrasikan taksonomi pendekatan deteksi DDoS berbasis ML/DL saat ini.



Gambar 4. Taksonomi sistem deteksi DDoS berbasis pembelajaran mesin dan pembelajaran mendalam.

4. Metodologi, Kekuatan, dan Kelemahan

Spesifikasi algoritma ML dan DL paling populer yang digunakan untuk membuat model deteksi DDoS yang efektif dijelaskan di bagian ini, bersama dengan teknik dasar untuk deteksi DDoS berbasis AI. Metode yang diawasi dan tidak diawasi digunakan dalam ML dan DL. Dalam algoritma yang diawasi, data perlu diberi label sebelum digunakan. Sebaliknya, algoritma yang tidak diawasi menggunakan data yang tidak diberi label untuk mengekstrak karakteristik dan detail yang penting. Metodologi, keuntungan, dan kerugian dari studi yang menggunakan pendekatan ini dirangkum dalam Tabel3.

Tabel 3. Metodologi, kekuatan, dan kelemahan berbagai penelitian yang menggunakan ML/DL untuk deteksi DDoS.

Referensi	Metodologi	Kekuatan	Kelemahan
Shen dan kawan-kawan. [43][Bahasa Indonesia]	Menggunakan Algoritma BAT dengan Metode Ensemble untuk Optimasi.	Saat digunakan dalam pengaturan ansambel, beberapa ELM menunjukkan kinerja yang baik.	Menggunakan kumpulan data lama, termasuk Kyoto, NSL-KDD, dan KDDCup99. Selain itu, akurasi deteksi model untuk kelas serangan U2R lebih rendah.
Bersinar dan lain-lain. [44][Bahasa Indonesia]	Memanfaatkan RF dengan Non-Simetris Dalam Pengkode Otomatis	Menyajikan deteksi DDoS berbasis AE non-simetris dan pengklasifikasi RF, yang menurunkan kompleksitas model	Model tersebut diperiksa dengan kumpulan data yang sudah ketinggalan zaman, dan kinerjanya pada kelas minoritas R2L dan U2R berada pada sisi yang rendah.
Ali dan kawan-kawan. [45][Bahasa Indonesia]	Menggunakan Algoritma Particle Swarm dan Fast Jaringan Pembelajaran	Model yang disarankan mengungguli model berbasis FLN lainnya menggunakan beberapa strategi optimasi tambahan	Dataset yang digunakan sudah usang. Selain itu, data pelatihan yang lebih sedikit menyebabkan tingkat deteksi yang lebih rendah.
Yan dan kawan-kawan. [46][Bahasa Indonesia]	Memanfaatkan SVM dan Sparse Auto Encoder	SVM secara efektif digunakan sebagai pengklasifikasi dengan SSAE untuk ekstraksi fitur untuk mengidentifikasi serangan DDoS	Model tersebut dievaluasi menggunakan kumpulan data yang sudah ketinggalan zaman; meskipun tingkat deteksi model untuk serangan U2R dan R2L cukup baik, namun tingkat deteksi tersebut lebih rendah dibandingkan dengan kelas serangan lain dalam kumpulan data tersebut.
Naseer dan lain-lain. [47][Bahasa Indonesia]	Perbandingan beberapa Model IDS berbasis ML/DL	Menggunakan testbed terintegrasi GPU untuk membandingkan metode deteksi DDoS berbasis ML/DL	Cacat tersebut dievaluasi menggunakan kumpulan data sebelumnya yang disebut NSL-KDD.
Al-Qatf dan lain-lain. [48][Bahasa Indonesia]	Model pembelajaran otodidak digunakan dengan menggunakan autoencoder dan SVM.	Gagasan efektif pembelajaran mandiri berdasarkan Sparse AE dan SVM diusulkan sebagai model deteksi DDoS	Kumpulan data lama yang disebut NSL-KDD digunakan. Selain itu, tidak ada hasil yang diberikan mengenai efektivitas model terhadap kelas serangan minoritas.

Tabel 3.*Lanjutan.*

Referensi	Metodologi	Kekuatan	Kelemahan
Marir dan lain-lain. [49][Bahasa Indonesia]	Menggunakan SVM dan Deep Belief Network	DBN digunakan untuk mengekstraksi fitur, yang kemudian diteruskan ke SVM ensemble sebelum diprediksi melalui metode pemungutan suara.	Kompleksitas dan pelatihan model memerlukan waktu lebih lama dengan lapisan yang lebih dalam.
Yao dan kawan-kawan. [50][Bahasa Indonesia]	Model multilevel berbasis Clustering K-Means dan Random Forest	Ide pengelompokan diterapkan dalam kombinasi dengan RF untuk menawarkan model deteksi intrusi multilayer; model tersebut berkinerja lebih baik daripada rata-rata dalam mengidentifikasi serangan	Menggunakan dataset KDDCup99 yang sudah ketinggalan zaman untuk menguji model.
Gao dan kawan-kawan. [51][Bahasa Indonesia]	Menggunakan sistem pemungutan suara dan teknik ML ensemble	Menggunakan model ensemble adaptif yang menggabungkan banyak pengklasifikasi dasar seperti DT, RF, KNN, dan DNN, dan menggunakan mekanisme pemungutan suara adaptif untuk memilih pengklasifikasi terbaik.	Kumpulan data sebelumnya yang disebut NSL-KDD digunakan untuk menguji model; hasil pada kelas serangan yang lebih lemah tidak mencukupi.
Karatas dan lain-lain. [52][Bahasa Indonesia]	Perbandingan kinerja beberapa algoritma ML dengan terlebih dahulu menurunkan rasio ketidakseimbangan dataset menggunakan SMOTE	SMOTE secara progresif meningkatkan tingkat deteksi untuk kelas serangan minoritas	Waktu eksekusi lebih lama
Sabil dan lain-lain. [53][Bahasa Indonesia]	Dua model ML (DNN dan LSTM) diusulkan untuk mendeteksi serangan DDoS	Performa model-model ini meningkat secara signifikan, dengan tingkat akurasi DNN dan LSTM masing-masing sebesar 98,72% dan 96,15%. Nilai AUC untuk DNN dan LSTM masing-masing sebesar 0,987 dan 0,989.	Penulis tidak menggunakan deteksi waktu nyata, dan hanya klasifikasi kelas biner yang dilakukan.
dkk. [54][Bahasa Indonesia]	Mengidentifikasi serangan DDoS di cloud menggunakan algoritma DT, KNN, NB, dan DNN	Klasifikasi DNN mengungguli DT, KNN, dan NB dalam hal akurasi dan presisi, mencapai 96% pada kumpulan data cloud	Menggunakan dataset yang sudah ketinggalan zaman; tidak ada informasi yang diberikan mengenai LAN atau dataset cloud.
Asad dan kawan-kawan. [55][Bahasa Indonesia]	Mengembangkan arsitektur DNN	Model DeepDetect yang diusulkan mengungguli strategi lain dan menghasilkan skor F1 sebesar 0,99. Selain itu, nilai AUC sangat mendekati 1, menunjukkan akurasi yang tinggi.	Strategi ini hanya diuji terhadap serangan DDoS pada lapisan aplikasi.
Lukisan dinding. dan lain-lain. [56][Bahasa Indonesia]	Mengidentifikasi serangan DoS yang lambat pada HTTP dan menyarankan algoritma DNN berbasis aliran data	Model ini dapat mengkategorikan serangan dengan akurasi keseluruhan 99,61%	Hanya serangan HTTP DoS lambat yang dinilai menggunakan metode ini; kumpulan data CICIDS2017 digunakan.
Sbai dan kawan-kawan. [57][Bahasa Indonesia]	Mengidentifikasi serangan DF atau UDPFL di MANET menggunakan dataset CI-CDDoS2019 dan menyarankan model DL DNN menggunakan dua lapisan tersembunyi dan enam epoch	Recall = 1, Presisi = 0,99, Skor F1 = 0,99, dan Akurasi = 0,99	Studi ini hanya berfokus pada serangan DF atau DPFL dan menggunakan kumpulan data CICDDoS2019.
Bahasa Amaizu dan lain-lain. [58][Bahasa Indonesia]	Menggabungkan dua model DNN dengan desain berbeda dan pendekatan ekstraksi fitur PCC untuk deteksi serangan DDoS dalam skenario 5G dan B5G	Tingkat akurasi 99,66% dan kerugian 0,011; semua model kecuali ansambel CNN dikalahkan oleh kerangka kerja yang disarankan	Karena strukturnya yang rumit, kinerja model yang disarankan dalam lingkungan waktu nyata mungkin menurun akibat waktu deteksi yang lebih lama.
Cil dan kawan-kawan. [59][Bahasa Indonesia]	Mekanisme model DL yang disarankan untuk ekstraksi fitur dan klasifikasi dibangun ke dalam kerangka model	Akurasi hampir 100% untuk DatasetA. Selain itu, saat menggunakan DatasetB, model tersebut mengkategorikan serangan DDoS dengan benar dengan tingkat akurasi 95%.	Untuk klasifikasi multikelas, model yang disarankan berkinerja kurang akurat.
Hasan dan lain-lain. [60][Bahasa Indonesia]	Menyarankan model CNN Dalam	Teknik yang diusulkan memiliki kinerja lebih baik dibandingkan tiga metode ML lainnya	Kumpulan data yang digunakan mencakup sejumlah kasus terbatas dan mengecualikan beberapa bentuk lalu lintas.
Ibu dan lain-lain. [61][Bahasa Indonesia]	Gabungan FCNN dengan Vektor VCNN	Teknik yang disarankan mengungguli pengklasifikasi dasar dan sistem deteksi serangan paling canggih dalam hal akurasi tinggi, mengurangi alarm palsu, dan meningkatkan tingkat deteksi.	Memanfaatkan kumpulan data yang sudah ketinggalan zaman dan menghilangkan uji coba mereka untuk mengidentifikasi serangan yang tidak teridentifikasi
Chen dan kawan-kawan. [62][Bahasa Indonesia]	Menyarankan arsitektur CNN multi-saluran untuk serangan DDoS	MCCNN bekerja lebih baik pada kumpulan data terbatas	Hasil model klasifikasi multi-kelas dan kelas tunggal tidak berbeda secara signifikan; kompleksitas model multi-kelas membuatnya tidak cocok untuk validasi dalam keadaan waktu nyata.

Tabel 3.*Lanjutan.*

Referensi	Metodologi	Kekuatan	Kelemahan
Syaban dan lain-lain. [63][Bahasa Indonesia]	Menggunakan dua set data untuk menguji model yang disarankan terhadap algoritma klasifikasi termasuk DT, SVM, KNN, dan NN	Model yang disarankan mendapat skor baik dan memberikan akurasi 99% pada kedua set data	Dalam metode ini, data diubah menjadi matriks dengan memperluas satu kolom. Akibatnya, hal ini dapat memengaruhi cara model belajar.
Haider dan lain-lain. [64][Bahasa Indonesia]	Menyarankan kerangka kerja CNN yang mendalam untuk mendeteksi serangan DDoS di SDN	Teknik CNN ensemble memiliki kinerja yang lebih baik dibandingkan pendekatan pesaing yang digunakan saat ini, dengan tingkat akurasi kolektif sebesar 99,45%	Strategi ini memerlukan periode pelatihan dan pengujian yang lebih lama. Akibatnya, mekanisme mitigasi dapat terpengaruh, yang berarti serangan dapat menyebabkan kerusakan yang lebih parah.
Wang dan lain-lain. [65][Bahasa Indonesia]	Menyarankan teknik entropi informasi dan DL untuk mengidentifikasi serangan DDoS dalam konteks SDN	CNN mengungguli alternatif dalam hal presisi, akurasi, skor F1, dan ingatan, dengan tingkat akurasi 98,98%	Model Memerlukan waktu lebih lama untuk melakukan deteksi waktu
Kim dan kawan-kawan. [66][Bahasa Indonesia]	Membuat model berbasis CNN untuk mengidentifikasi serangan DoS	Model CNN lebih mampu mengenali serangan DoS unik dengan fitur serupa. Selain itu, ukuran kernel CNN tidak memiliki efek yang jelas pada kategorisasi biner atau multikelas.	Deteksi waktu yang lebih lama
Doriguzzi dan lain-lain. [67][Bahasa Indonesia]	Serangan DDoS dideteksi menggunakan pendekatan LUCID	Performa LUCID lebih baik dalam hal akurasi	Padding dapat mengganggu kemampuan CNN untuk mempelajari pola. Selain itu, terdapat kompromi antara akurasi dan jumlah memori yang dibutuhkan. Waktu praproses tidak dihitung untuk situasi waktu nyata.
dari Assis dan lain-lain. [68][Bahasa Indonesia]	Menyarankan mekanisme pertahanan SDN	Temuan keseluruhan menunjukkan efektivitas CNN dalam mengidentifikasi serangan DDoS untuk setiap kasus pengujian	Saat menggunakan dataset CICDDoS 2019, model tersebut menunjukkan akurasi yang lebih buruk.
Husain dan lain-lain. [69][Bahasa Indonesia]	Menyarankan teknik untuk mengkonversi format gambar tiga saluran dari data jaringan non-gambar	Strategi yang disarankan memperoleh akurasi 99,92% dalam klasifikasi kelas biner	Waktu persiapan untuk mengubah nongambar menjadi gambar tidak dihitung. Selain itu, pemrosesan yang digunakan untuk mengubah 60 gambar asli*Bahasa Indonesia:*60*Bahasa Indonesia:*3 dimensi ke dalam 224*Bahasa Indonesia:*224*Bahasa Indonesia:*3 dimensi yang digunakan sebagai input untuk model ResNet telah ditentukan
Li C dan rekan. [70][Bahasa Indonesia]	Menyarankan pendekatan pembelajaran mendalam	Deteksi serangan DDoS memiliki akurasi 98%	Waktu yang lama diperlukan untuk deteksi
Priy. dkk. [71][Bahasa Indonesia]	Pendekatan berbasis DL dikembangkan	Untuk semua kasus pengujian, tercatat bahwa model LSTM menampilkan akurasi 98,88%. Modul tersebut mampu mencegah paket yang diserang mencapai server cloud melalui sakelar SDN OF.	Hanya serangan DDoS pada tingkat jaringan atau transportasi yang diperiksa; analisis kelayakan waktu nyata dari model yang diusulkan tidak dilakukan.
Liang dan lain-lain. [72][Bahasa Indonesia]	Model arsitektur empat lapis dengan dua lapisan LSTM disarankan	Temuan eksperimen menunjukkan bahwa teknik berbasis LSTM berkinerja lebih baik dibandingkan pendekatan lainnya	Bila alirannya terdiri dari paket-paket pendek, N diisi dengan paket-paket fiktif. Pengaturan pengisian ini berpotensi menurunkan kinerja, dan berdampak pada cara model yang disarankan belajar.
dkk. [Shu dan lainnya]73[Bahasa Indonesia]	Dua metode, IDS berbasis hybrid dan model DL berdasarkan LSTM, diusulkan untuk mendeteksi serangan DoS/DDoS	Model berbasis LSTM mencapai akurasi 99,19%	Butuh waktu lama untuk mendeteksinya
Assis dan kawan-kawan. [37][Bahasa Indonesia]	Mengusulkan mekanisme pertahanan terhadap serangan DDoS dan intrusi di lingkungan SDN	Rata-rata hasil akurasi, recall, presisi, dan f1-score masing-masing sebesar 99,94% dan 97,09%.	Model ini menggunakan kerangka kerja yang kompleks
Catak dan kawan-kawan. [7][Bahasa Indonesia]	Cpmbo model ANN dan AE yang mendalam	Nilai F1 terbaik diperoleh dengan fungsi aktivasi ReLu (0,8985). Untuk fungsi aktivasi softplus, softsign, relu, dan tanh, akurasi dan presisi keseluruhan mendekati 99%.	Fungsi aktivasi adalah satu-satunya hal yang menjadi fokus artikel ini
Ali dan kawan-kawan. [74][Bahasa Indonesia]	Mengusulkan AE mendalam untuk pembelajaran fitur dan kerangka kerja MKL untuk pembelajaran dan klasifikasi model deteksi	Pendekatan yang diusulkan ditemukan lebih akurat dibandingkan pendekatan alternatif	Menggunakan dataset yang sudah ketinggalan zaman

Tabel 3. *Lanjutan.*

Referensi	Metodologi	Kekuatan	Kelemahan
Yang dan lain-lain. [75] [Bahasa Indonesia]	Model AE lima lapis dikembangkan untuk deteksi DDoS tanpa pengawasan yang efisien	AE-D3F mencapai hampir 100% DR dengan FPR kurang dari 0,5%, meskipun nilai ambang batas RE harus ditentukan. Metode ini mengkompensasi kurangnya data serangan berlabel dengan melatih model hanya menggunakan lalu lintas biasa.	Menggunakan dataset yang sudah ketinggalan zaman
Kasim dan lain-lain. [76] [Bahasa Indonesia]	Menyarankan teknik hybrid AE–SVM	Dalam hal identifikasi anomali cepat dan tingkat positif palsu yang rendah, metode AE–SVM lebih baik daripada pendekatan lain	Dibandingkan dengan dua dataset lainnya, akurasi model yang disarankan pada dataset NSL-KDD lebih rendah
Bhardwaj dan lain-lain. [77] [Bahasa Indonesia]	Menggabungkan AE jarang bertumpuk untuk mempelajari fitur dengan DNN untuk mengkategorikan data jaringan	Hasilnya menunjukkan akurasi sebesar 98,92%. Pendekatan yang disarankan bekerja dengan baik untuk mengatasi masalah dengan pembelajaran fitur dan overfitting, karena AE dilatih dengan sampel data pelatihan acak untuk melakukan pembelajaran fitur dan overfitting dihindari dengan menggunakan parameter kelangkaan.	Melakukan studi offline alih-alih mengevaluasi kumpulan data terbaru. Selain itu, model yang disarankan tidak dapat menghitung waktu deteksi.
Moha. dan lain-lain. [41] [Bahasa Indonesia]	Menggabungkan teknik LSTM dan Bayes	Hasil penelitian menunjukkan bahwa indikator kinerja hanya mengalami sedikit penurunan dengan adanya data baru, dan hasilnya positif.	Serangan yang tidak sesuai untuk aplikasi real-time mungkin memerlukan waktu lebih lama untuk diidentifikasi oleh LSTM–BA. Jika dibandingkan dengan model yang disarankan dengan pendekatan DeepDefense saat ini, akurasinya hanya meningkat sebesar 0,16%. Alamat IP diubah menjadi vektor aktual menggunakan hashing fitur, dan waktu praproses tidak dihitung menggunakan BOW.
RoopakM dan lain-lain. [39] [Bahasa Indonesia]	Menggunakan optimasi multi-objektif, yaitu pendekatan NSGA	Nilai skor F1 sebesar 99,36% dan akurasi tinggi sebesar 99,03%. Selain itu, hasil penelitian menunjukkan bahwa model yang disarankan mengungguli penelitian sebelumnya. Jika dibandingkan dengan pendekatan DL sebelumnya, waktu pelatihan berkurang hingga sebelas kali lipat.	Mayoritas metode mutakhir yang digunakan dalam artikel ini tidak menggunakan kumpulan data CI-CIDS2017; oleh karena itu, analoginya tampak tidak tepat.
Elsa dan kawan-kawan. [42] [Bahasa Indonesia]	Menggabungkan AE dan RNN untuk menghasilkan DDoS-Net untuk mengidentifikasi serangan DDoS di SDN	Hasil penelitian menunjukkan bahwa DDoS-Net memiliki kinerja yang lebih baik dibandingkan dengan enam teknik ML tradisional (DT, NB, RF, SVM, Booster, dan LR) dalam hal akurasi, recall, presisi, dan skor F1. Metode yang diusulkan memperoleh akurasi 99% dan AUC sebesar 98,8	Dataset menggunakan analisis offline, dan klasifikasi multikelas tidak dilakukan.
Nugraha dan lain-lain. [40] [Bahasa Indonesia]	Strategi berbasis DL diusulkan untuk mengidentifikasi serangan DDoS yang lambat di SDN menggunakan model CNN–LSTM	Model yang disarankan memiliki kinerja lebih baik dibandingkan pendekatan lain, dengan perolehan lebih dari 99,5 persen pada semua kriteria kinerja	Dataset menggunakan analisis offline
Dia dan rekan-rekannya. 78 [Bahasa Indonesia]	Strategi berdasarkan DTL diusulkan untuk mengidentifikasi serangan DDoS	Peningkatan sebesar 20,8% dicapai pada deteksi jaringan 8LANN di domain target. Teknik DTN dengan fine-tuning menghindari penurunan kinerja deteksi yang disebabkan oleh penggunaan sampel kecil serangan DDoS.	Untuk evaluasi model, hanya satu serangan yang digunakan di domain sumber dan domain target.
Chen dan kawan-kawan. [79] [Bahasa Indonesia]	Menyarankan teknik pembelajaran penguatan mendalam berbasis gradien minimax	Jika dibandingkan dengan algoritma mutakhir, algoritma GPDS berbasis kebijakan yang disarankan mengungguli mereka dalam hal kinerja anti-jamming	

5. Dataset DDoS Benchmark yang Tersedia dan Kelas Serangan dalam Dataset

Kumpulan data dan jenis kelas serangan yang digunakan oleh penelitian yang diperiksa untuk deteksi serangan DDoS tercantum dalam Tabel4Delapan set data (KDD Cup99, Kyoto 2006+, NSL-KDD, UNSW-NB15, CIC-IDS2017, CSE-CIC-IDS2018, SCX2012, dan CICDDoS2019) digunakan di sebagian besar penelitian. Berikut ini adalah deskripsi dari set data tersebut.

Piala KDD99: Salah satu kumpulan data yang paling terkenal dan sering digunakan untuk IDS adalah KDD Cup99. Kumpulan data ini berisi sekitar lima juta dan dua juta rekaman untuk pelatihan dan pengujian. Setiap rekaman memiliki 41 karakteristik atau properti yang berbeda, dan diklasifikasikan sebagai serangan atau sebagai data normal. Empat kategori serangan ditetapkan untuk rekaman tersebut, yaitu Denial of Service (DoS), Probe, Remote to Local (R2L), dan User to Root (U2R) [80].

Tabel 4. Penelitian terkini tentang ML/DL untuk deteksi serangan DDoS, menampilkan teknik, kumpulan data, dan jenis serangan.

Ref.	Tahun	Mendekati	Kumpulan data	Kelas-kelas Serangan
Shen dan kawan-kawan. [43] Shone dan kawan-	Tahun 2018	BAT, Ensemble	KC, NK, New York	DoS, Probe, R2L, U2R DoS,
kawan. [44] Ali dan kawan-kawan. [45] Yan dan	Tahun 2018	RF, DAE	KC, Korea Utara	Probe, R2L, U2R DoS,
kawan-kawan. [46] Naseer dan kawan-kawan. [	Tahun 2018	Bahasa Inggris FLN	Bahasa Inggris: KC	Probe, R2L, U2R DoS,
47] Al-QatfM dan lainnya. [48] Marir dan	Tahun 2018	SVM, SAE	NK	Probe, R2L, U2R DoS,
kawan-kawan. [49] Yao dan kawan-kawan. [50]	Tahun 2018	GPU	NK	Probe, R2L, U2R DoS,
Gao dan kawan-kawan. [51] Karatas dkk. [52]	Tahun 2018	SAE, Bahasa Indonesia	NK	Probe, R2L, U2R DoS,
Sabeel dan kawan-kawan. [53] Virupakshar dan	Tahun 2018	SVM, DBN	NK, PBB, C7	Probe, R2L, DDoS, jaring
lainnya. [54] Asad dan kawan-kawan. [55]	Tahun 2018	KMC, Federasi Rusia	Bahasa Inggris: KC	DoS, Probe, R2L, U2R DoS,
Muraleedharan dkk. [56] Sbai dan kawan-	Tahun 2019	ansambel	NK	Probe, R2L, U2R HeartBleed,
kawan. [57] Amaizu dan kawan-kawan. [58] Cil	Tahun 2020	KNN, RF, DT	C8	DoS, Botnet, DDoS Jinak, DoS
dan kawan-kawan. [59] Hasan dkk. [60] Amma	Tahun 2019	DNN, LSTM	C7, A9	GoldenEye, DoS, DDoS.
dan kawan-kawan. [61] Chen dan kawan-	Tahun 2020	DT, KNN, NB, DNN	Bahasa Inggris: KC	DoS, Probe, R2L, Botnet U2R, DoS,
kawan. [62] Shaaban dan kawan-kawan. [63]	Tahun 2020	TTL	C7	DDoS, Botnet Web, DoS, DDoS,
Haider dan kawan-kawan. [64] Wang dan	Tahun 2020	TTL	C7	Serangan banjir Data Web atau
kawan-kawan. [65] Kim dan kawan-kawan. [66]	Tahun 2020	TTL	C9	serangan banjir UDP
Doriguzzi dan kawan-kawan. [67] dari Assis dan	Tahun 2021	TTL	C9	UDP, SYN, DNS, jinak
kawan-kawan. [68] Hussain dan kawan-kawan. [	Tahun 2021	TTL	C9	serangan DDoS
69] Li C dan rekan. [70] Priyadarshini dan	Tahun 2018	Berita CNN	Catatan Obs	Serangan DDoS
lainnya. [71] Liang dan kawan-kawan. [72]	Tahun 2019	Berita CNN	NK	Serangan DoS
ShurmanM dan kawan-kawan. [73] Assis dan	Tahun 2019	Berita CNN	C7,K9	DoS, Penyelidikan, R2L, U2R, DDoS
kawan-kawan. [37] Catak dan kawan-kawan. [7]	Tahun 2019	Berita CNN	NK	DoS, Probe, R2L, U2R
Ali dan kawan-kawan. [74] Yang dan kawan-	Tahun 2020	RNN, LSTM	C7	Botnet, DoS, DDoS, Web
kawan. [75] Kasim dan kawan-kawan. [76]	Tahun 2020	Entropi, CNN	C7	Botnet, DoS, DDoS, Web
Bhardwaj dan kawan-kawan. [77] Premkumar	Tahun 2020	Berita CNN	KC, C8	Botnet, DoS, DDoS, Web
dan kawan-kawan. [81] RoopakM dan kawan-	Tahun 2020	Berita CNN	Bahasa Indonesia:12, C7, C8	Botnet, DoS, DDoS, Web
kawan. [38] Mohammad dan kawan-kawan. [41	Tahun 2020	Berita CNN	C9	serangan DDoS
] RoopakM dan kawan-kawan. [39] ElsayedMS	Tahun 2020	Berita CNN	C9	Sinkronisasi, TFTP, DNS, LDAP, UDP
dan kawan-kawan. [42] Nugraha dkk. [40] Dia	Tahun 2018	LSTM, CNN, GRU	saya2	serangan DDoS
dan rekan-rekannya. [78] Chen dan kawan-	Tahun 2019	LSTM	saya2	serangan DDoS
kawan. [79[Bahasa Indonesia]	Tahun 2019	LSTM	C7	Serangan Botnet, DoS, DDoS
	Tahun 2020	LSTM	C9	MSSQL, SSDP, Pengisian Daya, LDAP, NTP
	Tahun 2021	GRU	C8, C9	serangan DDoS
	Tahun 2019	AE, JAM	U5, KC	DoS, Probe, R2L, U2R Fuzzers,
	Tahun 2019	AE, MKL	Saya2, U5	Backdoors, Analisis, Serangan DoS
	Tahun 2020	AE	U7	(HTTP, Hulk dan Slowloris) Serangan
	Tahun 2020	AE, SVM	C7, NSL, KDD	(HTTP, Hulk dan Slowloris) Serangan
	Tahun 2020	AE, TTD	C7, NSL, KDD	(HTTP, Hulk dan Slowloris)
	Tahun 2020	RBF	Dataset yang dihasilkan	Serangan DDoS
	Tahun 2019	MLP, CNN, LSTM	C7	DoS, Penyelidikan, R2L, U2R
	Tahun 2019	LST, BN	saya2	Serangan DDoS
	Tahun 2020	CNN, LSTM	C7	Serangan DDoS
	Tahun 2020	RNN, AE	C9	Serangan DDoS
	Tahun 2020	CNN, LSTM	dihasilkan	Serangan DDoS
	Tahun 2020	Bahasa Indonesia: LAN	dihasilkan	Serangan DDoS
	Tahun 2022	bantuan	dihasilkan	Serangan DDoS

Kyoto 2006+: kumpulan data ini dibuat menggunakan statistik lalu lintas jaringan yang dikumpulkan Universitas Kyoto melalui penggunaan honeypot, sensor darknet, server email, perayap web, dan mekanisme keamanan jaringan lainnya. Kumpulan data terbaru mencakup statistik lalu lintas untuk tahun 2006 hingga 2015. Setiap entri terdiri dari 24 atribut analitis, empat belas di antaranya diambil langsung dari kumpulan data KDD Cup99 dan sepuluh sisanya adalah fitur tambahan.

NSL-KDD: dataset ini terdiri dari dataset KDD Cup99 yang telah disempurnakan dan diubah dengan menghilangkan sejumlah masalah mendasarnya. Dataset ini memiliki 41 fitur, dan serangan dibagi menjadi empat kelompok, seperti yang dinyatakan dalam KDD Cup99.131 [82].

UNSW-NB15: Pusat Keamanan Siber Australia menghasilkan kumpulan data ini. Dengan menggunakan Bro-IDS, perangkat Argus, dan sejumlah metode yang baru dibuat, hampir dua juta catatan berhasil diambil dengan total 49 karakteristik. Worm, Shellcode, Reconnaissance, Port Scans, Generic, Backdoor, DoS, Exploits, dan Fuzzers termasuk di antara jenis serangan yang termasuk dalam kumpulan data ini.

CIC-IDS2017: Institut Keamanan Siber Kanada (CIC) menghasilkan kumpulan data ini pada tahun 2017. Serangan aktual baru dan aliran khas keduanya disertakan. CICFlowMeter menggunakan data dari catatan, alamat IP sumber dan tujuan, protokol, dan serangan untuk menilai lalu lintas jaringan. CICIDS2017 mencakup kasus serangan khas seperti Serangan Brute Force, Serangan HeartBleed, Botnet, Distributed DoS (DDoS), Denial of Service (DoS), Serangan Web, dan Serangan Infiltrasi [83].

CSE-CIC-IDS2018: Pada tahun 2018, Communications Security Establishment (CSE) dan CIC berkolaborasi untuk menghasilkan kumpulan data ini dengan membuat profil pengguna yang mencakup gambaran abstrak dari banyak kejadian. Semua profil ini kemudian diintegrasikan dengan serangkaian karakteristik khusus untuk membuat kumpulan data. Brute Force, Heartbleed, Botnet, DoS, DDoS, serangan web, dan penetrasi jaringan dari dalam hanyalah beberapa dari tujuh skenario serangan yang tercakup dalam kumpulan data ini [84].

ISCX 2012: Dataset ini, yang berisi data jaringan paket lengkap, dikembangkan pada tahun 2012 oleh Ali Shiravi et al. [20] Meliputi tujuh hari dari 11 Juni hingga 17 Juni 2010, dengan aktivitas jaringan yang mencakup lalu lintas yang sah dan berbahaya. Beberapa contoh lalu lintas berbahaya meliputi Distributed Denial of Service, HTTP Denial of Service, dan Brute Force SSH. Kumpulan data ini diproduksi dalam konteks jaringan yang disimulasikan, dan berisi data yang diberi label dan tidak seimbang. Dua profil umum, satu yang menggambarkan aktivitas serangan dan yang lainnya yang menggambarkan skenario pengguna yang umum, digunakan dalam kumpulan data ISCX [85].

CICDDoS2019: Sharafaldin dan kawan-kawan. [86] membuat kumpulan data CICDDoS2019 (2019). Lebih dari 80 karakteristik lalu lintas diambil dari informasi asli dengan menggunakan program CICFlowMeter-V3 untuk mengekstraksi fitur-fiturnya. CICDoS2019 berisi serangan DDoS umum yang aman dan terkini. Kumpulan data ini, yang dibuat menggunakan lalu lintas aktual, berisi berbagai serangan DDoS yang dibuat menggunakan protokol TCP/UDP [87].

6. Teknik Praproses, Pengaturan Hiperparameter, Konfigurasi Eksperimental, dan Metrik Kinerja

Meja4mencantumkan teknik praproses, pengaturan hiperparameter, konfigurasi pengujian, dan metrik kinerja yang digunakan oleh algoritma ML/DL saat ini untuk mendeteksi serangan DDoS. Pada awalnya, data diproses terlebih dahulu. Praproses data sangat penting, karena mengubah data mentah menjadi struktur yang meningkatkan kapasitas pembelajaran model [88]. Meja5dalam penelitian ini memberikan gambaran umum mengenai teknik praproses yang digunakan dalam literatur.

Tabel 5. Studi terkini tentang deteksi serangan DDoS menggunakan ML/DL.

Ref.	Praproses Strategi	Nilai Hiperparameter	Eksperimental Pengaturan	Metrik Kinerja
Shen dan kawan-kawan. [43][Bahasa Indonesia]		ELM dengan BAT		Akurasi = 99,3%, Sensitivitas = 99%, Spesifisitas = 99%, Presisi = 99%, Skor F1 = 99%, FPR = 1%, FNR = 1%
Shone dan kawan-kawan. [44][Bahasa Indonesia]		NDAE dengan RF	TensorFlow bawaan	98,81%, menghemat waktu dan meningkatkan akurasi hingga 5%.
Naseer dan kawan-kawan. [47][Bahasa Indonesia]		CNN, AE, dan RNN		Akurasi untuk DCNN dan LSTM masing-masing sebesar 85% dan 89%.
Al-QatfM dan kawan-kawan. [48][Bahasa Indonesia]		Teknik AE		Peningkatan akurasi dan waktu Klasifikasi SVM
Marir dan kawan-kawan. [49][Bahasa Indonesia]	Ensemble multi-lapis bisa SVM		klaster hadoop	Peningkatan kinerja IDS.
Yao dan kawan-kawan. [50][Bahasa Indonesia]	Bahasa Inggris MSML			MSML lebih unggul dibandingkan algoritma deteksi intrusi terkini lainnya dalam hal akurasi, skor F1, dan kapasitas.

Tabel 5.*Lanjutan.*

Ref.	Praproses Strategi	Nilai Hiperparameter	Eksperimental Pengaturan	Metrik Kinerja
Gao dan kawan-kawan. [51][Bahasa Indonesia]		Pembelajaran ansambel		Akurasi = 85,2%, Presisi = 86,5%, Recall = 85,2%, Skor F1 = 84,9%
Karatas dkk. [52][Bahasa Indonesia]		Enam model ML yang berbeda		Akurasi antara 4,01% dan 30,59%
Sabeel dan kawan-kawan. [53][Bahasa Indonesia]	DNN/LSTM	Lapisan masukan = 25 piksel, lapisan padat = 60 neuron, tingkat putus = 0,2, ukuran batch = 0,0001, tingkat pembelajaran = 0,0001	TensorFlow, Keras 1.1.0	TPR = 0,998, Akurasi = 98,72%, Presisi = 0,949, Skor F1 = 0,974, dan AUC = 0,987
Virupakshar dan lain-lain. [54][Bahasa Indonesia]			Dua komputer dengan inti ganda prosesor	Recall = 0,91, Skor F1 = 0,91, Dukungan = 2140
Asad dan kawan-kawan. [55][Bahasa Indonesia]	Pembelajaran yang peka terhadap biaya ing dan min-max penskalaan	Tujuh lapisan tersembunyi, lapisan input = 66 neuron, lapisan output = 5 neuron, epoch = 300, laju pembelajaran = 0,001	Intel Xeon E5 v2	AUC = 1, Skor F1 = 0,99, Akurasi = 98%
Muraleedharan dan lain-lain. [56][Bahasa Indonesia]		Delapan puluh neuron untuk input, lima neuron di lapisan output, empat lapisan tersembunyi, pengoptimal Adam	SciKit dan Keras API	Presisi: Jinak = 0,99, Slowloris = 1,00, Slowhttptest = 0,99, Hulk = 1,00, GoldenEye = 1,00, Akurasi = 99,61%.
Sbai dan kawan-kawan. [57][Bahasa Indonesia]				Recall = 1, F1-score = 0, Akurasi = 0,99997, Presisi = 0,99
Amaizu dan kawan-kawan. [58][Bahasa Indonesia]	Min-maks	Dua Lapisan Dropout, Tingkat Pembelajaran 0,001, 50 Epoch, dan ReLu	Empat PC, satu firewall, dua switch, dan satu server	Ingatan = 99,30%, Presisi = 99,52%, Skor F1 = 99,99%, Akurasi = 99,66%.
Cil dan kawan-kawan. [59][Bahasa Indonesia]	Min-maks	Tiga lapisan tersembunyi, masing-masing 50 unit neuron, dan sigmoid	Intel Core i7-7700	Kumpulan data 1: F1-Skor = 0,9998, Akurasi = 0,9997, Presisi = 0,9999, Ingatan = 0,9998; Dataset2: Skor F1 = 0,8721, Akurasi = 0,9457, Presisi = 0,8049, Ingatan = 0,9515.
Hasan dan kawan-kawan. [60][Bahasa Indonesia]		Dua lapisan konvolusional, lapisan pengumpulan maksimal, lapisan yang terhubung penuh (250 neuron), dan SoftMax		Skor F1 = 99%, FPR = 1%, FNR = 1%, Akurasi = 99%, Sensitivitas = 99%, Spesifisitas = 99%, Presisi = 99%
Amma dan kawan-kawan. [61][Bahasa Indonesia]	Min-maks	Ukuran pengumpulan maksimum = 2, ukuran filter = 3, dua lapisan tersembunyi, lapisan keluaran dengan 11-9-7-6 node, dan ReLu		Normal = 99,3% akurat; Kembali = 97,8% akurat; Neptunus = 99,1% akurat; Smurf = 99,2% akurat; Teardrop = 83,3% akurat; Lainnya = 87,1% akurat.
Chen dan kawan-kawan. [62][Bahasa Indonesia]		Menggunakan metode pelatihan progresif untuk melatih MC–CNN		Akurasi: C7 = 98,87%, KU (dua kelas) = 99,18%, KC (lima kelas) = 98,54%.
Shaaban dan kawan-kawan. [63][Bahasa Indonesia]	Padding (8 dan 41) diubah menjadi 3*Bahasa Indonesia:*3 dan 6*Bahasa Indonesia:*7 matriks, masing-masing	Model CNN dengan fungsi softmax, dan fungsi ReLu	Aliran Tenser Dan keras	Kumpulan data 1: Akurasi = 0,9933, Kehilangan = 0,0067; Kumpulan data 2: Akurasi = 0,9924, Kehilangan = 0,0076 (NSL-KDD)
Haider dan kawan-kawan. [64][Bahasa Indonesia]	Skor Z	Dua lapisan FC padat, satu lapisan untuk meratakan, tiga CL 2D, dua PL maks, dan tiga CL 2D dengan ReLu	Intel Core i7-6700	Skor F1 = 99,61%, Akurasi = 99,45%, Presisi = 99,57%, Ingatan = 99,64%, Pengujian = 0,061 menit, Pelatihan = 39,52 menit, Penggunaan CPU = 6,025.
Wang dan kawan-kawan. [65][Bahasa Indonesia]	Gambar sudah dibuat dengan memutar masing-masing byte dalam paket menjadi piksel	Dua lapisan FC, dua level PL, dan dua lapisan CL; batas nilai entropi = 100 paket/detik	Intel Inti bahasa Inggris: prosesor 7300HQ, Pengendali POX, satu server, dan enam switch dengan Hping3 dan kerangka kerja TensorFlow	Presisi = 98,99%, Recall = 98,96%, F1-score = 98,97%, Akurasi = 98,98%, Waktu pelatihan = 72,81 s, AUC = 0,949

Tabel 5. *Lanjutan.*

Ref.	Praproses Strategi	Nilai Hiperparameter	Eksperimental Pengaturan	Metrik Kinerja
Kim dan kawan-kawan. [66][Bahasa Indonesia]		117 fitur dan gambar, dengan 13 dan 9 piksel dan ukuran kernel ditetapkan masing-masing menjadi 2 dan 3	Python dan Tensor-Mengalir	Akurasi KC = 99%, CSE8 = 91,5%
Doriguzzi dan kawan-kawan. [67][Bahasa Indonesia]	Min-maks	n = 100, t = 100, k = 64, h = 3, m = 98, ukuran batch = 2048, LR = 0,01, pengoptimal Adam, dan sigmoid	Dua prosesor Intel 16-core Xeon Perak 4110 CPU dengan Tensor-Aliran dan Python	Akurasi = 0,9888, FPR = 0,0179, Presisi = 0,9827, Recall = 0,9952, Skor F1 = 0,9889
de Assis dan kawan-kawan. [68][Bahasa Indonesia]	Entropi Shannon	Model CNN terdiri dari tiga lapisan: lapisan Flatten, lapisan 0,5 Dropout, dan lapisan FC dengan sepuluh neuron, dua lapisan Conv1D, dan lapisan MaxPooling1D dengan sigmoid dan 1000 epoch	prosesor Intel Core i7	Data SDN pada rata-rata Akurasi, Presisi, Penarikan, dan F-measure (95,4%, 93,3%, 2,4%, 92,8%) untuk CI-CDDoS 2019.
Hussain dan kawan-kawan. [69][Bahasa Indonesia]	Min-maks	Sepuluh CL dan delapan PL dalam model ResNet18, tingkat pembelajaran = 0,0001, momentum = 0,9, epoch = 10 dan 50 dengan pengoptimal SGD		F1-ukuran = 86, Presisi = 87%, Ingat = 86%, Akurasi = 87,06% untuk multikelas dan 99,99% untuk biner
Li C dan rekan. [70][Bahasa Indonesia]	BOW dan matriks 3D digunakan untuk mengonversi matriks fitur 2D	Lapisan masukan, rekursif maju, rekursif terbalik, FC tersembunyi, dan lapisan keluaran yang membentuk model DL.	RAM 128 GB dan dua NVIDIA K80 GPU dengan keras dan Ubuntu	Akurasi = 98%
Liang dan kawan-kawan. [72][Bahasa Indonesia]	Memeriksa sub-urutan n-aliran paket	Dua lapisan LSTM, dengan serangkaian sepuluh paket yang diekstraksi dari setiap aliran		Skor F1 = 0,9991, Presisi = 0,9995, Ingatan = 0,9997
Shurman M., seorang mahasiswa pascasarjana di Universitas Yarmouk, Siswa Sains Frekuensi Radio dan lain-lain. [73][Bahasa Indonesia]		Tiga lapisan LSTM dengan masing-masing 128 neuron dan fungsi sigmoid, tiga lapisan putus sekolah, dan lapisan padat dengan fungsi tanh		Akurasi = 99,19%
Assis dan kawan-kawan. [37][Bahasa Indonesia]	Bahasa Indonesia: MD5	Lapisan putus sekolah dengan tingkat putus sekolah 0,5 dan lapisan FC dengan sepuluh neuron dan fungsi sigmoid	Intel Core i7, Keras dan perangkat lunak Sklearn barang	Metrik rata-rata untuk nilai akurasi, presisi, recall, dan F-measure pada dataset C8: masing-masing 97,1%, 99,4%, 94,7%, dan 97%. Tingkat klasifikasi aliran yang valid: 99,7%.
Catak dan kawan-kawan. [7][Bahasa Indonesia]	Normalisasi	Tiga lapisan tersembunyi, lapisan keluaran dengan 28, 19, 9, 19, dan 28 unit, dan fungsi aktivasi sigmoid. Lapisan masukan memiliki lima lapisan tersembunyi dengan 28, 500, 800, 1000, 800, dan 500 unit	NVIDIA Quadro, Python, Keras, Ten-sorFlow, dan SciKit-belajar perpustakaan	Skor F1, Akurasi, Presisi, dan nilai Recall: 0,8985, 0,9744, 0,8924, dan 0,9053, berturut-turut.
Ali dan kawan-kawan. [74][Bahasa Indonesia]	Fitur diskretisasi adalah yang tidak numerik	Sembilan MSDA dengan jumlah lapisan yang berbeda L = (1, 3, 5, 7, 9, 11)	NVIDIA Tesla V100 dengan MATLAB	Akurasi rata-rata pada Dataset D1 hingga D16, = 93%; Akurasi pada Dataset D2 = 97%.
Yang dan lain-lain. [75][Bahasa Indonesia]	Mengalir terbagi menjadi beberapa sub-aliran berdasarkan nilai ambang batas 10 milidetik	Satu lapisan masukan, tiga lapisan tersembunyi, dan satu lapisan keluaran, dengan masing-masing 27, 24, 16, 24, dan 27 neuron di setiap lapisan.		Eksp1: DR = 98,32%, FPR = 0,38%; U7: DR = 94,10%, FPR = 1,88%; SINTESIS: DR = 100%; FPR = 100%; Eksp2: DR = 94,14%, FPR = 1,91%.
Kasim dan kawan-kawan. [76][Bahasa Indonesia]	Min-maks	25 neuron tersembunyi, 82 neuron masukan tersembunyi dan 82 neuron keluaran tersembunyi, laju pembelajaran 0,3, momentum 0,2, dengan 25 simpul masukan dan dua simpul keluaran dalam SVM. Laju pembelajaran = 0,01 dan iterasi = 1000.	Intel Inti (Tanggal) i7-2760QM adalah model terbaru dari i Dan Python dengan Keras, Scapy, TensorFlow, dan perpustakaan SciKit, dan API Istirahat	Waktu Pelatihan = 2,03 d, Waktu Pengujian = 21 milidetik, Akurasi C7 = 99,90%. Untuk serangan DDoS yang dibuat, Akurasi = 99,1% dan AUC = 0,9988. Untuk pengujian NSL-KDD, Akurasi = 96,36%
Bhardwaj dan al. [77][Bahasa Indonesia]	Min-maks	Dua lapisan pengkodean dengan masing-masing 70 dan 50 neuron, satu lapisan pengkodean dengan 25 neuron, dua tingkat dekode dengan masing-masing 25 neuron, dan aktivasi ReLu di setiap lapisan. Memanfaatkan pengoptimal Adadelta dan aktivasi sigmoid di lapisan keluaran	Intel(R) Core i7 prosesor	NSL-KDD: Akurasi = 98,43%, Presisi = 99,22%, Recall = 97,12%, Skor F1 = 98,57%. C7: Akurasi = 98,92%, Presisi = 97,45%, Recall = 98,97%, Skor F1 = 98,35%

Tabel 5. *Lanjutan.*

Ref.	Praproses Strategi	Nilai Hiperparameter	Eksperimental Pengaturan	Metrik Kinerja
RoopakM dan kawan-kawan. [38][Bahasa Indonesia]		Lapisan CNN 1D dengan fungsi ReLu, lapisan LSTM dengan pengoptimal Adam, lapisan putus sekolah dengan tingkat 0,5, lapisan FC, dan lapisan padat dengan fungsi sigmoid membentuk model CNN–LSTM	Intel Core-i7 dengan Keras, TensorFlow, dan MATLAB	Presisi = 97,41%, Mengingat = 99,1%, Akurasi = 97,36%
Moh. dkk. [41][Bahasa Indonesia]	Fitur pengacakan dan BOW	Dua lapisan FC tersembunyi yang masing-masing terdiri dari 256 neuron dengan fungsi aktivasi ReLU dan satu neuron dengan fungsi aktivasi sigmoid membentuk modul LSTM.	Kartu Grafis NVIDIA GTX tahun 1050	Recall = 97,6%, Akurasi = 98,15%, Presisi = 98,42%, TNR = 98,4%, FPR = 1,6%, Skor F1 = 98,05%
RoopakM dan kawan-kawan. [39][Bahasa Indonesia]	Min-maks	Lapisan maxpooling, LSTM, dan dropout dengan fungsi aktivasi Relu setelah CNN 1D; laju pembelajaran = 0,001, ukuran batch = 256, epoch = 100, dan laju dropout = 0,2%.	NVIDIA Tesla GPU VIOO dengan Aliran Tensor Dan Perangkat lunak keras	Akurasi = 99,03%, Recall = 99,35%, Presisi = 99,26%, Skor F1 = 99,36%, Waktu Pelatihan = 15.313,10 detik
Elsay dan kawan-kawan. [42][Bahasa Indonesia]	Min-maks	Empat lapisan tersembunyi RNN di RNN-AE; jumlah saluran untuk fase encoder adalah 64, 32, 16, dan 8, dengan dua fungsi softmax		Akurasi identifikasi serangan adalah 0,99%, sedangkan untuk kasus jinak adalah 1,00. Pada skala F1, kasus serangan mendapat skor 0,99 dan kasus jinak mendapat skor 0,99%. AUC = 98,8
Premkumar dan lain-lain. [81][Bahasa Indonesia]			Kecepatan Bit Konstan (CBR) aplikasi, 200 node, durasi simulasi 500 detik tion, dan 5% hingga 20% dari node reguler sebagai node penyerang.	Tingkat serangan antara 5% dan 15%, tingkat deteksi antara 86% dan 99%, dan tingkat alarm palsu 15%
Nugraha dkk. [40][Bahasa Indonesia]	Min-Maks	Lapisan perataan, maxpool, dan dropout. Setelah lapisan LSTM, terdapat lapisan padat FC dengan fungsi ReLu, lapisan dropout, dan lapisan padat terakhir dengan fungsi sigmoid. Epoch = 50, pelatihan = 0,0005, tingkat dropout = 0,3, ukuran kernel = 5, dan filter CNN ditetapkan ke 64	Ular piton	Akurasi = 99,998%, Presisi = 99,989%, Spesifisitas = 99,997%, Recall = 100%, Skor F1 = 99,994%
Dia dan rekan-rekannya.78[Bahasa Indonesia]		Delapan lapisan FC dalam 8LANN. Lapisan pooling dan fungsi ReLu diterapkan setelah setiap lapisan, dengan lapisan kedelapan sebagai pengecualian. 500 batch, fungsi loss crossentropy, pengoptimal SGD, dan laju pelatihan 0,001 digunakan dalam percobaan ini.	Ubuntu tanggal 16.04 dengan NVIDIA RTX Seri 2080Ti	Akurasi = 87,8% dan Transferabilitas = 19,65.
Chen dan kawan-kawan. [79][Bahasa Indonesia]	Game dengan Post-Keadaan Keputusan (GPDS)	Mengatasi masalah optimasi MDP dengan menawarkan teknik permainan pembelajaran penguatan multi-pengguna berbasis kebijakan yang unik	Tensorflow dan Intelp(R)	Berdasarkan temuan percobaan, GPDS yang disarankan mengungguli algoritma SOTA dalam hal kinerja anti-jamming.

Hiperparameter sangat penting karena secara langsung memengaruhi perilaku algoritma pelatihan ML. Sebelum melatih model, nilai-nilai hiperparameter tertentu harus dipilih, yang memerlukan keahlian dan pengalaman khusus. Ada dua pendekatan untuk penyetelan hiperparameter, yaitu, pencarian manual dan teknik pencarian otomatis. Dalam pencarian manual, nilai-nilai untuk hiperparameter dipilih secara manual. Teknik pencarian otomatis mirip dengan pencarian grid, namun, pendekatan pencarian grid lebih mahal. Pendekatan lain, yang dikenal sebagai pencarian acak, telah diperkenalkan untuk mengatasi masalah pencarian grid. Contoh-contoh hiperparameter meliputi jumlah epoch, ukuran batch, laju pembelajaran, algoritma pelatihan, jumlah lapisan, jumlah neuron di setiap lapisan, dll.

Pengaturan eksperimen mencakup informasi tentang program, kumpulan data, perangkat keras fisik, dan aspek lain dari proses eksperimen. Saat pelatihan dan pengujian

Kerangka waktu bergantung pada pengaturan perangkat keras, hal ini sangat penting. Karena kompleksitas algoritma ML/DL, diperlukan konfigurasi perangkat keras yang sesuai.

Indikator kinerja adalah ukuran paling populer yang didefinisikan dalam bagian ini. Untuk klasifikasi biner, pengukuran kinerja yang umum adalah akurasi, recall, presisi, skor F1, AUC, dll.

Matriks kebingungan digambarkan sebagai gambaran umum hasil yang diperkirakan oleh model kategorisasi. Matriks ini mencakup (TP Positif Benar), Negatif Benar (TN), Positif Palsu (FP), dan Negatif Palsu (FN) [89].

Tingkat positif sebenarnya (TPR) ditentukan dengan mengikuti Persamaan (1) Selain itu, hal ini juga dikenal sebagai recall atau sensitivitas [90], dan harus setinggi mungkin.

$$\text{TPR} = \frac{T.P.}{(T.P. + \text{Bahasa Inggris FN})} \quad (1)$$

Presisi ditentukan dengan mengikuti Persamaan (2) dengan memeriksa berapa banyak kelas positif yang diprediksi secara memadai oleh model tersebut benar-benar positif [91].

$$\text{Presisi} = \frac{T.P.}{(T.P. + \text{Bahasa Inggris})} \quad (2)$$

Persamaan berikut (3), akurasi didefinisikan sebagai persentase prediksi benar yang dibuat oleh model di semua kelas. Tingkat tertinggi lebih disukai. Rumusnya adalah sebagai berikut [91]:

$$\text{Akurasi} = \frac{T.P. + \text{Bahasa Inggris}}{(Total)} \quad (3)$$

FPR atau False Positive Rate ditunjukkan pada Persamaan (4Bahasa Indonesia:90]; mengukur persentase kejadian negatif yang secara tidak tepat diprediksi oleh model sebagai positif.

$$\text{FPR} = \frac{\text{Bahasa Inggris}}{(\text{Bahasa Inggris} + \text{Bahasa Inggris})} \quad (4)$$

Persentase kasus positif yang salah diantisipasi sebagai kasus negatif dikenal sebagai tingkat negatif palsu (FNR), dan ditentukan seperti yang ditunjukkan pada Persamaan (5Bahasa Indonesia:90[Bahasa Indonesia]

$$\text{FNR} = \frac{\text{Bahasa Inggris FN}}{(T.P. + \text{Bahasa Inggris FN})} \quad (5)$$

TNR atau True Negative Rate ditunjukkan pada Persamaan (6); Spesifisitas adalah nama lain untuk hal ini. Hal ini digambarkan sebagai persentase kejadian buruk yang secara akurat diperkirakan sebagai kejadian buruk [90].

$$\text{TNR} = \frac{\text{Bahasa Inggris}}{(\text{Bahasa Inggris} + \text{Bahasa Inggris})} \quad (6)$$

Sulit untuk membandingkan dua model jika salah satunya memiliki daya ingat yang tinggi dan akurasi yang rendah atau sebaliknya. Oleh karena itu, skor F1 digunakan untuk membandingkannya. Skor ini digunakan untuk menilai daya ingat dan presisi secara bersamaan [92]. Persamaan (7) digunakan untuk menghitung skor F1:

$$\text{F1-Skor} = \frac{2 * Mengingat * Presisi}{(Mengingat + Presisi)} \quad (7)$$

Efisiensi pada tingkat ambang batas yang berbeda untuk masalah klasifikasi dikenal sebagai kurva AUC–ROC. Sebuah model membuat prediksi yang lebih akurat jika AUC mendekati 1 [93].

7. Kesenjangan Penelitian dalam Literatur yang Ada

Kesenjangan penelitian yang dirinci di bawah ini diidentifikasi melalui penilaian menyeluruh kami terhadap literatur.

• Kumpulan data yang tidak cukup besar: karena potensi kerugian reputasi atau uang, mayoritas organisasi korban enggan mengungkapkan informasi mengenai serangan yang dilakukan terhadap mereka. Lebih jauh, tidak ada basis data lengkap di domain publik yang mencakup semua jenis lalu lintas, termasuk lalu lintas asli, lalu lintas dengan kecepatan rendah, lalu lintas dengan kecepatan tinggi, dan lalu lintas kilat [37Bahasa Indonesia:39Bahasa Indonesia:40Bahasa Indonesia:42 Bahasa Indonesia:53–73Bahasa Indonesia:75–77Bahasa Indonesia:81]. Oleh karena itu, pengaturan eksperimental diperlukan untuk menyediakan kumpulan data yang luas untuk validasi menyeluruh metodologi deteksi DDoS.

• Akses ke kumpulan data yang bias: kejadian serangan DDoS biasanya sangat bias dibandingkan dengan kejadian sebenarnya dalam kumpulan data yang tersedia saat ini [37Bahasa Indonesia:39Bahasa Indonesia:40Bahasa Indonesia:53–56Bahasa Indonesia:60–67Bahasa Indonesia:70–72Bahasa Indonesia:75Bahasa Indonesia:77]. Oleh karena itu, sejumlah besar kasus di setiap kelas diperlukan untuk menjalankan teknik pembelajaran mendalam secara efektif. Untuk studi yang efektif di area ini, strategi peningkatan yang baik diperlukan untuk menyediakan volume yang cukup besar dari semua bentuk lalu lintas.

• Permintaan akan data praproses berkualitas tinggi: kualitas data praproses memengaruhi seberapa akurat model pembelajaran mendalam yang dihasilkan. Oleh karena itu, metode praproses yang efektif diperlukan untuk pelatihan model DL yang efektif [61–63Bahasa Indonesia:65–70Bahasa Indonesia:72Bahasa Indonesia:75].

• Kategorisasi biner: mayoritas literatur yang tersedia saat ini [37Bahasa Indonesia:39Bahasa Indonesia:40Bahasa Indonesia:42Bahasa Indonesia: 53Bahasa Indonesia: 54Bahasa Indonesia:57Bahasa Indonesia:63–65Bahasa Indonesia:67Bahasa Indonesia:68Bahasa Indonesia:70–73Bahasa Indonesia:75–78Bahasa Indonesia:81] berfokus pada kategorisasi biner serangan DDoS daripada klasifikasi multi-kelas.

• Upaya yang tidak memadai pada data yang tidak diketahui atau serangan zero-day: ketika kumpulan data instruksi dan penilaian berisi ciri atau pola yang sama, model ML dapat berfungsi dengan baik. Namun, algoritme berbasis ML tidak dapat secara akurat mendeteksi ancaman yang tidak diketahui dalam situasi kehidupan nyata, di mana serangan dapat diluncurkan menggunakan pola baru. Akibatnya, model ini harus sering diperbarui untuk memperhitungkan serangan baru dan belum teruji [53].

• Menggunakan kumpulan data offline untuk evaluasi: mayoritas penelitian yang kami tinjau menggunakan kumpulan data offline untuk menilai model pembelajaran mendalam [37Bahasa Indonesia:39Bahasa Indonesia:42Bahasa Indonesia:55–59Bahasa Indonesia:61–67Bahasa Indonesia:69Bahasa Indonesia:70Bahasa Indonesia:72Bahasa Indonesia: 73Bahasa Indonesia:75Bahasa Indonesia:77Bahasa Indonesia:78Bahasa Indonesia:81]. Implementasi model-model ini dalam jaringan aktual masih dalam tahap pengembangan. Evaluasi model secara real-time akan sangat bermanfaat untuk verifikasi yang memadai.

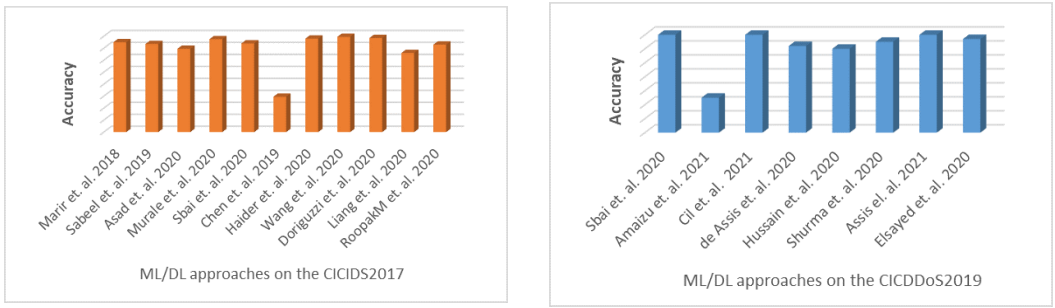
• Tidak ada penerapan model pertahanan real-time otomatis: sebagian besar serangan DDoS menguasai situs target dalam waktu yang relatif singkat, dan pengelola jaringan sering kali tidak dapat mengidentifikasi dan melawan serangan ini secara otomatis. Penyebab utamanya adalah strategi pertahanan itu sendiri menjadi rentan terhadap serangan DDoS berdasarkan banjir. Oleh karena itu, solusi DDoS berkecepatan tinggi dan efisien secara komputasi diperlukan untuk menghentikan serangan tersebut secara otomatis.

8. Kesimpulan dan Arah Masa Depan

Mungkin cukup sulit untuk membedakan antara serangan DDoS dengan berbagai tingkat dan pola dan lalu lintas normal. Selama bertahun-tahun, banyak metode ML/DL yang efektif untuk mendeteksi serangan DDoS telah disarankan oleh berbagai peneliti. Namun, sayangnya, penerapan teknik-teknik ini sangat dibatasi karena penyerang terus-menerus mengubah taktik serangan mereka. Temuan yang melibatkan protokol SLR dievaluasi dan diambil dari tinjauan ini untuk menilai sistem deteksi serangan DDoS terkini berdasarkan pendekatan ML/DL. Literatur telah dirangkum dalam Bagian4 sesuai dengan taksonomi yang disarankan untuk deteksi serangan DDoS menggunakan teknik ML/DL, dengan masing-masing kelebihan dan kekurangan yang tercantum pada setiap studi. Tingkat akurasi yang dilaporkan dalam banyak literatur lebih dari 99%. Karena sebagian besar studi ini menilai model mereka menggunakan analisis data offline untuk evaluasi dan perbandingan, metrik tertentu untuk kinerja dapat bervariasi dalam pengaturan dunia nyata atau produksi. Secara khusus, kami mencatat bahwa makalah yang ada umumnya tidak menggunakan DS atau teknik penilaian yang sama, sehingga sulit untuk membandingkan hasilnya.

Terkait dengan dataset yang paling sering digunakan dalam literatur, 29% penelitian memanfaatkan dataset penelitian terkenal saat ini CICIDS2017, 23% menggunakan dataset CICDDoS2019, 18% menggunakan dataset ISCX2012, 10% menggunakan dataset NSL-KDD, 10% menggunakan dataset KDDCUP99.

dataset, 5% menggunakan dataset UNSW-NB15, 3% menggunakan dataset CSE-CIC-IDS2018, dan 2% menggunakan dataset Kyoto 2006. Gambar5a menunjukkan kemanjuran teknik deteksi serangan DDoS berbasis ML/DL yang diteliti pada dataset CICIDS2017. Dapat dilihat bahwa metode yang mengandalkan CNN [64Bahasa Indonesia:67], DNN [56], AE–SVM [76], dan CNN–LSTM [39] semuanya mampu mencapai akurasi lebih baik dari 99%. Gambar5b menunjukkan seberapa baik metode deteksi serangan DDoS berbasis ML/DL yang diteliti bekerja pada dataset CICDoS2019. Teknik yang mengandalkan ResNet berbasis CNN [69], LSTM [73], DNN [57–59], dan GRU [37] semuanya menunjukkan akurasi lebih dari 99%.



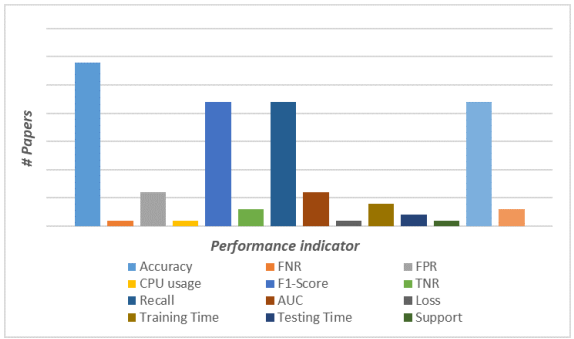
(A) **(B)**

Gambar 5. Keakuratan pendekatan ML/DL yang dipelajari pada (**A**) kumpulan data CICIDS2017 [38Bahasa Indonesia:49Bahasa Indonesia:53Bahasa Indonesia:55– 57Bahasa Indonesia:62Bahasa Indonesia:64Bahasa Indonesia:65Bahasa Indonesia:67Bahasa Indonesia:72] Dan (**B**) kumpulan data CICDDoS2019 [37Bahasa Indonesia:42Bahasa Indonesia:53Bahasa Indonesia:58Bahasa Indonesia:59Bahasa Indonesia:68Bahasa Indonesia:69Bahasa Indonesia:73].

Pada dataset ISCX2012, teknik LSTM, CNN, dan LSTM–Bayes semuanya menunjukkan akurasi kurang dari 98,8% [70Bahasa Indonesia:71]. Pada dataset NSL-KDD, hanya teknik CNN di [63] menunjukkan akurasi di atas 99%, dan diperlukan perhitungan rumit untuk mencapainya.

Kita dapat menyimpulkan dari penelitian ini bahwa teknik praproses yang paling umum digunakan adalah BOW, normalisasi Z-score, pengkodean one-hot, dan normalisasi min-max.

Kesimpulan lain dari tinjauan kami terkait dengan metrik kinerja. Dari studi yang ditinjau, 29 menggunakan pengukuran akurasi untuk mengevaluasi teknik mereka, dibandingkan dengan 22 studi yang masing-masing menggunakan metrik presisi, perolehan kembali, dan skor F1 dan enam studi yang masing-masing menggunakan metrik FPR dan AUC. Temuan ini ditunjukkan pada Gambar6; dapat dilihat bahwa sebagian besar makalah tidak melaporkan waktu pengujian/pelatihan untuk metodologi mereka, meskipun faktanya pengukuran ini sangat penting untuk implementasi sistem di dunia nyata atau pengaturan produksi.



Gambar 6. Proporsi metode ML/DL yang memanfaatkan indikator kinerja berbeda.

Sehubungan dengan arah penelitian di masa depan, penemuan kami mengenai teknik ML/DL untuk mendeteksi serangan DDoS mengarah pada jalur berikut untuk studi lebih lanjut:

- **Kurangnya implementasi sistem ML/DL yang sebenarnya:**sebagian besar penelitian yang berfokus pada analisis model-model ini telah mengabaikan kebutuhan penting untuk mengevaluasi kinerja model-model ini dalam situasi waktu nyata di mana serangan DDoS benar-benar terjadi. Masih ada kebutuhan mendesak untuk model ML/DL yang telah diverifikasi menggunakan skenario dunia nyata.

- **Model ML/DL bergantung pada pembaruan yang dinamis dan sering:**Model yang dapat diperbarui secara dinamis dan rutin sesuai dengan jenis serangan baru merupakan suatu keharusan karena pola serangan terus berubah dan cepat, dan merupakan elemen penting dalam dunia teknologi baru yang berkembang pesat saat ini yang disertai ancaman yang lebih canggih. Namun, tidak ada model DL seperti itu yang tersedia dalam literatur.
- **Persyaratan untuk model ML/DL ringan:**Model yang ringan diperlukan untuk jaringan seperti Internet of Things, MANETS, dan jaringan sensor nirkabel, karena jaringan ini memiliki daya komputasi dan memori yang terbatas serta sangat rentan terhadap ancaman keamanan. Di masa mendatang, diharapkan akan semakin diperlukan pengembangan model DL yang efektif dan portabel untuk konteks ini.
- **Kebutuhan akan kumpulan data yang sesuai:**Kumpulan data saat ini kurang beragam dalam hal jenis serangan dan kualitas rekaman data yang dikandungnya, sehingga menyebabkan sistem deteksi bias dan tidak dapat mengidentifikasi semua jenis serangan. Sangat penting untuk memiliki kumpulan data yang cukup guna memastikan model deteksi yang akurat dan efektif.

Sebagai penutup, menangani bidang penelitian ini penting untuk mewujudkan kemajuan signifikan dalam bidang ini dan menjembatani kesenjangan yang saat ini ada dalam literatur.

Kontribusi Penulis: Konseptualisasi, TEA dan Y.-WC; Metodologi, TEA dan Y.-WC; Perangkat Lunak, TEA dan Y.-WC; Validasi, TEA dan Y.-WC; Sumber daya, TEA dan Y.-WC; Penulisan draf asli, TEA; Supervisi, Y.-WC dan SM Semua penulis telah membaca dan menyetujui versi naskah yang diterbitkan.

Pendanaan: Penelitian ini didukung oleh Dana Publikasi di bawah Kantor Kreativitas dan Manajemen Penelitian, Universiti Sains Malaysia dan hibah eksternal Universiti Sains Malaysia (USM) (Nomor Hibah: 304/PNAV/650958/U154).

Pernyataan Dewan Peninjau Institusional: Artikel ini tidak memuat penelitian apa pun yang melibatkan partisipan manusia atau hewan yang dilakukan oleh penulis mana pun.

Pernyataan Persetujuan yang Diinformasikan: Persetujuan yang diinformasikan diperoleh dari semua peserta individu yang diikutsertakan dalam penelitian.

Konflik Kepentingan: Penulis menyatakan bahwa mereka tidak memiliki konflik kepentingan.

Singkatan

Singkatan berikut digunakan dalam naskah ini:

AE	Pengkode Otomatis
JAM	Jaringan Syaraf Tiruan
BUSUR	Bag of Word
CIC	Institut Keamanan Siber Kanada
KL	Lapisan Konvolusional
Berita CNN	Jaringan Syaraf Konvolusional
Serangan DDoS	Penolakan Layanan Terdistribusi
DL	Pembelajaran Mendalam
TTL	Jaringan Saraf Dalam
Serangan DoS	Penolakan Layanan
Tanggal	Pohon Keputusan
FNR	Tingkat Negatif Palsu
FPR	Tingkat Positif Palsu
GPU	Unit Pemrosesan Grafis
IDENTITAS	Sistem Deteksi Intrusi
Internet of Things (IoT)	Internet of Things
AKU P	Protokol Internet
KNN	k-Tetangga Terdekat
Bahasa Indonesia: LR	Regresi Logistik
LSTM	Memori jangka pendek panjang

JELAS	CNN Ringan dan Dapat Digunakan dalam Deteksi DDoS
MKL	Pembelajaran Kernel Ganda
Bahasa Inggris	Pembelajaran Mesin
Bahasa Inggris MLP	Perseptron Multilapis
MSE	Kesalahan Kuadrat Rata-rata
Catatan	Pendekatan Bayes Naif
NID	Deteksi Intrusi Jaringan
Tidak ada	Jaringan Syaraf
PDR	Rasio Pengiriman Paket
Bahasa Indonesia: Frekuensi Hutan	Hutan Acak
Bahasa Indonesia: RNN	Jaringan Syaraf Tiruan Berulang
SD	Tinjauan Literatur Sistematis
Kamera SLR	Jaringan Terdefinisi Perangkat
Bahasa Inggris: SML	Lunak Pembelajaran Mesin
Bahasa Indonesia: SVM	Dangkal Mesin Vektor Pendukung
TCP	Pembelajaran Transfer Protokol
Bahasa Inggris	Kontrol Transmisi
TNR	Tingkat Negatif Sejati
TPR	Tingkat Positif Sejati
Bahasa Indonesia: UDP	Protokol Datagram Pengguna
Bahasa Inggris WSN	Jaringan Sensor Nirkabel
DL	Jaringan Saraf Dalam
Bahasa Inggris ELM	Tingkat Alarm Palsu Mesin
JAUH	Pembelajaran Ekstrim
FCN	Jaringan yang Terhubung
Bahasa Inggris FN	Sepenuhnya Negatif Palsu
Bahasa Inggris	Positif Palsu
Bahasa Inggris	Negatif Benar
T.P.	Benar Positif
Kecerdasan buatan	Piala KDD
Bahasa Inggris: KC	Kecerdasan Buatan
Inggris	Kota Kyoto
NK	NSL-KDD
PBB	UNSW-NB15
C7	CIC-IDS 2017
C8	CSE-CIC-IDS2018
saya2	ISCX 2012
C9	Bahasa Indonesia: CICDDoS2019
FNR	Tingkat bunga negatif palsu
FPR	Tingkat Positif Palsu

Referensi

1. Ali, T.; Morad, A.; Abdala, M. Keseimbangan beban dalam jaringan pusat data sdn.*Int. J. Teknik Komputer Listrik.***Tahun 2018**Bahasa Indonesia:**8**, 3086–3092.
2. Ali, T.; Morad, A.; Abdala, M. Implementasi SDN di Jaringan Pusat Data.*J.Komunikasi.***Tahun 2019**, hal. 223–228. [Referensi silang[Bahasa Indonesia]
3. Ali, T.; Morad, A.; Abdala, M. Manajemen lalu lintas di dalam jaringan pusat data yang ditentukan perangkat lunak.*Bull. Insinyur Listrik. Menginformasikan.***Tahun 2020**Bahasa Indonesia: **9**, 2045–2054. [Referensi silang[Bahasa Indonesia]
4. Badan Keamanan Siber dan Keamanan Infrastruktur. Tersedia daring:https://www.cisa.gov/uscert/ncas/tips/ST04-015(diakses pada 20 November 2021).
5. Eliyan, LF; Di Pietro, R. Serangan DoS dan DDoS di Software Defined Networks: Survei solusi yang ada dan tantangan penelitian.*Sistem Komputer Umum Masa Depan* **Tahun 2021**Bahasa Indonesia:*122*, hal. 149–171. [Referensi silang[Bahasa Indonesia]
6. Bursa mata uang kripto EXMO telah ditutup karena serangan DDoS yang “besar-besaran”. Tersedia online:https://portswigger.net/daily-swig/bursa-mata-uang-kripto-Inggris-exmo-terputus-fungsi-oleh-serangan-ddos-besar-besaran(diakses pada 1 November 2021).
7. Catak, FO; Mustacoglu, AF Deteksi serangan penolakan layanan terdistribusi menggunakan autoencoder dan jaringan saraf dalam.*J. Intell. Sistem Fuzzy.***Tahun 2019**Bahasa Indonesia: *37*, 3969–3979. [Referensi silang[Bahasa Indonesia]

8. Li, Y.; Lu, Y. LSTM-BA: Pendekatan deteksi DDoS yang menggabungkan LSTM dan bayes. Dalam Prosiding Konferensi Internasional ke-7 tentang Cloud dan Big Data (CBD) Tingkat Lanjut tahun 2019, Suzhou, Tiongkok, 21–22 September 2019; hlm. 180–185.
9. Yuan, X.; Li, C.; Li, X. DeepDefense: Mengidentifikasi serangan DDoS melalui pembelajaran mendalam. Dalam Prosiding Konferensi Internasional IEEE tentang Komputasi Cerdas (SMARTCOMP) 2017, Hong Kong, Tiongkok, 29–31 Mei 2017.
10. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Metode pembelajaran mesin dan pembelajaran mendalam untuk keamanan siber.*Akses IEEE***Tahun 2018** Bahasa Indonesia:*6*, 35365–35381. [Referensi silang[Bahasa Indonesia]
11. Van NT; Thinh, TN; Sach, LT Sistem deteksi intrusi jaringan berbasis anomali menggunakan pembelajaran mendalam. Dalam Prosiding Konferensi Internasional tentang Ilmu Sistem dan Rekayasa (ICSSE) 2017, Kota Ho Chi Minh, Vietnam, 21–23 Juli 2017; hlm. 210–214.
12. Vinayakumar, R.; Soman, KP; Poornachandran, P. Menerapkan jaringan saraf konvolusional untuk deteksi intrusi jaringan. Dalam Prosiding Konferensi Internasional 2017 tentang Kemajuan dalam Komputasi, Komunikasi, dan Informatika (ICACCI), Udupi, India, 13–16 September 2017; hlm. 1222–1228.
13. Aldweesh, A.; Derhab, A.; Emam, AZ Pendekatan pembelajaran mendalam untuk sistem deteksi intrusi berbasis anomali: Survei, taksonomi, dan masalah terbuka.*Sistem Berbasis Pengetahuan***Tahun 2020**Bahasa Indonesia:*189*, 105124. [Referensi silang[Bahasa Indonesia]
14. Wang, Y.; Lou, X.; Fan, Z.; Wang, S.; Huang, G. Pembagian rahasia kuantum ambang batas multi-dimensi (t, n) yang dapat diverifikasi berdasarkan perjalanan kuantum.*Jurnal Int. Teori Fisik.***Tahun 2022** Bahasa Indonesia:*61*, 24. [Referensi silang[Bahasa Indonesia]
15. Berita Terkini tentang Kecerdasan Buatan. Ringkasan: Panduan Mendalam tentang Kecerdasan Buatan Kuantum. Tersedia daring: https://www.ai-summary.com/summary-in- depth-guide-to-quantum-artificial-intelligence/(diakses pada 22 Januari 2022).
16. Ferrag, MA; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Pembelajaran mendalam untuk deteksi intrusi keamanan siber: Pendekatan, kumpulan data, dan studi perbandingan.*J. Inf. Secur. Terapan.***Tahun 2020**Bahasa Indonesia:*50*, 102419. [Referensi silang[Bahasa Indonesia]
17. Aleesa, AM; Zaidan, BB; Zaidan, AA; Sahar, NM Tinjauan sistem deteksi intrusi berdasarkan teknik pembelajaran mendalam: Taksonomi yang koheren, tantangan, motivasi, rekomendasi, analisis substansial dan arah masa depan.*Komputasi Neural. Terapan.* **Tahun 2020**Bahasa Indonesia:*32*, 9827–9858. [Referensi silang[Bahasa Indonesia]
18. Gamage, S.; Samarabandu, J. Metode pembelajaran mendalam dalam deteksi intrusi jaringan: Survei dan perbandingan objektif. *J. Netw. Komputasi Terapan.***Tahun 2020**Bahasa Indonesia:*169*, 102767. [Referensi silang[Bahasa Indonesia]
19. Ahmad, Z.; Khan, AS; Shiang, CW; Abdullah, J.; Ahmad, F. Sistem deteksi intrusi jaringan: Studi sistematis tentang pendekatan pembelajaran mesin dan pembelajaran mendalam.*Trans. Telekomunikasi. Teknologi. Darurat.***Tahun 2021**Bahasa Indonesia:*32*, e4150. [Referensi silang[Bahasa Indonesia]
20. Ahmad, R.; Alsmadi, I. Pendekatan pembelajaran mesin untuk keamanan IoT: Tinjauan literatur sistematis.*Hal-hal Internet***Tahun 2021**Bahasa Indonesia: *14*, 100365. [Referensi silang [Bahasa Indonesia]
21. Keele, S.*Pedoman untuk Melakukan Tinjauan Literatur Sistematis dalam Rekayasa Perangkat Lunak*; Laporan Teknis, Ver. 2.3 Laporan Teknis EBSE; Laporan Bersama Universitas Keele dan Universitas Durham EBSE: Newcastle, Inggris, 2007
22. Costa, VG; Pedreira, CE Kemajuan terkini dalam pohon keputusan: Survei yang diperbarui.*Artif. Intelijen. Rev.***Tahun 2022**, 1–36. [Referensi silang[Bahasa Indonesia]
23. Zhang, Y.; Cao, G.; Wang, B.; Li, X. Metode ensemble baru untuk k-tetangga terdekat.*Pengenalan Pola***Tahun 2019**Bahasa Indonesia:*85*, 13–25. [Referensi silang[Bahasa Indonesia]
24. Yılmaz, A.; Küçüker, A.; Bayrak, G.; Ertekin, D.; Shafie-Khah, M.; Guerrero, JM Metode klasifikasi PQD otomatis yang ditingkatkan untuk generator terdistribusi dengan pendekatan berbasis SVM hibrid menggunakan transformasi wavelet yang tidak terdesimasi.*Jurnal Int. Sistem Energi Listrik.***Tahun 2022**Bahasa Indonesia:*136*, 107763. [Referensi silang[Bahasa Indonesia]
25. Ren, H.; Lu, H. Jaringan kapsul pengkodean komposisi dengan perutean k-means untuk klasifikasi teks.*Pengenalan Pola. Lett.***Tahun 2022**Bahasa Indonesia: *160*, 1–8. [Referensi silang [Bahasa Indonesia]
26. Gopi, R.; Sathiyamoorthi, V.; Selvakumar, S.; Manikandan, R.; Chatterjee, P.; Jhanjhi, Selandia Baru; Luhach, AK Peningkatan metode model berbasis ANN untuk mendeteksi serangan DDoS pada multimedia internet of things.*Multimed. Alat Aplikasi.***Tahun 2022**Bahasa Indonesia:*81*, 26739–26757. [Referensi silang[Bahasa Indonesia]
27. Zeinalpour, A.; Ahmed, HA Mengatasi Efektivitas Metode Deteksi Serangan DDoS Berdasarkan Metode Pengelompokan Menggunakan Metode Ensemble.*Elektronik* **Tahun 2022**Bahasa Indonesia:*11*, 2736. [Referensi silang[Bahasa Indonesia]
28. AI vs. Machine Learning vs. Deep Learning: Ketahui Perbedaannya. Tersedia online:https://www.simplilearn.com/tutorials/tutorial-kecerdasan-buatan/ai-vs-pembelajaran-mesin-vs-pembelajaran-mendalam#:~:text=Pembelajaran%20Mesin%20adalah%20subset, algoritma%20untuk%20melatih%20sebuah%20model(diakses pada 1 Januari 2023).
29. Bachouch, A.; Huré, C.; Langrené, N.; Pham, H. Algoritma jaringan saraf dalam untuk masalah kontrol stokastik pada horizon terbatas: Aplikasi numerik.*Metodologi. Komputasi. Terapan. Probab.***Tahun 2022**Bahasa Indonesia:*24*, 143–178. [Referensi silang[Bahasa Indonesia]
30. Sellami, A.; Tabbone, S. Pembelajaran representasi laten relevan berbasis jaringan saraf dalam untuk klasifikasi gambar hiperspektral. *Pengenalan Pola.***Tahun 2022**Bahasa Indonesia: *121*, 108224. [Referensi silang[Bahasa Indonesia]
31. Penguasaan Pembelajaran Mesin. Pengenalan Sederhana terhadap Rectified Linear Unit (ReLU). Tersedia daring:https://machinelearningmastery.com/rectified-linear-activation-function-for-deep-learning-neural-networks/ #:~:text=Fungsi%20aktivasi%20linier%20yang%20diperbaiki,jika%2C%20itu%20akan%20menghasilkan%20nol(diakses pada 1 Januari 2023).
32. Santos, CFGD; Papa, JP Menghindari overfitting: Survei tentang metode regularisasi untuk jaringan saraf konvolusional.*ACM Komputasi Surv. CSUR***Tahun 2022**Bahasa Indonesia:*54*, 213. [Referensi silang[Bahasa Indonesia]
33. Yadav, SP; Zaidi, S.; Mishra, A.; Yadav, V. Survei tentang pembelajaran mesin dalam pengenalan emosi ucapan dan sistem penglihatan menggunakan jaringan saraf berulang (RNN). *Arsitektur. Metode Komputasi.***Tahun 2022**Bahasa Indonesia:*29*, 1753–1770. [Referensi silang[Bahasa Indonesia]
34. Jenis-jenis Jaringan Syaraf Tiruan dan Definisi Jaringan Syaraf Tiruan. Tersedia online:https://www.mygreatlearning.com/blog/jenis-jaringan-saraf(diakses pada 25 November 2022).

35. Mehedi, MAA; Khosravi, M.; Yazdan, MMS; Shabanian, H. Menjelajahi Dinamika Temporal Debit Sungai menggunakan Jaringan Syaraf Rekursif Memori Jangka Panjang dan Pendek Univariat (LSTM) di Cabang Timur Sungai Delaware.*Hidrologi***Tahun 2022**Bahasa Indonesia:*9*, 202. [Referensi silang[Bahasa Indonesia]
36. Jaringan Syaraf Tiruan Berulang dan LSTM Dijelaskan. Tersedia online:https://purnasaigudikandula.medium.com/recurrentneural-networks-and-lstm-explained-7f51c7f6bbb9(diakses pada 25 November 2022).
37. Assis, MV; Carvalho, LF; Lloret, J.; Proença, ML Sistem pembelajaran mendalam GRU terhadap serangan dalam jaringan yang ditentukan perangkat lunak. *J. Netw. Komputasi Terapan.***Tahun 2021**Bahasa Indonesia:*177*, 102942. [Referensi silang[Bahasa Indonesia]
38. Roopak, M.; Tian, GY; Chambers, J. Model pembelajaran mendalam untuk keamanan siber dalam jaringan IoT. Dalam Prosiding Lokakarya dan Konferensi Komputasi dan Komunikasi Tahunan ke-9 IEEE 2019 (CCWC), Las Vegas, NV, AS, 7–9 Januari 2019; hlm. 452–457.
39. Roopak, M.; Tian, GY; Chambers, J. Sistem deteksi intrusi terhadap serangan DDoS di jaringan IoT. Dalam Prosiding Lokakarya dan Konferensi Komputasi dan Komunikasi Tahunan ke-10 tahun 2020 (CCWC), Las Vegas, NV, AS, 6–8 Januari 2020; hlm. 562–567.
40. Nugraha, B.; Murthy, RN Deteksi serangan DDoS lambat berbasis pembelajaran mendalam di jaringan berbasis SDN. Dalam Prosiding konferensi IEEE 2020 tentang Virtualisasi Fungsi Jaringan dan Jaringan yang Ditentukan Perangkat Lunak (NFV-SDN), Leganes, Spanyol, 10–12 November 2020; hlm. 51–56.
41. Mohammad, H.; Slimane, S. IoT-NETZ: Pendekatan mitigasi serangan spoofing praktis dalam jaringan SDWN. Dalam Prosiding Konferensi Internasional Ketujuh tentang Sistem yang Ditentukan Perangkat Lunak (SDS) 2020, Paris, Prancis, 20–23 April 2020; hlm. 5–13.
42. Elsayed, MS; Le-Khac, NA; Dev, S.; Jurcut, AD DDoSNet: Model deeplearning untuk mendeteksi serangan jaringan. Dalam Prosiding Simposium Internasional IEEE ke-21 tentang Dunia Jaringan Nirkabel, Seluler, dan Multimedia (WoWMoM), Cork, Irlandia, 31 Agustus–3 September 2020; hlm. 391–396.
43. Shen, Y.; Zheng, K.; Wu, C.; Zhang, M.; Niu, X.; Yang, Y. Metode ansambel berdasarkan seleksi menggunakan algoritma kelelawar untuk deteksi intrusi.*Komputasi J.***Tahun 2018**Bahasa Indonesia:*61*, 526–538. [Referensi silang[Bahasa Indonesia]
44. Shone, N.; Ngoc, TN; Phai, VD; Shi, Q. Pendekatan pembelajaran mendalam untuk deteksi intrusi jaringan.*IEEE Trans. Muncul. Komputasi Teratas. Intel.***Tahun 2018**Bahasa Indonesia:*2*, 41–50. [Referensi silang[Bahasa Indonesia]
45. Ali, MH; Al Mohammed, BAD; Ismail, A.; Zolkipli, MF Sistem deteksi intrusi baru berdasarkan jaringan pembelajaran cepat dan optimasi kumpulan partikel.*Akses IEEE* **Tahun 2018**Bahasa Indonesia:*6*, 20255–20261. [Referensi silang[Bahasa Indonesia]
46. Yan, B.; Han, G. Ekstraksi fitur yang efektif melalui autoencoder sparse bertumpuk untuk meningkatkan sistem deteksi intrusi.*Akses IEEE* **Tahun 2018**Bahasa Indonesia:*6*, 41238–41248. [Referensi silang[Bahasa Indonesia]
47. Naseer, S.; Saleem, Y.; Khalid, S.; Bashir, MK; Han, J.; Iqbal, MM; Han, K. Deteksi anomali jaringan yang disempurnakan berdasarkan jaringan saraf dalam.*Akses IEEE***Tahun 2018**Bahasa Indonesia:*6*, 48231–48246. [Referensi silang[Bahasa Indonesia]
48. Al-Qatf, M.; Lasheng, Y.; Al-Habib, M.; Al-Sabahi, K. Pendekatan pembelajaran mendalam yang menggabungkan sparse autoencoder dengan SVM untuk deteksi intrusi jaringan.*Akses IEEE***Tahun 2018**Bahasa Indonesia:*6*, 52843–52856. [Referensi silang[Bahasa Indonesia]
49. Marir, N.; Wang, H.; Feng, G.; Li, B.; Jia, M. Pendekatan deteksi perilaku abnormal terdistribusi berdasarkan jaringan keyakinan mendalam dan ensemble svm menggunakan spark. *Akses IEEE***Tahun 2018**Bahasa Indonesia:*6*, 59657–59671. [Referensi silang[Bahasa Indonesia]
50. Yao, H.; Fu, D.; Zhang, P.; Li, M.; Liu, Y. MSML: Kerangka kerja pembelajaran mesin semi-supervised multilevel yang baru untuk sistem deteksi intrusi.*Jurnal IEEE IoT.***Tahun 2018**Bahasa Indonesia:*6*, tahun 1949–1959. [Referensi silang[Bahasa Indonesia]
51. Gao, X.; Shan, C.; Hu, C.; Niu, Z.; Liu, Z. Model pembelajaran mesin ensemble adaptif untuk deteksi intrusi.*Akses IEEE***Tahun 2019**Bahasa Indonesia: *7*, 82512–82521. [Referensi silang[Bahasa Indonesia]
52. Karatas, G.; Demir, O.; Sahingoz, OK Meningkatkan kinerja IDS berbasis pembelajaran mesin pada kumpulan data yang tidak seimbang dan terkini.*Akses IEEE***Tahun 2020**Bahasa Indonesia:*8*, 32150–32162. [Referensi silang[Bahasa Indonesia]
53. Sabeel, U.; Heydari, SS; Mohanka, H.; Bendhaou, Y.; Elgazzar, K.; El-Khatib, K. Evaluasi pembelajaran mendalam dalam mendeteksi serangan jaringan yang tidak diketahui. Dalam Prosiding Konferensi Internasional 2019 tentang Aplikasi Cerdas, Komunikasi, dan Jaringan (SmartNets), Sharm El Sheikh, Mesir, 17–19 Desember 2019.
54. Virupakshar, KB; Asundi, M.; Channal, K.; Shettar, P.; Patil, S.; Narayan, DG Sistem deteksi serangan Distributed Denial of Service (DDoS) untuk Private Cloud berbasis OpenStack.*Procedia Ilmu Komputer.***Tahun 2020**Bahasa Indonesia:*167*, 2297–2307. [Referensi silang[Bahasa Indonesia]
55. Asad, M.; Asim, M.; Javed, T.; Beg, MO; Mujtaba, H.; Abbas, S. Deep-Detect: Deteksi serangan Distributed Denial of Service menggunakan pembelajaran mendalam.*Komputasi J.***Tahun 2020**Bahasa Indonesia:*63*, 983–994. [Referensi silang[Bahasa Indonesia]
56. Muraleedharan, N.; Janet, B. Pendekatan klasifikasi DoS lambat HTTP berbasis pembelajaran mendalam menggunakan data aliran.*ICT Ekspres***Tahun 2020**Bahasa Indonesia:*7*, 210–214.
57. Sbai, O.; El Boukhari, M. Sistem deteksi intrusi banjir data untuk manet menggunakan pendekatan pembelajaran mendalam. Dalam Prosiding SITA'20: Prosiding Konferensi Internasional ke-13 tentang Sistem Cerdas: Teori dan Aplikasi, Rabat, Maroko, 23–24 September 2020; hlm. 281–286.
58. Amaizu, GC; Nwakanma, CI; Bhardwaj, S.; Lee, JM; Kim, DS Kerangka kerja deteksi serangan DDoS yang komposit dan efisien untuk jaringan B5G.*Komputasi. Jaringan.***Tahun 2021** Bahasa Indonesia:*188*, 107871. [Referensi silang[Bahasa Indonesia]
59. Cil, AE; Yildiz, K.; Buldu, A. Deteksi serangan DDoS dengan model jaringan saraf dalam berbasis umpan maju.*Aplikasi Sistem Pakar* **Tahun 2021**Bahasa Indonesia:*169*, 114520. [Referensi silang[Bahasa Indonesia]
60. Hasan, MZ; Hasan, KMZ; Sattar, A. Deteksi banjir paket header burst dalam jaringan switching burst optik menggunakan model pembelajaran mendalam.*Procedia Ilmu Komputer.* **Tahun 2018**Bahasa Indonesia:*143*, 970–977. [Referensi silang[Bahasa Indonesia]

61. Amma, NGB; Subramanian, S. VCDeepFL: Pendekatan Vector Convolutional Deep Feature Learning untuk mengidentifikasi Serangan Denial of Service yang diketahui dan tidak diketahui. Dalam Prosiding Konferensi Internasional Tahunan IEEE Region 10, TENCON, Jeju, Republik Korea, 28–31 Oktober 2018; hlm. 640–645.
62. Chen, J.; Yang, Y.; Hu, K.; Zheng, H.; Wang, Z. DADMCNN: Deteksi serangan DDoS melalui CNN multisaluran. Dalam Prosiding ICMLC '19: Prosiding Konferensi Internasional ke-11 tentang Pembelajaran Mesin dan Komputasi 2019, Zhuhai, Tiongkok, 22–24 Februari 2019; hlm. 484–488.
63. Shaaban, AR; Abd-Elwanis, E.; Hussein, M. Deteksi dan klasifikasi serangan DDoS melalui Convolutional Neural Network (CNN). Dalam Prosiding Konferensi Internasional IEEE ke-9 tentang Komputasi Cerdas dan Sistem Informasi (ICICIS) 2019, Kairo, Mesir, 8–10 Desember 2019; hlm. 233–238.
64. Haider, S.; Akhunzada, A.; Mustafa, I.; Patel, TB; Fernandez, A.; Choo, KKR; Iqbal, J. Kerangka kerja ensembel CNN yang mendalam untuk deteksi serangan DDoS yang efisien dalam jaringan yang ditentukan perangkat lunak.*Akses IEEE***Tahun 2020**Bahasa Indonesia:*8*, 53972–53983. [Referensi silang[Bahasa Indonesia]
65. Wang, L.; Liu, Y. Metode deteksi serangan DDoS berdasarkan entropi informasi dan pembelajaran mendalam dalam SDN. Dalam Prosiding Konferensi Teknologi Informasi, Jaringan, Elektronik, dan Kontrol Otomasi IEEE ke-4 tahun 2020 (ITNEC), Chongqing, Tiongkok, 12–14 Juni 2020; hlm. 1084–1088.
66. Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. Deteksi intrusi jaringan berbasis CNN terhadap serangan Denial-of-Service.*Elektronik* **Tahun 2020**Bahasa Indonesia:*9*, 916. [Referensi silang [Bahasa Indonesia]
67. Doriguzzi-Corin, R.; Millar, S.; Scott-Hayward, S.; Martinez-Del-Rincon, J.; Siracusa, D. Lucid: Solusi pembelajaran mendalam yang praktis dan ringan untuk deteksi serangan DDoS.*Manajemen Layanan Jaringan Trans. IEEE***Tahun 2020**Bahasa Indonesia:*17*, 876–889. [Referensi silang[Bahasa Indonesia]
68. de Assis, MV; Carvalho, LF; Rodrigues, JJ; Lloret, J.; Proença, ML Sistem keamanan mendekati waktu nyata yang diterapkan pada lingkungan SDN di jaringan IoT menggunakan jaringan saraf konvolusional.*Komputer. Teknik Elektro.***Tahun 2020**Bahasa Indonesia:*86*, 106738. [Referensi silang[Bahasa Indonesia]
69. Husain, F.; Ghazanfar, S.; Al-Khawarizmi, A.; Husnain, M.; Fayyaz, UU; Syahzad, F.; Al-Khawarizmi, GAS IoTDoS dan deteksi serangan DDoS menggunakan ResNet. Dalam Prosiding Konferensi Multitopik Internasional (INMIC) ke-23 IEEE 2020, Bahawalpur, Pakistan, 5–7 November 2020.
70. Li, C.; Wu, Y.; Yuan, X.; Sun, Z.; Wang, W.; Li, X.; Gong, L. Deteksi dan pertahanan serangan DDoS berbasis pembelajaran mendalam di SDN berbasis OpenFlow.*Jurnal Int. Sistem Komunikasi***Tahun 2018**Bahasa Indonesia:*31*, e3497. [Referensi silang[Bahasa Indonesia]
71. Priyadarshini, R.; Barik, RK Kerangka kerja cerdas berbasis pembelajaran mendalam untuk mengurangi serangan DDoS di lingkungan fog.*J. King Saud Univ. Komputer Inf. Sains.* **Tahun 2019**Bahasa Indonesia:*34*, 825–831. [Referensi silang[Bahasa Indonesia]
72. Liang, X.; Znati, T. Kerangka kerja yang mendukung memori jangka pendek untuk deteksi DDoS. Dalam Prosiding Konferensi Komunikasi Global IEEE 2019 (GLOBECOM), Waikoloa, HI, AS, 9–13 Desember 2019.
73. Shurman, M.; Khrais, R.; Yateem, A. Deteksi serangan DoS dan DDoS menggunakan pembelajaran mendalam dan IDS.*Jurnal Arab Inf. Teknologi.***Tahun 2020**Bahasa Indonesia: *17*, 655–661. [Referensi silang[Bahasa Indonesia]
74. Ali, S.; Li, Y. Pembelajaran auto-encoder bertingkat untuk deteksi serangan DDoS di jaringan jaringan pintar.*Akses IEEE***Tahun 2019**Bahasa Indonesia:*7*, 108647–108659. [Referensi silang[Bahasa Indonesia]
75. Yang, K.; Zhang, J.; Xu, Y.; Chao, J. Deteksi serangan DDoS dengan AutoEncoder. Dalam Prosiding Simposium Manajemen dan Operasi Jaringan IEEE/IFIP 2020: Manajemen di Era Perangkat Lunak dan Kecerdasan Buatan (NOMS), Budapest, Hungaria, 20–24 April 2020.
76. Kasim, O. Deteksi anomali jaringan berbasis pembelajaran mendalam yang efisien dan tangguh terhadap serangan penolakan layanan terdistribusi. *Komputasi. Jaringan.***Tahun 2020**Bahasa Indonesia: *180*, 107390. [Referensi silang[Bahasa Indonesia]
77. Bhardwaj, A.; Mangat, V.; Vig, R. Jaringan saraf dalam yang disetel hyperband dengan AutoEncoder bertumpuk yang diatur dengan baik untuk mendeteksi serangan DDoS di Cloud. *Akses IEEE***Tahun 2020**Bahasa Indonesia:*8*, 181916–181929. [Referensi silang[Bahasa Indonesia]
78. He, J.; Tan, Y.; Guo, W.; Xian, M. Metode deteksi serangan DDoS sampel kecil berdasarkan pembelajaran transfer mendalam. Dalam Prosiding Konferensi Internasional tentang Komunikasi Komputer dan Keamanan Jaringan (CCNS) 2020, Xi'an, Tiongkok, 21–23 Agustus 2020; hlm. 47–50.
79. Chen, M.; Liu, W.; Zhang, N.; Li, J.; Ren, Y.; Yi, M.; Liu, A. GPDS: Permainan pembelajaran penguatan mendalam multi-agen untuk komputasi aman anti-jamming di jaringan MEC.*Aplikasi Sistem Pakar***Tahun 2022**Bahasa Indonesia:*210*, 118394. [Referensi silang[Bahasa Indonesia]
80. Deteksi Intrusi Jaringan Komputer. Tersedia online:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html(diakses pada 25 Oktober 2022).
81. Premkumar, M.; Sundararajan, TV DLDM: Mekanisme pertahanan berbasis pembelajaran mendalam untuk serangan penolakan layanan di jaringan sensor nirkabel.*Mikroproses. Mikrosistem.***Tahun 2020**Bahasa Indonesia:*79*, 103278. [Referensi silang[Bahasa Indonesia]
82. Institut Keamanan Siber Kanada. Tersedia daring:https://www.unb.ca/cic/datasets/nsl.html(diakses pada 1 Oktober 2022).
83. Institut Keamanan Siber Kanada. Tersedia daring:https://www.unb.ca/cic/datasets/ids-2017.html(diakses pada 1 Oktober 2022).
84. Institut Keamanan Siber Kanada. Tersedia daring:https://www.unb.ca/cic/datasets/ids-2018.html(diakses pada 1 Oktober 2022).
85. Institut Keamanan Siber Kanada. Tersedia daring:https://www.unb.ca/cic/datasets/ids.html(diakses pada 1 Oktober 2022).
86. Sharafaldin, I.; Lashkari, AH; Hakak, S.; Ghorbani, AA Mengembangkan kumpulan data dan taksonomi serangan penolakan layanan terdistribusi (DDoS) yang realistis. Dalam Prosiding Konferensi Carnahan Internasional tentang Teknologi Keamanan (ICCST), Chennai, India, 1–3 Oktober 2019.

87. Institut Keamanan Siber Kanada. Tersedia daring:https://www.unb.ca/cic/datasets/ddos-2019.html(diakses pada 1 Oktober 2022).

88. Holzinger, A. Data besar disebut sebagai pembelajaran mesin.*Ensiklopedia Biomed. Eng.***Tahun 2019**Bahasa Indonesia:*3*, 258–264.

89. Metrik untuk Mengevaluasi Algoritma Pembelajaran Mesin Anda. Tersedia online:https://towardsdatascience.com/metrics-to-evaluateyour-machine-learning-algorithm-f10ba6e38234(diakses pada 1 Oktober 2022).

90. Amanullah, MA; Habeeb, RAA; Nasaruddin, FH; Gani, A.; Ahmed, E.; Nainar, ASM; Akim, NM; Imran, M. Teknologi pembelajaran mendalam dan data besar untuk keamanan IoT.*Komputer. Komunikasi.***Tahun 2020**Bahasa Indonesia:*151*, 495–517. [Referensi silang[Bahasa Indonesia]

91. Memahami Confusion Matrix. Tersedia online:https://towardsdatascience.com/memahami-matriks-kebingungan-a9ad4 2dcfd62 (diakses pada 1 Oktober 2022).

92. Penguasaan Pembelajaran Mesin. Tersedia daring:https://machinelearningmastery.com/precision-recall-and-f-measure-for-imbalancedclassification/(diakses pada 1 Oktober 2022).

93. Memahami Kurva AUC—ROC. Tersedia online:https://towardsdatascience.com/understanding-auc-roc-curve-68b230 3cc9c5 (diakses pada 1 Oktober 2022).