Literature Review : Isu dan Tantangan Teknik Deteksi Serangan Botnet pada Trafik Jaringan

I Putu Genda Ariana Pratama [1a], Dandy Pramana Hostiadi [2b], Roy Rudolf Huizen [3c]
[1)]Magister Sistem Informasi Institut Teknologi dan Bisnis STIKOM Bali Denpasar, Indonesia
e-mail: [a)] 242011018@stikom-bali.ac.id, [b)] dandy@stikom-bali.ac.id, [c)] roy@stikom-bali.ac.id

Abstrak

Deteksi serangan botnet pada trafik jaringan merupakan tantangan utama dalam keamanan jaringan seiring meningkatnya volume data, kompleksitas pola komunikasi, dan dinamika serangan yang semakin beragam. Berbagai pendekatan berbasis pembelajaran mesin telah dikembangkan, namun masih menghadapi sejumlah permasalahan mendasar, antara lain skala data yang besar, ketidakseimbangan kelas, kebutuhan waktu komputasi yang tinggi, serta performa evaluasi yang belum optimal, khususnya pada tingkat false positive dan recall. Penelitian ini menyajikan Systematic Literature Review (SLR) untuk mengidentifikasi dan menganalisis isu serta tantangan pada teknik deteksi botnet berbasis trafik jaringan. Metodologi SLR dilakukan menggunakan kerangka PICOC dalam perumusan ruang lingkup penelitian dan alur PRISMA dalam proses identifikasi, penyaringan, dan seleksi literatur secara sistematis. Tinjauan literatur difokuskan pada analisis pendekatan deteksi dan strategi optimasi pembelajaran mesin, meliputi ekstraksi fitur, seleksi fitur, penanganan ketidakseimbangan data, serta hyperparameter tuning. Hasil sintesis menunjukkan bahwa penerapan seleksi fitur dan optimasi model berperan penting dalam meningkatkan recall, menurunkan tingkat false positive, dan mengurangi beban komputasi. Temuan ini diharapkan dapat menjadi acuan dalam pengembangan metode deteksi botnet yang lebih efektif, efisien, dan relevan untuk implementasi pada lingkungan jaringan nyata.

Kata kunci: *Botnet, Deteksi Serangan, Trafik Jaringan, Malware.*

1. Pendahuluan

Meningkatnya infrastruktur jaringan telah menyebabkan pertumbuhan trafik jaringan yang besar dan kompleks, sehingga memperluas potensi ancaman keamanan. Salah satu ancaman yang sering terjadi adalah serangan botnet, yaitu kumpulan perangkat yang terinfeksi *malware* dan dikendalikan secara terpusat untuk melakukan aktivitas berbahaya seperti gangguan layanan jaringan dan penyalahgunaan [1]. Sifat *botnet* yang adaptif dan tersembunyi menjadi sulit dideteksi pada jaringan. Deteksi *botnet* banyak dikembangkan karena mampu mengidentifikasi aktivitas berbahaya tanpa bergantung pada *payload* paket data. Namun, pendekatan ini menghadapi tantangan akibat pola *botnet* yang semakin menyerupai trafik normal serta volume data jaringan yang tinggi dan bersifat dinamis [2].

Pemanfaatan teknik pembelajaran mesin menunjukkan peningkatan kinerja mendeteksi serangan *botnet*. Meskipun demikian, permasalahan ketidakseimbangan data antara normal dan *botnet* masih menjadi kendala, karena dapat menurunkan nilai *recall* dan meningkatkan *false positive*. Selain itu, karakteristik dan kualitas data trafik memiliki pengaruh signifikan terhadap hasil evaluasi dan performa deteksi *botnet* [3]. Berbagai strategi optimasi, seperti ekstraksi dan seleksi fitur serta penyesuaian parameter model, telah diusulkan untuk mengatasi permasalahan tersebut. Namun, pendekatan yang digunakan masih beragam dan menunjukkan hasil yang bervariasi. Oleh karena itu, penelitian ini disusun dalam bentuk *Systematic Literature Review* (SLR) dengan kerangka PICOC dan alur PRISMA untuk mengidentifikasi isu dan tantangan utama dalam deteksi serangan *botnet* pada trafik jaringan serta merangkum arah pengembangan metode deteksi.

2. Metode Penelitian

2.1 Systematic Literature Review

Penelitian ini menggunakan kerangka PICOC agar literatur yang dikaji relevan dengan konteks penelitian. Berdasarkan kerangka tersebut, proses pencarian dan seleksi artikel diarahkan pada penelitian yang membahas teknik deteksi *botnet* berbasis analisis trafik jaringan dan pembelajaran mesin.

Tabel 1. Tabel PICOC

Elemen	Deskripsi
Population (P)	Trafik jaringan yang mengandung aktivitas normal dan aktivitas serangan *botnet*.
Intervention (I)	Teknik deteksi serangan botnet berbasis analisis trafik jaringan, khususnya menggunakan pendekatan pembelajaran mesin.
Comparison (C)	Perbandingan metode deteksi *botnet*, teknik pra-pemrosesan data, serta strategi optimasi model yang digunakan dalam penelitian.
Outcome (O)	Kinerja sistem deteksi *botnet* yang diukur menggunakan metrik evaluasi seperti *precision*, *recall*, *false positive rate*, dan efisiensi komputasi.
Context (C)	Studi eksperimental pada lingkungan jaringan dengan karakteristik trafik yang beragam dan berbagai skenario aktivitas serangan botnet.

2.2 Research Questions

Berdasarkan tujuan *Systematic Literature Review* dan kerangka PICOC, penelitian ini merumuskan pertanyaan penelitian sebagai berikut:

RQ1: Apa isu dan tantangan utama dalam deteksi serangan *botnet* pada trafik jaringan?

RQ2: Pendekatan pembelajaran mesin apa yang dominan digunakan untuk deteksi *botnet* berbasis trafik jaringan dan bagaimana kinerjanya berdasarkan metrik evaluasi utama?

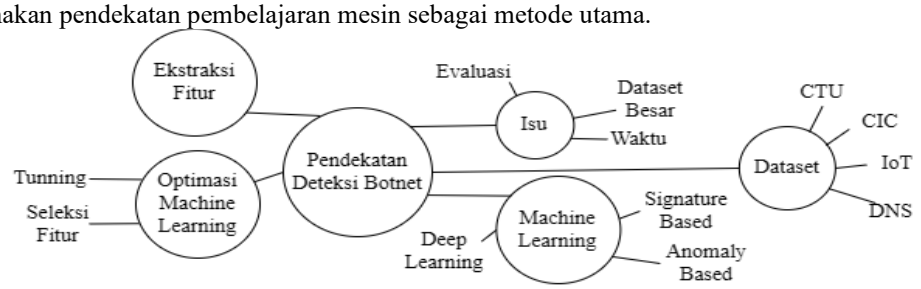
RQ3: Strategi optimasi apa yang paling efektif untuk meningkatkan kinerja deteksi *botnet*, khususnya dalam menekan *false positive* dan meningkatkan *recall*?

2.3 Pengumpulan dan seleksi data

Pengumpulan data dilakukan melalui pendekatan *Systematic Literature Review* dengan mengacu pada kerangka PICOC dan alur PRISMA. Pencarian artikel dilakukan pada basis data jurnal nasional terindeks SINTA pada rentang tahun 2022 sampai 2025. Pada tahap identifikasi awal diperoleh 164 artikel. Setelah penghapusan duplikasi dan penyaringan akses teks penuh, jumlah artikel berkurang menjadi 138 artikel. Tahap penyaringan judul dan abstrak menghasilkan 72 artikel yang relevan dengan topik penelitian. Selanjutnya, pada tahap seleksi kelayakan melalui telaah metodologi dan hasil, diperoleh 41 artikel. Penerapan kriteria inklusi dan eksklusi menghasilkan 23 artikel terpilih yang memenuhi kriteria jurnal nasional terindeks SINTA, membahas deteksi botnet berbasis trafik jaringan, menggunakan pendekatan eksperimental, serta menyajikan informasi dataset, fitur, metode, dan metrik evaluasi. Seluruh artikel terpilih digunakan sebagai sumber data utama dalam analisis SLR ini.

2.4 Analisis Data

Analisis data pada penelitian ini dilakukan terhadap artikel-artikel terpilih yang diperoleh melalui proses *Systematic Literature Review* dengan mengacu pada kerangka PICOC dan alur PRISMA. Artikel yang dianalisis merupakan penelitian yang membahas deteksi serangan botnet pada trafik jaringan menggunakan pendekatan pembelajaran mesin sebagai metode utama.



Gambar 1. Gambar Analisa Isu

Fokus analisis diarahkan pada beberapa aspek penting, meliputi karakteristik dataset yang digunakan, teknik ekstraksi fitur yang diterapkan, metode deteksi yang diusulkan, strategi optimasi model, serta metrik evaluasi kinerja yang digunakan untuk menilai efektivitas sistem deteksi botnet.

3. Hasil dan Pembahasan

3.1 Karakter Dataset

Karakteristik dataset pada penelitian deteksi *botnet* berbasis trafik jaringan menunjukkan perbedaan yang jelas dalam skala data, jumlah fitur, dan kompleksitas serangan. Dataset CTU-13 banyak digunakan

sebagai *benchmark* karena struktur data yang sederhana dan fitur *flow* yang terbatas, sehingga memudahkan pelatihan model. Namun, variasi serangan yang sempit dan sifat data yang homogen menyebabkan model kurang adaptif terhadap trafik nyata dan berpotensi menghasilkan false positive yang tinggi [1], [2], [3]. Dataset CIC, termasuk CICIDS2017, CICIDS2018, dan CIC-IoT, menyediakan data yang lebih besar dan kompleks dengan fitur *flow* yang kaya serta variasi serangan yang beragam, ini lebih representatif untuk evaluasi sistem deteksi *botnet* modern, tetapi ada tantangan komputasi dan ketidakseimbangan kelas.

Tabel 2. Tabel Penggunaan Dataset

Nama Dataset	Jumlah Row Dataset	Jumlah Fitur	Ukuran Dataset	Jenis Serangan	Sitasi Jurnal
CTU-13	±1,0–1,2 juta *flow*	13–20 fitur *flow*	±5–8 GB	IRC *botnet*, HTTP *botnet*, *spam*, DDoS	[1], [2], [3], [4], [5]
CICIDS2017	±2,8 juta record	±78 fitur *flow*	±11 GB	*Botnet*, DDoS, *PortScan*, DoS	[6]
CICIDS2018	>16 juta record	±80 fitur	>400 GB (raw)	*Botnet*, *brute force*, DDoS	[7]
CIC-IoT	±5–7 juta record	±60 fitur IoT	±25 GB	IoT *botnet*, DDoS, *scanning*	[8]
IoT-23	±20 juta *flow*	20–23 fitur	±30 GB	C2, DDoS, *malware* IoT	[9]
Bot-IoT	>72 juta record	±35 fitur	±69 GB	DDoS, DoS, *reconnaissance*	[10], [11]
UNSW-NB15	±2,5 juta record	49 fitur	±2 GB	*Exploit*, DoS, *malware*, *botnet*	[12]
DNS Traffic Dataset	±0,5–1 juta query	10–25 fitur DNS	<2 GB	DNS-*based botnet*, C2	[13], [14]
Passive DNS	>1 juta log (variatif)	8–15 fitur	Variatif	*Botnet* C2, *domain abuse*	[15]
Real Network / Campus	Ratusan ribu–jutaan *flow*	10–30 fitur	Variatif	*Botnet* aktual, *malware traffic*	[16]
Enterprise Network	Ratusan ribu–jutaan *flow*	10–30 fitur	Variatif	*Botnet*, *malware enterprise*	[17]
MTA-KDD'19 (Wireless)	±400 ribu record	±41 fitur	<1 GB	*Botnet*, *flooding*, DoS	[18]
Traffic Image Dataset	Variatif	Fitur visual	Variatif	Pola trafik *botnet*	[19]
IoT Network (Indonesia)	±300–600 ribu *flow*	15–30 fitur *flow*	±1–3 GB	IoT *botnet*, *scanning*, DDoS	[20], [21], [22]

Dataset seperti IoT-23, Bot-IoT, UNSW-NB15, serta dataset IoT lokal menampilkan trafik yang sangat heterogen dengan dominasi trafik normal. Kondisi ini meningkatkan risiko bias model dan penurunan *recall* apabila tidak disertai optimasi yang tepat, sehingga seleksi fitur dan penyeimbangan data menjadi pendekatan yang umum digunakan [9], [10], [11], [12], [20], [21], [22]. Dataset DNS/Passive DNS lebih ringan dan fokus pada pola kueri domain untuk mendeteksi komunikasi *command and control*, namun keterbatasan konteks trafik membuat rentan terhadap *false positive* jika digunakan secara tunggal [13], [14], [15]. Penggunaan lebih dari satu dataset menjadi strategi penting untuk meningkatkan validitas dan keandalan sistem deteksi *botnet* berbasis trafik jaringan.

3.2 Teknik Ekstraksi Fitur

Ekstraksi fitur merupakan komponen kunci dalam deteksi *botnet* karena menentukan kualitas representasi pola komunikasi serangan. Fitur statistik seperti jumlah paket, jumlah *byte*, dan durasi koneksi menjadi pendekatan umum karena ringan dan mudah diterapkan diberbagai dataset. Namun, penggunaan fitur statistik dasar saja sering menyebabkan model rentan terhadap *false positive* ketika trafik memiliki karakteristik yang mirip dengan normal [1], [2], [3]. Pada lingkungan *Internet of Things*, ekstraksi fitur diarahkan pada fitur perilaku dan domain-spesifik, seperti pola command and control, agar lebih sensitif terhadap botnet modern dengan tetap mempertimbangkan keterbatasan sumber daya komputasi [9], [10],

[11], [12], [20], [21], [22]. Selain itu, pendekatan fitur tingkat lanjut berbasis *byte-stream* dan visualisasi trafik mulai dieksplorasi untuk menangkap pola kompleks, meskipun penerapannya masih terbatas karena kebutuhan komputasi yang tinggi [19]. Kombinasi fitur statistik, temporal, dan perilaku yang disesuaikan dengan karakteristik dataset merupakan strategi yang cukup efektif untuk meningkatkan keandalan deteksi *botnet* berbasis trafik jaringan.

Tabel 3. Tabel Pendekatan Deteksi

Pendekatan Deteksi	Sitasi Jurnal
Machine Learning berbasis fitur statistik *flow*	[1], [2], [4], [5], [8], [10], [16], [17], [20], [22]
Machine Learning dengan penanganan ketidakseimbangan data (SMOTE / oversampling)	[2], [4], [18], [21]
Machine Learning dengan seleksi fitur	[5], [8], [9], [12], [14], [17], [20], [22]
Ensemble Learning (*Voting* / kombinasi model)	[7], [11], [23]
Deep Learning berbasis CNN / LSTM	[6], [12], [19]
Hybrid Deep Learning (CNN–BiLSTM)	[6], [12]
DNS-*based Botnet Detection*	[13], [14]
Passive DNS Analysis	[15]
Vision-based Traffic Analysis	[19]
Explainable AI (XAI) untuk IDS *Botnet*	[23]

3.3 Metode Deteksi

Deteksi *botnet* berbasis trafik jaringan didominasi oleh pendekatan *machine learning*, khususnya *Random Forest* dan *Support Vector Machine*, karena mampu mencapai akurasi tinggi dengan komputasi relatif efisien ketika menggunakan fitur *flow* statistik. Namun, metode ini sangat bergantung pada kualitas fitur dan distribusi data, sehingga rentan terhadap ketidakseimbangan kelas dan peningkatan *false positive* pada trafik yang menyerupai pola normal [1], [2], [4]. Untuk meningkatkan stabilitas dan *recall*, sejumlah penelitian menerapkan *ensemble learning* yang mengombinasikan beberapa model klasifikasi. Pendekatan ini terbukti lebih kuat terhadap variasi serangan, tetapi meningkatkan kompleksitas komputasi dan waktu [7], [11]. Pada dataset yang lebih kompleks, khususnya IoT dan UNSW-NB15, *deep learning* seperti CNN dan LSTM mulai digunakan untuk menangkap pola temporal dan nonlinier, meskipun memerlukan sumber daya komputasi yang lebih besar dan dataset berukuran memadai [6], [12]. Selain itu, pendekatan semi-*supervised* dan berbasis domain diterapkan untuk mengatasi keterbatasan label dan mendeteksi serangan baru, terutama pada trafik DNS. Meskipun menjanjikan, metode ini masih terbatas penerapannya dan memerlukan validasi lanjutan [13], [14], [15].

Tabel 4. Tabel Penggunaan Seleksi Fitur

Seleksi Fitur / Optimasi yang Digunakan	Sitasi Jurnal
Tanpa seleksi fitur (seluruh fitur *flow*)	[1], [3], [7], [10], [13], [16]
Filter-based feature selection	[5], [8], [9], [14], [20]
Feature importance berbasis *Random Forest*	[5], [6], [21], [23]
Embedded feature selection	[4], [6], [12], [21]
Reduksi dimensi (PCA / transformasi fitur)	[19]
Seleksi fitur domain-spesifik (IoT / DNS)	[13], [14], [15], [20], [22]
Penanganan data tidak seimbang (SMOTE / *oversampling*)	[2], [4], [18], [21]
Optimasi parameter model (*tuning*)	[5], [12]

3.4 Seleksi Fitur dan Optimasi Model

Berperan penting dalam meningkatkan efektivitas deteksi botnet berbasis trafik jaringan, khususnya pada dataset berukuran besar dan tidak seimbang. Sejumlah penelitian awal masih menggunakan seluruh fitur *flow* tanpa seleksi, meskipun menghasilkan akurasi tinggi, berdampak pada peningkatan kompleksitas komputasi dan risiko *false positive* [1], [3]. Kondisi ini mendorong penerapan seleksi fitur untuk memperoleh representasi data yang lebih ringkas dan relevan.

Teknik seleksi fitur yang paling banyak diterapkan adalah pendekatan *filter-based* dan *feature importance* berbasis *Random Forest*, karena mampu mengurangi dimensi data secara signifikan tanpa

menurunkan kinerja deteksi. Pendekatan ini terbukti meningkatkan efisiensi dan stabilitas model, terutama pada dataset CIC dan IoT [5], [8], [9]. Selain itu, beberapa penelitian menerapkan *embedded feature selection* pada model *ensemble* dan *deep learning* untuk menyesuaikan pemilihan fitur secara adaptif selama proses pelatihan [4], [6], [12]. Dalam aspek optimasi model, penanganan ketidakseimbangan data melalui SMOTE menjadi strategi dominan untuk meningkatkan *recall*. Meskipun efektif mengurangi bias kelas minoritas, teknik ini perlu dikombinasikan dengan seleksi fitur agar tidak meningkatkan *false positive* secara signifikan [2], [4], [18], [21].

3.5 Metrik Evaluasi

Evaluasi deteksi botnet berbasis trafik umumnya masih mengandalkan akurasi sebagai metrik utama karena kemudahan perhitungan dan interpretasinya. Namun, pada dataset distribusi kelas yang tidak seimbang, akurasi sering kali tidak mencerminkan kemampuan sistem dalam mendeteksi *botnet* secara efektif [1], [3]. Oleh karena itu, *recall* dan *false positive rate* (FPR) banyak digunakan untuk memberikan gambaran lebih relevan terhadap konteks keamanan jaringan. *Recall* menilai kemampuan sistem dalam mengidentifikasi serangan *botnet*, sedangkan FPR mengukur tingkat kesalahan terhadap trafik normal yang dapat meningkatkan beban operasional. Sejumlah penelitian menunjukkan adanya *trade-off* antara peningkatan *recall* dan kenaikan FPR, sehingga diperlukan evaluasi yang seimbang [2], [4], [18].

Pada beberapa studi, metrik tambahan seperti waktu komputasi dan latensi deteksi turut digunakan untuk menilai kelayakan implementasi sistem secara *real-time* [4], [5], [10]. Pendekatan ini memungkinkan penilaian kinerja deteksi *botnet* yang lebih komprehensif dan relevan untuk kondisi operasional nyata.

3.6 Tantangan

Deteksi botnet berbasis trafik jaringan menghadapi tantangan utama berupa ketidakseimbangan data, di mana trafik normal jauh lebih dominan dibandingkan trafik serangan. Kondisi ini menyebabkan model klasifikasi cenderung bias terhadap kelas mayoritas dan menurunkan kemampuan deteksi *botnet*, khususnya pada metrik *recall* [2], [4]. Penerapan teknik *oversampling* seperti SMOTE dapat membantu mengurangi bias, tetapi berpotensi meningkatkan *false positive* apabila tidak dikombinasikan dengan seleksi fitur yang tepat [18], [21]. Tantangan lain berkaitan dengan skala dan kompleksitas dataset. Dataset modern yang berukuran besar dan memiliki banyak fitur meningkatkan beban komputasi dan waktu pemrosesan, sehingga menyulitkan penerapan sistem deteksi secara *real-time* [5], [8], [9]. Tingginya tingkat *false positive* masih menjadi hambatan signifikan dalam implementasi sistem deteksi *botnet*. Pola komunikasi *botnet* yang semakin menyerupai trafik normal membuat fitur statistik dasar kurang efektif dalam membedakan kedua kelas, sehingga menurunkan keandalan sistem [1], [3]. Tantangan ini menunjukkan perlunya representasi fitur yang lebih informatif.

4. Kesimpulan

Berdasarkan *Systematic Literature Review*, ditemukan bahwa tantangan utama (RQ1) meliputi ketidakseimbangan data, skala dataset yang besar, tingginya *false positive rate*, serta keterbatasan generalisasi model antar dataset. Tantangan lainnya adalah keterbatasan generalisasi model, karena banyak penelitian hanya mengevaluasi kinerja pada satu dataset. Perbedaan karakteristik data dan skenario serangan menyebabkan kinerja model sulit direplikasi pada lingkungan jaringan yang berbeda, sehingga menegaskan kebutuhan validasi lintas dataset dan pendekatan yang lebih adaptif.

Menjawab RQ2, pendekatan *machine learning* khususnya *Random Forest, Support Vector Machine*, dan *k-Nearest Neighbor* merupakan metode yang paling dominan digunakan karena kestabilan kinerja dan efisiensi komputasinya. Pendekatan ini umumnya mencapai akurasi dan nilai recall yang tinggi ketika dikombinasikan dengan penanganan data tidak seimbang, meskipun masih ada peningkatan false positive rate pada dataset kompleks. Pada dataset heterogen, *deep learning* berbasis CNN dan LSTM digunakan untuk menangkap pola temporal dan nonlinier dengan peningkatan *recall*, tetapi perlu sumber daya komputasi yang lebih besar.

Menjawab RQ3, strategi optimasi yang efektif adalah penerapan penanganan ketidakseimbangan data yang dikombinasikan dengan seleksi fitur dan pemilihan model yang stabil. Penggunaan teknik *oversampling* seperti SMOTE dapat meningkatkan sensitivitas terhadap kelas *botnet* dan memperbaiki nilai *recall*, namun perlu dikendalikan melalui seleksi fitur berbasis *filter-based* dan *feature importance Random Forest* untuk menekan kesalahan klasifikasi dan menjaga efisiensi. Selain itu, *ensemble learning* efektif meningkatkan konsistensi kinerja dengan mengurangi bias, sementara *deep learning* digunakan pada dataset kompleks konsekuensi biaya yang lebih tinggi.

Daftar Pustaka

[1] I. Riadi, A. Fadlil, and Sunardi, "Analisis dan deteksi aktivitas botnet berbasis trafik jaringan," *Jurnal Teknologi dan Sistem Komputer*, vol. 10, pp. 85–94, 2022.
[2] A. Fadlil, I. Riadi, and Y. Prayudi, "Deteksi botnet berbasis machine learning menggunakan analisis trafik jaringan," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 3, pp. 421–429, 2022.
[3] R. Umar, I. Riadi, and A. Luthfi, "Analisis false positive pada sistem deteksi intrusi botnet," *Analisis false positive pada sistem deteksi intrusi botnet*, vol. 17, pp. 11–20, 2023.
[4] A. Nugroho, A. Fadlil, and I. Riadi, "Penanganan ketidakseimbangan data pada deteksi botnet berbasis pembelajaran mesin," *Penanganan ketidakseimbangan data pada deteksi botnet berbasis pembelajaran mesin*, vol. 10, pp. 789–798, 2023.
[5] H. Prasetyo and A. Nugroho, "Seleksi fitur untuk meningkatkan efisiensi deteksi botnet berbasis trafik jaringan," *Jurnal Ilmu Komputer dan Informasi (JIKI)*, vol. 17, pp. 101–110, 2024.
[6] M. R. Hakim, A. Fadlil, and I. Riadi, "Model deep learning untuk deteksi serangan jaringan berbasis trafik," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 11, p. 55, 2024.
[7] R. Hidayat, A. Nugroho, and I. Riadi, "Penerapan ensemble learning pada sistem deteksi intrusi berbasis trafik jaringan," *Jurnal Rekayasa Teknologi Informasi*, vol. 7, pp. 133–142, 2023.
[8] A. Wijaya and D. Pertiwi, "Deteksi botnet pada jaringan IoT menggunakan analisis trafik dan machine learning," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, p. 312, 2023.
[9] M. A. Putra, I. Riadi, and A. Fadlil, "Deteksi botnet pada lingkungan Internet of Things menggunakan artificial neural network," *Jurnal Teknologi dan Sistem Komputer*, vol. 10, p. 201, 2022.
[10] R. Setiawan, A. Nugroho, and I. Riadi, "Klasifikasi trafik Bot-IoT menggunakan algoritma pembelajaran mesin," *Jurnal Informatika Mulawarman*, vol. 17, p. 155, 2022.
[11] M. Kurniawan and H. Prasetyo, "Pendekatan ensemble learning untuk deteksi botnet pada jaringan IoT," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, p. 612, 2023.
[12] R. W. Saputra and D. Satria, "Deteksi botnet menggunakan model hybrid deep learning pada dataset UNSW-NB15," *Jurnal Ilmu Komputer dan Informasi (JIKI)*, vol. 18, pp. 1–10, 205AD.
[13] D. Pertiwi and A. Wijaya, "Deteksi botnet berbasis DNS menggunakan machine learning," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 8, p. 245, 2022.
[14] R. K. Prabowo and A. Nugroho, "Deteksi command and control botnet berbasis trafik DNS," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 8, p. 233, 2024.
[15] V. U. Putri and E. B. Cahyono, "Analisis passive DNS untuk deteksi botnet," *Jurnal Teknologi Informasi dan Terapan*, vol. 10, p. 33, 2023.
[16] M. Raharjo, I. Riadi, and A. Fadlil, "Deteksi botnet pada jaringan kampus menggunakan analisis NetFlow," *Jurnal Teknologi dan Sistem Komputer*, vol. 10, p. 15, 2022.
[17] A. Pratama and R. Firmansyah, "Sistem deteksi botnet pada jaringan enterprise berbasis NetFlow," *Jurnal Informatika*, vol. 18, p. 95, 2023.
[18] S. Wahyudi and A. Nugroho, "Deteksi botnet real-time pada jaringan nirkabel menggunakan machine learning," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 11, p. 255, 2024.
[19] A. Setyawan and B. Santoso, "Visualisasi trafik jaringan untuk deteksi botnet," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 9, p. 12, 2025.
[20] D. Pramana, A. Fadlil, and I. Riadi, "Deteksi serangan botnet pada trafik jaringan IoT menggunakan pendekatan machine learning," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, p. 401, 2023.
[21] D. Pramana, I. Riadi, and A. Fadlil, "Analisis trafik jaringan untuk deteksi botnet pada lingkungan IoT," *Jurnal Teknologi dan Sistem Komputer*, vol. 11, p. 95, 2024.
[22] D. Pramana, A. Fadlil, and I. Riadi, "Deteksi trafik botnet anomali pada smart network berbasis machine learning," *Jurnal Ilmu Komputer dan Informasi (JIKI)*, vol. 18, p. 21, 2025.
[23] M. A. Hakim and I. Riadi, "Explainable artificial intelligence untuk sistem deteksi intrusi botnet," *Jurnal Teknologi dan Sistem Komputer*, vol. 11, 2025.