Terbit *online* pada laman: http://jurnal.utu.ac.id/JTI

Jurnal Teknologi Informasi

ISSN (Online): 2829-8934

Evaluasi Validitas Shannon Entropy untuk Deteksi Flooding Pada Jaringan Perguruan Tinggi

Murhaban Murhaban[1*], Sanusi[2], Nirma Afriya[3], Suryadi[4], Nica Astrianda[5] Mukhlizar Mukhlizar[6]
[1,2,3,45] Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Teuku Umar, Indonesia
[6] Manajemen Pendidikan, Sekolah Tinggi Agama Islam Negeri Teungku Dirundeng Meulaboh, Aceh Barat, Indonesia
* [1]murhaban@utu.ac.id

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima: 11 Oktober 2026
Revisi: 19 Oktober 2026
Diterbitkan: 31 Oktober 2026

Kata Kunci:
Entropi Shannon
Validitas Fitur
Deteksi Flooding
Trafik Jaringan
Audit Pengukuran

ABSTRAK

Penelitian ini mengaudit validitas penggunaan Shannon entropy dalam dokumentasi eksperimen flooding pada jaringan universitas. Audit mencakup rekonstruksi skenario, verifikasi protokol, pemeriksaan semantik fitur, reproduksi numerik, serta uji normalisasi dan batas-batas matematis. Bukti mendukung terjadinya TCP SYN dan UDP flooding, tetapi belum memverifikasi label HTTP Flood maupun konfigurasi DDoS. Nilai 1 bit untuk port 80 terbukti berasal dari dua digit pada string "80", sedangkan 1,921928 dan 2,321928 bit dapat direproduksi dari digit jumlah paket, bukan dari distribusi panjang paket. Nilai entropi IP sebesar 5,710777 bit juga tidak memenuhi normalisasi probabilitas dan melebihi batas maksimum 4 bit untuk 16 kategori. Temuan ini menunjukkan bahwa kesesuaian unit fitur dan konsistensi matematis harus diverifikasi sebelum entropi diinterpretasikan sebagai indikator serangan. Kontribusi penelitian ini adalah prosedur audit tiga lapis yang memisahkan validitas protokol, validitas fitur semantik, dan validitas matematis sebelum mengevaluasi kinerja detektor.

Copyright © 2026 Jurnal Teknologi Informasi UTU
All rights reserved

1. Pendahuluan

Deteksi flooding berbasis entropi memanfaatkan perubahan distribusi fitur trafik untuk mengidentifikasi konsentrasi atau pola penyebaran komunikasi. Pendekatan ini menarik karena ukuran entropi ringkas dan dapat dihitung dari berbagai fitur, seperti alamat IP, port, dan ukuran paket [1]. Namun, validitas hasil tidak hanya ditentukan oleh rumus Shannon, melainkan juga oleh kesesuaian antara unit observasi yang dimaksud dan simbol yang digunakan. Jika alamat, port, atau ukuran paket direduksi menjadi karakter penyusun string, nilai entropi tetap dapat dihitung secara matematis, tetapi tidak lagi merepresentasikan distribusi lalu lintas jaringan. Karena itu, validitas semantik fitur perlu diperiksa sebelum nilai entropi digunakan sebagai indikator serangan[2].

Penelitian terdahulu terutama berfokus pada peningkatan kemampuan deteksi melalui pemilihan fitur, ambang dinamis, entropi bersyarat, serta evaluasi klasifikasi. [3] Menunjukkan bahwa kombinasi karakteristik aliran dan ukuran paket dapat membedakan beberapa tipe serangan DDoS. [4] Menunjukkan bahwa respons entropi dipengaruhi oleh laju serangan serta konfigurasi sumber dan target. Tsobdjou [5]mengembangkan deteksi daring dengan pembaruan ambang, sedangkan [6] memperlihatkan penggunaan entropi bersyarat untuk meningkatkan pemisahan lalu lintas. Dalam konteks Indonesia, Solichin [7] mengevaluasi entropi Shannon pada dataset InSDN menggunakan matriks kebingungan. Rangkaian studi tersebut menunjukkan kemajuan pada tahap pengambilan keputusan, tetapi mengasumsikan bahwa fitur yang dimasukkan dalam perhitungan telah didefinisikan

dan diekstraksi dengan benar. Asumsi inilah yang jarang diaudit secara eksplisit dalam eksperimen berskala kecil.

Mengaudit kembali dokumentasi eksperimen jaringan kampus dengan memeriksa apakah bukti protokol mendukung label skenario flooding yang dilaporkan, serta menguji apakah nilai entropi konsisten dengan semantik fitur, normalisasi probabilitas, dan batas matematis entropi Shannon. Kontribusi penelitian terdiri atas tiga lapis validasi, yaitu validasi bukti protokol, validasi semantik unit fitur, dan validasi konsistensi matematis. Berbeda dari studi yang menilai akurasi detektor, penelitian ini menempatkan validitas pengukuran sebagai prasyarat sebelum ambang atau performa klasifikasi diinterpretasikan. Analisis dibatasi pada bukti eksperimen yang terdokumentasi dan tidak menambahkan pengukuran jaringan baru.

2. Metodologi

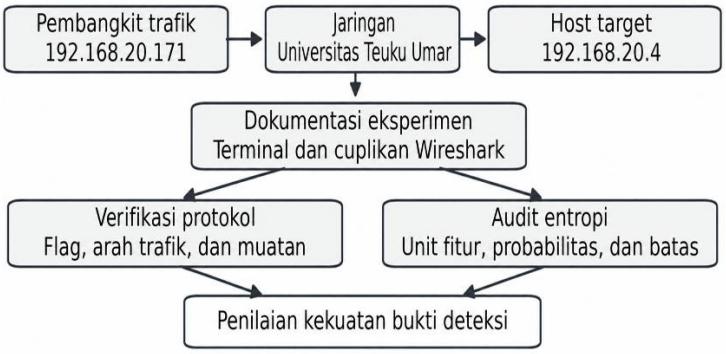
2.1. Desain Audit dan Sumber Bukti

Penelitian ini menggunakan desain studi kasus evaluatif dengan analisis retrospektif terhadap dokumen eksperimen yang dilaksanakan di salah satu universitas di Aceh Barat. Dokumentasi tersebut berasal dari eksperimen penelitian yang dilakukan pada tahun 2026. Bahan audit mencakup keluaran pembangkit trafik, tabel hasil pengujian, tangkapan layar terminal, cuplikan Wireshark, serta hasil perhitungan entropi. Unit analisis dalam penelitian ini bukan setiap paket jaringan sebagai replikasi independen, melainkan skenario pengujian dan objek masukan yang digunakan dalam perhitungan entropi. Pendekatan ini dipilih untuk mengevaluasi keterlacakan proses perhitungan dan memverifikasi konsistensi hasil yang telah dilaporkan, bukan untuk mengestimasi kinerja detektor pada populasi lalu lintas jaringan yang lebih luas.

Lingkungan eksperimen melibatkan satu komputer pembangkit berbasis Kali Linux dan satu komputer target yang terhubung ke jaringan. Alamat pembangkit yang tercatat adalah 192.168.20.171, sedangkan targetnya adalah 192.168.20.4. Perangkat lunak dan fungsinya disajikan pada Tabel 1. Rekonstruksi eksperimen dipisahkan dari audit validitas agar bukti pembangkitan trafik tidak langsung diperlakukan sebagai bukti keberhasilan deteksi. Alur audit pada Gambar 1 menelusuri hubungan antara skenario, bukti protokol, masukan fitur, dan keluaran entropi.

Tabel 1. Perangkat Lunak dan Perannya

Perangkat	Peran pada Eksperimen
Kali Linux dan VirtualBox 7.0	Lingkungan pembangkit dan virtualisasi
Nmap 7.93	Identifikasi host dan layanan
hping3	Pembangkitan paket TCP dan UDP
Wireshark	Perekaman dan inspeksi paket
Kalkulator entropi	Keluaran perhitungan yang diaudit



Gambar 1. Blok Fungsional Pengujian dan Analisis Ulang Dokumentasi Eksperimen

2.2. Rekonstruksi Skenario dan Validasi Protokol

Tiga keluaran pembangkit diberi kode S1-S3 untuk memungkinkan pemeriksaan label tanpa menjadikan label awal sebagai acuan kebenaran. S1 merekam TCP SYN dengan muatan 2.048 byte, S2 merekam UDP dengan muatan 2.048 byte, dan S3 merekam TCP SYN tanpa muatan ke port 80. Label HTTP Flood pada S3 diverifikasi berdasarkan flag TCP, muatan, arah komunikasi, dan keberadaan pesan aplikasi. Nmap digunakan untuk mengidentifikasi layanan, hping3 untuk menghasilkan trafik, dan Wireshark untuk melihat protokol, alamat, serta panjang frame.

Keterlacakan skenario diperiksa dengan mencocokkan jumlah paket pada keluaran terminal, alamat sumber-target, protokol, serta bukti pada cuplikan Wireshark. Jumlah pengiriman pada terminal diperlakukan sebagai hitungan pembangkit dan tidak disamakan dengan jumlah frame yang tertangkap atau laju paket per detik. Durasi skenario, jumlah pengulangan, PCAP lengkap, dan distribusi fitur pada kondisi normal tidak tersedia secara konsisten; karena itu, penelitian tidak merekonstruksi distribusi trafik secara penuh dari tangkapan layar maupun menafsirkan jumlah paket sebagai ukuran dampak serangan.

2.3. Audit Semantik dan Konsistensi Matematis Entropi

Shannon entropy dihitung berdasarkan distribusi probabilitas kategori [1]. Untuk N observasi fitur yang valid dan K kategori unik, frekuensi kategori ke-i dinyatakan sebagai f_i, probabilitas sebagai $p_i = f_i/N$, dan entropi sebagai $H(X) = -\Sigma p_i \log_2 p_i$. Audit memeriksa dua syarat dasar: probabilitas harus membentuk distribusi yang ternormalisasi dan nilai entropi harus berada pada rentang $0 \leq H(X) \leq \log_2 K$.

$$p_i = \frac{f_i}{N} \tag{1}$$

$$H(X) = -\sum_{i=1}^{K} p_i \log_2 p_i \tag{2}$$

Definisi kategori ditetapkan sesuai semantik jaringan: satu alamat IP lengkap diperlakukan sebagai satu kategori alamat, satu nomor port sebagai satu kategori port, dan setiap nilai panjang paket atau frame diperlakukan sebagai satu observasi ukuran. Header, muatan, panjang frame, dan jumlah paket merupakan besaran yang berbeda sehingga tidak dapat dipertukarkan sebagai satuan input. Dengan definisi ini, audit dapat membedakan kesalahan pada formula dari kesalahan pada representasi fitur.

$$\sum_{i=1}^{K} p_i = 1; \quad 0 \leq H(X) \leq \log_2 K \tag{3}$$

Audit dilakukan pada dua tingkat. Audit semantik memeriksa apakah objek yang dimasukkan ke kalkulator sesuai dengan fitur yang diklaim. Audit numerik kemudian mereproduksi nilai entropi dari string 192.168.20.4, 80, 27556, 82709, dan 43099 untuk menguji apakah keluaran kalkulator dapat dijelaskan oleh distribusi karakter. Reproduksi karakter berfungsi sebagai diagnosis terhadap mekanisme masukan; nilai tersebut tidak dianggap sebagai entropi trafik yang telah diperbaiki.

2.4. Kriteria Inferensi dan Batas Evaluasi

Interpretasi dibedakan menjadi tiga tingkat bukti: pembangkitan trafik, identifikasi pola/protokol, dan pengukuran performa detektor. Penelitian sebelumnya juga menyatakan bahwa mode flood hping3 tidak membaca atau menampilkan respons seperti pada mode biasa [8]. Sehingga nol paket diterima atau packet loss 100% pada terminal tidak dapat digunakan sebagai bukti langsung kegagalan target. Label HTTP Flood mensyaratkan bukti permintaan pada lapisan aplikasi yang terkait dengan skenario pembangkitan; semantik GET dan respons 206 Partial Content diperiksa sesuai RFC 9110 [9].

Ambang $H < 2{,}0$ bit sebagai indikasi serangan dan $H \geq 3{,}0$ bit sebagai kondisi normal diperlakukan sebagai aturan yang dilaporkan, bukan sebagai ambang optimal yang telah divalidasi. Konsistensi batas, rentang tanpa keputusan, dan keterkaitannya dengan jumlah kategori diperiksa secara deterministik. Akurasi, presisi, recall, F1-score, false positive rate, serta uji signifikansi tidak dihitung karena dokumentasi tidak menyediakan pasangan label acuan-prediksi per unit pengamatan maupun pengulangan yang independen.

3. Hasil dan Pembahasan

3.1. Bukti Empiris Skenario Flooding

Tiga skenario dapat ditelusuri secara langsung ke keluaran pembangkit trafik pada Tabel 2. S1 menghasilkan 27.556 paket TCP SYN dan S2 menghasilkan 82.709 paket UDP, keduanya dengan muatan 2.048 byte, sedangkan S3 menghasilkan 43.099 paket TCP SYN tanpa muatan. Angka tersebut membuktikan aktivitas pembangkitan pada sesi yang terdokumentasi, tetapi tidak dapat dibandingkan sebagai laju atau intensitas serangan karena durasi dan kondisi pengujian tidak seragam atau tidak tersedia.

Tabel 2. Keluaran Pembangkitan Trafik yang Terdokumentasi

Kode	Trafik	Paket	Muatan
S1	TCP SYN	27.556	2.048 byte
S2	UDP	82.709	2.048 byte
S3	TCP SYN	43.099	0 byte

Pada S1 dan S2, terminal mencatat fragmentasi otomatis dengan fragmen berukuran 1.480 byte pada MTU 1.500 byte, sedangkan cuplikan Wireshark memperlihatkan frame berukuran 1.514 byte serta pola TCP atau UDP yang berulang. Temuan ini menegaskan bahwa muatan yang ditetapkan pada pembangkit, fragmen IP, dan panjang frame merupakan lapisan pengukuran yang berbeda. Karena itu, jumlah paket yang dihasilkan tidak dapat langsung digunakan sebagai pengganti distribusi panjang paket tanpa aturan reassembly dan definisi unit yang jelas.

Bukti yang tersedia mendukung karakterisasi terjadinya flooding pada TCP dan UDP, tetapi belum menunjukkan adanya kehilangan paket jaringan atau penurunan ketersediaan layanan. Statistik terminal hping3 tidak memadai untuk inferensi tersebut karena perilaku mode flood memang membatasi pembacaan respons [10]. Cuplikan penggunaan CPU juga tidak sinkron dengan awal dan akhir setiap skenario. Dengan demikian, klaim empiris yang sah pada tahap ini adalah adanya pembangkitan trafik, bukan besarnya dampak terhadap layanan.

3.2. Validitas Label Serangan pada Tingkat Protokol

S3 memperlihatkan flag SYN, header TCP, dan muatan nol yang ditujukan ke port 80. Kombinasi ini konsisten dengan pembangkitan paket TCP SYN ke layanan pada port 80, tetapi tidak membuktikan adanya permintaan HTTP. Nomor port adalah atribut pada lapisan transport, sedangkan HTTP memerlukan bukti pesan pada lapisan aplikasi. Pemisahan kedua lapisan ini penting agar satu sesi SYN tidak ditafsirkan sekaligus sebagai keberhasilan pengujian HTTP Flood.

Cuplikan yang diberi label deteksi HTTP memang memuat metode GET dan respons HTTP/1.1 206 Partial Content. Namun, arah komunikasinya berasal dari host 192.168.20.4 menuju alamat eksternal, lalu respons kembali ke host lokal, berbeda dengan skenario pembangkit 192.168.20.171 menuju 192.168.20.4. RFC 9110 menjelaskan bahwa respons 206 merupakan mekanisme normal untuk pengiriman sebagian dari representasi [9]. Tanpa identitas sesi, frekuensi permintaan yang terukur, dan log aplikasi target, cuplikan tersebut hanya membuktikan adanya trafik HTTP, bukan serangan HTTP Flood.

Terminologi DDoS juga tidak didukung oleh konfigurasi eksperimen yang terdokumentasi karena hanya terdapat satu host pembangkit. Studi Habib [11], Misalnya, menggunakan arsitektur botnet untuk merepresentasikan beberapa sumber serangan. Oleh sebab itu, istilah flooding atau DoS lebih konsisten dengan bukti empiris penelitian ini, sedangkan kemampuan menghadapi sumber terdistribusi memerlukan skenario multi-sumber tersendiri [12].

3.3. Validitas Semantik Masukan Entropi

Temuan utama audit adalah bahwa beberapa nilai yang dilabeli sebagai entropi fitur dapat direproduksi dari karakter penyusun string masukan, bukan dari distribusi observasi fitur pada jaringan (Tabel 3). Untuk masukan 80, kalkulator menghasilkan dua simbol, 8 dan 0, masing-masing dengan probabilitas 0,5 sehingga H = 1 bit. Jika fitur yang dimaksud adalah destination port dan seluruh

observasi bernilai port 80, distribusi tersebut hanya memiliki satu kategori sehingga H = 0 bit. Perbedaannya berasal dari perubahan unit observasi, bukan dari perubahan kondisi lalu lintas.

Pola yang sama muncul pada nilai yang diberi label "packet_size". String 27556 menghasilkan H = 1,921928 bit karena digit 5 muncul 2 kali, sedangkan 3 digit lainnya masing-masing muncul 1 kali. String 82709 memiliki lima digit unik dan menghasilkan H = 2,321928 bit; string 43099 kembali menghasilkan H = 1,921928 bit karena digit 9 berulang. Ketiga string tersebut identik dengan jumlah paket pada S1-S3, bukan daftar paket yang panjang. Reproduksi numerik ini menunjukkan bahwa keluaran dapat benar sebagai entropi karakter, tetapi tidak valid secara semantik sebagai entropi ukuran paket.

Tabel 3. Reproduksi Entropi Karakter dan Evaluasi Makna Fitur

Masukan Terdokumentasi	Fitur yang Diklaim	H Karakter (bit)	Hasil Audit Semantik
192.168.20.4	src_ip	2,855389	Alamat target; angka yang dihitung merepresentasikan karakter alamat, bukan frekuensi IP sumber.
80	dst_port	1,000000	Dua digit dianggap sebagai dua simbol; satu kategori port tujuan seharusnya menghasilkan H = 0.
27556	packet_size S1	1,921928	Masukan harus sama dengan jumlah paket S1, bukan daftar panjang paket.
82709	packet_size S2	2,321928	Lima digit unik menjelaskan nilai hasil; variasi panjang paket belum dihitung.
43099	packet_size S3	1,921928	Nilai dapat direproduksi dari digit jumlah paket; bukan entropi trafik HTTP.

Konsekuensi metodologisnya penting: nilai entropi dapat berubah hanya karena representasi angka secara tekstual berubah, meskipun trafik fisik tidak berubah. Sebaliknya, dua himpunan paket dengan distribusi panjang yang berbeda dapat menghasilkan nilai karakter yang sama jika jumlah paketnya direpresentasikan oleh pola digit yang serupa. Dengan demikian, validitas formula saja tidak cukup; validitas semantik unit observasi harus dipastikan terlebih dahulu.

Untuk alamat 192.168.20.4, reproduksi pada tingkat karakter menghasilkan H = 2,855389 bit, sesuai dengan salah satu angka IP yang telah didokumentasikan. Selain itu, alamat tersebut berperan sebagai target pada keluaran terminal, bukan sebagai sumber. Temuan ini mengindikasikan dua ketidaksesuaian independen: masukan diperlakukan sebagai karakter dan identitas fitur sumber tidak konsisten. Entropi source IP trafik sebenarnya tidak dapat ditentukan tanpa frekuensi alamat dari rekaman paket lengkap.

3.4. Konsistensi Matematis dan Kelayakan Ambang

Keluaran kalkulator untuk IP mencantumkan jumlah probabilitas sebesar 2, jumlah simbol sebesar 16, dan entropi sebesar 5,710777 bit. Nilai tersebut tidak memenuhi dua syarat dasar entropi Shannon. Pertama, jumlah probabilitas dalam satu distribusi harus sama dengan 1. Kedua, untuk K = 16 kategori, entropi maksimum adalah $\log_2(16) = 4$ bit. Karena 5,710777 bit melampaui batas tersebut, angka itu tidak valid sebagai entropi distribusi dengan 16 kategori. Kedekatannya dengan dua kali entropi karakter string IP merupakan petunjuk numerik, tetapi penyebab implementasinya tidak dapat dipastikan tanpa kode kalkulator dan masukan yang lengkap.

Batas maksimum juga menunjukkan bahwa ambang universal 3 bit tidak dapat diterapkan tanpa mempertimbangkan kardinalitas fitur. Distribusi memerlukan setidaknya delapan kategori agar secara teoritis dapat mencapai 3 bit, dan nilai tersebut hanya tercapai pada delapan kategori dengan probabilitas yang seragam. Pada fitur dengan satu destination port, entropi maksimum tetap 0 bit. Oleh karena itu, entropi rendah hanya menunjukkan konsentrasi distribusi; status serangan memerlukan konteks protokol, baseline, dan definisi fitur yang relevan.

Aturan $H < 2{,}0$ bit dan $H \geq 3{,}0$ bit juga menyisakan interval $2{,}0 \leq H < 3{,}0$ bit tanpa keputusan, sementara sebagian dokumentasi menggunakan $H \leq 2{,}0$ bit. Ketidakkonsistenan ini memengaruhi interpretasi nilai yang berada di dekat batas. Dengan kondisi tersebut, tabel keputusan yang menyatakan seluruh skenario sebagai serangan tidak dapat dianggap sebagai validasi kuantitatif sebelum unit fitur, aturan agregasi, dan label acuan ditetapkan secara eksplisit.

Penelitian tentang ambang adaptif menunjukkan bahwa keputusan berbasis entropi memang sensitif terhadap kondisi lalu lintas. Mengevaluasi entropi gabungan Rényi pada variasi sumber, target, dan laju trafik [11]. Sedangkan [13] Mengembangkan penyesuaian ambang dengan melakukan evaluasi ulang terhadap IP yang dicurigai. Temuan penelitian ini melengkapi arah tersebut: adaptasi ambang baru bermakna setelah masukan memenuhi validitas semantik dan probabilitas yang digunakan membentuk distribusi yang valid.

4. Kesimpulan

Audit terhadap dokumentasi eksperimen menunjukkan bahwa validitas deteksi flooding berbasis entropi bergantung pada tiga lapisan konsistensi: bukti protokol, konsistensi semantik fitur, dan batasan matematis. Bukti yang tersedia mendukung terjadinya TCP SYN dan UDP flooding, tetapi tidak memverifikasi label HTTP Flood maupun sifat terdistribusi DDoS. Beberapa nilai entropi yang dilaporkan dapat direproduksi dari karakter string masukan, bukan dari distribusi fitur jaringan, sedangkan nilai entropi IP sebesar 5,710777 bit melanggar normalisasi probabilitas dan batas maksimum untuk 16 kategori. Temuan ini menunjukkan bahwa nilai entropi tidak boleh diinterpretasikan sebagai indikator serangan sebelum unit observasi dan distribusi probabilitas divalidasi. Evaluasi performa detektor selanjutnya memerlukan PCAP lengkap, baseline normal, pengulangan independen, serta data berlabel terpisah untuk kalibrasi dan pengujian.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat, Universitas Teuku Umar, atas dukungannya terhadap penelitian ini melalui skema Penelitian Riset Dasar Unggulan Universitas dengan nomor kontrak 124/UN59.L1.04/PL/2026.

Daftar Pustaka

[1] I. Sreeram, V. Praveen, and K. Vuppala, “Applied Computing and Informatics HTTP flood attack detection in application layer using machine learning metrics and bio-inspired bat algorithm,” *Appl. Comput. Informatics*, vol. 15, no. 1, pp. 59–66, 2019, doi: 10.1016/j.aci.2017.10.003.

[2] A. I. Hassan, E. Abd, E. Reheem, and S. K. Guirguis, “An entropy- and machine learning-based approach for DDoS attack detection in software-defined networks,” *Sci. Rep.*, pp. 1–18, 2024, doi: 10.1038/s41598-024-67984-w.

[3] L. Zhou, Y. Zhu, Y. Xiang, and T. Zong, “A novel feature-based framework enabling multi-type DDoS attack detection,” *World Wide Web*, pp. 163–185, 2023, doi: 10.1007/s11280-022-01040-3.

[4] M. A. Aladaileh *et al.*, “Applied Sciences: Effectiveness of an Entropy-Based Approach for Detecting Low- and High-Rate DDoS Attacks against the SDN Controller : Experimental Analysis,” *Appl. Sci.*, vol. 13, no. 1, pp. 1–12, 2023, doi: https://doi.org/10.3390/app13020775.

[5] L. D. Tsobdjou, S. Pierre, S. Member, A. Quintero, and S. Member, “An Online Entropy-Based DDoS Flooding Attack Detection System With Dynamic Threshold,” *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 2, pp. 1679–1689, 2022, doi: 10.1109/TNSM.2022.3142254.

[6] Q. Tian and S. Miyata, “IoT A DDoS Attack Detection Method Using Conditional Entropy Based on SDN Traffic,” *IoT*, vol. 4, no. April, pp. 95–111, 2023, doi: https://doi.org/10.3390/iot4020006.

[7] A. Solichin and L. Nugroho, "Deteksi Dini Gangguan Jaringan Distributed Denial of Service (DDOS) Menggunakan Metode Shannon Entropy Pada Software Defined Network (SDN)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 3, pp. 461–473, 2024, doi: 10.25126/JTIIK.938188.

[8] C. Chen and J. L. Lai, "An Experimental Detection of Distributed Denial of Service Attack in CDX 3 Platform Based on Snort," *Sensors*, vol. 23, no. Juli, pp. 2–19, 2023, doi: https://doi.org/10.3390/s23136139.

[9] B. Xie, Y. Wang, G. Wen, and X. Xu, "Application-Layer DDoS Attack Detection Using Explicit Duration Recurrent Network-Based Application-Layer Protocol Communication Models," *Int. J. intelligentent Syst.*, vol. 2023, no. June, pp. 1–23, 2023, doi: https://doi.org/10.1155/2023/2632678.

[10] W. Hill *et al.*, "DDoS in SDN : a review of open datasets , attack vectors and mitigation strategies," *Discov. Appl. Sci.*, vol. Agustus, no. 6, p. 472, 2024, doi: 10.1007/s42452-024-06172-x.

[11] B. Habib and F. Khursheed, "Real-Time Transmission Control Proto col-S ynchr onize -Base d Distributed Denial of Service Detection Framework Using Entropy Variations in Self-Coded Bot-Network Architecture," *Electrica*, vol. 23, no. 2, pp. 160–176, 2023, doi: 10.5152/electrica.2022.21188.

[12] K. Wang, Y. Fu, X. Duan, and T. Liu, "Detection and mitigation of DDoS attacks based on multi - dimensional characteristics in SDN," *Sci. Rep.*, vol. 14, pp. 1–19, 2024, doi: 10.1038/s41598-024-66907-z.

[13] J. Pebrianto and V. Suryani, "Adaptive DDoS Attack Detection : Entropy-Based Model With Dynamic Threshold and Suspicious IP Reevaluation," *IEEE Access*, vol. 13, no. April, pp. 55858–55876, 2025, doi: 10.1109/ACCESS.2025.3553144.