JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.10904

DETEKSI DAN ANALISIS FORENSIK SERANGAN DDOS DAN PORT SCANNING PADA TRAFIK TERENKRIPSI MENGGUNAKAN MULTI-METRIC FUSION

Dikhsan Dwirangga Tibong[1*], L. M. Fid Aksara[2], Isnawaty[3], Muh. Yamin[4], La Surimi[5], Asa Hari Wibowo[6]

[1,2,3,4,5,6]Jurusan Informatika, Fakultas Teknik, Universitas Halu Oleo; Jl. H.E.A. Mokodompit, Kendari, Sulawesi Tenggara 93232

Keywords:
DDoS;
Port Scanning;
multi-metric fusion;
entropi Shannon;
metadata trafik terenkripsi.

Corresponding Email:
dikhsan.tibong@student.uho.ac.id

Abstrak. Adopsi HTTPS/TLS secara luas menyebabkan metode deteksi ancaman berbasis inspeksi payload menjadi tidak efektif, sementara serangan Distributed Denial of Service (DDoS) dan Port Scanning tetap menjadi ancaman utama ketersediaan Server Web. Penelitian ini mengembangkan sistem deteksi dan forensik yang bekerja hanya pada metadata trafik terenkripsi tanpa dekripsi payload, dengan menggabungkan metrik temporal (Packet Per Second dan Inter-Arrival Time) dan metrik statistik (entropi Shannon alamat IP sumber dan Port tujuan) melalui rule-based multi-metric fusion. Sistem dikembangkan menggunakan Security Policy Development Life Cycle (SPDLC) dan diuji pada Server Web HTTPS/TLS berbasis Linux, dilengkapi mitigasi otomatis Iptables dan log forensik berformat JSON. Evaluasi menggunakan confusion matrix pada 233 window trafik menghasilkan akurasi 88,41%, dengan deteksi Port Scanning mencapai precision 100% dan recall 95,65%, sedangkan deteksi DDoS/DoS memperoleh precision 83,87% dan recall 55,32% akibat mitigasi pada level penyedia layanan. Validasi pada empat berkas dataset publik CIC-DDoS2019 menghasilkan rata-rata akurasi 90,35% dan precision 99,45%, menunjukkan kemampuan generalisasi sistem. Hasil ini membuktikan bahwa pendekatan multi-metric fusion efektif mendeteksi dan mendokumentasikan dua jenis ancaman jaringan secara simultan pada trafik terenkripsi tanpa mengorbankan privasi data pengguna.

Abstract. *The widespread adoption of HTTPS/TLS has rendered payload-inspection-based threat detection methods ineffective, while Distributed Denial of Service (DDoS) attacks and Port Scanning remain major threats to Web Server availability. This study develops a detection and forensic system that operates solely on encrypted traffic metadata without payload decryption, combining temporal metrics (Packets Per Second and Inter-Arrival Time) with statistical metrics (Shannon entropy of source IP and destination Port) through rule-based multi-metric fusion. The system was developed using the Security Policy Development Life Cycle (SPDLC) and tested on a Linux-based HTTPS/TLS Web Server, equipped with automatic Iptables mitigation and JSON forensic logging. Evaluation using a confusion matrix on 233 traffic windows yielded an overall accuracy of 88.41%, with Port Scanning detection achieving 100% precision and 95.65% recall, while DDoS/DoS detection achieved 83.87% precision and 55.32% recall due to provider-level mitigation. Validation on four CIC-DDoS2019 dataset files produced an average accuracy of 90.35% and precision of 99.45%, indicating good generalization capability. These results demonstrate that the multi-metric fusion approach effectively detects and documents two distinct network threats simultaneously on encrypted traffic without compromising user data privacy.*

1. PENDAHULUAN

Ketergantungan layanan pemerintahan, pendidikan, dan komersial terhadap infrastruktur Server Web menuntut jaminan ketersediaan yang tinggi agar kontinuitas operasional tidak terganggu [1]. Ancaman terhadap ketersediaan tersebut terus berkembang; serangan Distributed Denial of Service (DDoS) kini hadir dalam berbagai variasi, mulai dari flood berskala besar hingga pola low-rate yang sulit dikenali oleh pendeteksian konvensional [2]. Selain DDoS, aktivitas Port Scanning kerap mendahului eksploitasi lebih lanjut; meskipun payload komunikasi terenkripsi, aktivitas ini meninggalkan jejak statistik yang khas pada metadata trafik, seperti distribusi Port tujuan yang beragam dan Inter-Arrival Time yang sangat pendek dari satu alamat IP sumber [3].

Adopsi HTTPS/TLS sebagai standar komunikasi menyebabkan payload tidak dapat diinspeksi tanpa dekripsi, sehingga metode deteksi berbasis isi paket menjadi kurang efektif. Analisis metadata trafik—seperti timestamp, ukuran paket, Port, dan laju paket—muncul sebagai pendekatan praktis untuk mendeteksi anomali pada trafik terenkripsi [4]. Dua metrik yang umum dimanfaatkan dalam pendekatan ini adalah packet timing (mis. Inter-Arrival Time dan Packets Per Second) dan entropi distribusi atribut trafik. Penelitian terdahulu menunjukkan bahwa kombinasi metrik temporal dan statistik—dikenal sebagai multi-metric fusion—dapat meningkatkan kemampuan deteksi anomali pada trafik terenkripsi dibandingkan penggunaan metrik tunggal [5].

Meskipun demikian, kajian terhadap penelitian terdahulu memperlihatkan bahwa mayoritas studi menangani aspek deteksi secara terpisah. Sebagian memanfaatkan entropi trafik [6], sebagian menggabungkan beberapa metrik namun hanya difokuskan pada deteksi DDoS tanpa mengintegrasikan Port Scanning [7], dan sebagian lain menekankan aspek forensik tanpa modul deteksi multi-metrik yang menyatu [8]. Belum ditemukan penelitian yang secara eksplisit mengintegrasikan deteksi dua jenis ancaman—DDoS dan Port Scanning—sekaligus modul forensik dan mitigasi otomatis dalam satu sistem yang bekerja murni pada metadata trafik terenkripsi.

Berdasarkan kesenjangan tersebut, penelitian ini mengembangkan dan mengevaluasi sistem deteksi dan analisis forensik yang menggabungkan metrik temporal (Packet Per Second dan Inter-Arrival Time) dan metrik statistik (entropi Shannon alamat IP sumber dan Port tujuan) melalui pendekatan rule-based multi-metric fusion, dilengkapi mekanisme mitigasi otomatis berbasis Iptables dan pencatatan log forensik terstruktur. Dua pertanyaan penelitian diajukan: (1) bagaimana merancang sistem multi-metric fusion yang mengklasifikasikan trafik metadata terenkripsi HTTPS/TLS ke dalam kelas Normal, DDoS, dan Port Scanning tanpa dekripsi payload sekaligus menghasilkan bukti digital; dan (2) seberapa efektif sistem tersebut mendeteksi kedua jenis ancaman, diukur menggunakan confusion matrix, baik pada data pengujian langsung maupun pada dataset publik sebagai validasi generalisasi.

Kebaruan penelitian ini terletak pada integrasi menyeluruh tiga aspek yang pada penelitian terdahulu umumnya ditangani terpisah: penggabungan metrik temporal dan statistik secara simultan, deteksi dua jenis ancaman sekaligus dalam satu sistem klasifikasi, serta integrasi modul forensik dan mitigasi otomatis pada metadata trafik terenkripsi HTTPS/TLS. Urgensi penelitian ini sejalan dengan kebutuhan peningkatan kapasitas deteksi ancaman siber pada organisasi di Indonesia yang kian bergantung pada layanan web terenkripsi, sebagaimana ditekankan pada kajian sistematis mengenai tren kebocoran data dan DDoS pada layanan cloud terkini [17], dan sejalan dengan amanat Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dalam melindungi keamanan sistem elektronik nasional.

2. TINJAUAN PUSTAKA

Beberapa penelitian terdahulu menjadi dasar konseptual dan pembanding penelitian ini. Shbair dkk. [9] membuktikan bahwa metadata trafik—meskipun payload terenkripsi—tetap dapat dimanfaatkan untuk mendeteksi aktivitas anomali melalui atribut waktu, ukuran paket, dan pola aliran. Li dkk. [6] mengusulkan deteksi anomali berbasis entropi pada trafik terenkripsi dan menunjukkan bahwa penurunan nilai entropi secara signifikan mengindikasikan serangan flooding, sejalan dengan temuan Tian dan Miyata [10] bahwa perubahan entropi kondisional merupakan indikator kuat serangan DDoS pada trafik SDN. Solichin dan Nugroho [11] menerapkan Shannon Entropy pada lingkungan Software Defined Network dan membuktikan efektivitasnya dalam mengidentifikasi pola trafik tidak normal, sedangkan Riadi dkk. [12] menunjukkan bahwa distribusi Port tujuan dan pola Inter-Arrival Time dapat membedakan trafik Port Scanning dari trafik normal berbasis analisis statistik metadata semata.

Pada sisi penggabungan metrik, Wang dkk. [7] mengusulkan pendekatan multi-metric fusion yang mampu meningkatkan akurasi deteksi DDoS dibandingkan metrik tunggal, dan Wang dkk. [5] memperkuat temuan tersebut melalui pendekatan fusi multi-granularitas yang menurunkan false positive dan meningkatkan recall pada trafik terenkripsi. Kedua penelitian ini hanya berfokus pada deteksi DDoS tanpa mengintegrasikan deteksi Port Scanning. Dari sisi forensik, Murti dkk. [8] menerapkan Network Forensic Development Life Cycle untuk menganalisis serangan DDoS, menegaskan pentingnya pencatatan trafik sebagai bukti digital, namun belum menyatukan mekanisme deteksi multi-metrik dan mitigasi otomatis dalam satu alur sistem.

Isu keamanan jaringan berbasis pengujian dan pemantauan real-time turut dibahas oleh Shafiyyah dkk. [13], yang menerapkan platform Wazuh dengan metode PPDIOO untuk mendeteksi dan merespons serangan brute force dan Denial of Service pada jaringan kampus, mengonfirmasi relevansi pendekatan deteksi-dan-respons otomatis pada infrastruktur jaringan institusi di Indonesia. Prinsip dasar deteksi dan pencegahan intrusi merujuk pada panduan NIST [14] serta konsep keamanan jaringan umum [15], sedangkan mekanisme mitigasi berbasis firewall Iptables mengacu pada penerapan Port Knocking dan Honeypot yang telah terbukti efektif pada penelitian sebelumnya [16]. Berbeda dengan studi-studi tersebut, penelitian ini mengintegrasikan deteksi dua jenis ancaman, forensik, dan mitigasi otomatis dalam satu sistem multi-metric fusion yang bekerja murni pada metadata trafik terenkripsi.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental untuk merancang, mengimplementasikan, dan mengevaluasi sistem deteksi. Data bersumber dari dua sumber yang saling melengkapi. Data primer diperoleh dari eksperimen terkontrol pada Server Web berbasis HTTPS/TLS milik peneliti, mencakup rekaman trafik normal (baseline) minimal 60 menit serta trafik hasil simulasi serangan DoS/DDoS menggunakan hping3 dan Port Scanning menggunakan Nmap, yang ditangkap melalui tcpdump dalam format PCAP dan diekstraksi metadatanya (alamat IP, Port, protokol, dan timestamp) tanpa menyentuh payload terenkripsi. Data sekunder berupa dataset publik CIC-DDoS2019 dari Canadian Institute for Cybersecurity digunakan sebagai validasi generalisasi pada empat berkas serangan, yaitu DrDoS_DNS, DrDoS_NTP, Syn, dan UDPLag, dengan kolom Flow Packets/s dipetakan sebagai metrik PPS dan kolom Label sebagai ground truth.

Sistem dikembangkan menggunakan metode Security Policy Development Life Cycle (SPDLC) yang terdiri atas lima tahap: (1) Analysis, identifikasi aset (Server Web HTTPS) dan ancaman (DoS/DDoS, Port Scanning); (2) Design, perancangan arsitektur deteksi multi-metric fusion beserta mekanisme mitigasi Iptables dan log forensik; (3) Implementation,

realisasi modul pemantauan trafik, ekstraksi metadata, dan perhitungan metrik pada Server Web pengujian; (4) Enforcement, operasional sistem secara real-time untuk memantau, mengklasifikasi, memitigasi, dan mencatat trafik; serta (5) Enhancement, evaluasi kinerja dan penyempurnaan parameter deteksi berdasarkan hasil pengujian.

Metrik trafik dihitung pada setiap window pengamatan menggunakan Packet Per Second (Persamaan 1), Inter-Arrival Time (Persamaan 2), dan entropi Shannon terhadap distribusi alamat IP sumber maupun Port tujuan (Persamaan 3).

$$PPS = N / T \quad (1)$$

$$IATi = ti - ti-1 \quad (2)$$

$$H(X) = -\Sigma\, p(xi)\, log_2\, p(xi) \quad (3)$$

dengan N adalah jumlah paket yang diterima, T interval waktu pengamatan, ti waktu kedatangan paket ke-i, dan p(xi) probabilitas kemunculan atribut ke-i pada window pengamatan.

Ambang batas (threshold) deteksi ditentukan melalui uji normalitas data baseline (Shapiro-Wilk untuk n < 50 window, atau Kolmogorov-Smirnov untuk sampel lebih besar). Apabila distribusi mendekati normal, threshold dihitung menggunakan Persamaan 4; apabila distribusi condong (skewed), digunakan pendekatan berbasis persentil ke-99 dari data baseline.

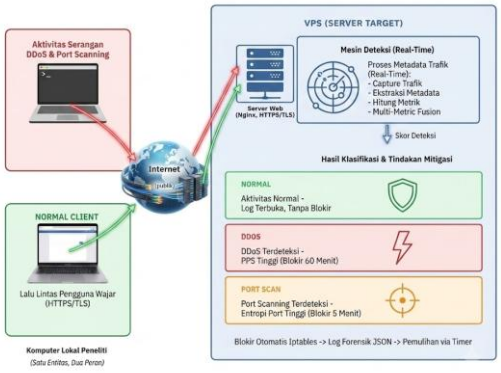
$$\theta = \mu + k\sigma \quad (4)$$

dengan μ nilai rata-rata dan σ standar deviasi metrik pada kondisi normal, serta k konstanta sensitivitas yang ditetapkan awal k = 3 mengikuti kaidah Empirical Rule (mencakup 99,73% observasi normal pada distribusi normal) dan dioptimasi secara eksperimental pada rentang {2,0; 2,5; 3,0; 3,5; 4,0} berdasarkan nilai F1-Score tertinggi pada data validasi. Trafik diklasifikasikan sebagai DDoS apabila PPS tinggi disertai entropi IP sumber rendah dan konsisten selama minimal N window berturut-turut—mekanisme yang diterapkan untuk mengurangi false positive akibat lonjakan trafik sesaat—serta sebagai Port Scanning apabila entropi Port tujuan dan jumlah Port unik per window melampaui ambang batasnya. Kinerja sistem dievaluasi menggunakan confusion matrix dengan skema One-vs-Rest (OvR) melalui metrik akurasi, precision, recall, F1-score, dan false positive rate (FPR).

4. HASIL DAN PEMBAHASAN

4.1 Arsitektur dan Alur Deteksi Sistem

Sistem dirancang dengan enam modul utama yang bekerja pada sisi server secara real-time tanpa dekripsi payload, yaitu Server Web, Traffic Capture Module, Metadata Extraction Module, Traffic Analysis Module, Detection and Classification Module, serta Forensic Logging and Mitigation Module (Gambar 1). Traffic Capture Module menangkap paket melalui packet sniffing pada antarmuka jaringan server, kemudian Metadata Extraction Module mengekstraksi atribut yang dapat diamati tanpa dekripsi—timestamp, alamat IP sumber dan tujuan, Port tujuan, ukuran paket, dan protokol. Traffic Analysis Module selanjutnya menghitung PPS, IAT, entropi IP sumber (Hsrc), entropi Port tujuan (Hport), dan jumlah Port unik per window (UDP-W) secara periodik.



Gambar 1. Arsitektur Sistem Deteksi dan Forensik

Detection and Classification Module menjalankan rule-based multi-metric fusion melalui dua jalur paralel: jalur DDoS

berdasarkan kombinasi PPS tinggi, IAT rendah, dan Hsrc rendah; serta jalur Port Scanning berdasarkan Hport tinggi dan UDP-W yang meningkat signifikan. Untuk mengurangi false positive akibat lonjakan trafik sesaat, indikasi DDoS harus konsisten selama minimal N window berturut-turut sebelum mitigasi dijalankan, sedangkan Port Scanning—karena polanya khas dan dapat dikenali dari satu window pengamatan—dimitigasi seketika. Ketika ambang batas terlampaui, Forensic Logging and Mitigation Module mencatat seluruh informasi kejadian (waktu, IP sumber, nilai metrik, jenis ancaman, tindakan) ke dalam log forensik berformat JSON dan menambahkan aturan pemblokiran pada firewall Iptables, dengan pelepasan blokir otomatis melalui timer serta cron job cadangan setiap 1 menit.

4.2 Statistik Baseline dan Ambang Batas Deteksi

Statistik baseline dihitung dari data trafik normal untuk memperoleh nilai rata-rata (μ), standar deviasi (σ), dan ambang batas ($\theta = \mu + 3\sigma$) setiap metrik, sebagaimana disajikan pada Tabel 1.

Metrik	μ	σ	θ = μ+3σ
PPS	76,0124	65,4865	272,472
IAT (s)	0,0483	0,1642	0,5409
Hsrc	0,0092	0,0805	0,2505
Hport	0,0092	0,0805	0,2505
UDP-W	1,0249	0,1558	1,4923

Tabel 1. Statistik Baseline Trafik Normal

Nilai θPPS sebesar 272,47 paket/detik digunakan sebagai batas atas trafik normal; window dengan PPS melampaui nilai ini dan entropi IP sumber mendekati nol berpotensi diklasifikasikan sebagai serangan flood. Standar deviasi PPS yang relatif besar (65,49) terhadap rata-ratanya (76,01) mencerminkan fluktuasi alami trafik Server Web pada jaringan internet publik, yang menegaskan pentingnya penggunaan konstanta k = 3 agar lonjakan trafik wajar tidak langsung memicu alarm. Sementara itu, nilai baseline entropi IP sumber dan Port tujuan yang mendekati nol (μ = 0,0092) konsisten dengan karakteristik Server Web yang umumnya melayani permintaan pada Port terbatas (80 dan 443), sehingga lonjakan entropi Port tujuan menjadi diskriminator yang sangat kuat bagi jalur deteksi Port Scanning.

4.3 Hasil Pengujian Skenario Serangan

Pengujian skenario DoS satu-sumber (HTTP Flood dan TCP SYN Flood menggunakan Apache Bench/Siege dan hping3) menghasilkan nilai PPS tinggi (hingga 114 paket/detik pada salah satu entri log) dengan entropi IP sumber mendekati nol, konsisten dengan karakteristik konsentrasi trafik dari satu sumber. Pengujian Port Scanning menggunakan Nmap mode SYN scan dan TCP Connect scan menghasilkan entropi Port tujuan tinggi disertai 23 Port unik per window pada kedua mode, sedangkan entropi IP sumber tetap mendekati nol karena berasal dari satu alamat pemindai (Tabel 2).

Mode Scan	Hport	UDP-W	Hsrc	Status
SYN scan (-sS)	4,248	23	≈ 0	Port Scan
TCP Connect (-sT)	4,524	23	≈ 0	Port Scan

Tabel 2. Hasil Deteksi Aktivitas Port Scanning

Pola-pola tersebut menegaskan bahwa metadata trafik terenkripsi tetap mampu membedakan karakteristik jenis ancaman tanpa memerlukan dekripsi payload.

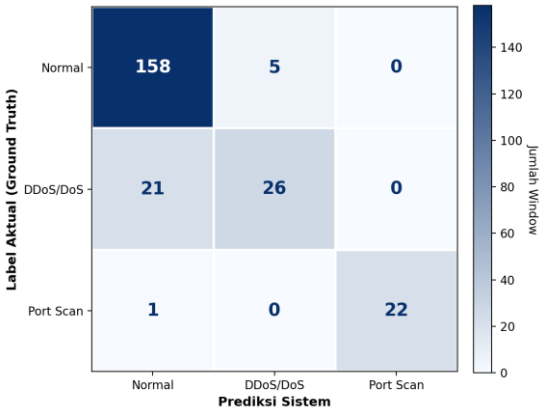
4.4 Evaluasi Kinerja Sistem

Pengujian menghasilkan 233 window trafik yang dianalisis, terdiri atas 163 window Normal, 47 window flood (DoS/DDoS), dan 23 window Port Scanning. Confusion matrix hasil klasifikasi ditunjukkan pada Tabel 3 dan divisualisasikan pada Gambar 2.

Aktual\Prediksi	Normal	DDoS/DoS	Port Scan
Normal	158	5	0

Aktual\Prediksi	Normal	DDoS/DoS	Port Scan
DDoS/DoS	21	26	0
Port Scan	1	0	22

Tabel 3. Confusion Matrix Hasil Klasifikasi Sistem



Gambar 2. Visualisasi Confusion Matrix

Dari 47 window serangan flood, sebanyak 26 window terdeteksi benar sebagai DDoS/DoS sedangkan 21 window terklasifikasi Normal; dari 23 window Port Scanning, 22 window terdeteksi benar. Berdasarkan confusion matrix tersebut, metrik evaluasi per kelas menggunakan skema One-vs-Rest disajikan pada Tabel 4.

Kelas (OvR)	Akurasi	Precision	Recall	F1	FPR
Normal	88,41 %	87,78 %	96,93%	92,13%	31,43%
DDoS	88,84 %	83,87 %	55,32%	66,67%	2,69 %
Port Scan	99,57 %	100%	95,65%	97,78%	0%
Rata2 tertimbang	89,60 %	88,20 %	88,41%	87,55%	22,53%

Tabel 4. Hasil Evaluasi Kinerja Sistem per Kelas

Sistem mencapai akurasi keseluruhan 88,41% dengan performa yang berbeda signifikan antar kelas. Deteksi Port Scanning menunjukkan efektivitas tertinggi (precision 100%, recall 95,65%, F1-score 97,78%, FPR 0%), sedangkan deteksi DDoS/DoS memperoleh precision 83,87% namun recall lebih rendah (55,32%). Perbedaan sensitivitas kedua jalur deteksi ini dapat dijelaskan dari karakteristik metrik yang digunakan: jalur Port Scanning mengandalkan lonjakan entropi Port tujuan yang secara statistik sangat kontras terhadap baseline mendekati nol, sehingga hampir tidak ada tumpang tindih dengan trafik normal; sedangkan jalur DDoS mengandalkan metrik volume (PPS) yang rentangnya beririsan dengan lonjakan trafik normal yang sah, ditambah mekanisme persistensi minimal N window yang sengaja memperlambat konfirmasi demi menekan false positive.

4.5 Analisis Log Forensik

Setiap kejadian deteksi dicatat dalam log forensik berformat JSON yang memuat dua belas parameter, di antaranya timestamp, alamat IP sumber dan tujuan, protokol, nilai PPS, IAT, entropi IP sumber, entropi Port tujuan, jumlah Port unik per window, skor deteksi, jenis ancaman terdeteksi, serta tindakan mitigasi yang dijalankan. Sebagai contoh, entri log pada skenario DoS satu-sumber merekam nilai pps 114,0, iat 0,0003 detik, entropy_src_ip 0,0, threat_detected “DDoS Detected”, dan action_taken berupa pemblokiran alamat IP sumber—informasi yang secara langsung dapat memverifikasi konsistensi keputusan klasifikasi terhadap nilai metrik yang tercatat.

Analisis dilakukan dengan memuat berkas log ke dalam Pandas DataFrame sehingga rekapitulasi dan visualisasi dapat dilakukan secara sistematis. Melalui pendekatan ini, log forensik tidak hanya berfungsi sebagai bukti digital pasif, tetapi juga dapat digunakan secara aktif untuk merekonstruksi garis waktu (timeline) kejadian serangan, memverifikasi konsistensi nilai metrik terhadap keputusan klasifikasi, serta mendukung proses audit keamanan dan investigasi pasca-insiden sesuai prinsip network forensics.

4.6 Validasi Generalisasi dengan Dataset CIC-DDoS2019

Untuk menguji generalisasi sistem pada lingkungan berbeda, dilakukan validasi pada empat berkas dataset CIC-DDoS2019 (DrDoS_DNS, DrDoS_NTP, Syn, UDPLag) yang secara keseluruhan mencakup lebih dari 7,8 juta aliran trafik, dengan θ dihitung ulang dari karakteristik BENIGN masing-masing berkas. Hasil evaluasi disajikan pada Tabel 5.

Dataset	Akurasi	Precision	Recall	F1
DrDoS_DNS	99,93%	99,94%	99,98%	99,96%
DrDoS_NTP	98,83%	99,07%	99,75%	99,41%
Syn	89,18%	99,98%	89,20%	94,28%
UDPLag	73,46%	98,83%	74,03%	84,65%
Rata-rata	90,35%	99,45%	90,74%	94,58%

Tabel 5. Hasil Evaluasi Sistem pada Empat Dataset CIC-DDoS2019

Sistem mencapai rata-rata akurasi 90,35%, precision 99,45%, recall 90,74%, dan F1-score 94,58% pada keempat dataset, dengan performa terbaik pada serangan amplification (DrDoS_DNS 99,93%; DrDoS_NTP 98,83%) dan performa terendah pada UDPLag (73,46%) akibat volume serangan yang tidak sederas serangan flood lain sehingga sebagian polanya menyerupai trafik normal.

Nilai False Positive Rate pada pengujian dataset CIC-DDoS2019 (berkisar 78% hingga 81%) perlu dimaknai secara hati-hati. Seluruh berkas yang diuji memiliki komposisi sangat tidak seimbang: trafik normal (BENIGN) hanya berkisar 0,03% hingga 1,2% dari total aliran, sehingga sejumlah kecil kesalahan klasifikasi menghasilkan persentase FPR yang tinggi secara proporsional. Dengan demikian, FPR tinggi pada pengujian ini merupakan konsekuensi komposisi dataset yang didominasi serangan, bukan indikasi lemahnya kemampuan sistem membedakan trafik normal; hal ini diperkuat oleh precision yang tetap di atas 98% pada seluruh berkas serta FPR rendah pada kelas serangan di data primer.

4.7 Pembahasan

Hasil pengujian menjawab kedua rumusan masalah penelitian. Pertama, sistem terbukti mampu mengklasifikasikan trafik metadata terenkripsi ke dalam tiga kelas tanpa dekripsi payload, dengan pola metrik yang konsisten terhadap karakteristik teoritis: serangan flood ditandai PPS tinggi dan entropi IP sumber mendekati nol, sedangkan Port Scanning ditandai lonjakan entropi Port tujuan dan jumlah Port unik. Kedua, efektivitas deteksi bervariasi signifikan antar kelas ancaman; recall deteksi DDoS/DoS yang lebih rendah (55,32%) dibandingkan Port Scanning (95,65%) bukan disebabkan oleh kelemahan algoritma klasifikasi, melainkan oleh kondisi jaringan pengujian: penyedia layanan VPS menerapkan mitigasi DDoS pada level infrastruktur sehingga sebagian volume serangan flood telah diredam sebelum mencapai server, sementara Port Scanning yang bervolume rendah tidak memicu mitigasi tersebut dan terekam sepenuhnya oleh sistem. Temuan ini konsisten dengan pengamatan pada penelitian deteksi intrusi berbasis IDS terhadap serangan DDoS lambat (slow HTTPS), yang juga menekankan pentingnya mempertimbangkan lapisan mitigasi eksternal dalam menginterpretasikan hasil deteksi berbasis volume [18].

Nilai FPR yang rendah pada kelas serangan (2,69% untuk DDoS/DoS dan 0% untuk Port Scanning) menunjukkan sistem jarang salah menuduh trafik sebagai serangan, sedangkan FPR pada kelas Normal (31,43%) sebagian besar berasal dari lonjakan trafik wajar yang sesaat melewati threshold—sebuah keterbatasan yang dapat diperbaiki melalui baseline yang lebih representatif pada penelitian lanjutan. Konsistensi performa antara pengujian langsung dan validasi dataset publik independen (precision di atas 98% pada seluruh berkas CIC-DDoS2019) memperkuat kesimpulan bahwa pendekatan multi-metric fusion memiliki kemampuan generalisasi yang baik terhadap beragam varian serangan flood di luar lingkungan pengujian utama, sekaligus menjadi kontribusi tambahan yang memberikan

pemahaman realistis tentang perilaku sistem deteksi pada lingkungan produksi yang telah dilindungi mitigasi berlapis.

Dibandingkan dengan penelitian terdahulu, temuan ini menegaskan sekaligus memperluas hasil yang ada. Efektivitas kombinasi metrik yang diperoleh sejalan dengan Wang dkk. [7] yang melaporkan peningkatan akurasi deteksi DDoS melalui multi-metric fusion, namun penelitian ini memperluas cakupannya dengan membuktikan bahwa kerangka fusi yang sama dapat mendeteksi Port Scanning secara simultan—aspek yang belum ditangani pada [5], [7]. Kinerja jalur entropi konsisten dengan temuan Li dkk. [6] dan Solichin–Nugroho [11] bahwa perubahan entropi merupakan indikator kuat serangan flooding, sedangkan kinerja jalur Port Scanning (precision 100%) mengonfirmasi klaim Riadi dkk. [12] dan Khalil dkk. [3] bahwa distribusi Port tujuan dan pola IAT pada metadata cukup diskriminatif tanpa inspeksi payload. Berbeda dengan Murti dkk. [8] yang menempatkan forensik sebagai proses analisis terpisah pasca-insiden, sistem ini menghasilkan bukti digital secara inline pada saat deteksi, sehingga rantai kejadian—deteksi, mitigasi, dan pencatatan—terdokumentasi dalam satu alur yang dapat diaudit.

Implikasi teoretis dari temuan ini adalah bahwa penggabungan dimensi temporal dan statistik pada metadata terbukti saling melengkapi: metrik timing menangkap intensitas serangan, sedangkan entropi menangkap struktur distribusinya, sehingga dua jenis ancaman dengan karakteristik berlawanan (flood bervolume tinggi vs. scanning bervolume rendah) dapat dipisahkan dalam satu kerangka klasifikasi. Implikasi praktisnya, sistem dapat diadopsi sebagai modul deteksi dini dan forensik pada infrastruktur Server Web produksi tanpa mengorbankan privasi pengguna, karena seluruh analisis dilakukan tanpa dekripsi payload.

Beberapa keterbatasan tetap perlu diperhatikan: skala simulasi DDoS jauh lebih kecil dibandingkan serangan botnet nyata yang melibatkan ribuan hingga jutaan alamat IP; kondisi jaringan internet publik yang dinamis (variasi latency, jitter, dan packet loss) berpotensi memerlukan kalibrasi ulang threshold adaptif; pengujian dilakukan pada satu penyedia VPS dan satu konfigurasi Server Web sehingga belum merepresentasikan seluruh kemungkinan infrastruktur; dan validasi CIC-DDoS2019 pada berkas yang didominasi trafik serangan (>99%) membuat nilai FPR pada pengujian tersebut kurang representatif untuk menilai perilaku sistem terhadap trafik normal.

5. KESIMPULAN

1. Sistem deteksi multi-metric fusion berbasis rule-based berhasil dirancang dan diimplementasikan untuk mengklasifikasikan trafik metadata terenkripsi HTTPS/TLS ke dalam kelas Normal, DDoS, dan Port Scanning tanpa dekripsi payload, dilengkapi mitigasi otomatis Iptables dan log forensik JSON.
2. Evaluasi pada 233 window trafik menghasilkan akurasi keseluruhan 88,41%; deteksi Port Scanning mencapai precision 100% dan recall 95,65%, sedangkan deteksi DDoS/DoS memperoleh precision 83,87% dan recall 55,32% sebagai konsekuensi mitigasi pada level penyedia layanan, bukan kelemahan algoritma.
3. Validasi pada empat berkas dataset publik CIC-DDoS2019 menghasilkan rata-rata akurasi 90,35% dan precision 99,45%, mengonfirmasi kemampuan generalisasi sistem pada varian serangan flood di luar lingkungan pengujian utama.
4. Penelitian lanjutan disarankan mengarah pada pengujian skala serangan yang lebih besar, mekanisme kalibrasi ulang threshold adaptif, serta kombinasi pendekatan rule-based dengan machine learning untuk menangani pola serangan low-rate/slow attacks.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Jurusan Informatika, Fakultas Teknik, Universitas Halu Oleo atas dukungan fasilitas penelitian, kepada tim penguji — Bapak Muh. Yamin, Bapak La Surimi, dan Bapak Asa Hari Wibowo — atas saran dan masukan yang berharga dalam penyempurnaan penelitian ini, serta kepada seluruh pihak yang telah memberikan bimbingan selama penelitian ini berlangsung.

DAFTAR PUSTAKA

[1] J. Mirkovic, P. Reiher, and B. Hall, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, 2004.

[2] C. Fu, Q. Li, and K. Xu, "Detecting unknown encrypted malicious traffic in real time via flow interaction graph analysis," in Proc. 30th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2023.

[3] I. Khalil, L. Gao, and T. Yu, "Encrypted traffic analysis for port scan detection using flow-level features," IEEE Access, vol. 11, pp. 45123–45136, 2023.

[4] O. A. Ticleanu, T. Popa, D. I. Hunyadi, and N. Constantinescu, "Detecting encrypted and unencrypted network data using entropy analysis and confidence intervals," Entropy, vol. 25, no. 3, 2023.

[5] J. Wang, L. Wang, and R. Wang, "MFFLR-DDoS: An encrypted LR-DDoS attack detection method based on multi-granularity feature fusions in SDN," Math. Biosci. Eng., vol. 21, no. 3, 2024.

[6] Y. Li, Z. Chen, and H. Wang, "Entropy-based anomaly detection for encrypted network traffic," IEEE Access, vol. 11, 2023.

[7] X. Wang, J. Liu, and Y. Zhang, "Multi-metric fusion approach for DDoS detection in encrypted networks," Future Gener. Comput. Syst., vol. 149, pp. 215–227, 2024.

[8] R. H. W. Murti, I. Riadi, N. Anwar, and T. Ismail, "Forensik jaringan terhadap serangan DDoS menggunakan metode Network Forensic Development Life Cycle," J. Sarjana Tek. Inform., vol. 11, no. 3, p. 107, 2023.

[9] W. Shbair, T. Cholez, and J. Francois, "Leveraging traffic metadata for encrypted traffic analysis," Comput. Netw., vol. 227, p. 109723, 2023.

[10] Q. Tian and S. Miyata, "A DDoS attack detection method using conditional entropy based on SDN traffic," Internet of Things, vol. 4, no. 2, pp. 95–111, 2023.

[11] 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. 461–474, 2024.

[12] I. Riadi, R. Umar, and A. Sugandi, "Deteksi port scanning menggunakan analisis statistik metadata trafik jaringan," J. Teknol. Inf. dan Ilmu Komput., vol. 9, no. 4, pp. 123–132, 2022.

[13] A. Shafiyyah, G. F. Nama, and R. A. Pradipta, "Implementasi Wazuh menggunakan metode PPDIOO di sistem keamanan jaringan PSDKU Universitas Lampung Waykanan sebagai deteksi dan respon serangan siber," JITET (Jurnal Informatika dan Teknik Elektro Terapan), vol. 12, no. 2, pp. 970–976, 2024.

[14] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2023.

[15] W. Stallings, Network Security Essentials: Applications and Standards, 7th ed. Pearson, 2023.

[16] A. Z. Mardiansyah, Y. M. Abdussyakur, and A. H. Jatmika, "Optimasi Port Knocking dan Honeypot menggunakan Iptables sebagai keamanan jaringan pada server," JTIKA, vol. 3, no. 2, 2021.

[17] IPSSJ, "Kebocoran data dan Distributed Denial of Service (DDoS) dalam cloud computing: A systematic literature review," Integr. Perspect. Soc. Sci. J., vol. 6, no. 1, pp. 45–60, 2025.

[18] Restikom, "Implementasi IDS untuk deteksi serangan DDoS slow HTTPS," J. Riset Teknol. Inf. dan Komun., vol. 7, no. 1, pp. 12–22, 2025.