Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

IMPLEMENTASI WEBSITE MONITORING LOG JARINGAN UNTUK IDENTIFIKASI SERANGAN DDOS

Alvin Hafiz[1], Dedy Kiswanto[2], Rangga Wahyu Pratama[3], Peter Tymothy Hutabarat[4]

[1234,] Program Studi Ilmu Komputer, FMIPA, Universitas Negeri Medan

Jl. William Iskandar Ps. V, Kenangan Baru, Kec. Percut Sei Tuan Kabupaten Deli Serdang, Sumatera Utara 20221

[1] alvinhafiz1145@gmail.com, [2] dedykiswanto@unimed.ac.id, [3] ranggawahyupratama386@gmail.com, [4] petertymotyhutabarat08@gmail.com

Abstract

Distributed Denial-of-Service (DDoS) attacks pose a serious threat to the availability of web-based services, especially in academic institutions relying heavily on online infrastructure. This research aims to implement a web-based network log monitoring system to detect and respond to DDoS attacks in real-time, thereby enhancing overall network security posture. The methodology involves analyzing Apache access logs on an Ubuntu 24.04 server to identify suspicious IP addresses exceeding a specific request per minute threshold. Upon detection, the system automatically blocks the offending IP via iptables for 10 minutes and sends an immediate email notification to the administrator. The user interface is developed using Flask, Chart.js, and Tailwind CSS to provide interactive data visualization. Testing was conducted using Apache Bench from a Kali Linux machine to simulate realistic DDoS attack scenarios. The results demonstrate that the system accurately detects all simulated attacks with 100% accuracy, where all 161 log entries were classified as attacks matching actual labels without any prediction errors. Server load graphs indicate request spikes exceeding 5,000 requests per minute, far surpassing the set threshold of 5 requests per minute. The system successfully updates the dashboard within seconds, blocks attacker IPs effectively, and sends timely email notifications. This solution significantly improves early detection capabilities and reduces manual monitoring burdens. However, the system currently uses a static threshold and does not support encrypted HTTPS traffic. This research contributes a practical and affordable integrated monitoring tool for small-to-medium organizations in network attack mitigation.

Keywords : *Ddos, Network Log Monitoring, Network Security, Iptables, Attack Detection*

Abstrak

Serangan Distributed Denial-of-Service (DDoS) merupakan ancaman serius terhadap ketersediaan layanan berbasis web, terutama di lingkungan institusi akademik yang bergantung pada infrastruktur daring. Penelitian ini bertujuan mengimplementasikan sistem monitoring log jaringan berbasis website untuk mendeteksi dan merespons serangan DDoS secara real-time guna meningkatkan keamanan jaringan. Metode penelitian melibatkan analisis log akses Apache pada server Ubuntu 24.04 untuk mengidentifikasi alamat IP mencurigakan yang melebihi ambang batas permintaan per menit. Ketika terdeteksi, sistem secara otomatis memblokir IP tersebut melalui iptables selama 10 menit dan mengirim notifikasi email kepada administrator. Antarmuka pengguna dikembangkan menggunakan Flask, Chart.js, dan Tailwind CSS untuk visualisasi data interaktif. Pengujian dilakukan dengan Apache Bench dari mesin Kali Linux untuk mensimulasikan serangan DDoS. Hasil penelitian menunjukkan sistem mampu mendeteksi semua serangan simulasi secara akurat dengan tingkat akurasi 100%, dimana seluruh

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

161 entri log diklasifikasikan sebagai serangan sesuai label aktual tanpa kesalahan prediksi. Grafik beban server menunjukkan lonjakan permintaan hingga lebih dari 5.000 request per menit, jauh melebihi ambang batas 5 request per menit yang ditetapkan. Sistem berhasil memperbarui dashboard dalam hitungan detik, memblokir IP penyerang, serta mengirim notifikasi email tepat waktu. Solusi ini meningkatkan kemampuan deteksi dini dan mengurangi beban pemantauan manual secara signifikan. Meskipun demikian, sistem masih menggunakan threshold statis dan belum mendukung lalu lintas terenkripsi HTTPS. Penelitian ini memberikan kontribusi berupa alat monitoring terpadu yang praktis dan terjangkau bagi organisasi skala kecil-menengah dalam mitigasi serangan jaringan.

Kata Kunci : *Ddos, Monitoring Log Jaringan, Keamanan Jaringan, Iptables, Deteksi Serangan*

1. PENDAHULUAN

Perkembangan layanan digital dan meningkatnya tingkat konektivitas di berbagai institusi mulai dari perguruan tinggi, pemerintahan, hingga perusahaan swasta mendorong ketergantungan yang semakin tinggi terhadap infrastruktur jaringan [1]. Setiap institusi mengelola jaringannya secara berbeda sesuai kebutuhan, skala, dan karakteristik layanannya. Bahkan dalam satu jaringan, berbagai segmen sering memiliki aturan khusus untuk mengatur arus lalu lintas data demi menjaga efisiensi dan keamanan [2]. Seiring dengan kompleksitas arsitektur sistem informasi modern, aspek keamanan jaringan menjadi semakin krusial karena rentan terhadap serangan siber [3]. Keamanan tersebut berperan penting dalam menjaga integritas, validitas, serta ketersediaan data yang digunakan oleh pengguna, sehingga kerentanan kecil sekalipun dapat dimanfaatkan pihak tidak sah untuk mengganggu operasional atau bahkan mencuri data sensitif [4][5].

Salah satu ancaman yang paling merusak dalam keamanan jaringan adalah serangan Distributed Denial-of-Service (DDoS) [6]. Serangan ini berupaya membuat layanan tidak tersedia dengan membanjiri server menggunakan permintaan dalam jumlah besar [7]. Sifatnya yang terdistribusi sering memanfaatkan botnet atau perangkat "zombie" menjadikan DDoS sulit dideteksi maupun dilacak [8]. Teknik seperti IP spoofing turut memperburuk situasi karena dapat menyamarkan identitas pelaku [9]. Selain itu, banyaknya sistem yang memiliki celah keamanan mempermudah penyerang melakukan eksploitasi untuk melancarkan serangan DDoS [10]. Akibatnya, gangguan yang ditimbulkan tidak hanya bersifat teknis, tetapi juga berdampak pada kerugian finansial serta reputasi penyedia layanan [11].

Untuk mengatasi ancaman tersebut, pemantauan log jaringan menjadi salah satu pendekatan penting dalam mendeteksi anomali lalu lintas yang berpotensi mengindikasikan serangan DDoS. Monitoring jaringan berperan dalam memastikan layanan tetap stabil dan berkinerja baik [12]. Log jaringan menyimpan informasi penting seperti alamat IP sumber, waktu akses, jenis protokol, serta volume lalu lintas, sehingga dapat dianalisis untuk mengidentifikasi pola aktivitas yang tidak wajar. Namun, integritas log harus dijaga melalui mekanisme keamanan yang memadai agar tidak dapat dimanipulasi oleh pihak tidak sah, karena akurasi data sangat menentukan kualitas analisis keamanan [13][14].

Berdasarkan kondisi tersebut, penelitian ini bertujuan mengimplementasikan website monitoring log jaringan yang mampu mengidentifikasi serangan DDoS secara real-time melalui analisis pola lalu lintas jaringan. Sistem ini diharapkan dapat meningkatkan deteksi dini terhadap ancaman, memberikan visualisasi log yang informatif, serta membantu administrator jaringan dalam mengambil keputusan cepat untuk memitigasi dampak serangan sebelum mengganggu ketersediaan layanan.

2. TINJAUAN PUSTAKA

Monitoring berbasis log jaringan merupakan salah satu pendekatan yang banyak digunakan dalam mendeteksi anomali lalu lintas, termasuk serangan Distributed Denial-of-Service (DDoS). Penelitian oleh [15] membahas implementasi analisis log menggunakan Wireshark untuk mendeteksi anomali lalu lintas yang mengindikasikan serangan DDoS. Pendekatan

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

tersebut menunjukkan bahwa monitoring log dapat membantu mengidentifikasi pola serangan berdasarkan karakteristik paket dan volume lalu lintas. Kelebihan penelitian ini terletak pada pemanfaatan log analisis yang komprehensif, namun teknik mitigasi yang digunakan masih bersifat manual sehingga tidak dapat memberikan deteksi maupun respons otomatis secara real-time.

Penelitian lain oleh [16] mengusulkan mekanisme deteksi DDoS pada arsitektur Software Defined Network (SDN) menggunakan Snort IDS sebagai alat deteksi dan iptables untuk mitigasi. Hasil penelitian menunjukkan akurasi deteksi yang tinggi, dengan waktu respons sangat cepat. Meskipun demikian, pendekatan ini terbatas pada lingkungan SDN dan belum menyediakan visualisasi terintegrasi ataupun dashboard interaktif yang membantu administrator memahami pola serangan secara langsung. Selain itu, Snort masih mengandalkan aturan statis sehingga respons terhadap serangan baru yang bersifat dinamis dapat kurang optimal.

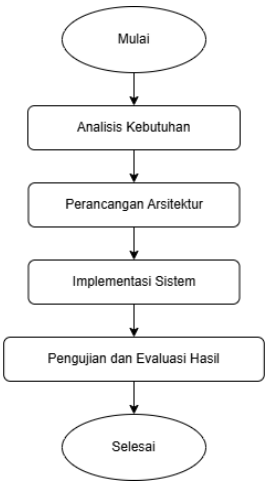
Sementara itu, [17] menyoroti kerentanan website institusi pendidikan terhadap lonjakan akses dan serangan DDoS. Penggunaan penetration testing dan analisis log server membantu mengidentifikasi kelemahan kapasitas jaringan. Namun, penelitian tersebut belum mengintegrasikan sistem monitoring otomatis yang mampu menampilkan data secara real-time atau mengirimkan peringatan dini kepada administrator. Pendekatan yang digunakan masih lebih berfokus pada pengujian kerentanan, bukan deteksi dan mitigasi berkelanjutan melalui dashboard terpusat.

Dari ketiga penelitian tersebut, terlihat bahwa pendekatan deteksi serangan DDoS melalui analisis log, Intrusion Detection System (IDS), maupun pengujian penetrasi masih cenderung terpisah, bersifat manual, atau minim visualisasi interaktif, sehingga kurang efektif untuk respons cepat, khususnya di lingkungan institusi pendidikan dengan pola lalu lintas khas. Menjawab keterbatasan tersebut, penelitian ini mengusulkan solusi terpadu berupa website monitoring log jaringan yang mengintegrasikan dashboard interaktif, deteksi anomali berbasis threshold, visualisasi metrik secara real-time, serta mekanisme respons otomatis berupa notifikasi dan pemblokiran IP. Dengan pendekatan holistik ini, sistem diharapkan tidak hanya menutup celah penelitian sebelumnya, tetapi juga menyediakan alat yang praktis, responsif, dan mudah diadopsi pada jaringan berskala kecil hingga menengah.

3. METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Metode penelitian ini disusun untuk menjelaskan secara sistematis tahapan-tahapan dalam perancangan, pengembangan, dan pengujian website monitoring log jaringan yang bertujuan mengidentifikasi serangan Distributed Denial of Service (DDoS). Pendekatan yang digunakan bersifat eksperimental, dengan tujuan mengimplementasikan sistem pemantauan berbasis web yang mampu menganalisis log lalu lintas jaringan secara real-time untuk mendeteksi indikasi serangan DDoS.



Gambar 1. Diagram Alur Penelitian

3.2. Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk mengidentifikasi fungsi-fungsi inti yang diperlukan dalam sistem monitoring. Kebutuhan fungsional mencakup kemampuan membaca dan memproses log Apache secara real-time, mendeteksi anomali berbasis threshold, menampilkan visualisasi data melalui dashboard, menyimpan riwayat aktivitas ke dalam basis data, serta melakukan respons otomatis berupa notifikasi dan pemblokiran IP.

Kebutuhan non-fungsional mencakup keandalan sistem, waktu respons deteksi, keamanan autentikasi pengguna, serta

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

kompatibilitas dengan lingkungan server. Pada tahap ini ditetapkan pula parameter *threshold* sebagai batas jumlah permintaan per menit yang dianggap mencurigakan. Penetapan threshold didasarkan pada observasi lalu lintas normal di server uji, serta mengacu pada prinsip *rate limiting* untuk mendeteksi lonjakan permintaan yang tidak wajar. Parameter threshold ini dapat disesuaikan secara dinamis, tetapi pada penelitian ini digunakan nilai statis untuk konsistensi pengujian.

3.3. Perancangan Arsitektur

Perancangan arsitektur dilakukan untuk menyusun hubungan antar komponen sistem, yang meliputi sumber data log, mesin pemrosesan, dan antarmuka pengguna. Komponen utama sistem meliputi:

1. Sumber Data Log, yaitu file *access.log* dari Apache yang menjadi input utama pemantauan.
2. Mesin Pemrosesan, berupa aplikasi backend Python (Flask) yang melakukan parsing log, analisis pola permintaan, deteksi anomali, penyimpanan data ke SQLite, serta eksekusi respons otomatis.
3. Dashboard Monitoring, yaitu antarmuka web yang menampilkan grafik real-time, statistik harian, log historis, serta informasi serangan dalam format yang mudah dipahami.

Perancangan menggunakan pendekatan modular agar tiap fungsi seperti deteksi, notifikasi, dan pemblokiran dapat diuji dan dikembangkan secara terpisah. Pada tahap ini juga didefinisikan alur data yang menghubungkan proses pembacaan log analisis visualisasi dan respons otomatis.

3.4. Implementasi Sistem

Implementasi dilakukan berdasarkan rancangan arsitektur yang telah ditetapkan. Backend dikembangkan menggunakan Python dan modul Flask dengan tugas utama membaca log secara *streaming*, menghitung jumlah permintaan per IP per menit, serta membandingkannya dengan threshold yang telah ditentukan. Jika terdeteksi anomali, sistem mencatat aktivitas ke basis data, memperbarui dashboard, mengirimkan notifikasi email, dan memblokir IP melalui *iptables*.

Antarmuka pengguna dibangun menggunakan HTML, Tailwind CSS, dan Chart.js untuk menampilkan grafik real-time dan statistik harian. Seluruh komponen dijalankan di lingkungan server Ubuntu 24.04, sementara mesin penyerang menggunakan Kali Linux. Penjelasan teknis seperti perintah *iptables*, konfigurasi SMTP, atau pengaturan virtual environment disederhanakan dalam metodologi agar tidak menyerupai panduan teknis.

3.5. Pengujian dan Evaluasi Hasil

Pengujian dilakukan dengan melakukan simulasi serangan DDoS menggunakan Apache Bench (ab) dan Slowloris. Parameter pengujian meliputi jumlah permintaan, tingkat koneksi simultan, dan durasi serangan. Evaluasi meliputi empat aspek:

1. Akurasi Deteksi, yaitu kemampuan sistem mengidentifikasi IP yang melebihi threshold secara konsisten.
2. Waktu Respons, yaitu selang waktu antara terjadinya serangan dan munculnya notifikasi atau pembaruan dashboard.
3. Keandalan Penyimpanan Data, melalui pemeriksaan integritas log pada basis data SQLite.
4. Efektivitas Respons Otomatis, yaitu keberhasilan pemblokiran IP dan pengiriman notifikasi secara real-time.

Data hasil pengujian dianalisis secara deskriptif, kemudian dibandingkan dengan perilaku yang diharapkan berdasarkan teori deteksi anomali pada lalu lintas jaringan.

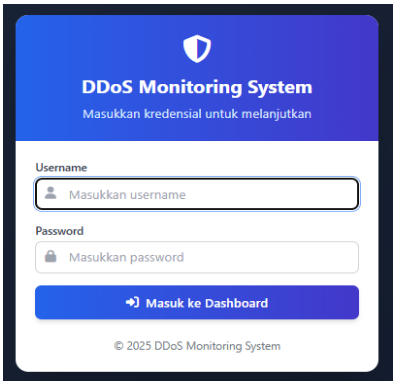
4. HASIL DAN PEMBAHASAN

4.1. Pengimplementasian Sistem

Sistem ini diimplementasikan dalam lingkungan pengujian yang terdiri dari Ubuntu 24.04 sebagai server target dan Kali Linux sebagai mesin penyerang, dengan arsitektur yang berbasis pada log akses Apache. Inti dari mekanisme deteksi terletak pada kemampuan sistem untuk membaca file /var/log/apache2/access.log secara *real-time* melalui skrip Python yang secara terus-menerus menganalisis jumlah permintaan (*request*) yang berasal dari setiap alamat IP dalam rentang waktu satu menit. Jika suatu IP melebihi ambang batas yang telah ditentukan, sistem

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

mengidentifikasinya sebagai potensi serangan DDoS.



Gambar 2. Tampilan Halaman Login

Sebagai lapisan keamanan tambahan, akses ke dashboard pemantauan dilindungi melalui mekanisme autentikasi. Pengguna harus melewati halaman login terlebih dahulu sebelum dapat mengakses dashboard utama. Pendekatan ini memastikan bahwa hanya pihak yang memiliki kredensial sah seperti administrator jaringan—yang dapat melihat data sensitif atau mengelola sistem, sehingga menjaga integritas dan kerahasiaan informasi pemantauan.

Gambar 3. Tampilan Awal Halaman Dashboard

Setelah berhasil login, pengguna akan diarahkan ke dashboard utama yang dirancang untuk memantau aktivitas jaringan dan mendeteksi serangan DDoS secara *real-time*. Tampilan dashboard dibuat bersih, informatif, dan fungsional, dengan fokus utama pada visualisasi data yang mudah dipahami. Bagian paling dominan adalah grafik "Monitoring Real-Time", yang menampilkan jumlah *request* per menit berdasarkan data dari 5 detik terakhir. Di bawahnya, terdapat empat panel statistik harian: "Total Request Hari Ini", "Serangan Terdeteksi", "Rata-rata RPM (Request per Menit)", dan "Serangan Terakhir". Lebih lanjut, pada bagian bawah dashboard disajikan grafik batang "Request per Jam (24 Jam Terakhir)" untuk memberikan gambaran tren aktivitas jaringan dalam jangka waktu lebih panjang. Secara keseluruhan, antarmuka ini memungkinkan administrator untuk dengan cepat menilai kesehatan server dan mengenali anomali lalu lintas yang mencurigakan.

Selain kemampuan deteksi dan visualisasi, sistem juga dilengkapi fitur respons otomatis. Ketika suatu alamat IP terdeteksi melebihi ambang batas permintaan per menit, sistem secara langsung memblokir IP tersebut selama 10 menit menggunakan perintah iptables. Langkah ini bertujuan untuk memutus alur serangan dan melindungi server dari beban berlebih yang dapat menyebabkan gangguan layanan. Sebagai bentuk peringatan dini, administrator juga menerima notifikasi email secara *real-time* setiap kali serangan terdeteksi, sehingga memungkinkan tindakan lanjutan jika diperlukan.

4.2. Pengujian Sistem

Pengujian sistem dilakukan secara eksperimental dengan mensimulasikan serangan *Distributed Denial-of-Service* (DDoS) menggunakan *Apache Bench* (ab) dari mesin Kali Linux ke server Ubuntu 24.04 yang menjalankan sistem monitoring yang dikembangkan. Skenario pengujian dirancang untuk mengevaluasi tiga aspek utama yakni akurasi deteksi, respons otomatis, dan konsistensi visualisasi data.

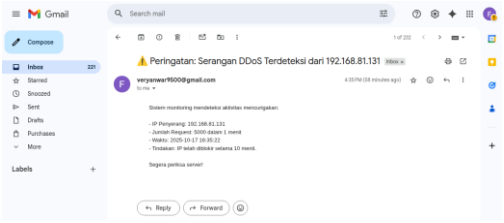
Gambar 4. Eksekusi Serangan DDoS

Pada tahap awal pengujian, terminal Kali Linux menjalankan perintah ab -n 5000 -c 50 http://192.168.81.128/, yang berarti mengirimkan 5.000 permintaan HTTP secara paralel dengan 50 koneksi simultan ke alamat IP server target (192.168.81.128). Simulasi ini merepresentasikan pola serangan DDoS ringan namun cukup signifikan untuk menguji kemampuan sistem dalam mendeteksi lonjakan lalu lintas abnormal.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

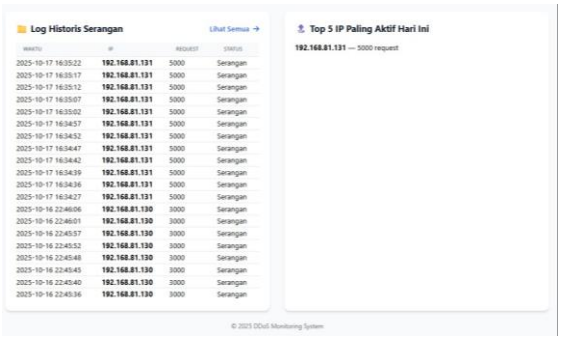
Gambar 5. Aktivitas Serangan DDoS

Saat serangan berlangsung, sistem monitoring langsung menanggapi secara *real-time*. Di antarmuka web, grafik "Monitoring Real-Time" menunjukkan lonjakan dramatis pada jumlah request per menit dari nilai nol menjadi lebih dari 5.000 dalam waktu singkat, mengindikasikan serangan DDoS sedang berlangsung. Status di pojok kanan atas langsung berubah menjadi "⚠ SERANGAN TERDETEKSI!" dengan latar belakang oranye, memberikan peringatan visual yang jelas kepada administrator. Panel statistik di bawahnya memperkuat temuan ini: "Total Request Hari Ini" mencatat angka 5.000, "Serangan Terdeteksi" menampilkan angka 1 (menandakan satu IP aktif yang melebihi threshold), dan "Rata-rata RPM" melonjak ke 83.33, yang menunjukkan beban server sangat tinggi. Panel "Serangan Terakhir" juga diperbarui dengan waktu terjadinya serangan terkini, yaitu 10/17/2025, 4:34:27 PM. Di bagian bawah, grafik "Request per Jam (24 Jam Terakhir)" menyoroti puncak aktivitas yang tajam pada pukul 16:00, sejalan dengan waktu serangan.



Gambar 6. Notifikasi Serangan DDoS via Gmail

Tak hanya memberikan peringatan visual, sistem juga mengaktifkan respons otomatis berupa notifikasi email yang dikirim melalui Gmail. Email ini dikirim oleh sistem ke alamat email pengguna dan berisi peringatan penting tentang serangan DDoS yang langsung menginformasikan sumber ancaman. Isi email secara rinci menyebutkan IP penyerang (192.168.81.131), jumlah request yang mencurigakan (5.000 dalam satu menit), waktu kejadian (2025-10-17 16:35:22), serta tindakan yang telah diambil oleh sistem yaitu pemblokiran IP tersebut selama 10 menit. Pesan penutup "Segera periksa server!" menambahkan urgensi bagi administrator untuk segera melakukan investigasi atau mitigasi lebih lanjut. Tampilan email yang jelas, terstruktur, dan informatif ini menunjukkan bahwa fitur notifikasi berfungsi dengan baik, memastikan bahwa tim keamanan dapat merespons ancaman secara cepat meskipun tidak sedang memantau dashboard secara langsung.



Gambar 7. Log Historis Serangan DDoS dan Daftar IP Aktif Teratas

Setelah simulasi selesai, sistem secara otomatis mencatat seluruh aktivitas serangan ke dalam log historis, yang ditampilkan dalam dua panel utama yaitu "Log Historis Serangan" dan "Top 5 IP Paling Aktif". Panel pertama menampilkan daftar kronologis dengan kolom waktu, alamat IP, jumlah *request*, dan status semua entri ditandai sebagai "Serangan". Data menunjukkan bahwa IP 192.168.81.131 melakukan serangan berulang dengan pola konsisten (misalnya, 5.000 *request* per sesi), mengindikasikan aktivitas terorganisir khas DDoS.

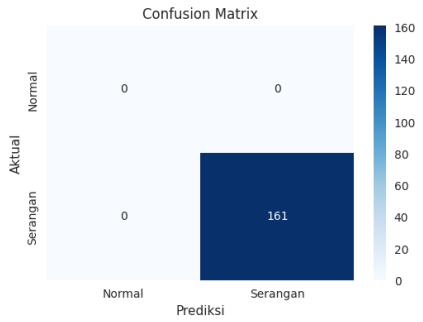
Sementara itu, panel "Top 5 IP Paling Aktif" menegaskan dominasi IP tersebut sebagai

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

sumber lalu lintas paling agresif, dengan kontribusi mencapai 5.000 *request* dalam satu sesi. Kedua panel ini tidak hanya berfungsi sebagai bukti forensik pasca-serangan, tetapi juga menjadi alat bantu yang efektif bagi administrator untuk mengidentifikasi, menganalisis, dan mengambil tindakan mitigasi terhadap sumber ancaman secara cepat dan akurat. Secara keseluruhan, hasil pengujian menunjukkan bahwa sistem monitoring mampu mendeteksi serangan DDoS secara akurat, memberikan respons otomatis yang efektif, serta menyajikan visualisasi data yang konsisten dan informatif semua dalam waktu nyata.

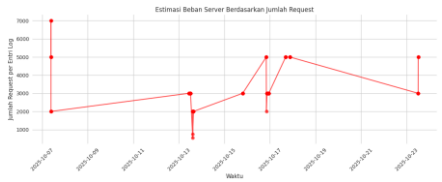
4.3. Evaluasi Performa Sistem

Evaluasi performa sistem dilakukan pasca-pengujian untuk mengukur efektivitas deteksi. Pada tahap ini, disajikan *Confusion Matrix* yang memetakan hubungan antara label aktual dan prediksi sistem, di mana nilai numerik menunjukkan jumlah entri pada masing-masing sel. Dari visualisasi, terlihat bahwa semua 161 entri log diklasifikasikan sebagai *Serangan* oleh sistem, dan semuanya sesuai dengan label aktual (*Serangan*), sehingga sel True Positive (TP) = 161, sedangkan sel False Positive (FP), False Negative (FN), dan True Negative (TN) semuanya bernilai 0.



Gambar 8. Confusion Matrix Sistem Klasifikasi

Hasil tersebut mengindikasikan bahwa sistem mencapai akurasi 100%, dengan False Positive Rate (FPR) = 0% dan False Negative Rate (FNR) = 0%, sebagaimana tercantum di atas gambar. Dengan kata lain, matriks ini merepresentasikan kemampuan sistem dalam mendeteksi serangan yang sudah diketahui sebagai serangan.



Gambar 9. Grafik Beban Server Selama Serangan DDoS

Selanjutnya, untuk bagian pola grafik dari beban proses server, terlihat adanya beberapa puncak tajam, di mana nilai RPM melonjak hingga lebih dari 5.000 request/menit. Lonjakan ini mengindikasikan beban server yang sangat tinggi, karena setiap request memerlukan alokasi sumber daya (CPU, memori, koneksi socket), dan pada tingkat 5.000 RPM (~83 RPS), server Apache tanpa optimasi akan mengalami peningkatan signifikan pada penggunaan CPU dan kemungkinan *connection queue overflow*. Selain itu, grafik juga menunjukkan fluktuasi berulang pada rentang waktu tertentu, yang mencerminkan pengujian berulang terhadap IP yang sama, sehingga memperkuat bahwa sistem mampu mendeteksi dan mencatat serangan berulang secara konsisten. Dengan demikian, meskipun grafik ini tidak menampilkan metrik hardware langsung, ia memberikan bukti kuat bahwa beban proses server mencapai tingkat kritis selama serangan, yang sejalan dengan respons sistem berupa pemblokiran IP dan notifikasi email menunjukkan bahwa deteksi dilakukan tepat pada saat beban maksimum terjadi.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian dan pembahasan, dapat disimpulkan bahwa sistem website monitoring log jaringan yang dikembangkan mampu mengidentifikasi serangan DDoS secara real-time dengan akurasi 100% melalui analisis pola lalu lintas berdasarkan jumlah request per menit serta memberikan respons otomatis berupa pemblokiran IP melalui iptables dan notifikasi email, di mana keunggulan sistem terletak pada integrasi deteksi, visualisasi dashboard yang intuitif, dan respons otomatis dalam satu platform yang mudah diakses untuk mendukung deteksi dini dan pengambilan keputusan cepat,

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

meskipun terdapat kelemahan pada ketergantungan threshold statis yang belum mampu menyesuaikan dinamika lalu lintas normal secara adaptif serta belum mendukung skenario serangan DDoS multi-vektor atau berbasis enkripsi (HTTPS), sehingga untuk penelitian lanjutan disarankan mengembangkan sistem dengan pendekatan machine learning untuk deteksi anomali adaptif, integrasi protokol HTTPS melalui parsing log SSL/TLS, dukungan pemantauan multi-server, serta peningkatan mekanisme notifikasi dengan platform tambahan seperti Telegram atau webhook guna meningkatkan akurasi, cakupan, dan skalabilitas dalam lingkungan jaringan yang lebih kompleks.

6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada rekan-rekan sejawat dan dosen pembimbing yang telah memberikan masukan konstruktif, saran berharga, serta bimbingan akademik selama proses pengembangan dan implementasi website monitoring log jaringan untuk identifikasi serangan DDoS. Tanpa kerja sama dan semangat kolaborasi tersebut, implementasi sistem ini tidak akan dapat terwujud dengan baik.

DAFTAR PUSTAKA:

[1] 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, doi: 10.25126/jtiik.938188.

[2] M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 4, pp. 244–247, 2021, doi: 10.32672/jnkti.v4i4.3098.

[3] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 6, no. 1, pp. 162–167, 2024, doi: 10.47233/jteksis.v6i1.1124.

[4] G. Pradita and A. Pramono, "Implementasi Monitoring Keamanan Jaringan Pada Server Ubuntu Menggunakan Snort Intrusion Detection Prevention System (Idps) Dan Telegram Bot Sebagai Media Notifikasi Di Pt Ss Utama," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 4, pp. 5827–5834, 2024, doi: 10.36040/jati.v8i4.10069.

[5] M. A. F. Tanjung and J. L. Ma'arif, Muhammad Fadhli Tamaela, "Literature Review Mekanisme Pertahanan Terhadap Serangan Distributed Denial Of Service (DDOS)," *J. Teknol. Inf.*, vol. 10, no. 2, 2024, [Online]. Available: https://ejournal.urindo.ac.id/index.php/TI/index

[6] S. Munawarah, Kurniabudi, and E. A. Winanto, "Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM) Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN)," *J. Inform. dan Rekayasa Komput.*, vol. 4, no. 1, pp. 982–990, 2024, [Online]. Available: http://ejournal.unama.ac.id/index.php/jakakom

[7] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 1, pp. 172–180, 2022, [Online]. Available: http://j-ptiik.ub.ac.id

[8] M. K. Harto and A. Basuki, "Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, pp. 1329–1333, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[9] M. Iqbal, Yuhandri, and S. Arlis, "Audit Keamanan Jaringan Komputer Server dari Serangan DDoS Menggunakan Snort Intrusion Detection System," *Indones. J. Comput. Sci.*, vol. 13, no. 5, pp. 8334–8348, 2024.

[10] F. Nisa and S. Ramadona, "Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 3, pp. 22–30, 2023, doi: 10.60083/jsisfotek.v5i3.269.

[11] D. Kiswanto, F. Ramadhani, N. M. Surbakti, and N. A. Nasution, "Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest," *Bull. Inf. Technol.*, vol. 6, no. 3, pp. 247–256, 2025, doi:

10.47065/bit.v5i2.2203.

[12] Irwansyah and S. Sitohang, "Monitoring Jaringan Mikrotik Menggunakan the Dude Dan Bot Telegram," *J. Comasie*, vol. 10, no. 2, pp. 111–120, 2024.

[13] N. T. Fadilla Inggriani, J. M. Parenreng, and M. Syahid Nur Wahid, "Implementasi Log Mikrotik Berbasis Database PostgreSQL dengan Teknologi Logging Syslog terhadap Serangan Brute Force," *JIMU J. Ilm. Multi Disiplin*, vol. 3, no. 1, pp. 76–85, 2025.

[14] Giovanni VictoAraya and S. Cahyono, "Implementasi Skema SecLaaS-RW dalam Membuat Aplikasi Secure Logging," *Info Kripto J. Keamanan Siber dan Kriptologi*, vol. 16, no. 3, pp. 85–94, 2022, doi: 10.56706/ik.v16i3.44.

[15] A. Rodhiyatun Nisa, A. D. Wijayanto, A. Prabudi Jaya Priana, and A. Setiawan, "Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website," *J. Internet Softw. Eng.*, vol. 1, no. 3, pp. 1–17, 2024, doi: 10.47134/pjise.v1i3.2612.

[16] D. Y. D. Pratiwi and R. Adrian, "Deteksi Dan Mitigasi Serangan Distributed Denial of Service Pada Software Defined Network," *J. Tek. Inform. dan Sist. Inf.*, vol. 10, no. 1, pp. 63–75, 2024, doi: 10.28932/jutisi.v10i1.6995.

[17] T. A. Madina and M. Fadhli, "Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 7, no. 6, pp. 1730–1736, 2024, doi: 10.32672/jnkti.v7i6.8273.