Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14324 p-ISSN : 2089-9424

Terbit : 12 Desember 2024

Integrasi Deep Packet Inspection dengan Intrusion Detection System (IDS) untuk Identifikasi Serangan DDoS dalam Jaringan Skala Besar

[1]Ahmad Rois Syujak, [2]Karno Diantoro, [3]Veronika Yuni T, [4]Ahmad Soderi, [5]Purwo Agus Sucipto
[1]Universitas Islam Negeri Salatiga, [2,4]STMIK Mercusuar, [3,5]Universitas Jayabaya

[1]ahmad.rois.syujak@uinsalatiga.ac.id, [2]karno@mercusuar.ac.id, [3]veronikayuni2020@gmail.com, [4]ahmad@mercusuar.ac.id, [5]purwoagussucipto@gmail.com

ABSTRAK

Perkembangan teknologi jaringan yang pesat menghadirkan tantangan baru dalam keamanan siber, terutama dalam mendeteksi dan mencegah serangan Distributed Denial of Service (DDoS) pada jaringan skala besar. Penelitian ini bertujuan untuk mengintegrasikan teknologi Deep Packet Inspection (DPI) dengan Intrusion Detection System (IDS) sebagai solusi inovatif dalam identifikasi dini serangan DDoS. Metode penelitian melibatkan pengembangan arsitektur sistem yang menggabungkan kemampuan analisis mendalam paket data melalui DPI dengan algoritme deteksi anomali pada IDS. Pengujian dilakukan pada lingkungan simulasi jaringan menggunakan dataset serangan DDoS yang umum digunakan, seperti CICDDoS2019. Hasil penelitian menunjukkan bahwa integrasi DPI dan IDS mampu meningkatkan tingkat deteksi serangan DDoS hingga 94,7% dengan tingkat false positive yang rendah. Sistem ini juga mampu memproses lalu lintas jaringan dengan throughput tinggi, menjadikannya efektif untuk implementasi pada jaringan skala besar. Penelitian ini memberikan kontribusi signifikan terhadap pengembangan sistem keamanan jaringan yang lebih adaptif dan efisien, khususnya dalam menghadapi ancaman serangan DDoS yang semakin kompleks. Rekomendasi untuk penelitian selanjutnya meliputi pengembangan sistem berbasis kecerdasan buatan untuk meningkatkan kemampuan prediktif dalam mendeteksi pola serangan baru.

Kata Kunci: Deep Packet Inspection, Intrusion Detection System, Serangan DDoS, Keamanan Jaringan.

PENDAHULUAN

Keamanan jaringan komputer telah menjadi salah satu isu paling krusial dalam era transformasi digital, terutama dengan meningkatnya penggunaan teknologi informasi di berbagai sektor. Jaringan skala besar, seperti yang dimiliki oleh perusahaan multinasional, penyedia layanan internet, dan instansi pemerintahan, menghadapi ancaman siber yang semakin kompleks. Salah satu ancaman paling merusak dan sulit dideteksi adalah serangan Distributed Denial of Service (DDoS). Serangan ini bertujuan untuk melumpuhkan sistem jaringan dengan membanjiri server target menggunakan lalu lintas data yang berlebihan, sehingga mengakibatkan gangguan serius pada layanan yang disediakan.

Metode konvensional dalam mendeteksi dan mencegah serangan DDoS sering kali menghadapi keterbatasan, terutama dalam menangani volume lalu lintas yang tinggi dan pola serangan yang semakin kompleks. Sistem Intrusion Detection System (IDS) telah lama digunakan untuk mendeteksi ancaman siber dengan memonitor dan menganalisis aktivitas jaringan. Namun, IDS tradisional memiliki keterbatasan dalam menganalisis konten data secara mendalam, yang menjadi penting dalam mengidentifikasi karakteristik spesifik dari serangan DDoS.

Di sisi lain, Deep Packet Inspection (DPI) menawarkan kemampuan untuk menganalisis

Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14324 p-ISSN : 2089-9424

isi setiap paket data yang melewati jaringan, termasuk header dan payload. DPI dapat mengidentifikasi pola lalu lintas yang mencurigakan berdasarkan karakteristik spesifik, sehingga memungkinkan deteksi ancaman yang lebih akurat. Namun, DPI sering kali dihadapkan pada tantangan kinerja ketika harus memproses volume data yang sangat besar secara real-time. Oleh karena itu, integrasi antara IDS dan DPI menjadi sebuah pendekatan potensial yang mampu menggabungkan keunggulan kedua teknologi tersebut.

Penelitian ini bertujuan untuk mengembangkan sistem yang mengintegrasikan DPI dengan IDS untuk mendeteksi serangan DDoS secara lebih efektif pada jaringan skala besar. Sistem ini dirancang untuk mampu memproses data secara efisien, mengidentifikasi pola anomali secara real-time, dan meminimalkan tingkat kesalahan deteksi (false positive). Pendekatan yang diusulkan diharapkan dapat memberikan solusi yang adaptif dan scalable untuk menangani ancaman siber yang terus berkembang. Penelitian ini memberikan kontribusi signifikan dalam dua aspek utama. Pertama, pengembangan model integrasi DPI dan IDS untuk deteksi serangan DDoS, yang memberikan tingkat akurasi lebih tinggi dibandingkan metode konvensional. Kedua, evaluasi performa sistem pada lingkungan simulasi jaringan skala besar untuk memastikan bahwa solusi yang diusulkan dapat diterapkan secara praktis. Dengan demikian, penelitian ini diharapkan dapat menjadi acuan bagi pengembangan sistem keamanan jaringan yang lebih efektif dan efisien di masa depan.

TINJAUAN PUSTAKA

Dalam penelitian ini, pendekatan integrasi Deep Packet Inspection (DPI) dan Intrusion Detection System (IDS) untuk mendeteksi serangan Distributed Denial of Service (DDoS) didasarkan pada tinjauan literatur yang relevan. Tinjauan ini mencakup konsep dasar, perkembangan terkini, serta kajian terhadap teknologi dan metode yang mendasari solusi yang diusulkan. (Khairunnisa et al., 2024)

Serangan DDoS merupakan salah satu ancaman paling signifikan dalam keamanan jaringan. DDoS dilakukan dengan membanjiri target dengan lalu lintas data dalam jumlah besar, sehingga menyebabkan gangguan layanan. Menurut (Sufardy & Widiasari, 2024), DDoS memiliki berbagai jenis, termasuk serangan berbasis aplikasi, protokol, dan volume. Kompleksitas serangan ini semakin meningkat seiring dengan perkembangan teknik seperti spoofing dan penggunaan botnet, yang membuat deteksi menjadi lebih sulit. (Harja et al., 2019)

IDS adalah sistem keamanan yang dirancang untuk mendeteksi aktivitas mencurigakan atau serangan dalam jaringan. IDS dapat dibagi menjadi dua kategori utama: Signature-Based Detection dan Anomaly-Based Detection. Sistem berbasis tanda tangan mengidentifikasi ancaman berdasarkan pola yang telah diketahui, sementara sistem berbasis anomali mendeteksi perilaku yang tidak biasa dibandingkan dengan profil normal. Menurut (Adzimi et al., 2024), IDS berbasis anomali memiliki potensi yang lebih besar untuk mendeteksi serangan baru, termasuk serangan DDoS yang sebelumnya tidak diketahui. Namun, kelemahan utama IDS tradisional adalah ketergantungan pada analisis header paket tanpa kemampuan untuk mengevaluasi isi data secara mendalam. Kelemahan ini mengurangi efektivitasnya dalam mendeteksi pola serangan kompleks yang terkandung dalam payload. (Farzaneh et al., 2024)

DPI adalah teknik analisis jaringan yang mampu memeriksa header dan payload dari setiap paket data. Teknologi ini memberikan wawasan mendalam tentang isi data, termasuk aplikasi, protokol, dan pola lalu lintas tertentu. Menurut (Hore et al., 2024), DPI sangat efektif dalam mengidentifikasi pola serangan tertentu, seperti serangan berbasis protokol dan aplikasi. Namun, implementasi DPI dalam skala besar menghadapi tantangan seperti latensi yang tinggi dan konsumsi sumber daya yang besar. Oleh karena itu, diperlukan optimasi dan integrasi dengan teknologi lain untuk meningkatkan efisiensi dan skalabilitasnya. (Shirsath et al., 2024)

Integrasi DPI dengan IDS menawarkan pendekatan yang lebih holistik untuk deteksi ancaman siber. DPI memberikan analisis mendalam terhadap isi data, sementara IDS menyediakan kerangka untuk mendeteksi pola anomali dalam lalu lintas jaringan. Kajian oleh (Yungaicela-Naula et al., 2022) menunjukkan bahwa integrasi kedua teknologi ini dapat meningkatkan akurasi deteksi serangan, termasuk serangan DDoS, dengan tetap menjaga performa sistem secara keseluruhan.

Penggunaan machine learning (ML) dalam deteksi ancaman siber telah menjadi fokus

Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14324 p-ISSN : 2089-9424

utama dalam beberapa tahun terakhir. Algoritma seperti Random Forest, Support Vector Machine (SVM), dan Neural Networks digunakan untuk mendeteksi pola serangan dengan tingkat akurasi tinggi. Menurut (Li et al., 2024), kombinasi ML dengan DPI dan IDS dapat mempercepat proses deteksi dan mengurangi tingkat kesalahan. Pengujian sistem keamanan pada jaringan skala besar memerlukan pertimbangan khusus, termasuk throughput, latency, dan scalability. Menurut laporan dari (Phu et al., 2023),solusi keamanan yang efektif harus mampu menangani lalu lintas data dalam volume tinggi tanpa mengorbankan akurasi deteksi atau kinerja jaringan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen kuantitatif, di mana pengujian dilakukan untuk mengukur efektivitas integrasi antara Deep Packet Inspection (DPI) dan Intrusion Detection System (IDS) dalam mendeteksi serangan Distributed Denial of Service (DDoS) di jaringan berskala besar. Penelitian ini dilakukan melalui beberapa tahapan sebagai berikut:

a. Studi Literatur :Mengumpulkan referensi terkait teknologi DPI, IDS, serta jenis dan karakteristik serangan DDoS. Memahami arsitektur jaringan skala besar dan parameter evaluasi performa IDS-DPI.
b. Perancangan Sistem: Merancang arsitektur sistem yang mengintegrasikan DPI dengan IDS. Menentukan perangkat lunak, algoritma, atau framework yang digunakan, misalnya Snort untuk IDS dan libdnet untuk DPI. Menentukan parameter evaluasi seperti true positive rate (TPR), false positive rate (FPR), latensi, dan throughput.
c. Implementasi : Membangun lingkungan pengujian (testbed) berupa simulasi jaringan berskala besar menggunakan alat seperti Mininet atau NS-3. Mengintegrasikan fungsi DPI dan IDS dalam sistem. Menyiapkan dataset serangan DDoS (misalnya, CIC-DDoS2019 atau CAIDA DDoS Dataset) sebagai input untuk simulasi.
d. Pengumpulan Data : Melakukan simulasi serangan DDoS pada jaringan. Mengukur respons sistem IDS-DPI terhadap serangan berdasarkan parameter yang telah ditentukan.
e. Analisis Data : Menganalisis performa integrasi DPI dan IDS berdasarkan hasil simulasi. Membandingkan hasil dengan pendekatan IDS tanpa integrasi DPI.
f. Validasi : Menggunakan teknik validasi silang atau pengujian pada dataset lain untuk memastikan keandalan hasil penelitian.

HASIL DAN PEMBAHASAN

Prototipe sistem yang mengintegrasikan DPI dengan IDS berhasil dikembangkan dengan menggunakan: IDS berbasis Snort yang dikonfigurasi untuk mendeteksi pola serangan jaringan. Modul DPI yang memeriksa isi payload paket menggunakan algoritma inspeksi berbasis string matching. Hasil implementasi menunjukkan bahwa sistem mampu bekerja pada lingkungan jaringan berskala besar dengan simulasi 500-1.000 node.

Pengujian dilakukan dengan menggunakan CIC-DDoS2019 Dataset yang mencakup berbagai jenis serangan DDoS (e.g., HTTP Flood, SYN Flood). Parameter yang diukur meliputi True Positive Rate (TPR), False Positive Rate (FPR), latensi, dan throughput.

Tabel 1. Hasil pengujian Dataset

Parameter	Tanpa DPI	Dengan DPI
True Positive Rate (TPR)	87.4%	95.2%
False Positive Rate (FPR)	12.6%	4.8%
Latensi (ms)	3.2	5.8
Throughput (Mbps)	850	830

Dataset: Data serangan HTTP Flood diambil dari CIC-DDoS2019 Dataset, yang mencakup lalu lintas serangan aplikasi menggunakan protokol HTTP.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14324 p-ISSN : 2089-9424

Simulasi Trafik:
a. Total trafik: 10.000 permintaan HTTP, terdiri dari: 8.000 trafik normal (permintaan GET/POST sah). 2.000 permintaan malicious (serangan HTTP Flood).
b. Konfigurasi IDS Konvensional: IDS berbasis Snort dengan rule set untuk mendeteksi pola serangan berdasarkan header protokol HTTP.
c. Konfigurasi IDS-DPI: IDS terintegrasi DPI yang memeriksa payload untuk mendeteksi pola berulang, seperti repetisi GET/POST identik atau payload besar tanpa variasi.
Evaluasi dilakukan dengan menghitung True Positive Rate (TPR): IDS Konvensional: 89% dari 2.000 serangan berhasil terdeteksi. IDS-DPI: 96% dari 2.000 serangan berhasil terdeteksi.

Dataset: Data serangan SYN Flood diambil dari CAIDA DDoS Dataset, yang mencakup serangan DDoS berbasis protokol TCP.
Simulasi Trafik:
a. Total trafik: 50.000 paket TCP, terdiri dari: 45.000 trafik normal. 5.000 paket malicious SYN Flood.
b. Konfigurasi IDS Konvensional: IDS berbasis Snort mendeteksi paket SYN abnormal berdasarkan pola header.
c. Konfigurasi IDS-DPI: DPI memeriksa header dan payload untuk mendeteksi pola serangan SYN Flood yang memiliki interval pengiriman sangat tinggi atau anomali pada flag TCP. Deteksi dengan TPR: IDS Konvensional: 87% dari 5.000 serangan berhasil terdeteksi. IDS-DPI: 94% dari 5.000 serangan berhasil terdeteksi. False Positive Rate (FPR): IDS Konvensional: 12% dari 45.000 trafik normal salah dideteksi sebagai ancaman. IDS-DPI: 2% dari 45.000 trafik normal salah dideteksi sebagai ancaman.

KESIMPULAN

Penelitian ini bertujuan untuk mengembangkan dan menguji sistem yang mengintegrasikan Deep Packet Inspection (DPI) dengan Intrusion Detection System (IDS) dalam rangka mendeteksi serangan Distributed Denial of Service (DDoS) pada jaringan berskala besar. Berdasarkan hasil implementasi dan analisis, berikut adalah kesimpulan yang diperoleh:
1. Efektivitas Sistem dalam Deteksi Serangan DDoS
a. HTTP Flood: Integrasi DPI dengan IDS meningkatkan tingkat deteksi menjadi 96%, dibandingkan dengan 89% pada IDS konvensional. Peningkatan ini disebabkan oleh kemampuan DPI untuk menganalisis payload dan mendeteksi pola permintaan HTTP yang menyerupai trafik sah tetapi dalam volume besar.
b. SYN Flood: Tingkat deteksi meningkat menjadi 94%, dengan pengurangan false alarms sebesar 10% dibandingkan dengan IDS konvensional. DPI dapat mengidentifikasi pola pengiriman SYN abnormal dengan lebih baik melalui inspeksi mendalam terhadap header dan struktur paket.
c. UDP Flood: Sistem mencapai akurasi deteksi 93%, meskipun throughput jaringan sedikit menurun sebesar 2.35% akibat beban tambahan yang disebabkan oleh proses inspeksi payload.

2. Skalabilitas Sistem
Pengujian dilakukan pada jaringan simulasi berskala besar dengan 500 hingga 1.000 node. Hasil menunjukkan bahwa:
a. Sistem mampu memproses trafik hingga 10 Gbps tanpa kehilangan deteksi signifikan.
b. Latensi tambahan akibat integrasi DPI berada pada rata-rata 2.6 ms hingga 5.8 ms, yang masih dapat diterima dalam lingkungan jaringan berskala besar.
c. Sistem tetap stabil dan mampu mendeteksi serangan secara akurat meskipun terjadi peningkatan volume trafik dan jumlah node.

3. Keunggulan DPI dalam IDS
Integrasi DPI memberikan beberapa keuntungan signifikan:
a. Analisis Payload yang Mendalam: DPI dapat membaca isi payload, sehingga mampu mendeteksi pola serangan yang tidak terlihat hanya dari analisis header.
b. Pengurangan False Positive: DPI berhasil mengurangi tingkat false alarms, terutama untuk serangan seperti SYN Flood, yang memiliki karakteristik serupa dengan trafik normal.

c. Deteksi Serangan Aplikasi: DPI memperbaiki kelemahan IDS konvensional dalam mendeteksi serangan berbasis aplikasi seperti HTTP Flood.

4. Dampak pada Kinerja Jaringan
a. Penambahan proses DPI memberikan dampak minimal terhadap kinerja jaringan. Penurunan throughput sebesar 2.35% dan peningkatan latensi rata-rata sebesar 2.6 ms dianggap dapat diterima untuk meningkatkan keamanan jaringan.
b. Sistem berhasil menjaga keseimbangan antara akurasi deteksi dan efisiensi kinerja dalam kondisi trafik tinggi pada jaringan besar.

REFERENSI

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2024). Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian. *Journal of Internet and Software Engineering*, *1*(4), 12–12. https://doi.org/10.47134/PJISE.V1I4.2681

Farzaneh, B., Shahriar, N., Muktadir, A. H. Al, Towhid, M. S., & Khosravani, M. S. (2024). DTL-5G: Deep transfer learning-based DDoS attack detection in 5G and beyond networks. *Computer Communications*, *228*, 107927. https://doi.org/10.1016/J.COMCOM.2024.107927

Harja, D. P., Rakhmatsyah, A., & Nugroho, M. A. (2019). Implementasi untuk Meningkatkan Keamanan Jaringan Menggunakan Deep Packet Inspection pada Software Defined Networks. *Indonesian Journal on Computing (Indo-JC)*, *4*(1), 133–146. https://doi.org/10.21108/INDOJC.2019.4.1.286

Hore, S., Ghadermazi, J., Shah, A., & Bastian, N. D. (2024). A sequential deep learning framework for a robust and resilient network intrusion detection system. *Computers & Security*, *144*, 103928. https://doi.org/10.1016/J.COSE.2024.103928

Khairunnisa, P. A., Annisa, N., & Parhusip, J. (2024). Penerapan Teknologi SDN (Software-Defined Networking) untuk Meningkatkan Keamanan Jaringan Perusahaan. *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 1–8. https://doi.org/10.51903/TEKNIK.V4I2.569

Li, M., Zhou, H., & Deng, S. (2024). Parallel path selection mechanism for DDoS attack detection. *Journal of Network and Computer Applications*, *230*, 103938. https://doi.org/10.1016/J.JNCA.2024.103938

Phu, A. T., Li, B., Ullah, F., Ul Huque, T., Naha, R., Babar, M. A., & Nguyen, H. (2023). Defending SDN against packet injection attacks using deep learning. *Computer Networks*, *234*, 109935. https://doi.org/10.1016/J.COMNET.2023.109935

Shirsath, V. A., Chandane, M. M., Lal, C., & Conti, M. (2024). SYNTROPY: TCP SYN DDoS attack detection for Software Defined Network based on Rényi entropy. *Computer Networks*, *244*, 110327. https://doi.org/10.1016/J.COMNET.2024.110327

Sufardy, D. B., & Widiasari, I. R. (2024). The Use of PFSense and Suricata as a Network Security Attack Detection and Prevention Tool on Web servers. *INOVTEK Polbeng - Seri Informatika*, *9*(2), 765–777. https://doi.org/10.35314/SHXY2045

Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Carrera, D. F. (2022). A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning. *Journal of Network and Computer Applications*, *205*, 103444. https://doi.org/10.1016/J.JNCA.2022.103444