Evaluasi Efektivitas *Intrusion Prevention Systems* (IPS) dalam Memitigasi *Modern Network Threats*: Tinjauan Sistematis

1st Sumitra Adriansyah
Informatics Department
UIN Sunan Gunung Djati Bandung
Jawa Barat, Indonesia
sumitraadriansyah@gmail.com

***Abstract*—Penelitian ini bertujuan untuk mengevaluasi efektivitas Intrusion Prevention Systems (IPS) dalam menghadapi berbagai ancaman jaringan modern, seperti serangan DDoS, SQL Injection, dan pemindaian port. Penelitian menggunakan pendekatan tinjauan sistematis terhadap sepuluh penelitian sebelumnya, penelitian ini menganalisis masalah, metode dan teknologi, serta hasil yang dilaporkan untuk memahami sejauh mana IPS dapat mendeteksi serta mencegah ancaman tersebut. Analisis dilakukan dengan mengevaluasi akurasi deteksi, kecepatan respons, dan dampaknya terhadap kinerja sistem. Hasilnya dapat memberikan gambaran tentang keberhasilan berbagai pendekatan yang digunakan, termasuk penggunaan teknologi kecerdasan buatan dan algoritma machine learning, selain itu memberikan rekomendasi untuk pengembangan IPS yang lebih efektif di masa depan.**

***Index Terms*—Intrusion Prevention Systems (IPS), Keamanan Jaringan, Mitigasi Ancaman, Keamanan Siber, Tinjauan Sistematis.**

I. Pendahuluan

Pada era digital yang terus berkembang pesat ini, keamanan jaringan komputer telah menjadi perhatian utaman bagi organisasi di seluruh dunia. Seiring terus meningkatnya ketergantungan terkait pada teknologi informasi serta komunikasi, ternyata ancaman siber ikut serta berkembang menjadi lebih canggih dan berbahaya. Menurut laporan terbaru dari Cisco Annual Internet Report tahun 2028 sampai 2023, bahwa jumlah perangkat yang terhubung ke jaringan internet diperkirakan mencapai 29,3 miliar pada tahun 2023, dengan terjadinya pertumbuhan yang signifikan dari 2018 yakni sebesar 18,4 miliar [1]. Dengan pertumbuhan yang sangat pesat ini sehingga memberikan tantangan besar dalam aspek keamanan jaringan, khususnya dalam menghadapi ancaman siber yang terus semakin canggih.

Sistem Pencegahan Intrusi (Intrusion Prevention System - IPS) telah hadir sebagai salah satu komponen kritis dalam arsitektur keamanan jaringan modern yang menjadi solusi dalam menghadapi ancaman siber modern saat ini. Intrusion Prevention System (IPS) merupakan suatu alat keamanan jaringan yang dapat mendeteksi dan mencegah serangan dengan memeriksa lalu lintas jaringan. Untuk perlindungan lainnya , IPS dapat memblokir paket berbahaya dan mencatat aktivitas yang mencurigakan tersebut [2]. Sedangankan Intrusion Detection Systems (IDS) merupakan suatu alat yang sangat penting bagi keamanan jaringan, yang dirancang untuk mendeteksi dan merespons akses atau serangan yang tidak sah [3]. Sehingga berbeda dengan sistem deteksi intrusi (IDS) yang hanya memantau serta melaporkan aktivitas mencurigakan, IPS ini memiliki kemampuan untuk dapat secara aktif mencegah ataupun memblokir ancaman yang terdeteksi secara real-time.

Perkembangan ancaman siber dalam beberapa tahun ini menunjukkan peningkatan yang mengkhwatirkan. Berdasarkan Badan Siber dan Sandi Negar (BSSN) Indonesia, menyatakan bahwa adanya 74 juta anomali trafik dari bulan januari hingga bulan Mei tahun 2024, dimana dengan 44 juta anomali tersebut terdeteksi sebagai aktivitas malware, serta sisanya merupakan trojan [4]. Dari data tersebut menunjukkan bahwa perlu adanya peningkatan keamanan siber di era teknologi yang semakin canggih ini.

Implementasi IPS dalam lingkungan jaringan modern ini menghadapai berbagai tantangan. Tantangan tersebut misalnya dimana kemanan siber semakin kompleks dengan terus meningkat, sehingga menyulitkan IPS konvensional dalam mengimbagi ancaman yang terus berkembang [5]. Kemudian dengan linkungan jaringan yang dinamis, ternyata memerlukan variabilitas lalu lintas jaringan dan asimentri data serangan yang dapat mempersulit upaya pendeteksian, hal ini disebabkan karena IPS harus beradaptasi dengan kondisi yang terus berubah-ubah [5].

Tinjauan sistematis ini bertujuan untuk mengevaluasi efektivitas teknologi IPS dalam menghadapi Modern Network Threats. Fokus pada penelitian ini khusus kepada kemampuan adaptasi sistem terhadap ancaman baru dan dampaknya terhadap kinerja jaringan secara keseluruhan.

II. Tinjauan Literatur

Dalam beberapa tahun terakhir, penelitian tentang efektivitas Intrusion Prevention System (IPS) dalam mengatasi modern network threats, ternyata telah banyak dilakukan. Banyak

penelitian telah meneliti keefektifan penggunaan metode ini dalam mencegah adanya serangan siber.

Maulani, I, E, et. al mengengemukakan permasalahan terkait ancaman siber yang semakin kompleks, sehingga memerlukan IDS yang efektif. Penelitian tersebut menggunakan metode wawancara secara mendalam dengan ahli jaringan dan kemanan untuk memahami kebutuhan sistem. Sehingga hasil yang ditemukan dalam penelitian bahwa IDS mampu menjadi garis pertahanan pertama yang mendeteksi aktivitas mencurigakan dan melindungi jaringan [6].

Kurniawan, A, et. al juga menyoroti bahwa ancaman seperti port scanning, brute force, dan DDoS. Ancaman tersebut ternyata dapat ditanganin secara efektif dalam menungkatkan keamanan jaringan, oleh Suricata IPS yang telah diuji untuk mendeteksi searngan tersebut [7].

Penelitian yang dilakukan Deepaa Selva et. al juga berhasil untuk membangun sistem keamanan jaringan yang lebih cerdas dengan menggunakan algoritma seperti genetika dan jaringan saraf. Hasil dari penelitian tersebut menyatakan bahawa sistem deteksi intrusi lebih adaftif dan akurat, sehingga dapat mengangani ancaman yang terus berkembang [8].

Deinega et.al juga berhasil menemukan sistem yang berhasil mendeteksi ancaman dengan akurasi tinggi dengan melampaui konvensional, dalam mengatasi keterbatasan sistem tradisional dengan menginterasikan algoritma kecerdasan buatan, seperti jaringan saraf dan logika fuzzy [9].

Faula Tanang Anugrah et al, dalam penelitiannya berfokus pada deteksi serangan SQL Injection menggunakan Suricata dengan pengecekan melalui signature rule. Hasilnya menunjukkan Suricata efektif mendeteksi berbagai jenis serangan, meskipun ada peningkatan waktu respons server [2].

Fazar Dawamsyach et al, dalam penelitiannya mengembangkan sistem IPS dengan Fail2ban untuk mencegah serangan brute force dan DDoS. Arsitektur Fail2ban yang diterapkan dalam penelitian tersebut dapat dilihat pada Fig. 1.

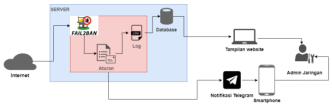

Fig. 1: Arsitektur Fail2ban [10]

Ternyata hasilnya menunjukkan bahwa Fail2ban efektif dalam mendeteksi dan menangkal ancaman serta mencegah serangan DDoS dan brute force, dengan hasil ternyata lebih cepat mendeteksi serangan DDoS daripada brute force. Fail2ban ini ternyata lebih cepat untuk melakukan aksi unban dibandingkan ban, sehingga meskipun adanya kelebihan tersebut, ternyata terdapat dampak pada kinerja CPU dan memori [10].

Rayco William, et al. Menyatakan dalam penelitiannya yakni menggunakan IPS dengan Suricata yang digunakan untuk menangani serangan DDoS dan ping attack. Rangcangan sistem yang dilakukan oleh penelitian tersebut dilihat pada Fig. 2 berikut.

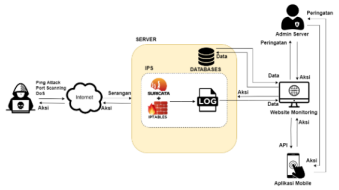

Fig. 2: Rancangan Sistem Penelitan

Sistem pada Fig. 2. ini ternyata dilengkapi notifikasi melalui Telegram, yang mempercepat respons terhadap ancaman dan meningkatkan keamanan server [11].

Patrick Vanin et al. Dalam penelitian yang dilakukan yakni berfokus pada perbaikan IDS dengan metode hybrid dan algoritma seperti SVM dan CNN. Pendekatan ini meningkatkan akurasi, meskipun masih menggunakan dataset lama yang kurang relevan dengan lingkungan modern [12].

Farah Jemili dalam penelitiannya yang dilakuakan dalam mengembangkan sistem deteksi berbasis Big Data dan komputasi awan yang dilengkapi sistem pakar untuk memberikan rekomendasi keamanan yang lebih spesifik. Hasilnya adalah peningkatan akurasi deteksi dan prediksi ancaman [13].

Michael Hart, et. al, meneliti perancangan lingkungan big data untuk menghasilkan input dan output penting dengan merancang, mengonfigurasi, dan mengevaluasi beberapa lapisan arsitektur. Dengan pendekatan desain sains, penelian tersebut mengembangkan artefak untuk menyelesaikan masalah bisnis, termasuk penempatan Intrusion Detection and Prevention Systems (IDPS) dalam arsitektur jaringan yang terus berkembang. Metodologi penelitian melibatkan delapan langkah untuk merancang, menguji, dan membenchmark sistem di berbagai lingkungan jaringan. Hasilnya, mereka berhasil menciptakan model yang matang untuk IDPS, dengan efektivitas tinggi dalam menangani serangan, seperti DDoS, pada arsitektur berbasis perimeter. Penelitian ini juga mengungkap pentingnya optimasi desain sistem keamanan dan batasan implementasi yang dipengaruhi oleh faktor lingkungan serta jumlah arsitektur yang diuji [14].

III. Methodologi

Metodologi penelitian yang digunakan dalam penelitian ini adalah dengan menggunakan pendekatan tinjauan sistematis untuk mengevaluasi efektivitas sistem Intrusion Prevention System (IPS) dalam memitigasi ancaman jaringan modern. Dalam penelitian ini melibatkan beberapa tahapan berikut:

A. Desain Penelitian

Penelitian ini menggunakan metode tinjauan sistematis yang bertujuan untuk mengumpulkan, menganalisis, serta menyintesis hasil penelitian terkait Intrusion Prevention System (IPS) dari berbahai sumber yang relevan.

B. Proses Pengumpulan Data

Data yang dikumpulkan dalam penelitian ini berasal dari jurnal, konferensi, dan publikasi ilmiah terpercaya, dengan menggunakan kombinasi kata kunci Intrusion Prevention System, Modern Network Threats, IPS effectiveness, Machine

Learning in IPS, dan Network Security. Artikel yang dipilih merupakan artikel yang dipublikasi dalam rentang tahun 2021 sampai 2024.

C. Identifikasi Masalah

Permasalahan utama yang diangkat dalam penelitian ini meliputi:

- Kompleksitas dan keragaman ancaman jaringan modern seperti DDoS, *brute force*, dan SQL Injection.
- Kebutuhan akan integrasi algoritma cerdas untuk meningkatkan akurasi deteksi intrusi.
- Tantangan dalam penerapan IPS di lingkungan nyata, termasuk *trade-off* antara keamanan dan kinerja.

D. Analisis Kerangka Kerja

Penelitian ini kemudian mengevaluasi efektivitas kerangka kerja dari Intrusion Prevention Systems (IPS) dalam Memitigasi Modern Network Threats. Proses ini dilakukan dengan mengidentifikasi serta menganalisis hasil penelitian terdahulu yang relevan untuk memahami efektivitas berbagai jenis IPS dalam menangani berbagai jenis ancaman seperti DDoS, SQL Injection, port scanning, dan brute force attacks. Fokus dari kerangka kerja ini pada jenis ancaman yang dapat dideteksi dan dicegah oleh IPS serta menganalisis efektivitas IPS dalam merespons ancaman tersebut. Kemudian, mengukur kinerja IPS dengan parameter seperti waktu respons, akurasi deteksi, serta dampak terhadap kinerja sistem. Terakhir, dengan menilai teknologi dan algoritma yang digunakan dalam setiap penelitian untuk meningkatkan kemampuan IPS.

E. Analisis Data

Proses analisis data dilakukan dengan cara mengkaji hasil dari sepuluh penelitian yang dipilih secara sistematik. Setiap artikel dianalisis berdasarkan, masalah, metodologi, dan hasil penelitian yang diperoleh kemudian dimuatkan menjadi kunci hasil penemuan, yang kemudian dikategorikan untuk mengidentifikasi pola umum dan temuan signifikan terkait efektivitas IPS dalam memitigasi ancaman jaringan modern

F. Validasi Hasil

Hasil penemuan dalam studi literatur dibandingkan satu sama lain untuk memvalidasi efektivitas solusi yang diusulkan. Evaluasi ini mencakup perbandingan dengan metode yang digunakan serta inovasi terbaru dalam sistem IPS atau akurasi dan efisiensi IPS.

IV. Hasil dan Pembahasan

Hasil dari analisis 10 studi yang telah dievaluasi ditampilkan dalam Tabel. 1. berikut, yang memberikan gambaran terkait temuan yang didapatkan dari setiap penelitian.

Hasil analisis dari literatur review, dapat disimpulkan bahwa, penelitian terkait efektivitas Intrusion Prevention System (IPS) dalam menghadapi ancaman jaringan modern menunjukkan solusi, ternyata IPS ini memiliki peran penting dalam meningkatkan keamanan jaringan secara keseluruhan.

TABLE I: Hasil Analisis Temuan Terbaru Penelitian Efektivitas Intrusion Prevention Systems (IPS) dalam Memitigasi Modern Network Threats

No.	Researcher	Key Findings
1	Isma Elan Maulani, Aldo Faisal Umam	IPS berperan sebagai garis pertahanan pertama, membantu mendeteksi aktivitas mencurigakan dan mengurangi dampak serangan.
2	Andhika Kurniawan, Lukman Medriavin Silalahi	Suricata efektif dalam mendeteksi serangan port scanning, brute force, dan DDoS.
3	Deepaa Selva et al.	Algoritma cerdas, termasuk jaringan saraf dan algoritma genetika, meningkatkan deteksi dan pencegahan intrusi.
4	T. S. Deinega et al.	Model berbasis jaringan saraf dan logika fuzzy meningkatkan keandalan dan efisiensi dalam deteksi intrusi.
5	Faula Tanang Anugrah et al.	Suricata efektif dalam mendeteksi SQL Injection, dengan penurunan sedikit pada waktu respons.
6	Fazar Dawamsyach et al.	Fail2ban efektif dalam mengatasi serangan DDoS dan brute force, meskipun ada tradeoff dalam kinerja.
7	Rayco William et al.	Suricata efektif dalam mendeteksi DDoS, ping attack, dan port scanning, dengan notifikasi otomatis via Telegram.
8	Patrick Vanin et al.	Pendekatan hybrid dan ensemble mengarah pada deteksi yang lebih akurat, meskipun masih menggunakan dataset lama.
9	Farah Jemili	Sistem deteksi berbasis Big Data dan komputasi awan memiliki presisi dan akurasi tinggi dalam deteksi intrusi.
10	Farah Jemili	Penempatan IDPS dalam arsitektur big data dapat meningkatkan efektivitas sistem deteksi dan pencegahan intrusi.

A. Deteksi dan Pencegahan Ancaman Jaringan

IPS ternyata terbukti efektif untuk mendeteksi dan mencegah berbagai jenis ancaman, seperti serangan brute force, port scanning, DDoS, hingga SQL injection. Sistem dengan menggunakan seperti Suricata yang telah digunakan pada beberapa studi, ternyata berhasil memblokir aktivitas berbahaya dengan akurasi tinggi, sehingga menunjukkan bahwa IPS memiliki kemampuan dalam mengurangi dampak serangan yang sebelumnya dapat merugikan jaringan.

Sebagai contoh, dalam pengujian yang melibatkan Suricata terhadap serangan port scanning dan brute force, sistem mampu merespons ancaman dengan cepat dan akurat. Bahkan, penelitian tersebut menyoroti efektifitas algoritma pendukung seperti algoritma genetika, jaringan saraf, dan logika fuzzy dalam mendeteksi pola serangan yang lebih komplek dan sulit diprediksi.

B. Peningkatan Kecepatan dan Ketepatan Deteksi

Pendekatan dengan menggabungkan antara metode *machine learning* dan algoritma kecerdasan buatan, ternyata menunjukkan hasil yang signifikan. Sistem yang menggunakan *supervised learning* dan algoritma seperti neural networks ternyata berhasil mencapai akurasi hingga 98% dalam mendeteksi ancaman. Dengan hal ini tidak hanya membantu mempercepat waktu respons tetapi juga meningkatkan kemampuan sistem

dalam menyesuaikan diri dengan pola serangan yang terus berkembang.

C. Adaptasi Terhadap Ancaman Modern

Hasil penelitian yang telah dilakukan pada penelitian sebelumya tersebut mengungkapkan bahwa ternyata pentingnya menggunakan dataset yang lebih representatif dan mengembangkan model yang dapat secara adaptif belajar dari data lalu lintas jaringan yang baru, karena salah satu kelemahan sistem deteksi tradisional adalah ketergantungan pada dataset lama yang tidak relevan dengan lalu lintas jaringan modern. Untuk menangani *big data* dan memberikan rekomendasi keamanan secara real-time, sistem berbasis *big data* dan komputasi awan ini mulai bermunculan.

D. Efisiensi Operasional

Salah satu tantangan terbesar dalam penerapan IPS adalah menemukan keseimbangan antara keamanan jaringan dengan kinerja jaringan. Dari penelitian sebelumnya tersebut menunjukkan bahwa meskipun sistem seperti Suricata meningkatkan keamanan secara signifikan, ternyata ada trade-off berupa peningkatan latensi serta konsumsi sumber daya. Misalnya, saat menghadapi serangan SQL injection, waktu respons server sedikit meningkat, meskipun ancaman dapat dikelola dengan baik.

Akan tetapi, dengan pemilihan aturan yang cerdas serta optimasi parameter seperti maxretry, sistem dapat memberikan perlindungan yang optimal tanpa mengorbankan kinerja jaringan secara drastis.

E. Keterbatasan dan Area untuk Perbaikan

Meskipun hasil menunjukkan banyak keunggulan, tetapi masih terdapat tantangan baru yang perlu diatasi. Sistem saat ini masih memiliki kelemahan dalam menghadapi jenis serangan tertentu yang lebih spesifik ataupun serangan baru yang belum dikenali. Tantangan lainnya adalah kebutuhan sumber daya yang tinggi, terutama untuk implementasi sistem yang berbasis algortma kecerdasan buatan. Meskipun hasilnya menjanjikan, tetapi sistem ini ternyata masih membutuhkan pengoptimalan yang lebih lanjut untuk dapat diimplementasikan secara lebih luas dalam skala yang lebih besar.

V. Kesimpulan

Berdasarkan hasil penelitian yang telah dikaji pada penelitian ini, dapat ditarik kesimpulan bahwa Intrusion Prevention System adalah komponen yang sangat penting dalam ekosistem keamaman jaringan modern. Dengan mengintergarikan algoritma cerdas serta pendekatan dengan machine learning, ternyata IPS dapat secara efektif untuk mendeteksi, mencegah, serta merespons berbagai ancaman jaringan yang terus berkembang. Akan tetapi, masih perlu adanya peningkatan berkelanjutan pada metode deteksi, efisiensi sumber daya, serta masih dibutuhkannya pengembangan dataset yang lebih relevan dalam menghadapai tantanga yang ada di masa depan.

Acknowledgment

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Jurusan Teknik Informatika UIN Sunan Gunung Djati Bandung atas dukungan dan penyediaan sumber daya yang sangat membantu dalam menyelesaikan penelitian ini. Terima kasih secara khusus kami sampaikan kepada Bapak Gitarja Sandi S.T., M.T., yang telah memberikan bimbingan dan nasihat yang sangat berharga selama proses penelitian. Kontribusinya sangat memperkaya kualitas penelitian ini.

References

[1] Cisco, "Cisco annual internet report (2018–2023) white paper," 2020, accessed: [23/12/2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] F. Tanang Anugrah, S. Ikhwan, and J. Gusti A.G, "Implementasi intrusion prevention system (ips) menggunakan suricata untuk serangan sql injection," *Techné : Jurnal Ilmiah Elektroteknika*, vol. 21, no. 2, p. 199–210, Sep. 2022. [Online]. Available: https://ojs.jurnaltechne.org/index.php/techne/article/view/320

[3] A. M. Affan, "Evolving adversarial training (eat) for ai-powered intrusion detection systems (ids)," *American Journal of Computer Science and Technology*, vol. 7, no. 3, pp. 115–121, 2024. [Online]. Available: https://doi.org/10.11648/j.ajcst.20240703.16

[4] tim cnn indonesia. (2024) Bssn deteksi 44 juta aktivitas malware hingga mei 2024. Accessed: 23/12/2024. [Online]. Available: https://www.cnnindonesia.com/teknologi/20240516184354-185-1098626/bssn-deteksi-44-juta-aktivitas-malware-hingga-mei-2024

[5] H. Han, H. Kim, and Y. Kim, "An efficient hyperparameter control method for a network intrusion detection system based on proximal policy optimization," *Symmetry*, vol. 14, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2073-8994/14/1/161

[6] I. Elan Maulani and A. faisal umam, "Evaluasi efektivitas sistem deteksi intrusi dalam menjamin keamanan jaringan," *Jurnal Sosial Teknologi*, vol. 3, no. 8, p. 662–667, Aug. 2023. [Online]. Available: https://sostech.greenvest.co.id/index.php/sostech/article/view/907

[7] L. M. Silalahi and A. Kurniawan, "Analisis keamanan jaringan menggunakan intrusion prevention system (ips) dengan metode traffic behavior," *Electrician : Jurnal Rekayasa dan Teknologi Elektro*, vol. 17, no. 1, pp. 71–76, Jan. 2023. [Online]. Available: https://electrician.unila.ac.id/index.php/ojs/article/view/2296

[8] D. Selva, B. Nagaraj, D. Pelusi, R. Arunkumar, and A. Nair, "Intelligent network intrusion prevention feature collection and classification algorithms," *Algorithms*, vol. 14, no. 8, 2021. [Online]. Available: https://www.mdpi.com/1999-4893/14/8/224

[9] T. Deineha and I. Svatovskiy, "Research of using the artificial intelligence algorithms in intrusion detection/prevention systems," *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modeling. Information technology. Automated control systems*, vol. 54, pp. 16–26, Jun. 2022. [Online]. Available: https://periodicals.karazin.ua/mia/article/view/22222

[10] F. Dawamsyach, I. Ruslianto, and U. Ristian, "Implementation of ips (intrusion prevention system) fail2ban on server for ddos and brute force attacks," *CESS (Journal of Computer Engineering, System and Science)*, vol. 8, no. 1, pp. 149–149, 2023.

[11] R. D. William, I. Ruslianto, and U. Ristian, "Implementation of intrusion prevention system (ips) as a website-based server security system and mobile application," *CESS (Journal of Computer Engineering, System and Science)*, vol. 8, no. 1, pp. 123–123, 2023.

[12] P. Vanin, T. Newe, L. L. Dhirani, E. O'Connell, D. O'Shea, B. Lee, and M. Rao, "A study of network intrusion detection systems using artificial intelligence/machine learning," *Applied Sciences*, vol. 12, no. 22, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/22/11752

[13] F. Jemili, "Active intrusion detection & prediction based on temporal big data analytics," https://doi.org/10.21203/rs.3.rs-2838468/v1, Apr. 2023, pREPRINT (Version 1).

[14] M. Hart, R. Dave, and E. Richardson, "Next-generation intrusion detection and prevention system performance in distributed big data network security architectures," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2023.01409103