Jurnal Ilmiah Universitas Satya Negara Indonesia

Published by : LP3M Universitas Satya Negara Indonesia
Vol. 04 No.02, 2026
Page 58-65
P-ISSN : 1979-5246 | E–ISSN : 3090-8736

NETWORK SECURITY THREATS ANALYSIS AND IMPLEMENTATION OF FIREWALLS, IDS, AND IPS TO IMPROVE SYSTEM PROTECTION IN COMPUTER NETWORK ENVIRONMENTS

ANALISIS ANCAMAN KEAMANAN JARINGAN SERTA IMPLEMENTASI FIREWALL, IDS, DAN IPS DALAM MENINGKATKAN PERLINDUNGAN SISTEM PADA LINGKUNGAN JARINGAN KOMPUTER

Sophia Widiana[1], Sri Ayu Kartika[2], Reni Try Setianingsih[3], Reyna Aulia Zavira[4*], Anita Sindar[5]
[1,2,3,4*,5]STMIK Pelita Nusantara, Medan, Indonesia
[4]reynaaulia165@gmail.com

INFORMASI ARTIKEL
Submitted:
17-06-2026

Accepted:
09-07-2026

Published:
20-07-2026

Keywords:
Network Security; DDoS; firewall; IDS; IPS; System Protection

Kata Kunci:
Keamanan Jaringan; DDoS; firewall; IDS; IPS; Perlindungan Sistem

ABSTRACT

The development of information technology has increased the use of computer networks in various sectors, including educational settings. However, this increased network usage has also been accompanied by an increase in cybersecurity threats that can disrupt service availability and data security. One frequently encountered threat is a Distributed Denial of Service (DDoS) attack, which can degrade network performance and disrupt academic activities. This study aims to analyze network security threats and the implementation of firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to improve system protection in computer network environments. The method used is a literature review with a qualitative descriptive approach through an analysis of several studies discussing DDoS attacks in educational environments. The results indicate that DDoS attacks can degrade the quality of network services and hinder user access to academic systems. Furthermore, the implementation of firewalls, IDS, and IPS has been proven to improve network security through more effective filtering, detection, and prevention of attacks. Based on the analysis, implementing layered security that combines firewalls, IDS, and IPS can be an effective solution for improving system protection and maintaining the stability of computer network services.

ABSTRAK

Perkembangan teknologi informasi telah meningkatkan penggunaan jaringan komputer pada berbagai sektor, termasuk lingkungan pendidikan. Namun, peningkatan penggunaan jaringan juga diikuti oleh bertambahnya ancaman keamanan siber yang dapat mengganggu ketersediaan layanan dan keamanan data. Salah satu ancaman yang sering ditemukan adalah serangan Distributed Denial of Service (DDoS) yang dapat menyebabkan penurunan performa jaringan hingga mengganggu aktivitas akademik. Penelitian ini bertujuan untuk menganalisis ancaman keamanan jaringan serta implementasi firewall, Intrusion Detection System (IDS), dan Intrusion Prevention System (IPS) dalam meningkatkan perlindungan sistem pada lingkungan jaringan komputer. Metode yang digunakan adalah studi literatur dengan pendekatan deskriptif kualitatif melalui analisis beberapa penelitian yang membahas serangan DDoS pada lingkungan pendidikan. Hasil penelitian menunjukkan bahwa serangan DDoS dapat menurunkan kualitas layanan jaringan dan menghambat akses pengguna terhadap sistem akademik. Selain itu, implementasi firewall, IDS, dan IPS terbukti mampu meningkatkan keamanan jaringan melalui proses penyaringan, deteksi, dan pencegahan serangan secara lebih efektif. Berdasarkan hasil analisis, penerapan keamanan berlapis yang mengombinasikan firewall, IDS, dan IPS dapat menjadi solusi yang efektif untuk meningkatkan perlindungan sistem dan menjaga stabilitas layanan jaringan komputer.

INTRODUKSI

Perkembangan teknologi informasi membuat jaringan komputer semakin penting dalam seluruh aktivitas digital sehari-hari. Jaringan digunakan di berbagai bidang, mulai dari pendidikan, pemerintahan, hingga kebutuhan pribadi. Hampir semua proses pertukaran data dan komunikasi dilakukan melalui jaringan komputer. Karena itu, risiko ancaman keamanan juga ikut meningkat, sehingga keamanan jaringan kini menjadi kebutuhan utama untuk melindungi sistem dan data [1].

Ancaman keamanan jaringan saat ini berkembang jauh lebih kompleks dibandingkan tahun-tahun sebelumnya. Berbagai serangan seperti malware, brute force attack, DDoS, dan phishing kini lebih sering terjadi serta dapat menyerang berbagai jenis sistem. Di lingkungan pendidikan, serangan siber bisa menyebabkan kebocoran data mahasiswa, gangguan layanan akademik, hingga kerusakan website institusi. Dampaknya tidak hanya merugikan secara teknis, tetapi juga dapat menurunkan kepercayaan pengguna terhadap keamanan sistem. Karena itu, ancaman siber tidak lagi bisa dianggap sebagai masalah kecil [2].

Dari berbagai ancaman serangan pada jaringan, serangan Distributed Denial of Service (DDoS) menjadi salah satu serangan yang sering ditemukan karena dapat mengganggu ketersediaan layanan. Serangan DDoS menyerang dengan cara membanjiri server jaringan menggunakan trafik palsu sehingga layanan tidak dapat di akses oleh pengguna [3].

Serangan DDoS tidak hanya terjadi pada sektor industri ataupun pemerintahan, tetapi juga mulai banyak ditemukan di lingkungan pendidikan. Institusi Pendidikan yang menghandalkan website dan layanan jaringan memiliki risiko yang cukup besar terhadap gangguan layanan. Ketika website akademik, portal mahasiswa, atau sistem untuk ujian tidak dapat diakses, akibatnya aktivitas pembelajaran dan layanan kampus dapat terganggu [4].

Beberapa penelitian sebelumnya menunjukkan bahwa integrasi firewall, IDS, dan IPS mampu meningkatkan tingkat keamanan jaringan secara signifikan. Penelitian yang dilakukan oleh [4] pada website Universitas Teknologi Sumbawa menunjukkan bahwa serangan DDoS dapat menyebabkan penurunan performa layanan pada website. Hasil pengujian telah perlihatkan bahwa semakin besar jumlah paket yang dikirim oleh penyerang, semakin lambat respons website. Walaupun website masih dapat diakses, performa website mengalami penurunan sehingga diperlukan penerapan balcklist IP dan firewall sebagai langkah pencegahan serangan ini.

Penelitian lainnya yang dilakukan oleh [5] pada jaringan SMK PGRI Kras menunjukkan ternyata serangan Dos (Denial of Service) dan DDoS (Distributed Denial of Service) dapat menggangu kestabilan jaringan terutama saat dilakukannya pelaksanaan ujian berbasis komputer. Untuk mengatasi permasalahan tersebut, peneliti mengimplementasikan Intrusion Prevention System (IPS) menggunakan Sericata yang mampu mendeteksi dan memblokir trafik berbahaya secara real-time, hasilnya performa jaringan dapat kembali stabil setelah terjadi serangan.

Di sisi lain, perkembangan pola serangan membuat metode keamanan tradisional mulai memiliki keterbatasan. Firewall memang masih menjadi sistem keamanan utama karena mampu menyaring lalu lintas data berdasarkan aturan tertentu. Namun, penggunaan firewall saja sering kali belum cukup untuk menghadapi serangan modern yang semakin dinamis dan sulit dikenali. Beberapa serangan bahkan dapat lolos dengan memanfaatkan celah aplikasi, perilaku pengguna, atau lalu lintas yang terlihat normal [1].

Karena itulah banyak penelitian mulai menggabungkan firewall dengan teknologi keamanan lain seperti Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). IDS digunakan untuk mendeteksi aktivitas mencurigakan dalam jaringan dengan cara menganalisis pola lalu lintas data secara real-time dengan cara memberikan peringatan. Sementara itu, IPS bekerja lebih aktif karena tidak hanya mendeteksi, tetapi juga dapat langsung melakukan pencegahan atau pemblokiran terhadap ancaman yang teridentifikasi. Kombinasi ketiga sistem tersebut dinilai lebih efektif karena mampu membentuk mekanisme pertahanan berlapis pada jaringan komputer [2].

Seperti penelitian yang dilakukan oleh [6] pada portal web Universitas Bina Darma menunjukkan bahwa penggunaan Next-Generation Firewall (NGFW) yang dikombinasikan dengan Intrusion Prevention System (IPS) mampu mendeteksi serta mencegah berbagai ancaman siber, termasuk DDoS. Ternyata pendekatan keamanan berlapis dapat meningkatkan perlindungan server serta menjaga ketersediaan layanan akademik.

Penerapan keamanan jaringan masih menghadapi beberapa permasalahan salah satunya adalah kompleksitas konfigurasi sistem keamanan, terutama pada IDS dan IPS yang memerlukan aturan deteksi yang tepat agar tidak menimbulkan terlalu banyak false positive. Karena itu, pengelolaan keamanan jaringan perlu dilakukan secara berkelanjutan melalui pembaruan aturan keamanan, monitoring log, dan evaluasi sistem secara rutin agar perlindungan jaringan tetap optimal menghadapi ancaman siber yang terus berkembang [7], [8].

Berdasarkan uraian tersebut, keamanan jaringan memiliki peran penting dalam menjaga stabilitas, kerahasiaan, dan integritas sistem komputer. Firewall, IDS, dan IPS saling melengkapi dalam membangun pertahanan jaringan yang lebih kuat. Karena itu, penelitian ini dilakukan untuk menganalisis ancaman keamanan jaringan serta penerapan firewall, IDS, dan IPS dalam meningkatkan perlindungan sistem di lingkungan pendidikan. Penelitian ini diharapkan dapat memberikan pemahaman mengenai efektivitas sistem keamanan terpadu dan menjadi referensi untuk pengembangan strategi keamanan jaringan yang lebih baik di masa mendatang.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan pendekatan deskriptif kualitatif. Metode ini dipilih karena penelitian berfokus pada analisis ancaman keamanan jaringan serta implementasi firewall, IDS, dan IPS berdasarkan berbagai sumber ilmiah seperti jurnal, buku, dan artikel penelitian yang relevan. Pendekatan deskriptif digunakan untuk menjelaskan bagaimana ancaman jaringan terjadi serta bagaimana sistem keamanan diterapkan dalam meningkatkan perlindungan jaringan komputer [14].

Melalui metode ini, penulis mengumpulkan berbagai referensi yang berkaitan dengan keamanan jaringan, jenis serangan siber, firewall, Intrusion Detection System (IDS), dan Intrusion Prevention System (IPS). Setelah itu, informasi yang diperoleh dianalisis dan disusun untuk memahami hubungan antara ancaman jaringan dan solusi keamanan yang digunakan. Pendekatan studi literatur dipilih karena lebih sesuai untuk membahas konsep, strategi, serta hasil implementasi keamanan jaringan yang telah dilakukan pada penelitian sebelumnya [14].

Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini dilakukan melalui studi pustaka. Data diperoleh dari jurnal nasional dan internasional, buku, artikel ilmiah, serta beberapa penelitian terdahulu yang membahas keamanan jaringan komputer. Referensi yang digunakan berfokus pada implementasi firewall, IDS, IPS, ancaman siber, serta konsep keamanan berlapis (Defense in Depth) (Nasution & Munandar, 2025).

Jurnal yang digunakan dalam penelitian ini dipilih berdasarkan kesesuaian topik penelitian, publikasi terbaru, dan sama dengan impementasi sistem keamanan jaringan. Data yang dikumpulkan adalah hasil penelitian, bentuk serangan yang dianalisis, sampai solusi yang diterapkan.

Tahapan Analisis Data

Analisis data pada penelitian ini dilakukan melalui beberapa tahapan supaya informasi yang didapat dari berbagai jurnal dapat disusun dengan baik.

1. **Identifikasi ancaman keamanan jaringan**
   Langkah awal yaitu dilakukannya identifikasi terhadap banyaknya ancaman jaringan yang dibahas dalam jurnal. Fokus analisis ini diarahkan pada ancaman jaringan Distributed Denial of Service (DDoS) dikarenakan ancaman yang paling sering menyebabkan gangguan pada layanan jaringan. Selain itu, tahapan ini juga membahas dampak yang ditimbulkan terhadap kinerja dan ketersediaannya sistem.

2. **Analisis implementasi Firewall, IDS, dan IPS**
   Menganalisis bagaimana sistem keamanan jaringan Firewall, IDS, dan IPS diterapkan pada masing-masing penelitian. Analisis dilakukan dengan cara melihat fungsi setiap mekanisme keamanan, metode konfigurasi, serta peran masing-masing sistem dalam mendeteksi ataupun mencegah serangan keamanan jaringan.

3. **Analisis permasalahan dan Solusi**
   Mengidentifikasi berbagai permasalahan yang muncul selama implementasi sistem keamanan jaringan. Kemudian permasalahan yang ada dibandingkan dengan solusi yang diberikan pada setiap penelitian agar bisa mengetahui efektivitas pendekatan yang digunakan dalam meningkatkan keamanan jaringan.

Teknik Analisis Data

Data yang telah dikumpulkan kemudian dianalisis menggunakan metode analisis deskriptif. Pada tahap ini, penulis membandingkan dan mempelajari informasi dari beberapa sumber untuk memperoleh pemahaman mengenai ancaman keamanan jaringan DDoS dan penerapan firewall, IDS, serta IPS dalam melindungi sistem jaringan komputer [11].

Hasil analisis kemudian disusun secara sistematis agar dapat menjelaskan hubungan antara ancaman jaringan dengan strategi keamanan yang digunakan. Dengan cara ini, penelitian diharapkan mampu memberikan gambaran mengenai pentingnya penerapan sistem keamanan jaringan secara berlapis dalam menghadapi perkembangan ancaman siber saat ini [9].

HASIL DAN PEMBAHASAN

Penelitian ini difokuskan pada analisis ancaman keamanan jaringan yaitu serangan Distributed Denial of Service (DDoS) yang terjadi lingkungan Pendidikan. Alasan dipilihnya lingkungan pendidikan karena meningkatnya penggunaan layanan berbasis web dan jaringan komputer dalam kegiatan akademik, administrasi, maupun proses pembelajaran. Berdasarkan kondisi tersebut menjadikan sekolah dan perguruan tinggi sebagai salah satu target yang rentan terhadap serangan siber.

Berdasarkan hasil studi literatur yang telah dilakukan, didapatkan bahwa serangan DDoS dapat menyebabkan penurunan performa jaringan, lalu memperlambat akses layanan, serta menyebabkan layanan tidak dapat digunakan untuk beberapa waktu. Dampaknya dapat mengganggu aktivitas akademik yang bergantung pada jaringan dan sistem informasi.

Salah satu penelitian yang dilakukan pada website Universitas Teknologi Sumbawa (UTS), penelitian tersebut menganalisis serangan Distributed Denial of Service (DDoS) menggunakan metode NIST dengan bantuan tool Low Orbit Ion Cannon (LOIC). Pengujian dilakukan dengan mengirimkan serangan mulai dari 500 paket hingga 10.000 paket ke website kampus. Hasil dari pengujian menunjukkan bahwa website masih dapat diakses walaupun mengalami penurunan performa yang cukup signifikan. Waktu akses yang biasanya rata-rata bisa diakses sekitar 3 detik kini meningkat menjadi 90 detik saat jumlah paket serangan diperbesar. Namun dengan demikian, website tidak mengalami kondisi down sehingga dapat dikatakan bahwa sistem masih memiliki tinggkat ketahanan yang cukup baik terhadap serangan DDoS [4].

Penelitian berikutnya dilakukan pada jaringan laboratorium komputer SMK PGRI Kras yang mengalami gangguan jaringan saat pelaksaan ujian berbasis komputer akibat serangan Denial of Service (DoS) dan Distributed Denial of Service (DDoS). Dalam penelitian tersebut dilakukannya simulasi serangan Ping Flood, HTTP Flood, dan SYN Flood untuk mengetahui dampak yang terjadi terhadap performa jaringan. Hasil pengujian menunjukkan bahwa serangan SYN Flood menjadi salah satu serangan yang paling berdampak karena mampu menurunkan throughput hingga 10,3 Kbps, meningkatkan latency lebih dari 500 ms, dan telah menyebabkan packet drop mencapai 84,5% [5].

Selanjutnya ada penelitian yang dilakukan pada server portal web Universitas Bina Darma yang menunjukkan bahwa ancaman yang dihadapi tidak hanya berupa DDoS, tetapi juga ada ancaman backdoor attack, brute force attack dan berbagai bentuk akses yang tidak sah lainnya. Serangan tersebut berpotensi menggangu layanan akademik yang digunakan mahasiswa dan para dosen sehingga deperlukan mekanisme perlindungan yang lebih adaptif dan mampu bekerja secara terang-terangan atau secara real-time [6].

Penelitian lain yang dilakukan oleh [15] pada lingkungan Wireless Local Area Network (WLAN) menggunakan kombinasi Intrusion Detection System (IDS) Snort dan Intrusion Prevention System (IPS) berbasis IP Tables. Pada penelitian tersebut dilakukannya simulasi berbagai serangan jaringan, seperti ARP Spoofing, Port Scanning, serta Distributed Denial of Service (DDoS) terhadap server yang menjadi target serangan. Hasil dari pengujian menunjukkan bahwa serangan Distributed Denial of Service (DDoS) mampu menghasilkan lalu lintas jaringan yang tidak normal dan berpotensi mengganggu ketersediaan layanan jaringan. Selain it, aktivitas serangan dapat menyebabkan peningkatan penggunaan sumber daya server dan menurunkan tingkat keamanan jaringan apabila tidak segera ditangani. Penelitian ini menunjukkan bahwa lingkungan jaringan Pendidikan yang memanfaatkan WLAN juga memiliki risiko tinggi terhadap berbagai serangan ancaman siber, termasuk serngan Distributed Denial of Service (DDoS).

Berdasarkan keempat penelitian tersebut dapat ditarik kesimpulannya bahwa serangan Distributed Denial of Service (DDoS) masih menjadi salah satu ancaman utama pada lingkungan pendidikan, baik pada website perguruan tinggi, portal akademik, jaringan laboratorium sekolah, maupun lingkungan jaringan nirkabel yang digunakan untuk mendukung kegiatan pembelajaran. Meskipun dampaknya berbeda-beda pada setiap institusi, seluruh penelitian menunjukkan bahwa serangan tersebut dapat menurunkan kualitas layanan jaringan, mengganggu akses pengguna, dan tentunya berpotensi menghambat aktivitas akademik apabila tidak ditangani dengan sistem keamanan yang memadai. Penelitian-penelitian tersebut juga menunjukkan bahwa penerapan mekanisme keamanan seperti firewall, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) menjadi kebutuhan penting untuk menjaga keamanan atau ketersediaan layanan jaringan dilingkungan pendidikan.

Analisis Implementasi Firewall, IDS, dan IPS

Untuk mengatasi ancaman Distributed Denial of Service (DDoS), setiap penelitian menerapkan mekanisme keamanan jaringan yang berbeda sesuai dengan kebutuhan dan kondisi infrastrukturnya.

Tabel 1. Perbandingan hasil implementasi sistem keamanan jaringan pada lingkungan pendidikan

Penelitian	Lokasi penelitian	Sistem keamanan	Hasil implementasi
[4]	Universitas Teknologi Sumbawa	*Firewall* dan Blacklist IP	Website tetap dapat diakses meskipun mengalami perlambatan saat menerima serangan DDoS
[5]	SMK PGRI Kras	IPS *Suricata* dan IP Tables	Trafik berbahaya berhasil diblokir secara *real-time,* performa jaringan kembali stabil
[6]	Universitas Bina Darma	*Next Generation Firewall* (NGFW) dan IPS	Mampu mendeteksi serta memblokir serangan *backdoor, brute force,* dan DDoS secara *real-time*
[15]	Lingkungan WLAN Universitas Islam Riau	IDS Snort dan IPS IP Tables	Serangan DDoS, ARP Spoofing, dan Port Scanning berhasil dideteksi serta akses penyerang berhasil diputus

Sumber : Olahan Peneliti

Berdasarkan hasil dari penelitian [4] fokus utama penelitian tersebut adalah melakukan analisis terhadap ketahanan website Universitas Teknologi Sumbawa ketika menerima serangan Distributed Denial of Service (DDoS). Penelitian ini belum melakukan implementasi sistem keamanan secara langsung, namun memberikan rekomendasi penggunaan firewall dan teknik blacklist IP sebagai langkah untuk mencegah terhadap serangan yang terdeteksi.

Selanjutnya penelitian oleh [5] telah menunjukkan hasil yang lebih komprehensif karena menerapkan Intrusion Prevention System (IPS) menggunakan Suricata yang dikombinasikan dengan IP Tables. Setelah sistem keamanan berhasil diterapkan, throughput jaringan meningkat menjadi lebih dari 1 Gbps, latency turun menjadi kurang dari 50 ms, dan packet drop berhasil diturunkan hingga di bawah 10%. Hasil ini menunjukkan bahwa Intrusion Prevention System (IPS) mampu menjaga kestabilan jaringan meskipun berada dalam kondisi serangan.

Sementara itu, penelitian oleh [6] menerapkan Next Generation Firewall (NGFW) yang dikombinasikan dengan Intrusion Prevention System (IPS) pada portal web Universitas Bina Darma. Sistem mampu mendeteksi backdoor, brute force attack, port scanning, serta anomali yang berkaitan dengan Distributed Denial of Service (DDoS). Hasil simulasi menunjukkan bahwa serangan dapat dihentikan sebelum mencapai sumber daya server sehingga kinerja layanan tetap stabil.

Dan terakhir penelitian yang dilakukan oleh [15] telah menerapkan kombinasi IDS Snort dan IPS berbasis IP Tables. Snort digunakan untuk mendeteksi aktivitas serangan, sedangkan IP Tables digunakan untuk memblokir alamat IP penyerang secara otomatis. Hasil pengujian telah menunjukkan bahwa sistem berhasil mendeteksi serangan DDoS TCP, DDoS UDP, ARP Spoofing, dan Port Scanning. Setelah alamat IP penyerang teridentifikasi, akses menuju server dapat langsung diputus menggunakan aturan firewall yang telah dikonfigurasi.

Dari keempat penelitian tersebut terlihat bahwa kombinasi firewall, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) memberikan tingkat perlindungan yang lebih baik dibandingkan penggunaan satu mekanisme keamanan saja. Firewall berfungsi sebagai penyaring lalu lintas jaringan, IDS bertugas mendeteksi aktivitas mencurigakan, sedangkan IPS mampu melakukan tindakan pencegahan secara otomatis ketika ancaman terdeteksi.

Permasalahan yang Muncul dan Solusi yang Diterapkan

Berdasarkan hasil analisis dari empat penelitian yang digunakan, terdapat beberapa permasalahan yang sering muncul pada lingkungan pendidikan terkait keamanan jaringan. Permasalahan pertama adalah tingginya volume trafik yang dikirimkan penyerang saat melakukan DDoS. Pada penelitian [4], peningkatan jumlah paket serangan tealah menyebabkan waktu akses website menjadi jauh lebih lambat dibandingkan kondisi normal. Hal ini menunjukkan bahwa server harus bekerja lebih keras untuk melayani permintaan yang masuk secara bersamaan. Solusi yang direkomendasikan adalah penggunaan firewall dan teknik blacklist IP untuk memfilter sumber serangan sebelum mencapai server utama.

Permasalahan kedua adalah menurunnya performa jaringan ketika serangan berlangsung. Pada penelitian [5] serangan SYN Flood menyebabkan throughput turun drastis, packet drop meningkat, dan penggunaan CPU menjadi sangat tinggi. Solusi yang diterapkan adalah penggunaan IPS Suricata yang mampu mendeteksi serta memblokir trafik berbahaya secara langsung atau real-time sehingga performa jaringan dapat kembali stabil.

Permasalahan ketiga adalah semakin kompleksnya jenis serangan yang menargetkan layanan akademik berbasis web. Pada penelitian [6] ancaman yang ditemukan tidak hanya berupa DDoS tetapi juga backdoor dan brute force attack. Oleh karena itu diterapkannya NGFW yang dilengkapi IPS agar mampu melakukan inspeksi paket secara lebih mendalam dan memberikan perlindungan berlapis terhadap berbagai jenis ancaman siber.

Permasalahan terakhir adalah adanya akses tidak sah yang dilakukan oleh penyerang melalui teknik ARP Spoofing, Port Scanning, maupun DDoS. Penelitian oleh [15] menunjukkan bahwa aktivitas tersebut dapat diidentifikasi dengan menggunakan Snort dan kemudian diblokir menggunakan IP Tables. Dengan pendekatan ini, sistem tidak hanya mendeteksi ancaman tetapi juga langsung melakukan tindakan pencegahan.

Secara keseluruhan, hasil pembahasan menunjukkan bahwa penerapan Firewall, IDS, dan IPS merupakan solusi yang efektif untuk meningkatkan keamanan jaringan pada lingkungan pendidikan. Ketiga teknologi tersebut saling melengkapi dalam mendeteksi, memfilter, dan mencegah serangan DDoS maupun ancaman jaringan lainnya sehingga layanan akademik dapat berjalan dengan lebih aman dan stabil.

KESIMPULAN

Berdasarkan hasil studi literatur yang telah dilakukan, dapat disimpulkan bahwa ancaman keamanan jaringan masih menjadi tantangan yang serius dalam menjaga ketersediaan dan stabilitas layanan pada lingkungan jaringan komputer, khususnya di sektor pendidikan. Dari berbagai ancaman yang ada, serangan Distributed Denial of Service (DDoS) menjadi salah satu ancaman yang paling sering ditemukan karena dapat menyebabkan penurunan performa jaringan, memperlambat akses layanan, bahkan mengganggu aktivitas akademik yang bergantung pada sistem berbasis jaringan. Hasil analisis terhadap beberapa penelitian menunjukkan bahwa setiap institusi memiliki tingkat kerentanan yang berbeda, namun seluruhnya menghadapi risiko yang sama terhadap gangguan layanan akibat serangan siber. Selain itu, implementasi firewall, Intrusion Detection System (IDS), dan Intrusion Prevention System (IPS) terbukti mampu meningkatkan perlindungan sistem melalui proses penyaringan lalu lintas jaringan, deteksi aktivitas mencurigakan, serta pencegahan serangan secara otomatis. Penerapan keamanan berlapis yang menggabungkan ketiga mekanisme tersebut memberikan tingkat perlindungan yang lebih baik dibandingkan penggunaan satu sistem keamanan saja, sehingga dapat membantu menjaga keamanan, stabilitas, dan ketersediaan layanan jaringan komputer. Berdasarkan hasil penelitian ini, organisasi atau institusi yang memanfaatkan jaringan komputer disarankan untuk menerapkan sistem keamanan secara berlapis dengan mengombinasikan firewall, IDS, dan IPS agar mampu menghadapi perkembangan ancaman siber yang semakin kompleks. Selain itu, perlu dilakukan pemantauan jaringan, pembaruan aturan keamanan, dan evaluasi sistem secara berkala untuk memastikan mekanisme perlindungan tetap berjalan secara optimal. Untuk penelitian selanjutnya, kajian dapat dikembangkan dengan melakukan pengujian langsung pada lingkungan jaringan nyata atau membandingkan efektivitas berbagai teknologi keamanan jaringan terhadap jenis serangan siber lainnya selain DDoS.

DAFTAR PUSTAKA

[1] R. Hadi, R. K. Abdullah, and H. P. Fitrian, "Penerapan Firewall dan Intrusion Detection System pada Jaringan Komputer," *Journal of Computer Science and Information Technology*, vol. 2, no. 1, pp. 9–15, Mar. 2026, doi: 10.70716/jocsit.v2i1.411.

[2] L. R. A. Putri *et al.*, "PERAN DAN STRATEGI KEAMANAN JARINGAN KOMPUTER DALAM MENGATASI SERANGAN SIBER DI WEBSITE INSTITUSI PENDIDIKAN," *SEMINAR NASIONAL PENDIDIKAN TEKNOLOGI INFORMASI DAN PENDIDIKAN MATEMATIKA FPMIPA*, vol. 3, no. 1, pp. 209–219, Jun. 2025.

[3] R. A. Halim, A. Nugrohojati, and Mahmudin, "Analisis dan Mitigasi Serangan Distributed Denial of Service (DDoS) pada Jaringan Berbasis SDN (Software-Defined Networking)," *Sindoro Cendika Pendidikan*, vol. 17, no. 8, Aug. 2025, doi: 10.9644/sindoro.v3i9.252.

[4] Y. W, Yuliadi, F. Hamdani, Y. B. Fitriani, and N. Oper, "Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)," *Kajian Ilmiah Informatika dan Komputer*, vol. 3, no. 6, pp. 1296–1302, Jun. 2023, doi: 10.30865/klik.v3i6.830.

[5] M. R. Alim, R. N. Sarbini, and I. Kurniasari, "Implementasi Intrusion Prevention System Suricata sebagai Pengamanan Dari Serangan DoS dan DDoS," *Portal Riset dan Inovasi Sistem Perangkat Lunak*, vol. 2, no. 2, pp. 91–96, Apr. 2024, doi: 10.59696/prinsip.v2i2.113.

[6] V. Pranata, "Next-Generation Firewall Design Using an Intrusion Prevention System (IPS) Method for Securing the Web Portal Server of Universitas Bina Darma," *Jurnal Jaringan Komputer dan Keamanan*, vol. 6, no. 2, pp. 87–92, Jun. 2025, doi: https://doi.org/10.61346/jjkk.v6i2.243.

[7] Muzaki, M. Tahir, Khoironi, Romadhoni. Abd. Bhazid, and Moh. Ridwan, "Simulasi dan Evaluasi Sistem IPS/IDS Berbasis Honeypot dan Firewall pada Server Ubuntu," *Riset Teknik Informatika dan Komputer*, vol. 7, no. 1, pp. 106–110, Apr. 2025, doi: https://doi.org/10.52005/restikom.v71.419.

[8] L. D. Samsumar, B. Imran, M. M. Efendi, R. Muslim, Z. Muahidin, and Z. Mutaqin, "Optimalisasi Keamanan Web Server Ubuntu dengan Teknologi IPS Berbasis Iptables," *Jurnal Teknologi Rekayasa*, vol. 9, no. 2, pp. 69–76, Dec. 2024, doi: 10.31544/jtera.v9.i1.2024.69-76.

[9] E. A. Syaputra *et al.*, *KEAMANAN JARINGAN KOMPUTER*. 2025.

[10] P. A. Khairunnisa, N. Annisa, Yukandri, and J. Parhusip, "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia," *Jurnal Ilmu Teknik dan Informatika*, vol. 4, no. 2, pp. 9–16, Oct. 2024, doi: https://doi.org/10.51903/teknik.

[11] F. A. Syaifuddin, D. A. Maulana, and M. F. Amrulloh, "Analisis Keamanan Jaringan Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud," *Digital Transformation Technology*, vol. 4, no. 2, pp. 895–902, Dec. 2024, doi: 10.47709/digitech.v4i2.5003.

[12] M. Nasution and H. M. Munandar, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan IDS pada Infrastruktur Jaringan Skala Kecil-Menengah," *JURNAL MEDIA INFORMATIKA*, vol. 6, pp. 2732–2741, Nov. 2025, doi: https://doi.org/10.55338/jumin.v6i6.6763.

[13] A. P. L. Gaol, A. Tedyyana, and N. Hidayasari, "Penerapan Sistem Keamanan Jaringan menggunakan Intrusion Prevention System dengan Machine Learning," *Jurnal Sistem Informasi*, vol. 14, no. 6, pp. 2615–2629, 2025, [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[14] A. Widiastono, Nurafdaliah, A. K. D. I. Paenrongi, F. Tamer, and A. J. Abrar, "Analisis Ancaman Siber dan Strategi Keamanan Jaringan di Universitas Doktor Husni Ingratubun Tual," *Saintek Review*, vol. 2, no. 1, pp. 10–14, 2025.

[15] L. D. Naldi and A. Siswanto, "Design and Implement of Intrusion Prevention System Based on Snort and IP Tables," *Journal of Computing Research and Innovation*, vol. 10, no. 1, pp. 89–97, Mar. 2025, doi: 10.24191/jcrinn.v10i1.498.