JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume XIV No 1, Juni 2025
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

MITIGASI KOMPREHENSIF SERANGAN DDOS PADA SERVER WEB BERBASIS LINUX MENGGUNAKAN *ADVANCED POLICY FIREWALL* (APF) DAN TEKNIK PEMBLOKIRAN IP BERLAPIS

Tomy Satria Alasi[1)], Suhendri Nasution[2)], Riandy Yap[3)], Irwan Jani Tarigan[4)], Reza Alamsyah[5)]
[1,2,3,4]Program Studi Sistem Informasi
[5]Program Studi Teknik Informatika
STMIK Methodist Binjai
Jl. Jenderal Gatot Subroto, Bandar Senembah, Kec. Binjai Bar., Kota Binjai, Sumatera Utara 20716
email: tomysatriaalasi@live.com[1)], suhendri@stmikmethodistbinjai.ac.id[2)], rianz12junior@gmail.com[3)], ijtarigan0105128105@gmail.com[4)], 89rezaalamsyah@gmail.com[5)]

Abstrak
Penelitian ini bertujuan untuk menganalisis serangan DDoS dan mengembangkan mekanisme pertahanan menggunakan *Advanced Policy Firewall* (APF) pada sistem operasi Linux Ubuntu Server. APF bekerja di atas iptables, namun memiliki algoritma yang lebih adaptif dalam menghasilkan aturan firewall secara dinamis serta mampu membedakan antara permintaan normal dan serangan DDoS. Selain itu, APF dilengkapi dengan fitur anti-DDoS yang mampu mengidentifikasi dan memblokir alamat IP penyerang secara otomatis. Hasil penelitian menunjukkan bahwa penggunaan APF efektif dalam meningkatkan keamanan sistem terhadap serangan DDoS. Serangan *Distributed Denial of Service* (DDoS) merupakan upaya yang dilakukan oleh penyerang untuk mengganggu akses pengguna terhadap sistem atau layanan jaringan dengan membanjiri lalu lintas data (*traffic flooding)*, mengirimkan permintaan layanan secara berlebihan (request flooding), atau mengacaukan komunikasi antara host dan klien. Salah satu bentuk sederhana serangan ini dapat dilakukan dengan perintah "ping" dari banyak perangkat secara bersamaan, yang jika tidak ditangani, dapat menyebabkan penurunan kinerja atau bahkan kegagalan sistem.
Kata Kunci: Mitigasi Serangan; DdoS; Server Linux; *Advanced Policy Firewall*

1. Pendahuluan

Serangan DDoS mengakibatkan setiap korbannya akan berhenti merespons atau “bertingkah” tidak lazim. Biasanya serangan DDoS menyerang celah yang terdapat pada layanan sistem[1] atau pada protokol jaringan[2] untuk menyebabkan layanan tidak dapat digunakan. Teknik yang lainnya adalah menyebabkan sistem jaringan “tersedak” dikarenakan banyaknya paket yang diterima yang harus diproses melebihi kemampuan dari sistem itu sendiri atau menyebabkan terjadinya “bottleneck” pada bandwidth yang dipakai oleh sistem[3].

Dalam sebuah serangan denial of service, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan[4]. Teknik ini disebut sebagai traffic flooding, membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut[5], [6]. Teknik ini disebut sebagai request flooding, dan mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server[7].

Secara sederhana serangan DDoS bisa dilakukan dengan menggunakan perintah “ping” yang dimiliki oleh windows. Proses “ping” ini ditujukan kepada situs yang akan menjadi korban. Jika perintah ini hanya dilakukan oleh sebuah komputer, perintah ini mungkin tidak menimbulkan efek bagi komputer korban. Akan tetapi, jika perintah ini dilakukan oleh banyak komputer kepada satu situs maka perintah ini bisa memperlambat kerja komputer.

Penelitian ini menggunakan Advance Policy Firewall (APF). APF menggunakan iptables yang sudah pernah dicoba juga sebelumnya tetapi hebatnya APF memiliki algoritma yang lebih canggih sehingga bisa menghasilkan rule iptables yang dinamis dan mampu mengidentifikasi mana request normal dan mana request DDoS bahkan APF memiliki Anti DDoS sehingga mampu menangkap alamat-alamat IP penyerang[1].

2. Landasan Teori

Mitigasi Serangan

Mitigasi serangan merupakan upaya strategis yang dilakukan untuk mengurangi dampak negatif dari serangan terhadap sistem atau jaringan komputer[8]. Dalam dunia keamanan siber, mitigasi tidak hanya berfokus pada

pencegahan, tetapi juga mencakup deteksi dini, respons cepat, dan pemulihan sistem setelah serangan terjadi[9]. Tujuannya adalah untuk menjaga agar sistem tetap berfungsi secara normal, memastikan ketersediaan layanan, dan melindungi data dari kerusakan atau kehilangan. Mitigasi menjadi sangat penting terutama dalam menghadapi serangan yang bersifat masif dan terkoordinasi seperti *Distributed Denial of Service* (DDoS), yang dapat melumpuhkan layanan secara total dalam waktu singkat[10].

DDoS

DDoS (*Distributed Denial of Service*) adalah jenis serangan siber yang bertujuan untuk melumpuhkan suatu layanan, server, atau jaringan dengan membanjirinya menggunakan lalu lintas data dalam jumlah besar dari berbagai sumber secara bersamaan. Serangan ini biasanya dilakukan oleh jaringan komputer yang telah dikendalikan oleh penyerang (*botnet*), sehingga permintaan terhadap server target menjadi sangat tinggi dan melebihi kapasitas yang mampu ditangani. Akibatnya, layanan menjadi lambat, tidak responsif, atau bahkan tidak dapat diakses sama sekali oleh pengguna yang sah. DDoS merupakan ancaman serius terhadap ketersediaan layanan digital dan sering menimbulkan kerugian operasional serta reputasi bagi organisasi atau penyedia layanan[11], [12].

Server

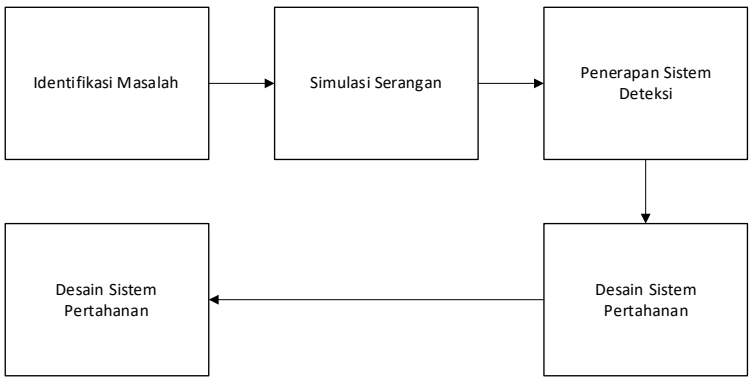
File Transfer Protokol (FTP) adalah suatu protokol yang berfungsi untuk tukar-menukar file dalam suatu network yang mensupport TCP/IP protokol. Dua hal penting yang ada dalam FTP adalah FTP server dan FTP Client. FTP server menjalankan software yang digunakan untuk tukar menukar file, yang selalu siap memberian layanan FTP apabila mendapat request dari FTP client. FTP client adalah komputer yang merequest koneksi ke FTP server untuk tujuan tukar menukar file (mengupload atau mendownload file)[13], [14]. *Domain Name System* (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (*name resolution*) di jaringan yang mengunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan host name sebuah komputer ke IP address[15], [16].

Firewall

Firewall adalah suatu sistem atau group sistem yang menjalankan kontrol akses keamanan diantara jaringan internal yang aman dan jaringan yang untrusted seperti internet. Firewall didesain untuk mengijinkan trusted data yang lewat, menolak layanan yang mudah diserang, mencegah jaringan internal dari serangan luar yang bisa menembus firewall setiap waktu[17], [18], [19], [20].

3. Metode Penelitian

Penelitian ini dilakukan untuk mengidentifikasi, mensimulasikan, dan menganalisis serangan DDoS serta mengembangkan strategi pertahanan pada server berbasis Linux. Penyerangan dilakukan menggunakan tools Tribe Flood Network (TFN) yang mendukung berbagai jenis serangan seperti SYN Flood, ICMP Flood, UDP Flood, dan Smurf Attack. Serangan disimulasikan dari beberapa komputer zombie yang dikendalikan oleh attacker melalui komunikasi ICMP. Untuk menguji efektivitas sistem pertahanan, teknik signature-based detection dan anomaly detection digunakan dalam mendeteksi pola serangan berdasarkan basis data maupun perilaku lalu lintas jaringan.



Gambar 1. Metode penelitian mitigasi serangan ddos pada server linux dengan advanced policy firewall

Untuk mitigasi, penelitian ini mengimplementasikan kombinasi beberapa mekanisme, antara lain Advanced Policy Firewall (APF), mod_evasive, serta metode ICMP Traceback dan Ingress/Egress Filtering untuk pelacakan serta penyaringan IP yang mencurigakan. Honeypot digunakan sebagai umpan untuk menarik serangan dan merekam aktivitas penyerang. Sistem secara otomatis menghasilkan daftar alamat IP penyerang yang kemudian difilter secara berkala menggunakan skrip berbasis wget dan FTP uploader agar firewall dapat melakukan aksi drop terhadap semua lalu lintas dari IP yang teridentifikasi. Topologi jaringan dirancang untuk memvisualisasikan

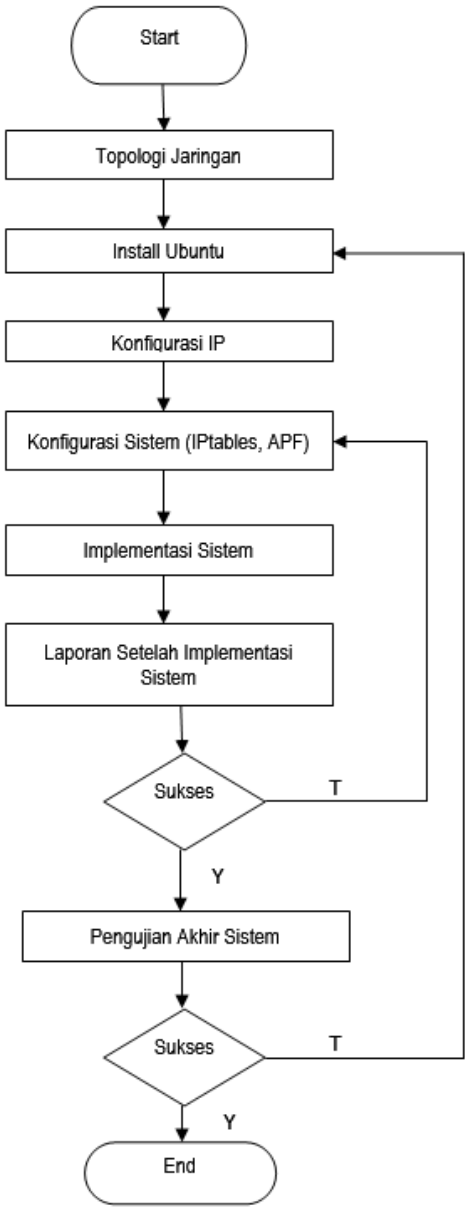
alur serangan hingga tahap mitigasi, dengan tujuan akhir untuk meningkatkan ketahanan sistem terhadap serangan DDoS secara real-time dan adaptif.

4. Hasil Penelitian

Analisa Peracangan dan Implementasi

Algoritma Mitigasi Serangan DDoS pada Server Linux dengan Advanced Policy Firewall

Setelah konfigurasi selesai, sistem masuk ke tahap implementasi, kemudian dilakukan pencatatan hasil implementasi dalam bentuk laporan. Proses akan diverifikasi pada tahap evaluasi awal (pengecekan "Sukses"), jika belum berhasil maka dilakukan perbaikan dengan kembali ke tahap konfigurasi. Jika implementasi dianggap sukses, dilanjutkan ke pengujian akhir sistem. Pengujian akhir ini juga akan diverifikasi, dan apabila sistem berjalan dengan baik, proses berakhir. Namun jika belum sukses, maka siklus pengujian dilakukan kembali. Diagram ini menunjukkan pendekatan iteratif untuk memastikan sistem pertahanan yang diterapkan benar-benar efektif sebelum dinyatakan selesai.



Gambar 2. Algoritma Mitigasi Serangan DDoS pada Server Linux dengan Advanced Policy Firewall

Gambar tersebut menunjukkan diagram alur metode penelitian dalam bentuk flowchart yang digunakan untuk proses mitigasi serangan DDoS pada server berbasis Linux. Proses dimulai dari tahap perancangan topologi jaringan, yang menjadi dasar dari seluruh pengujian dan implementasi sistem. Selanjutnya dilakukan instalasi sistem operasi Ubuntu, diikuti oleh konfigurasi alamat IP pada masing-masing perangkat. Setelah itu, sistem dikonfigurasi menggunakan iptables dan Advanced Policy Firewall (APF) untuk menyiapkan mekanisme pertahanan terhadap potensi serangan.

Ubuntu Server

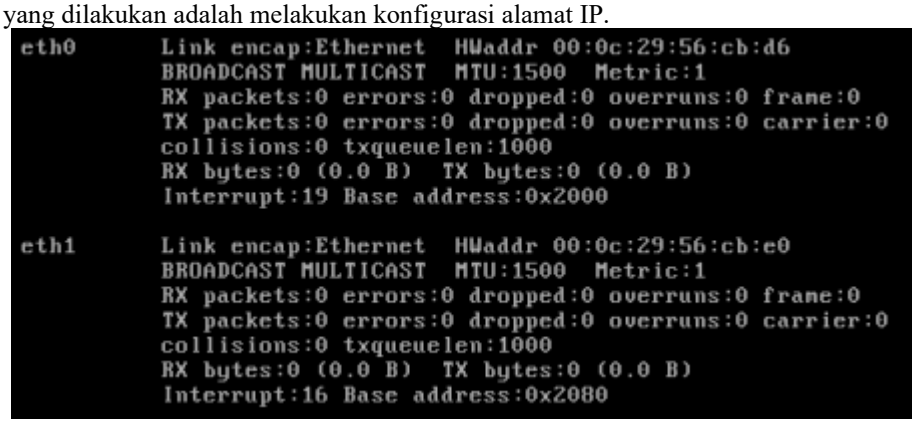
Ubuntu Server adalah varian dari Distri Linux Ubuntu yang dispesialisasikan untuk kebutuhan penggunaan dalam hal *server*. 30. Setelah first boot diubah ke hard drive dan maka setelah selesai booting akan langsung

muncul tampilan awal dari Ubuntu Server 10.10 yang langsung meminta pengguna untuk login dengan tampilan CLI (Command Line Interface).

Gambar 3. Ubuntu Server Berhasil Di Simpan

Konfigurasi IP Address, DNS, dan NAT

Agar Ubuntu Server 10.10 bisa melakukan koneksi ke jaringan, baik itu jaringan lokal maupun internet, maka langkah awal yang dilakukan adalah melakukan konfigurasi alamat IP.



Gambar 4. Tampilan Interface Card

Untuk menghubungkan Ubuntu Server 10.10 ke jaringan, dilakukan konfigurasi IP statis dengan dua interface, yaitu eth0 untuk koneksi internet dan eth1 untuk jaringan lokal. Proses diawali dengan login, masuk ke mode root (sudo su), lalu identifikasi nama interface menggunakan ifconfig -a. Konfigurasi IP dilakukan di file /etc/network/interfaces dan DNS diatur melalui /etc/resolv.conf. Setelah konfigurasi, jaringan direstart agar perubahan terbaca sistem.

Aktivasi interface dilakukan dengan ifconfig eth0 up dan ifconfig eth1 up, kemudian diuji konektivitas dengan ping yahoo.com. Untuk menghubungkan klien lokal ke internet, NAT dikonfigurasi menggunakan iptables dengan perintah iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE, dan IP forwarding diaktifkan di /etc/sysctl.conf dengan mengubah net.ipv4.ip_forward=1.

Advance Policy Firewall (APF)

Untuk melakukan konfigurasi APF di Linux Ubuntu, maka dilakukan tahapan-tahapan berikut ini :
Download paket APF, bash# wget http://www.rfxnetworks.com/downloads/apf-current.tar.gz. Lakukan ekstraksi paket APF bash# tar –zxf apf-current.tar.gz. Install APF yang telah diekstrak tersebut :
bash# cd apf-9.7.9.6
bash# ./install.sh
Selanjutnya, APF dikonfigurasi dengan cara berikut ini :
Edit file conf.apf yang berada pada /etc/apf/conf.apf
Aktifkan Anti DOS mode di APF dan pastikan adanya baris berikut pada /file/crontab
*/8**** root /etc/apf/ad/antidos –a >> /dev/null 2>&1
Berikut ini beberapa potongan skrip konfigurasi APF yang penulis gunakan adalah :
 # !!! Do not leave set to (1) !!!
 # When set to enabled; 5 minute cronjob is set to stop the firewall. Set

```
# this off (0) when firewall is determined to be operating as desired.
DEVEL_MODE="0"
```

Skrip ini maksudnya bila mau buat testing Devel Mode bisa diaktifkan dengan DEVEL_MODE=”1”, tetapi firewall akan off setelah 5 menit, jadi untuk implementasinya Devel Mode harus =”0” artinya tidak aktif.
Karena server yang digunakan dua interface maka diset masing-masing yaitu eth0 dan eth1, eth0 merupakan interface yang terkoneksi keluar dan eth1 interface yang terkoneksi ke dalama atau local. Berikut skrip yang digunakan.

```
# Untrusted Network interface(s); all traffic on defined interface will be
# subject to all firewall rules. This should be your internet exposed
# interfaces. Only one interface is accepted for each value.
IFACE_IN="eth1"
IFACE_OUT="eth0"
```

Berikut skrip untuk DROP paket data langsung dibuat tanpa ada konfirmasi, kalau REJECT setelah data dibuang ada konfirmasi ke pengirim, skrip tersebut adalah :

```
#  DROP  (drop the packet; stealth ?)
#  REJECT (reject the packet)
TCP_STOP="DROP"

#  RESET (sends a icmp-port-unreachable; TCP/IP default)
#  DROP  (drop the packet; stealth ?)
#  REJECT (reject the packet)
#  PROHIBIT (send an icmp-host-prohibited)
UDP_STOP="DROP"
```

Berikut skrip untuk mengaktifkan anti serangan paket data yang berlebihan atau flooding data, skrip tersebut adalah :

```
# These are system control (sysctl) option changes intended to help mitigate
# syn-flood attacks by lowering syn retry, syn backlog & syn time-out values.
SYSCTL_SYN="1"

# These are system control (sysctl) option changes to provide protection from
# spoofed packets and ip/arp/route redirection. If you are performing advanced
# routing policies on this host such as NAT/MASQ you should disable this.
SYSCTL_ROUTE="1"
```

Setelah melakukan perancangan Modifikasi Algoritma Vigenere Cipher maka tahap selanjutnya adalah penulisan kode program (coding) dan pembuatan aplikasi. Tampilan Modifikasi Algoritma Vigenere Cipher untuk melakukan enkripsi dan dekripsi dapat dilihat seperti pada Gambar 5.

Mitigasi Serangan DDoS

Untuk mengantisipasi dan menangani serangan Distributed Denial of Service (DDoS), sistem pertahanan perlu dikonfigurasi secara efisien agar mampu mendeteksi serta memblokir aktivitas mencurigakan secara otomatis. Salah satu metode yang digunakan adalah melalui skrip konfigurasi yang terintegrasi dengan sistem firewall dan routing pada server.

Skrip berikut disiapkan sebagai bagian dari mekanisme Anti-DDoS. Parameter pertama ROUTE_REJ="1" berfungsi untuk menghapus alamat IP penyerang dari tabel routing, sehingga permintaan dari alamat tersebut tidak akan diarahkan lagi ke sistem. Ini adalah langkah preventif agar IP yang teridentifikasi sebagai sumber serangan langsung diputus koneksinya tanpa diproses lebih lanjut.

Selanjutnya, parameter IPT_BL="1" akan mengaktifkan blokir otomatis menggunakan iptables, yaitu sistem firewall internal Linux. Ketika IP penyerang dikenali, aturan firewall secara dinamis dibuat untuk menolak seluruh koneksi dari IP tersebut. Ini membantu mengurangi beban sistem dari lalu lintas yang tidak sah.

Selain memblokir per alamat IP, konfigurasi NETBLOCK="1" digunakan untuk memblokir seluruh blok jaringan (network block) apabila terdeteksi beberapa IP dalam rentang jaringan yang sama melakukan serangan. Strategi ini penting untuk mengantisipasi serangan dari botnet yang menyebar dalam satu subnet, sehingga serangan bisa dihentikan secara menyeluruh, bukan hanya pada satu titik.

Dengan konfigurasi ini, sistem pertahanan menjadi lebih responsif, adaptif, dan otomatis dalam menghadapi potensi serangan DDoS, serta mengurangi intervensi manual dalam pengelolaan ancaman jaringan.

5. Kesimpulan

Serangan *Distributed Denial of Service (DDoS)* merupakan ancaman serius yang dapat membahayakan serta merusak kinerja server, terutama pada sistem yang tidak memiliki perlindungan yang memadai. Dalam penelitian ini, analisis terhadap serangan DDoS pada sistem jaringan komputer yang dilakukan penulis masih belum sepenuhnya optimal, sehingga diperlukan penyempurnaan dan evaluasi lanjutan agar hasilnya lebih akurat dan efektif. Meskipun demikian, implementasi sistem pertahanan menggunakan **Advanced Policy Firewall (APF)** menunjukkan hasil yang cukup baik dan mampu berjalan stabil pada sistem operasi **Linux Ubuntu Server**. Selain itu, langkah-langkah penanggulangan serangan DDoS yang diterapkan dalam penelitian ini dapat berfungsi dengan baik dalam meredam lalu lintas berbahaya dan mempertahankan kestabilan sistem secara keseluruhan.

6. References

[1] A. Allwine and T. S. Alasi, "Manajemen Bandwidth Dan Gateway Dengan Router Mikrotik Pada STMIK Methodist Binjai," *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.

[2] M. Tania, T. S. Alasi, and R. Yap, "ALGORITMA AES UNTUK KEAMANAN DATA DIGITAL BERBASIS WEB DI KANTOR DESA AMAN DAMAI," *J. TIMES*, vol. 13, no. 2, pp. 142–149, 2024.

[3] W. Soetrisno *et al.*, "Meningkatkan Keamanan dan Mitigasi pada Arsitektur Software Defined Network," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 20, no. 1, pp. 18–28, 2025.

[4] A. Yani, N. Ruseno, D. Irfansyah, and G. Santoso, "Strategi Mitigasi Serangan Siber, Data Science, dan Database dalam Infrastruktur Jaringan Pemerintahan Digital," *J. PASTI J. Publ. Artik. Sist. Teknol. Inf.*, vol. 1, no. 1, pp. 54–62, 2025.

[5] B. S. Dharma, A. R. Muslikh, and others, "Implementasi rate limiting dan Bot Telegram untuk mitigasi serangan HTTP GET Flood," *J. Inf. Syst. Appl. Dev.*, vol. 3, no. 1, 2025.

[6] A. Ardiansyah, A. A. M. Suradi, and W. Saputra, "Strategi Keamanan Router MikroTik: Deteksi dan Mitigasi Serangan Brute Force Berbasis Scripting," *JUKI J. Komput. dan Inform.*, vol. 7, no. 1, pp. 12–19, 2025.

[7] T. S. Alasi, "Ilmu Komputer." Media Publikasi Idpress, 2024.

[8] T. S. Alasi and P. Fitriani, "Peningkatan Keamanan untuk Password menggunakan Algoritma Vigenere Cipher," *J. Mantik Penusa*, vol. 6, no. 1, pp. 1–10, 2022.

[9] S. Abiramasundari and V. Ramaswamy, "Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms," *Sci. Rep.*, vol. 15, no. 1, p. 13098, 2025.

[10] V. Prasad *et al.*, "Blockchain enhanced distributed denial of service detection in IoT using deep learning and evolutionary computation," *Sci. Rep.*, vol. 15, no. 1, p. 22537, 2025.

[11] A. Zaman, S. A. Khan, M. Nazeeruddin, A. A. Ateya, A. Sadique, and M. A. ElAffendi, "Distributed Denial of Service Attack Detection in Software-Defined Networks Using Decision Tree Algorithms," *Futur. Internet*, vol. 17, no. 4, p. 136, 2025.

[12] S. Zarei, S. Azizi, and A. Ahmed, "Optimizing edge server placement and load distribution in mobile edge computing using ACO and heuristic algorithms," *J. Supercomput.*, vol. 81, no. 1, p. 257, 2025.

[13] X. Li, M. Teng, Y. Bu, J. Qiu, X. Qin, and J. Wu, "Cooperation-based server deployment strategy in mobile edge computing system," *Comput. Networks*, vol. 257, p. 110932, 2025.

[14] U. Babayi\ugit and A. Gezer, "Determination of optimum network topology with the consideration of firewall security policies," *Recep Tayyip Erdogan Univ. J. Sci. Eng.*, vol. 6, no. 1, pp. 69–81, 2025.

[15] K. Madhura *et al.*, "Software defined network (SDN) based data server computing system," *Int. J. Inf. Technol.*, vol. 17, no. 1, pp. 607–613, 2025.

[16] Y. Pan, "Exploration of Effective Application of Firewall Technology in Computer Network Information Security," *J. Theory Pract. Manag. Sci.*, vol. 5, no. 6, pp. 58–62, 2025.

[17] R. N. Dasmen, T. D. Purwanto, and others, "Implementation of Tarpit Firewall for Network Security Optimization with The NIST SP800-86 Method in KP Room," *Tech-E*, vol. 8, no. 2, pp. 75–85, 2025.

[18] Y. Xu, "Research on Computer Information Network Security Technology and Development Direction," *J. Comput. Electron. Inf. Manag.*, vol. 16, no. 2, pp. 21–24, 2025.

[19] A. Al Sadik, "ENHANCED NETWORK SECURITY SYSTEM USING FIRWALLS," 2025.

[20] P. R. Reddy, Y. D. Reddy, and others, "Machine Learning based Enhanced Firewall for Network Security," in *2025 8th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2025, pp. 750–755.