DETEKSI SERANGAN DDOS PADA JARINGAN *SMART HOME* IPV6 MENGGUNAKAN METODE *RANDOM FOREST*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

Ardi Tri Yudha

09011282126043

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

Deteksi Serangan DDOS Pada Jaringan Smart Home IPv6 Menggunakan Metode Random Forest

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

ARDI TRI YUDHA

09011282126043

Pembimbing 1	:	**Prof. Ir. Deris Stiawan, M.T., Ph.D.**
		NIP. 197806172006041002
Pembimbing 2	:	**Adi Hermansyah, M.T.**
		NIP. 198904302024211001

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

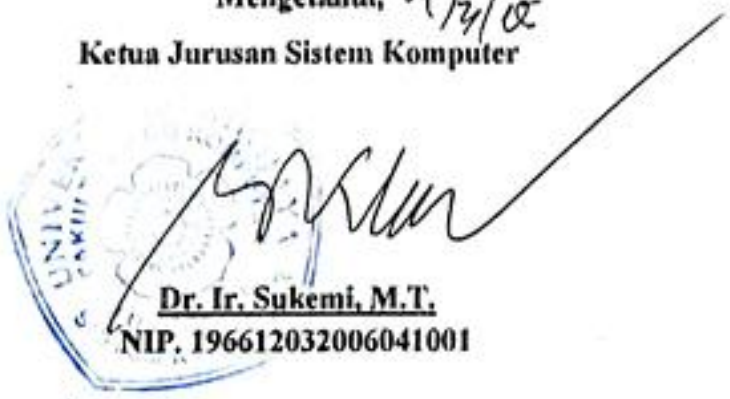
Tanggal : 14 Maret 2025

Tim Penguji :

1. **Ketua : Ahmad Fali Oklilas, M.T.**
2. **Pembimbing 1 : Prof. Ir. Deris Stiawan, M.T., Ph.D.**
3. **Pembimbing 2 : Adi Hermansyah, M.T.**
4. **Penguji : Dr. Ahmad Zarkasi, M.T.**

Mengetahui, 4/4/25

Ketua Jurusan Sistem Komputer



Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Ardi Tri Yudha

NIM : 09011282126043

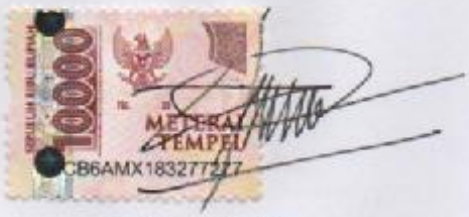
Judul : Deteksi Serangan DDOS Pada Jaringan *Smart Home* IPv6 Menggunakan Metode *Random Forest*

Hasil Pengecekan Software iThenticate/Turnitin : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Maret 2025



Ardi Tri Yudha

NIM. 09011282126043

DDOS Attack Detection on Smart Home IPv6 Network Using Random Forest Method

Ardi Tri Yudha (09011282126043)
Dept. Of Computer System, Faculty of Computer Science, Sriwijaya University
Email : arditriyudha9876@gmail.com

ABSTRACT

DDoS attacks are one of the most common network security threats on the internet. This attack utilizes various sources to send excessive traffic to a server, resulting in system disruption. This makes DDoS a serious threat to IPv6-based topologies and infrastructure. This study uses a dataset from COMNETS Smart Home IPv6, which consists of two types of classes, namely benign and DDoS, to detect DDoS attacks using the Random Forest method. The results of the study show that the Random Forest method is an effective technique in detecting DDoS attacks and has good overall performance with an accuracy of 90.74%, precision 100%, recall 81.60% and f1_score 89.87%..

Keyword : *DDoS, IPv6, Random Forest, Accuracy, Precision, F1_score*

Deteksi Serangan DDOS Pada Jaringan *Smart Home* IPv6 Menggunakan Metode *Random Forest*

Ardi Tri Yudha (09011282126043)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : arditriyudha9876@gmail.com

ABSTRAK

Serangan DDoS adalah salah satu ancaman keamanan jaringan yang sering terjadi di internet. Serangan ini memanfaatkan berbagai sumber untuk mengirimkan lalu lintas berlebihan ke suatu server, yang mengakibatkan gangguan pada sistem. Hal ini menjadikan DDoS sebagai ancaman serius bagi topologi dan infrastruktur berbasis IPv6. Penelitian ini menggunakan dataset dari COMNETS Smart Home IPv6, yang terdiri dari dua jenis kelas, yaitu benign dan DDoS, untuk mendeteksi serangan DDoS menggunakan metode Random Forest. Hasil penelitian menunjukkan bahwa metode Random Forest merupakan teknik yang efektif dalam mendeteksi serangan DDoS dan memiliki performa yang baik secara keseluruhan dengan akurasi sebesar 90,74%, presisi 100%, recall 81,60% dan f1_score 89,87%.

Kata Kunci : *DDoS*, *IPv6, Random Forest*, *Akurasi, Presisi, F1_score*

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur kita panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "**Deteksi Serangan DDoS Pada Jaringan *Smart Home* IPV6 Menggunakan Metode *Random Forest***". Penulis juga ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, saran, kritik, serta motivasi selama proses penyusunan skripsi ini. Rasa terima kasih ini penulis persembahkan kepada:

1. Allah SWT yang senantiasa telah memberikan rahmat serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan skripsi ini.
2. Orang tua tercinta yang dengan penuh kesabaran dan kasih sayang telah membesarkan dan mendidik saya hingga saat ini. Terima kasih atas nasihat, semangat, dan motivasi yang tak pernah berhenti diberikan.
3. Bapak Prof. DR. Erwin, S.Si., M.Si. yang merupakan Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., yang merupakan Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing 1 dan Bapak Adi Hermansyah, M.T. selaku Dosen Pembimbing 2 skripsi, yang telah dengan penuh perhatian meluangkan waktu dan tenaga untuk membimbing, memberikan saran, serta memberikan motivasi kepada penulis sepanjang proses penulisan skripsi ini.
6. Admin jurusan sistem komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
7. Muthia Safira selaku teman, sahabat sekaligus partner yang selalu ada dalam setiap proses, senantiasa menemani, memberikan semangat, dukungan, doa dan motivasi baik melalui kata dan tindakan.

8. Muhammad Aldoni, A. Gofar, Efrilira Syafira, Rahma Aprilia, Risky Gunawan yang tergabung dalam grup ”Menyala Abangku” yang senantiasa menemani, mendukung, memotivasi, serta menghibur penulis menghadapi kejenuhan disaat penulisan skripsi ini.
9. Teman – teman tim penelitian *Smart Home* IPv6 yang senantiasa membantu, berdiskusi dan bertukar pikiran dalam penelitian ini
10. Teman – teman Sistem Komputer Angkatan 2021 Indralaya yang selalu memberikan hiburan, menemani, dan mendukung penulis dengan semangat dan motivasi selama masa perkuliahan.
11. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik, maupun juga memberikan semangat kepada penulis yang mana tidak bisa disebutkan satu persatu.

Penulis menyadari bahwa penyusunan Proposal skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, penulis sangat mengharapkan kritik, saran, serta ide-ide konstruktif yang dapat membantu penulis untuk memperbaiki dan meningkatkan kualitas skripsi di masa yang akan datang.

Palembang, Maret 2025

Ardi Tri Yudha

NIM. 09011282126043

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Smart Home adalah Perangkat elektronik yang saling berhubungan dan dapat diatur secara bersamaan[1]. *Smart home* mengacu pada sistem otomatisasi rumah yang menggunakan perangkat elektronik yang terhubung ke internet dan memungkinkan pengguna untuk memantau, mengontrol, dan mengelola secara efisien berbagai tugas rumah tangga. Perangkat ini meliputi sistem pencahayaan, keamanan, pengatur suhu, serta peralatan rumah tangga lainnya yang dapat dioperasikan melalui aplikasi *smartphone* atau perintah suara.

Internet of things (IoT) adalah perangkat fisik, bangunan, dan barang-barang lainnya yang memiliki konektivitas internet, daya komputasi, papan elektronik, aplikasi, *power unit*, sensor, aktuator, dan sistem kontrol yang memungkinkan hal-hal ini berkomunikasi, menghasilkan, mengumpulkan, bertukar, dan mengonsumsi data tanpa intervensi manusia[2].

Smart Home terus mengalami peningkatan sebagai akibat dari permintaan yang tinggi dan keberhasilan pasar. Menurut Statista, Pasar *Smart Home* global diperkirakan mencapai 99,41 miliar USD pada tahun 2021. Sedangkan, Menurut prediksi dan analisis *World Economic Forum* (WEF), nilai industri ini kemungkinan besar akan mencapai 13 triliun USD pada tahun 2030[3]. Hal ini didukung oleh sebuah studi yang dilakukan oleh Cisco, menunjukkan pertumbuhan eksponensial perangkat pribadi yang terhubung dengan Internet. Secara khusus, terdapat 12 miliar perangkat yang terhubung pada tahun 2010, 25 miliar pada tahun 2015, 50 miliar pada tahun 2020, dan diproyeksikan bahwa jumlah perangkat yang terhubung dengan Internet akan mencapai 1 triliun pada tahun 2035[4].

Internet Engineering Task Force (IETF) memprediksi bahwa kumpulan alamat IPv4 akan habis dalam beberapa dekade mendatang. Namun, setelah pertumbuhan eksponensial yang tidak terduga dari teknologi baru seperti perangkat seluler, *Internet of Things* (IoT), dan layanan *Cloud Computing*, prediksi mereka

datang lebih awal dari yang diharapkan. Oleh karena itu, protokol IPv6 dirancang untuk mengatasi kekurangan IPv4[5].

Untuk mengatasi permasalahan tersebut, Pemerintah Indonesia melalui Menteri Komunikasi dan Informatika mengeluarkan Surat Edaran Nomor 5 Tahun 2024 Tentang Himbauan Mengaktifkan dan Menggunakan Alamat Protokol Internet Versi 6 (IPv6) Pada Kementerian/Lembaga dan Pemerintahan Daerah. Hal ini diharapkan menjadi langkah strategis dalam menjaga ketahanan dan fleksibilitas infrastruktur jaringan di Indonesia.

IPv6 memperkenalkan *Internet Control Message Protocol* versi 6 (ICMPv6), salah satu protokol penting dalam IPv6. IPv6 tidak dapat berfungsi tanpa fungsionalitas protokol ICMPv6 karena pesan ICMPv6 menjalankan banyak fungsi penting yang memungkinkan perutean data di sepanjang jalur jaringan melalui *node*. Namun, pesan ICMPv6 tidak memiliki autentikasi secara *default*, sehingga rentan terhadap eksploitasi. Di antara serangan yang paling serius dan umum terhadap protokol ICMPv6 adalah *Distributed Denial of Services* (DDoS) dan *Denial of Services* (DoS)[6].

IPv6 atau *Internet Protocol Version* 6 dikembangkan untuk menggantikan protokol IPv4 untuk komunikasi di Internet atau jaringan komputer. Protokol IPv6 menawarkan perluasan ruang alamat yang sangat besar, dan memungkinkan setiap perangkat untuk memberikan alamat IPv6 mereka sendiri[7]. IPv6 menghadirkan sejumlah perbaikan dan penyederhanaan dibandingkan dengan IPv4. Perbedaan utama antara keduanya adalah bahwa IPv6 menggunakan alamat 128 bit, sedangkan IPv4 menggunakan alamat 32 bit[8]. IPv6 meningkatkan banyak aspek IPv4, seperti keamanan, *address auto-configuration, router discovery, successful transmission notification,* dan mobilitas[9].

Pendekatan *machine learning* dapat memperkuat strategi keamanan IoT dengan memodelkan perilaku serangan DDoS berbasis IPv6. Metode seperti *Random Forest*, yang menggunakan pohon keputusan untuk klasifikasi dan regresi, efektif dalam memprediksi serangan. Keunggulan *Random Forest* meliputi waktu pelatihan yang singkat, kemampuan menangani data tidak konsisten, klasifikasi fitur otomatis, dan metrik internal untuk mengukur pengaruh fitur, menjadikannya

lebih unggul dibandingkan metode pembelajaran mesin lainnya. Berdasarkan penjelasan diatas maka penulis akan mengangkat judul "Deteksi Serangan DDoS Pada Jaringan *Smart Home* IPv6 menggunakan Metode *Random Forest*". Tujuan penelitian ini adalah untuk meningkatkan akurasi sistem deteksi serangan DDoS pada IPv6.

Pada penelitian terdahulu yang dilakukan oleh Mona Alduailij [10] dan Yini Chen [11]. Mereka menggunakan metode *Random Forest* untuk mendeteksi serangan DDoS, kemudian dilakukan perbandingan hasil prediksi *Random Forest* dengan hasil prediksi yang dilakukan menggunakan metode lainnya. Dari hasil perbandingan, deteksi serangan DDoS dengan menggunakan metode *Random Forest* memiliki *detection rate* yang lebih tinggi dan *false alarm rate* lebih rendah.

Penelitian oleh Redhwan M. A. Saad [12] menggunakan algoritma Neuro-fuzzy dan DENFIS (*Dynamic Evolving Neural Fuzzy Inference System*) untuk mendeteksi serangan ICMPv6 *Flood* dengan hasil akurasi tinggi dan *root mean square error* yang rendah, yaitu sebesar 0,26. Sementara itu, penelitian oleh Omar E. Elejla [5] menggabungkan algoritma IGR, *chi-square*, dan LSTM dalam mendeteksi serangan ICMPv6 *Flood* DDoS. Hasil penelitian ini menunjukkan bahwa LSTM mengungguli RNN dan GRU dalam berbagai metrik performa, seperti TNR, FNR, FPR, akurasi, *F-measure*, *recall*, dan presisi.

Penelitian oleh Mohammed Anbar [8] mendeteksi serangan *flooding* RA DDoS menggunakan metode pemilihan fitur *principal component analysis* (PCA) dan *information gain ratio* (IGR), serta algoritma SVM sebagai model prediksi, dengan hasil akurasi deteksi sebesar 98,55% dan *false-positive rate* 3,3%. Sementara itu, Redhwan M. A. Saad [9] juga menggunakan IGR dan PCA untuk memilih fitur jaringan yang relevan sebelum menerapkan algoritma *back-propagation neural network* (BPNN). Model tersebut mencapai akurasi deteksi 98,3%, namun terbatas pada deteksi serangan *echo request* ICMPv6.

1.2 Tujuan

Adapun tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut :

1. Menggunakan *Random Forest Classifier* sebagai teknik reduksi fitur untuk memilih kumpulan fitur yang digunakan dalam mendeteksi serangan DDoS jaringan *smart home* IPv6.
2. Menggunakan metode *Random Forest* untuk mendeteksi serangan DDoS pada jaringan *smart home* IPv6.
3. Mengukur kinerja metode *Random Forest* dalam mendeteksi serangan DDoS pada jaringan *smart home* IPv6.

1.3 Manfaat

Adapun manfaat yang dapat diambil dari penelitian skripsi adalah :

1. Untuk mengetahui fitur penting yang efektif untuk mendeteksi serangan DDoS Pada IPv6.
2. Untuk mengetahui bagaimana penerapan metode *Random Forest* dalam mendeteksi serangan DDoS pada jaringan *smart home* IPv6.
3. Untuk mengetahui kinerja metode *Random Forest* dalam mendeteksi serangan DDoS pada jaringan *smart home* IPv6

1.4 Perumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, permasalahan utama yang akan dibahas pada penelitian ini yaitu :

1. Bagaimana penerapan dari seleksi fitur agar didapatkan fitur penting pada deteksi serangan DDoS?
2. Bagaimana mengaplikasikan metode *Random Forest* untuk mendeteksi serangan DDoS?
3. Bagaimana hasil kinerja metode *Random Forest* dalam mendeteksi serangan DDoS?

1.5 Batasan Masalah

Adapun batasan-batasan masalah dari penyusunan skripsi ini, yaitu :

1. Penelitian ini menggunakan dataset serangan DDoS pada jaringan *smart home* IPv6 yang dibuat sendiri menggunakan *tools* THC-IPv6.
2. Penelitian ini dilakukan hanya sebatas pendeteksian sebuah serangan DDoS terhadap IPv6.
3. *Output* yang dihasilkan dari penelitian ini seberapa akurat metode *Random Forest* dalam mendeteksi sebuah serangan DDoS terhadap IPv6.

1.6 Metodologi Penelitian

Berikut ini adalah tahapan penelitian yang digunakan dalam penelitian skripsi untuk mencapai tujuan penelitian:

1. Studi Literatur

Tahap ini dilakukan dengan cara mengkaji dan mempelajari literatur dan referensi berupa naskah ilmiah, buku, internet dan lain-lain yang dapat menunjang metodologi dan pendekatan yang akan diterapkan pada penelitian skripsi.

2. Perancangan Sistem

Tahap ini membahas mengenai proses bagaimana membangun sistem dengan menggunakan metode atau pendekatan tertentu. Menentukan perangkat dan topologi untuk membangun jaringan *smart home* IPv6, kemudian bagaimana proses instalasi dan konfigurasi sistem, serta implementasi metode *Random Forest.*

3. Pengujian

Tahap ini merupakan tahap lanjutan dari proses perancangan yang telah dilakukan sebelumnya. Dalam tahap ini, pengujian dilakukan menggunakan metodologi penelitian dan penelitian sebelumnya sehingga data hasil pengujian sesuai dengan batasan masalah dan sesuai dengan parameter pengujian yang telah ditetapkan untuk mendapatkan hasil terbaik.

4. Analisa

Selanjutnya, hasil dari pengujian tahap sebelumnya akan dievaluasi untuk menentukan kesalahan dalam hasil perancangan dan penyebabnya, sehingga dapat dilakukan penelitian tambahan.

5. Kesimpulan dan Saran

Pada tahap ini, kesimpulan akan dibuat berdasarkan studi literatur dan pustaka, metodologi penelitian, dan analisis hasil pengujian sistem. Selanjutnya, penulis akan membuat beberapa rekomendasi yang dapat digunakan sebagai landasan untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Untuk membuat proses penyusunan skripsi lebih mudah dan membuat isi tiap bab lebih jelas, sistem penulisan berikut dibuat:

BAB I PENDAHULUAN

Bab ini berisikan tentang sistematik mengenai topik yang diambil serta uraian singkat tentang latar belakang, tujuan, manfaat, dan perumusan masalah dalam penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai teori-teori utama tentang *Random Forest*, *Distributed Denial of Service* (DDoS), dan teori-teori lain yang memiliki hubungan dengan penelitian skripsi

BAB III METODOLOGI PENELITIAN

Metodologi penelitian ini akan mencakup metodologi penelitian, persiapan perangkat & *tools,* pembuatan *dataset*, pengolahan data dan implementasi *random forest.*

BAB IV PENGUJIAN DAN ANALISA

Bab ini menjelaskan bagaimana dilakukannya pengujian dan analisa data yang didapat dari hasil pengujian yang dilakukan.

BAB V KESIMPULAN

Pada bab ini akan dilakukan penarikan beberapa kesimpulan dari penjelasan yang ada di bab sebelumnya serta diberikan saran yang dapat membangun guna penelitian selanjutnya.

DAFTAR PUSTAKA

[1] B. Yuan, J. Wan, Y. H. Wu, D. Q. Zou, and H. Jin, "A Survey on the Applications of Smart Home Systems," *J. Comput. Sci. Technol.*, vol. 38, no. 2, pp. 228–247, 2023, doi: 10.1007/s11390-023-2488-3.

[2] A. K. Ray and A. Bagwari, "IoT based smart home: Security aspects and security architecture," *Proc. - 2020 IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2020*, vol. 1, pp. 218–222, 2020, doi: 10.1109/CSNT48778.2020.9115737.

[3] A. Chakraborty, M. Islam, F. Shahriyar, S. Islam, H. U. Zaman, and M. Hasan, "Smart Home System: A Comprehensive Review," *J. Electr. Comput. Eng.*, vol. 2023, 2023, doi: 10.1155/2023/7616683.

[4] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of Smart-Home Security Using the Internet of Things," *Electron.*, vol. 13, no. 16, 2024, doi: 10.3390/electronics13163343.

[5] O. E. Elejla, M. Anbar, S. Hamouda, S. Faisal, A. A. Bahashwan, and I. H. Hasbullah, "Deep-Learning-Based Approach to Detect ICMPv6 Flooding DDoS Attacks on IPv6 Networks," *Appl. Sci.*, vol. 12, no. 12, 2022, doi: 10.3390/app12126150.

[6] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "Intrusion Detection Systems of ICMPv6-based DDoS attacks," *Neural Comput. Appl.*, vol. 30, no. 1, pp. 45–56, 2018, doi: 10.1007/s00521-016-2812-8.

[7] M. Šimon and L. Huraj, "A Study of DDoS Reflection Attack on Internet of Things in IPv4/IPv6 Networks," *Adv. Intell. Syst. Comput.*, vol. 984, pp. 109–118, 2019, doi: 10.1007/978-3-030-19807-7_12.

[8] M. Anbar, R. Abdullah, B. N. Al-Tamimi, and A. Hussain, "A Machine Learning Approach to Detect Router Advertisement Flooding Attacks in Next-Generation IPv6 Networks," *Cognit. Comput.*, vol. 10, no. 2, pp. 201–214, 2018, doi: 10.1007/s12559-017-9519-8.

[9] R. M. A. Saad, M. Anbar, S. Manickam, and E. Alomari, "An intelligent ICMPv6 DDoS flooding-attack detection framework (V6IIDS) using back-propagation neural network," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 33, no. 3, pp. 244–255, 2016, doi: 10.1080/02564602.2015.1098576.

[10] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," *Symmetry (Basel).*, vol. 14, no. 6, pp. 1–15, 2022, doi: 10.3390/sym14061095.

[11] H. Chen, Yini; Hou, Jun; Qianmu, Li; Long, "DDoS Attack Detection Based on Random Forest," *ieee*, pp. 1–7, 2020.

[12] R. M. A. Saad, A. Almomani, A. Altaher, B. B. Gupta, and S. Manickam,

"ICMPv6 flood attack detection using DENFIS algorithms," *Indian J. Sci. Technol.*, vol. 7, no. 2, pp. 168–173, 2014, doi: 10.17485/ijst/2014/v7i2.5.

[13] J. S. Nixon and M. Amenu, "Investigating Security Issues and Preventive Mechanisms in Ipv6 Deployment," *Int. J. Adv. Eng. Nano Technol.*, vol. 9, no. 2, pp. 1–20, 2022, doi: 10.35940/ijaent.b0466.029222.

[14] A. Alsadhan *et al.*, "Locally weighted classifiers for detection of neighbor discovery protocol distributed denial-of-service and replayed attacks," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, pp. 1–15, 2022, doi: 10.1002/ett.3700.

[15] M. Tayyab, B. Belaton, and M. Anbar, "ICMPV6-based DOS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review," *IEEE Access*, vol. 8, pp. 170529–170547, 2020, doi: 10.1109/ACCESS.2020.3022963.

[16] G. M. H. Amlak, F. Q. Kamal, and A. K. Al-Ani, "Denial of service attack on neighbor discovery protocol processes in the network of IPv6 link-local," *Int. J. Electr. Electron. Eng. Telecommun.*, vol. 9, no. 4, pp. 247–251, 2020, doi: 10.18178/ijeetc.9.4.247-251.

[17] O. V. P. Salmakayala, S. S. Ghidary, and C. Howard, "Detection of ICMPv6 DDoS Attacks using Hybridization of RNN and GRU," pp. 297–317, 2024, doi: 10.5121/csit.2024.141423.

[18] Y. Alharbi, A. Alferaidi, K. Yadav, G. Dhiman, and S. Kautish, "Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/8000869.

[19] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi, and A. K. Al-Ani, *Comparison of classification algorithms on ICMPv6-based DDoS attacks detection*, vol. 481. Springer Singapore, 2019. doi: 10.1007/978-981-13-2622-6_34.

[20] A. A. Anitha and D. L. Arockiam, "Ada-IDS: AdaBoost Intrusion Detection System for ICMPv6 based Attacks in Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 11, pp. 499–506, 2021, doi: 10.14569/IJACSA.2021.0121156.

[21] T. A. H. H. . Elejla, Omar E.; ANBAR, MUHAMMED; Hamouda, Shady; Belaton, Bahari; Al-Amiedy, "Flow-Based IDS Features Enrichment for ICMPv6-DDoS Attacks Detection," *Symmetry (Basel).*, pp. 1–25, 2022.

[22] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-Prevention Technique against Denial-of-Service Attack on Address Resolution and Duplicate Address Detection Processes in IPv6 Link-Local Network," *IEEE Access*, vol. 8, pp. 27122–27138, 2020, doi: 10.1109/ACCESS.2020.2970787.

[23] A. F. Daru, K. D. Hartomo, and H. D. Purnomo, "IPv6 flood attack detection based on epsilon greedy optimized Q learning in single board computer," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 5, pp. 5782–5791, 2023, doi:

10.11591/ijece.v13i5.pp5782-5791.

[24] O. A. Quadri and A. O. David, “Detection and Mitigation of Flood Attacks in IPv6 Enabled Software Defined Networks,” *Adv. Res.*, no. July, pp. 1–9, 2020, doi: 10.9734/air/2020/v21i830221.

[25] N. Alsharabi, M. Alqunun, and B. A. H. Murshed, “Detecting Unusual Activities in Local Network Using Snort and Wireshark Tools,” *J. Adv. Inf. Technol.*, vol. 14, no. 4, pp. 616–624, 2023, doi: 10.12720/jait.14.4.616-624.

[26] B. Dodiya and U. K. Singh, “Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise,” *Int. J. Comput. Appl.*, vol. 183, no. 53, pp. 1–6, 2022, doi: 10.5120/ijca2022921876.

[27] M. F. Wofford, B. M. Boscoe, C. L. Borgman, I. V. Pasquetto, and M. S. Golshan, “Jupyter Notebooks as Discovery Mechanisms for Open Science: Citation Practices in the Astronomy Community,” *Comput. Sci. Eng.*, vol. 22, no. 1, pp. 5–15, 2020, doi: 10.1109/MCSE.2019.2932067.

[28] A. Suárez-García, E. Arce-Fariña, M. Álvarez Hernández, and M. Fernández-Gavilanes, “Teaching structural analysis theory with Jupyter Notebooks,” *Comput. Appl. Eng. Educ.*, vol. 29, no. 5, pp. 1257–1266, 2021, doi: 10.1002/cae.22383.

[29] J. Xu, Y. Zhang, and D. Miao, “Three-way confusion matrix for classification: A measure driven view,” *Inf. Sci. (Ny).*, vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[30] E. Jukes, *Encyclopedia of Machine Learning and Data Mining (2nd edition)*, vol. 32, no. 7/8. 2018. doi: 10.1108/rr-05-2018-0084.