DETEKSI SERANGAN *FLOODING* PADA JARINGAN SMART HOME *IPv6* MENGGUNAKAN METODE *DECISION TREE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

DHANI SAPUTRA

09011182126019

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

DETEKSI SERANGAN *FLOODING* PADA JARINGAN *SMART HOME* IPv6 MENGGUNAKAN METODE *DECISION TREE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :
DHANI SAPUTRA
09011182126019

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN *FLOODING* PADA JARINGAN *SMART HOME IPv6* MENGGUNAKAN METODE *DECISION TREE*

Sebagai salah satu syarat untuk penyelesaian studi di
Program Studi S1 Sistem Komputer

Oleh:

DHANI SAPUTRA

09011182126019

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.
NIP. 196612032006041001

AUTHENTICATION PAGE

FINAL TASK

FLOODING ATTACK DETECTION IN IPv6-BASED SMART HOME NETWORKS USING THE DECISION TREE METHOD

As one of the requirements for completing the
Bachelor's Degree Program in Computer Systems

By:

DHANI SAPUTRA

09011182126019

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

Approved by,
Head of Computer System Department

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 25 Juli 2025

Tim Penguji :

1. Ketua Sidang : Dr. Ir. Ahmad Heryanto, M.T. _____
2. Penguji Sidang : Ahmad Fali Oklilas, M.T. _____
3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D. _____
4. Pembimbing II : Adi Hermansyah, M.T. _____

Mengetahui, 26/8/25
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

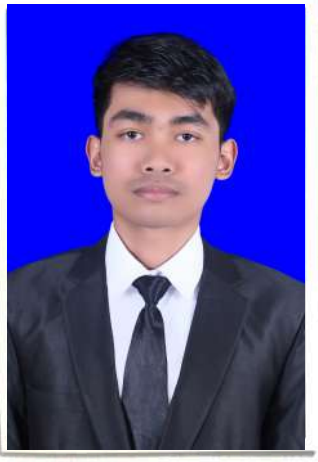
Yang bertanda Tangan dibawah ini:

Nama	**: Dhani Saputra**
Nim	**: 09011182126019**
Judul Tugas Akhir	**: Deteksi Serangan *Flooding* pada Jaringan *Smart Home IPv6* Menggunakan Metode *Decision Tree***

Hasil pemeriksaan iThenticate/Turnitin : 2%

Menyatakan bahwa laporan Tugas Akhir ini adalah hasil karya Saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, Saya siap menerima sanksi akademik di Universitas Sriwijaya.

Demikian, pernyataan ini Saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.



Indralaya, 13 Agustus 2025

Dhani Saputra
NIM. 09011182126019

Flooding Attack Detection in IPv6-Based Smart Home Networks Using The Decision Tree Method

Dhani Saputra (09011182126019)

Dept. of Computer System, Faculty of Computer Science, Sriwijaya University

Email : dhanisaputra772@gmail.com

ABSTRACT

The ICMPv6 "Packet TOO BIG" Flooding attack poses a serious threat to IPv6 network security, particularly when exploiting vulnerabilities in the EUI-64-based automatic address configuration mechanism and the Privacy Extension feature. In this scenario, an attacker uses a single fixed source to send a large number of malicious ICMPv6 packets to various destination address variations derived from the same address structure. This technique takes advantage of weaknesses in packet handling and the deterministic nature of the EUI-64 format, potentially leading to network overload and degraded performance. This study utilizes a simulated dataset to detect such attacks using the Decision Tree algorithm. The model is trained on labeled traffic data consisting of two classes: Benign and Flood. Evaluation results show an accuracy of 92.38%. The precision for the Benign class reaches 100%, while the Flood class achieves 86.77%. The recall for the Benign class is 84.74%, and 100% for the Flood class. The F1-Score indicates balanced performance: 91.70% for Benign and 92.91% for Flood.

Keyword : *ICMPv6 Flooding, IPv6, Packet TOO BIG, Decision Tree, EUI-64 Vulnerability, Privacy Extension, Machine Learning*

Deteksi Serangan *Flooding* Pada Jaringan *Smart Home IPv6* Menggunakan Metode *Decision Tree*

Dhani Saputra (09011182126019)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : dhanisaputra772@gmail.com

ABSTRAK

Serangan *Flooding ICMPv6 "Packet TOO BIG"* merupakan ancaman serius bagi keamanan jaringan *IPv6*, khususnya saat mengeksploitasi kerentanan pada mekanisme alamat otomatis *EUI-64* dan fitur *Privacy Extension*. Dalam skenario ini, penyerang menggunakan satu sumber tetap untuk mengirim banyak paket *ICMPv6* berbahaya ke variasi alamat tujuan dari struktur alamat yang sama. Teknik ini memanfaatkan kelemahan penanganan paket dan sifat deterministik *EUI-64*, yang dapat menyebabkan beban berlebih dan penurunan performa jaringan. Penelitian ini menggunakan dataset simulasi untuk mendeteksi serangan menggunakan algoritma *Decision Tree*. Model dilatih pada data yang dilabeli dua kelas: *Benign* dan *Flood*. Hasil evaluasi menunjukkan akurasi terbaik sebesar 92,37%. Presisi kelas *Benign* mencapai 100%, kelas *Flood* 86,77%. Recall kelas *Benign* 84,74%, sedangkan *Flood* mencapai 100%. F1-Score menunjukkan keseimbangan kinerja: 91,70% untuk kelas *Benign* dan 92,91% untuk kelas *Flood*.

Kata Kunci : *ICMPv6 Flooding, IPv6,* Paket *"Packet TOO BIG", Decision Tree,* Kerentanan *EUI-64, Privacy Extension, Machine Learning*

KATA PENGANTAR

Assalamu'alaikum Wr. Wb. Puji syukur penulis panjatkan ke hadirat Allah SWT yang telah melimpahkan rahmat, kasih sayang, dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul "**Deteksi Serangan *Flooding* Pada Jaringan *Smart Home IPV6* menggunakan metode *Decision Tree***". Shalawat beriringkan salam senantiasa tercurahkan kepada Nabi Muhammad SAW yang telah membawa cahaya petunjuk bagi umat manusia dan menjadi teladan utama dalam kehidupan**.**

Sepanjang proses penulisan Tugas Akhir ini yang merupakan salah satu syarat untuk memenuhi sebagian kurikulum dan syarat kelulusan Mata Kuliah Skripsi pada Jurusan Sistem Komputer, Universitas Sriwijaya, Dalam penyusunan Tugas Akhir ini penulis tidak berjalan sendirian. Banyak pihak yang telah memberikan bantuan, bimbingan, dan dukungan. Pada kesempatan yang penuh rasa syukur ini, penulis ingin menyampaikan ucapan terima kasih yang tulus kepada:

1. Allah SWT, yang dengan segala limpahan rahmat dan kasih-Nya, memberikan kesehatan, kekuatan, dan kesempatan sehingga penulis dapat menyelesaikan proposal ini.
2. Kedua orang tua tercinta, yang tak pernah lelah memberikan cinta, doa, dan dukungan tanpa syarat. Setiap tetes keringat, setiap doa yang dipanjatkan, dan setiap nasihat yang diberikan adalah sumber kekuatan bagi penulis. Tanpa mereka, pencapaian ini tentu tidak akan mungkin terwujud. Terima kasih telah menjadi pelita dalam kegelapan dan tempat berpulang dalam setiap langkah perjuangan hidup.
3. Prof. Dr. Erwin, S.Si, M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya, atas segala bantuan dan dukungannya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Akademik serta Dosen Pembimbing I Tugas Akhir yang dengan sabar dan teliti telah memberikan bimbingan, motivasi, serta nasihat yang sangat berharga dalam proses penyusunan tugas akhir ini.

6. Bapak Adi Hermansyah,M.T., selaku Dosen Pembimbing II Tugas Akhir yang dengan sabar dan teliti telah memberikan bimbingan, motivasi, serta nasihat yang sangat berharga dalam proses penyusunan tugas akhir ini.
7. Kakak Angga, selaku admin Jurusan Sistem Komputer, yang dengan cepat dan sigap membantu dalam pengurusan berkas administrasi.
8. Semua Dosen dan Staff Administrasi Jurusan Sistem Komputer Universitas Sriwijaya.
9. Kepada Mutiah Andini dan rekan-rekan dari tim riset *Smart Home* IPv6 dan COMNETS, serta seluruh teman seperjuangan Angkatan 2021 Jurusan Sistem Komputer, saya ucapkan terima kasih atas segala bentuk dukungan yang telah diberikan selama ini.
10. Serta seluruh pihak yang telah memberikan bantuan, dukungan, dan dorongan semangat yang tak dapat disebutkan satu per satu. Terima kasih untuk segalanya.
11. Alamemeter Universitas Sriwijaya

Penulis menyadari bahwa laporan ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa depan. Semoga Proposal Tugas Akhir ini dapat bermanfaat bagi semua pihak yang membacanya.

Wassalamu'alaikum Wr. Wb.

Indralaya, 13 Agustus 2025

Dhani Saputra
NIM. 09011182126019

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Smart Home adalah sebuah sistem rumah pintar yang terdiri dari perangkat elektronik yang saling terhubung dan dapat dikendalikan secara langsung maupun jarak jauh [1]. Sistem ini memanfaatkan teknologi otomatisasi serta koneksi internet untuk memungkinkan pengguna memantau, mengontrol, dan mengelola berbagai fungsi di dalam rumah, seperti pencahayaan, sistem keamanan, pengaturan suhu, dan perangkat elektronik lainnya dengan lebih mudah dan efisien. Pengoperasian perangkat-perangkat tersebut dapat dilakukan melalui aplikasi smartphone ataupun perintah suara, sehingga *Smart Home* menjadi solusi modern yang praktis untuk meningkatkan kenyamanan, efisiensi, dan keamanan dalam kehidupan sehari-hari.

Semakin berkembangnya teknologi *Internet Of Thing*s (IoT), penggunaan jaringan IPv6 di lingkungan *Smart Home* semakin meluas. IoT telah menjadi salah satu pendorong utama transisi dari IPv4 ke IPv6. Menurut perkiraan [2], pada tahun 2025 akan ada lebih dari 75 miliar perangkat IoT yang aktif di seluruh dunia. Setiap perangkat ini membutuhkan alamat IP unik untuk dapat terhubung ke jaringan, menjadikan ketersediaan ruang alamat IPv6 yang sangat besar sebagai kebutuhan yang mendesak.

Sebagai respons terhadap tantangan ini, Kementerian Komunikasi dan Informatika Republik Indonesia [3]. Menerbitkan Surat Edaran Nomor 5 dan Nomor 6 Tahun 2024 yang menghimbau Kementerian atau Lembaga dan Pemerintah Daerah untuk mengaktifkan dan menggunakan alamat Protokol Internet Versi 6 (IPv6). Surat edaran ini menekankan pentingnya adopsi IPv6 dalam menciptakan ekosistem infrastruktur yang aman dan andal, serta memberikan kepastian keamanan dalam penggunaan data publik.

Meskipun adopsi IPv6 terus meningkat, hal ini juga disertai dengan berbagai tantangan keamanan yang perlu mendapat perhatian, khususnya yang berkaitan dengan protokol-protokol dalam pengelolaan perangkat serta komunikasi jaringan, sebagaimana disampaikan dalam penelitian sebelumnya [4]. Eksploitasi serangan *Flooding* melalui protokol ICMPv6 dapat secara langsung mengakibatkan

kehabisan sumber daya pada perangkat jaringan. Serangan *Flooding* ICMPv6 terjadi ketika penyerang mengirimkan sejumlah besar pesan ke dalam jaringan, yang membanjiri sistem dan mengganggu komunikasi antar perangkat, sebagaimana dijelaskan dalam penelitian [5]. Salah satu bentuk serangan ini adalah pengiriman pesan ICMPv6 'Packet *TOO BIG*', yang mengeksploitasi Path MTU (Maximum Transmission Unit) untuk mengganggu komunikasi dengan memaksa perangkat menerima paket secara berlebihan.

Pada penelitian [6], mendeteksi serangan pada *Routing Protocol for Low-Power and Lossy Networks* (RPL), yang umum digunakan dalam aplikasi *Internet Of Thing*s (IoT) berbasis IPv6. Menggunakan dataset ROUT-4-2023 yang dibuat dengan simulator Cooja, penelitian ini mencakup deteksi empat jenis serangan routing: Blackhole, *Flooding*, DODAG Version Number, dan Decreased Rank Attack. Algoritma *Decision Tree* dan Bagging mencapai akurasi tertinggi 99,99%, sedangkan pada dataset yang diberi kebisingan 10%, algoritma Random Forest menunjukkan akurasi 84,80%. Hasil ini menunjukkan potensi teknik pembelajaran mesin sebagai Sistem Deteksi Intrusi (IDS) untuk melindungi jaringan IoT dari berbagai serangan.

Dalam penelitian [7], memiliki beberapa kelebihan dan kelemahan. Kelebihan utamanya adalah kemampuannya untuk menghasilkan model yang mudah diinterpretasikan, sehingga pengguna dapat dengan cepat memahami aturan klasifikasi yang dihasilkan. *Decision Tree* juga efektif dalam menangani data dengan fitur yang tidak linier dan dapat mengklasifikasikan data dengan akurasi yang tinggi, seperti yang ditunjukkan dengan hasil akurasi 99,99% dalam beberapa pengujian. Namun, kelemahannya termasuk kecenderungan untuk melakukan overfitting yang dimana dapat mengurangi generalisasi model terhadap data baru. Selain itu, *Decision Tree* sangat sensitif terhadap perubahan kecil dalam data, yang dapat menyebabkan perbedaan yang signifikan dalam struktur pohon yang dihasilkan.

1.2 Tujuan

Berdasarkan latar belakang yang telah diuraikan, penelitian ini memiliki beberapa tujuan, antara lain:

1. Menjelaskan proses ekstraksi data untuk menemukan informasi dari file pcapng menggunakan *Tshark*.
2. Mengidentifikasi perbedaan antara pola lalu lintas normal dan pola lalu lintas serangan.
3. Mengevaluasi kinerja model *Decision Tree* dalam mendeteksi serangan *Flooding* ICMPv6 *Packet TOO BIG* pada jaringan *Smart Home* berbasis IPv6.

1.3 Manfaat

Adapun manfaat yang diharapkan dari penulisan Tugas Akhir ini mencakup beberapa hal penting yang dapat berkontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan jaringan, sebagai berikut:

1. Memahami karakteristik unik antara paket serangan *Flooding* dan paket normal, sehingga dapat membantu mengidentifikasi pola serangan secara lebih efisien.
2. Memahami pola lalu lintas yang mencurigakan sehingga memverifikasi serangan *Flooding ICMPv6* benar-benar terjadi..
3. Dapat mendeteksi serangan *Flooding ICMPv6* melakukan evaluasi untuk mencari nilai optimal dari metode *Decision Tree*.

1.4 Perumusan dan Batasan Masalah

1.4.1 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, Dengan semakin berkembangnya teknologi IoT dan adopsi *IPv6* pada jaringan *Smart Home*, muncul tantangan terkait potensi serangan *Flooding* yang dapat mengganggu komunikasi dan ketersediaan jaringan. Oleh karena itu, penelitian ini memiliki beberapa rumusan masalah, antara lain:

1. Apa saja informasi penting yang dapat diekstraksi dari file .pcapng terkait lalu lintas jaringan?
2. Bagaimana cara membedakan pola lalu-lintas normal dan pola lalu-lintas serangan?
3. Bagaimana efektivitas penerapan metode *Decision Tree*, dalam mendeteksi serangan *Flooding ICMPv6* di jaringan IPv6 *Smart Home*?

1.4.2 Batasan Masalah

Untuk memfokuskan penelitian ini, ruang lingkup dan aspek yang diteliti perlu dibatasi. Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Dataset yang digunakan merupakan dataset hasil riset dari ComNets yang digunakan sebagai data latih dan data uji yang terdiri dari data normal, data serangan dan data gabungan.
2. Penelitian ini dilakukan hanya sebatas pendeteksian sebuah serangan *Flooding* terhadap *Smart Home* di jaringan IPv6.
3. Output yang dihasilkan dari penelitian ini seberapa akurat metode *Decision Tree* dalam mendeteksi sebuah serangan *Flooding* pada jaringan IPv6 pada perangkat *Smart Home*.

1.5 Metodologi Penelitian

1.5.1 Metode Tinjauan Pustaka dan Literatur

Metode ini dilakukan dengan mencari dan mengumpulkan referensi dari tinjauan pustaka serta literatur yang terdapat dalam jurnal-jurnal akses terbuka. Fokusnya adalah pada studi-studi yang membahas tentang deteksi serangan *Flooding* di IPv6

1.5.2 Metode Konsultasi

Penulis melakukan diskusi intensif dengan para pakar dan ahli di bidang terkait untuk memperoleh wawasan mendalam dan memvalidasi hasil penelitian melalui komunikasi langsung atau platform online. Konsultasi ini bertujuan untuk mendapatkan pemahaman yang lebih baik serta solusi atas permasalahan yang ditemui selama proses riset.

1.5.3 Metode Pengolahan Data

Dalam metode ini, penulis mengekstrak data yang ditangkap oleh Wireshark dari file pcapng ke format CSV menggunakan *T-Shark*. Setelah itu penulis melakukan Pembersihan Data, Eksplorasi Data, Pemilihan Fitur, Pelabelan data berdasarkan pola serangan yang akan diidentifikasi dan dideteksi, Normalisasi Data dan melakukan balancing data menggunakan metode *SMOTE (Synthetic Minority Over-sampling Technique)*.

1.5.4 Metode Perancangan model dan pengujian

Dalam metode ini, penulis menggunakan algoritma *Decision Tree* untuk merancang model berdasarkan dataset yang telah diproses sebelumnya, kemudian melakukan pengujian dengan tujuan untuk mencapai akurasi yang optimal.

1.5.5 Metode Analisa dan Kesimpulan

Pada tahap ini, penulis melakukan analisis komprehensif terhadap hasil penelitian, mengidentifikasi kesimpulan dan mengembangkan rekomendasi konstruktif untuk penelitian masa mendatang.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

BAB I membahas latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan juga sistematika penulisan pada penelitian ini.

BAB II TINJAUAN PUSTAKA

BAB II berisi ulasan literatur tentang penelitian sebelumnya serta teori yang relevan untuk mendukung penelitian ini. Teori-teori yang dibahas mengenai IPv6, *Smart Home*, *Flooding*, machine learning dan *Decision Tree*.

BAB III METODOLOGI PENELITIAN

BAB III menjelaskan tentang proses penelitian, kerangka kerja, dimulai dari proses pembuatan dataset, pengolahan data, serta perancangan model dan pelatihan model *Decision Tree*.

BAB IV HASIL DAN ANALISA

BAB IV menyajikan hasil penelitian, dimulai dari evaluasi model dan kinerja, akurasi dan visualisasi dalam ” Deteksi Serangan *Flooding* Pada Jaringan *Smart Home IPv6*”

BAB V KESIMPULAN DAN SARAN

BAB V menyajikan kesimpulan penelitian, dan memberikan rekomendasi strategis untuk penelitian selanjutnya.

DAFTAR PUSTAKA

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

[2] R. Liu, Z. Weng, S. Hao, D. Chang, C. Bao, and X. Li, "Addressless: Enhancing IoT Server Security Using IPv6," *IEEE Access*, vol. 8, pp. 90294–90315, 2020, doi: 10.1109/ACCESS.2020.2993700.

[3] Kementerian Komunikasi dan Informatika, "Surat Edaran Menteri Kominfo Nomor 5 dan Nomor 6 Tahun 2024 tentang Himbauan Mengaktifkan dan Menggunakan Alamat Protokol Internet Versi 6 (IPv6) pada Kementerian/Lembaga dan Pemerintah Daerah serta pada Penyelenggara Telekomunik asi," https://dittel.kominfo.go.id/berita/artikel/memahami-lebih-jauh-kebijakan-implementasi-ipv6-di-indonesia.html.

[4] L. Zhang, W. Xia, W. Huang, W. Du, Y. Guo, and L. Cheng, "6*Flood*Detector: An IPv6 *Flooding* Behaviors Detection Technology Based on Eigenvalues and Thresholds," in *2022 IEEE 22nd International Conference on Communication Technology (ICCT)*, IEEE, Nov. 2022, pp. 1375–1379. doi: 10.1109/ICCT56141.2022.10072952.

[5] Y. Huang, S. Nazir, X. Ma, S. Kong, and Y. Liu, "Acquiring Data Traffic for Sustainable IoT and Smart Devices Using Machine Learning Algorithm," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/1852466.

[6] B. Aydın, H. Aydın, S. Görmüş, and E. Mollahasanoğlu, "Detection of RPL-based Routing Attacks Using Machine Learning Algorithms," *DÜMF Mühendislik Dergisi*, Nov. 2024, doi: 10.24012/dumf.1490367.

[7] D. Tymoshchuk, O. Yasniy, V. Tymoshchuk, O. Yasniy, M. Mytnyk, and N. Zagorodna, "Detection and classification of DDoS *Flooding* attacks by machine learning method," 2024. [Online]. Available: https://www.researchgate.net/publication/387511341

[8] Zerin Hasan Sahosh, Azraf Faheem, Marzana Bintay Tuba, Md. Istiaq Ahmed, and Syed Anika Tasnim, "A Comparative Review on DDoS Attack Detection Using Machine Learning Techniques," *Malaysian Journal of Science and Advanced Technology*, pp. 75–83, Mar. 2024, doi: 10.56532/mjsat.v4i2.208.

[9] R. Panigrahi *et al.*, "A consolidated *Decision Tree*-based intrusion detection system for binary and multiclass imbalanced datasets," *Mathematics*, vol. 9, no. 7, Apr. 2021, doi: 10.3390/math9070751.

[10] O. E. Elejla, B. Belaton, M. Anbar, and I. M. Smadi, “A New Set of Features for Detecting Router Advertisement *Flooding* Attacks,” in *Proceedings - 2017 Palestinian International Conference on Information and Communication Technology, PICICT 2017*, Institute of Electrical and Electronics Engineers Inc., Sep. 2017, pp. 1–5. doi: 10.1109/PICICT.2017.19.

[11] A. A. Najar and M. N. S., “A Robust DDoS Intrusion Detection System Using Convolutional Neural Network,” *Computers and Electrical Engineering*, vol. 117, Jul. 2024, doi: 10.1016/j.compeleceng.2024.109277.

[12] K. Muthamil Sudar and P. Deepalakshmi, “A two level security mechanism to detect a DDoS *Flooding* attack in software-defined networks using entropy-based and C4.5 technique,” *Journal of High Speed Networks*, vol. 26, no. 1, pp. 55–76, 2020, doi: 10.3233/jhs-200630.

[13] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram, “A Reliable Network Intrusion Detection Approach Using *Decision Tree* with Enhanced Data Quality,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/1230593.

[14] F. Najjar, Q. Bsoul, and H. Al-Refai, “An Analysis of Neighbor Discovery Protocol Attacks,” *Computers*, vol. 12, no. 6, Jun. 2023, doi: 10.3390/computers12060125.

[15] 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, Apr. 2018, doi: 10.1007/s12559-017-9519-8.

[16] S. Wang *et al.*, “Detecting *Flooding* DDoS attacks in software defined networks using supervised learning techniques,” *Engineering Science and Technology, an International Journal*, vol. 35, Nov. 2022, doi: 10.1016/j.jestch.2022.101176.

[17] F. Najjar, M. M. Kadhum, and H. El-Taj, “Detecting neighbor discovery protocol-based *Flooding* attack using machine learning techniques,” in *Lecture Notes in Electrical Engineering*, Springer Verlag, 2016, pp. 129–139. doi: 10.1007/978-3-319-32213-1_12.

[18] D. Tymoshchuk, O. Yasniy, M. Mytnyk, N. Zagorodna, and V. Tymoshchuk, “Detection and classification of DDoS *Flooding* attacks by machine learning method,” 2024.

[19] Y. Han, L. Zhang, Y. Wang, X. Deng, Z. Gu, and X. Zhang, “Research on the Security of IPv6 Communication Based on Petri Net under IoT,” *Sensors*, vol. 23, no. 11, Jun. 2023, doi: 10.3390/s23115192.

[20] O. M. Almorabea, T. J. S. Khanzada, M. A. Aslam, F. A. Hendi, and A. M. Almorabea, “IoT Network-Based Intrusion Detection Framework: A Solution to Process Ping *Flood*s Originating from Embedded Devices,” *IEEE Access*, vol. 11, pp. 119118–119145, 2023, doi: 10.1109/ACCESS.2023.3327061.

[21] 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,” *Applied Sciences (Switzerland)*, vol. 12, no. 12, Jun. 2022, doi: 10.3390/app12126150.

[22] A. S. Ahmed, R. Hassan, N. E. Othman, N. I. Ahmad, and Y. Kenish, “Impacts evaluation of DoS attacks over IPv6 neighbor discovery protocol,” *Journal of Computer Science*, vol. 15, no. 5, pp. 702–727, 2019, doi: 10.3844/jcssp.2019.702.727.

[23] M. Schrötter, T. Scheffler, and B. Schnor, “Evaluation of intrusion detection systems in IPv6 networks,” in *ICETE 2019 - Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, SciTePress, 2019, pp. 408–416. doi: 10.5220/0007840104080416.

[24] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, “A DDoS Attack Detection Method Based on SVM in Software Defined Network,” *Security and Communication Networks*, vol. 2018, Apr. 2018, doi: 10.1155/2018/9804061.

[25] J. David and C. Thomas, “Efficient DDoS *Flood* attack detection using dynamic thresholding on flow-based network traffic,” *Comput Secur*, vol. 82, pp. 284–295, May 2019, doi: 10.1016/j.cose.2019.01.002.

[26] A. Alsadhan *et al.*, “Locally weighted classifiers for detection of neighbor discovery protocol distributed denial-of-service and replayed attacks,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3700.

[27] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, “*Smart Home* : architecture, technologies and systems,” in *Procedia Computer Science*, Elsevier B.V., 2018, pp. 393–400. doi: 10.1016/j.procs.2018.04.219.

[28] Dhani Saputra, “‘DALL·E: AI system that creates images from text,’” OpenAI.

[29] Md. Hossain, J. Binti, and Md. Uddin, “A Review Paper on IPv4 and IPv6: A Comprehensive Survey,” *American Journal of Computer Science and Technology*, vol. 7, no. 4, pp. 170–175, Oct. 2024, doi: 10.11648/j.ajcst.20240704.14.

[30] S. Zander and X. Wang, “Are we there yet? ipv6 in Australia and China,” *ACM Trans Internet Technol*, vol. 18, no. 3, Feb. 2018, doi: 10.1145/3158374.

[31] B. R. Dawadi, D. B. Rawat, S. R. Joshi, and P. Manzoni, “Towards Smart Networking with SDN Enabled IPv6 Network,” Mar. 2022, [Online]. Available: http://arxiv.org/abs/2203.01528

[32] 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,” 2020, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2020.3022963.

[33] A. Conta, Transwitch, and S. Deering, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,” Mar. 2006. Accessed: May 19, 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4443

[34] A. S. A. Mohamed Sid Ahmed, R. Hassan, and N. E. Othman, “IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey,” *IEEE Access*, vol. 5, pp. 18187–18210, Aug. 2017, doi: 10.1109/ACCESS.2017.2737524.

[35] W. Simpson and D. H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” 2007.

[36] R. Hinden and S. Deering, “IP Version 6 Addressing Architecture,” Feb. 2006. doi: 10.17487/RFC4291.

[37] T. Narten, R. Draves, S. Krishnan, and Ericsson Research, “*Privacy Extensions* for Stateless Address Autoconfiguration in IPv6,” Sep. 2007. Accessed: May 19, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4941/

[38] T. R. Reshmi, S. M. Manoharan, and K. Murugan, “Internal Hardware States Based Privacy Extension of IPv6 Addresses,” in *Communications in Computer and Information Science*, Springer Verlag, 2014, pp. 263–271. doi: 10.1007/978-3-662-44966-0_25.

[39] A. Conta, S. Deering, and M. Gupta, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,” Mar. 2006. Accessed: Feb. 19, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4443

[40] L. Rokach and O. Maimon, “*DECISION TREE*S,” Jan. 2005. Accessed: Feb. 22, 2025. [Online]. Available: DOI:10.1007/0-387-25465-X_9

[41] I. D. Mienye and N. Jere, “A Survey of *Decision Tree*s: Concepts, Algorithms, and Applications,” *IEEE Access*, vol. 12, pp. 86716–86727, 2024, doi: 10.1109/ACCESS.2024.3416838.

[42] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, “An improved method to construct basic probability assignment based on the confusion matrix for classification problem,” *Inf Sci (N Y)*, vol. 340–341, pp. 250–261, May 2016, doi: 10.1016/j.ins.2016.01.033.

[43] S. J. Saidi, O. Gasser, and G. Smaragdakis, “One Bad Apple Can Spoil Your IPv6 Privacy,” Mar. 2022, [Online]. Available: http://arxiv.org/abs/2203.08946