DETEKSI SERANGAN DDoS PADA IPv6 MENGGUNAKAN METODE PENGKLASIFIKASIAN *SUPPORT VECTOR MACHINE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH :

Muhammad Abimanyu Iwari Rama Putra

09011381823104

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

DETEKSI SERANGAN DDoS PADA IPv6 MENGGUNAKAN METODE PENGKLASIFIKASIAN *SUPPORT VECTOR MACHINE*

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh

Muhammad Abimanyu Iwari Rama Putra

09011381823104

Palembang, 28 Maret 2023

Mengetahui,

Pembimbing 1 Tugas Akhir	Pembimbing 2 Tugas Akhir
Ahmad Heryanto, S. Kom, M.T.	**Tri Wanda Septian, M.Sc.**
NIP. 198701222015041002	**NIK. 1901062809890001**

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 07 Maret 2023

Tim Penguji :

1. **Ketua : Rossi Passarella, S.T., M. Eng**
2. **Sekretaris : Muhammad Ali Buchari. S.Kom., M.T**
3. **Pembimbing 1 : Ahmad Heryanto, S. Kom, M.T.**
4. **Pembimbing 2 : Tri Wanda Septian, M.Sc.**
5. **Penguji : Aditya Putra Perdana P, M.T.**

Mengetahui, 27/2/23

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhammad Abimanyu Iwari Rama Putra

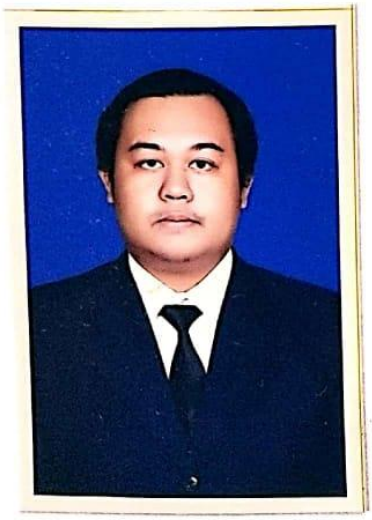
NIM : 09011381823104

Judul : Deteksi Serangan DDoS Pada IPv6 Menggunakan Metode Pengklasifikasian Support Vector Machine

Hasil Pengecekan Software iThenticate/Turnitin : 7%

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, 28 Maret 2023

Muhammad Abimanyu Iwari Rama Putra
NIM. 09011381823104

Detection of DDoS Attacks on IPv6 Using Support Vector Machine Classification Method

Muhammad Abimanyu Iwari Rama Putra (09011381823104)

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

Email : abimanyuiwari@gmail.com

ABSTRACT

DDoS attack is one of the security threats frequently experienced on the internet, which utilizes multiple sources to send excessive traffic to a server, causing system failure, making DDoS a significant threat. To detect attacks, this research seeks to find parameters that play a significant role in the DDoS dataset. Therefore, feature selection is applied, namely the Random Forest Classifier (RFC), which is then combined with classification using the Support Vector Machine (SVM) method. In this study, the researchers use a self-made dataset.

Keyword : *DDoS, IPv6, Support Vector Machine, Random Forest Classifier.*

Palembang, 8 Maret 2023

Acknownledged By,

Supervisor

Ahmad Heryanto, S. Kom, M.T.
NIP. 198701222015041002

Co-Supervisor

Tri Wanda Septian, M.Sc.
NIK. 1901062809890001

Head of Computer Systems Department

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

Deteksi Serangan DDoS Pada IPv6 Menggunakan Metode Pengklasifikasian Support Vector Machine

Muhammad Abimanyu Iwari Rama Putra (09011381823104)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : abimanyuiwari@gmail.com

ABSTRAK

Serangan DDoS merupakan salah satu ancaman keamanan jaringan yang sering di alami di internet, dengan memanfaatkan banyak sumber untuk mengirimkan trafik yang berlebihan ke suatu server sehingga menyebabkan kegagalan pada sistem, membuat DDoS menjadi sebuah ancaman yang cukup berbahaya. Adapun untuk mengetahui pendeteksi serangan, dalam penyajian penelitian ini mencari parameter yang berperan besar dalam dataset DDoS. Maka perlu diterapkan fitur seleksi yaitu *Random Forest Classifier* (RFC). Yang kemudian di kolaborasikan dengan klasifikasi menggunakan metode *Support Vector Machine* (SVM). Pada penelitian ini menggunakan dataset yang peneliti buat sendiri.

Kata Kunci : *DDoS, IPv6, Support Vector Machine, Random Forest Classifier.*

Palembang, 21 Maret 2023

Mengetahui,

Pembimbing 1 Tugas Akhir	**Pembimbing 2 Tugas Akhir**
Ahmad Heryanto, S. Kom, M.T.	**Tri Wanda Septian, M.Sc.**
NIP. 198701222015041002	**NIK. 1901062809890001**

Ketua Jurusan Sistem Komputer

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

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

Assalamu'alaikum Warahmatullahi Wabarakatuh

Marilah kita panjatkan puji serta syukur atas kehadirat Allah SWT karena atas berkat hidayah dan karunia – Nya penulis telah dapat menyelesaikan penyusunan tugas akhir ini yang berjudul "**Deteksi Serangan DDoS Pada IPv6 Menggunakan Metode Pengklasifikasian *Support Vector Machine***". Sebelumnya, penulis ingin memberikan serta mengucapkan terima kasih kepada beberapa pihak yang senantiasa memberikan ide, masukan, kritik, serta motivasi selama penulis melakukan penyusunan Tugas Akhir. Ucapan terima kasih tersebut ingin penulis sampaikan kepada :

1. Allah SWT yang senantiasa telah memberikan rahmat serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan Tugas Akhir ini.
2. Orang tua saya tercinta Muhammad Rais dan Aries Maya Sofie yang tidak letih - letih dalam mengasuh serta mendidik saya hingga saat ini dan tak ada hentinya juga dalam memberikan nasihat, semangat, serta juga dalam memberikan motivasi.
3. Bapak Jaidan Jauhari, S. Pd. M.T. yang merupakan Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., yang merupakan Ketua Jurusan sekaligus Pembimbing Akademik Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing 1 dan Bapak Tri Wanda Septian, M.Sc. selaku Dosen Pembimbing 2 Tugas Akhir yang telah berkenan meluangkan waktu dan tenaga dalam membimbing, memberikan saran serta motivasi kepada penulis selama proses penulisan Tugas Akhir ini.

6. Mbak Sari Nuzulastri dan Mbak Renny Virgasari selaku admin jurusan sistem komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
7. Rizky Angga Pratama dan M. Alfath Hayatur Rizon selaku asisten lab jaringan komputer yang telah meminjamkan fasilitas lab semasa pengerjaan tugas akhir.
8. Muhammad Wahyu Fadli selaku teman penulis yang telah membantu penulis dalam mengerjakan penelitian ini.
9. Teman – teman Sistem Komputer Angkatan 2018 bukit saya lainnya yang selalu menghibur, menemani dan juga memberikan motivasi kepada penulis selama dalam masa perkuliahan.
10. 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 bahwasanya penyusunan Tugas Akhir yang telah diselesaikan ini masih tidak mendekati kata sempurna. Maka dari itu penulis meminta kritik, masukan, serta ide yang dapat digunakan oleh penulis agar penyusunan Tugas Akhir akan menjadi jauh lebih baik lagi di masa mendatang.

Palembang, 28 Maret 2023

Muhammad Abimanyu Iwari Rama Putra

NIM. 09011381823104

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

IPv6 atau yang lebih dikenal dengan *Internet Protocol* versi 6, merupakan *internet protocol* dengan versi terbaru yang dirancang untuk menggantikan internet *protocol* saat ini yaitu IPv4. Setelah memiliki penipisan dalam alamat, kini masa depan jaringan komputer dan internet akan sepenuhnya bergantung kepada IPv6. Dikarenakan pada pengembangan IPv6 memiliki tujuan untuk menyelesaikan suatu masalah kelelahan dalam alamat IP[1]. Dalam sudut pandang keamanan IPv6 memiliki protokol keamanan yang lebih maju dibandingkan IPv4.

Pada masa sekarang IPv6 masih merupakan teknologi baru yang dengan semakin berkembangnya penggunaan IPv6 dapat menimbulkan kerentanan baru yang dapat di eksploitasi oleh penyerang untuk mendapatkan akses ke sebuah jaringan. Protokol keamanan yang dimiliki oleh IPv6 sangatlah rentan terhadap berbagai jenis serangan, contohnya seperti *Distributed Denial of Service* (DDoS) atau *Denial of Services* (DoS).

Serangan DDoS adalah salah satu ancaman keamanan jaringan yang dialami internet. Serangan DDoS merupakan serangan yang sangat banyak dilakukan pada IPv6, akan tetapi administrator jaringan IPv6 tidak dapat memanfaatkan mekanisme pencegahan seperti IPv4. Serangan DDoS sering terjadi pada IPv6, terutama pada *Network Discovery Protocol*. Yang dimana *Network Discovery Protocol* itu sendiri merupakan protokol utama dalam IPv6 yang memiliki banyak proses seperti resolusi alamat, deteksi tidak terjangkau, dan deteksi alamat duplikat. Dimana serangan DDoS memiliki tujuan utama untuk mencegah sebuah pengguna mengakses layanan untuk waktu yang lama. Dengan cara mengirimkan sejumlah paket dengan berukuran besar secara bersamaan dalam waktu singkat untuk membuat komputer target tidak dapat diakses.

Pemodelan perilaku serangan DDoS berbasis IPv6 dapat dilakukan dengan pendekatan berbasis *machine learning* yang dapat dianggap lebih baik karena dapat mempelajari dan membangun model yang baik berdasarkan kumpulan data DDoS.

yang diberikan. Kemudian tantangan utamanya adalah identifikasi serangkaian fitur yang dalam memodelkan perilaku grup dari serangan DDoS berbasis IPv6[2]. Untuk menemukan cara yang baik untuk mencapai akurasi yang sama yang dihasilkan, dapat menggunakan metode pembelajaran seperti *Support Vector Machine* (SVM). Yang dimana *Support Vector Machine* adalah sebuah metode pembelajaran berdasarkan teori pembelajaran statistik, yang dimana dapat menghasilkan hasil klasifikasi yang baik tanpa banyak data pelatihan. Kemudian perlu lebih banyak upaya yang dilakukan untuk meningkatkan hasil deteksi dengan mengoptimalkan algoritma klasifikasi atau menyesuaikan parameter pengklasifikasi. Berdasarkan penjabaran diatas maka penulis akan mengangkat judul "Deteksi Serangan DDoS Pada IPv6 Menggunakan Metode Pengklasifikasian *Support Vector Machine*". Dimana hasil penelitian ini diharapkan dapat meningkatkan akurasi dari sistem deteksi serangan DDoS pada IPv6.

Pada penelitian terdahulu yang dilakukan oleh Zhoui Ma[3]. Ia mendeteksi suatu serangan DDoS pada *SDN* dengan menggunakan metode algoritma *KNN* dan dukungan dari *Support Vector Machine* (SVM). Yang dimana metode tersebut memanfaatkan sebuah karakteristik kontrol terpusat dari *SDN*. Dengan mengumpulkan informasi karakteristik tersebut secara efisien, hasil dari eksperimen yang ia lakukan menunjukan bahwa tingkat konsumsi sumber daya model sebesar 11%, sementara itu tingkat akurasinya melebihi 99%. Dengan menggunakan kedua algoritma yang berbeda pada percobaan kali ini terdapat kekurangan yaitu pada frekuensi serangan, mode serangan penyerang, dan ukuran *network* korban tidak dapat dibandingkan dengan jaringan nyata. Kemudian juga dengan menggunakan dua metode algoritma ini yaitu menggunakan konsumsi sumber daya yang besar.

Deteksi serangan DDoS menggunakan metode SVM juga pernah dilakukan oleh Mohammed Anbar[4]. Ia menggunakan tiga metode yang berbeda yaitu PCA, IGR, SVM. Yang dimana ketiga metode ini dikombinasikan untuk dijadikan teknik baru yang digunakan untuk mendeteksi RA *flooding attack* pada IPv6. Teknik IGR dan PCA merupakan teknik pengurangan fitur yang digunakan untuk memilih seperangkat fitur baru yang memiliki kontribusi signifikan dalam mendeteksi serangan RA *flooding attack*. Sedangkan teknik SVM memanfaatkan hasil dari

Teknik IGR dan PCA untuk melatih model prediksi. Oleh karena itu karena ketiga teknik tadi dikombinasikan, *input Anomaly traffic* dapat di deteksi dengan model ini. Namun dari menggabungkan ketiga metode tersebut terdapat sebuah kelemahan yaitu jika mengabaikan salah satu fitur akan berdampak negatif pada akurasi teknik yang digunakan. Kemudian juga kurangnya efektivitas dalam mendeteksi sebuah serangan.

Penulis bernama Jin Ye[5]. Dalam penelitiannya ia menggunakan metode SVM untuk membedakan antara lalu lintas normal dan lalu lintas abnormal. Kemudian lalu lintas serangan terdiri dari tigas jenis lalu lintas yang terpisah, yang dimana tingkat akurasi dan *false alarm rate* dari deteksi paket untuk panjang yang berbeda dari ketiga jenis lalu lintas serangan yang ditunjukkan. Tingkat akurasi deteksi rata-rata dari percobaan ini adalah 95.24%, dan tingkat *false* alarm rata-rata adalah 1.26%, dan efek yang diharapkan tercapai. Tetapi pada metode yang ia gunakan terdapat sebuah kelemahan yaitu pada tingkat akurasi yang relatif rendah dari deteksi aliran ICMP yang memungkinkan disebabkan oleh fakta lalu lintas ICMP yang tidak memiliki *port* sumber dan *port* tujuan, sehingga matriks karakteristiknya hanya 4 dimensi.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, terdapat beberapa masalah yang timbul yang mengungkapkan bahwa IDS ini tidak dapat secara akurat mendeteksi serangan dan mengalami *high false alarm* dikarenakan fakta bahwa teknik tersebut kurang mempertimbangkan fitur yang terkait dengan serangan. Dan juga tidak ada dari teknik yang digunakan yang sepenuhnya menyertakan semua serangan DDoS berbasis IPv6 dalam rangkaian serangan yang dapat dideteksi. Terdapat solusi untuk mengatasi masalah tersebut yaitu dengan cara mengoptimalkan klasifikasi agar dapat membedakan antara serangan IPv6-DDoS dan *traffic* normal dengan memeriksa fitur IPv6 dari aliran yang terdeteksi. Akan tetapi terdapat masalah pada sebagian besar dataset karena sangat bergantung pada representasi berbasis paket yang tidak sesuai untuk sifat deteksi serangan. Selain itu, kumpulan data ini direpresentasikan menggunakan fitur yang tidak memenuhi syarat yang menyebabkan masalah kesalahan klasifikasi saat klasifikasi diterapkan. Dan juga teknik pemilihan fitur yang kurang efisien untuk memilih fitur penting

yang terkait dengan serangan DDoS akan berdampak *negative* pada akurasi pendeteksian sehingga administrator jaringan kesulitan untuk mengambil tindakan yang tepat untuk menahan keberadaan serangan DDoS pada jaringan IPv6. Terdapat solusi dalam mengatasi permasalahan ini yaitu dengan teknik pemilihan fitur *Random Forest Classifier* untuk memilih fitur yang terkait dengan serangan DDoS IPv6 yang akan berdampak positif pada akurasi pendeteksian yang kemudian hasil dari *Random Forest Classifier* dapat digunakan untuk melatih model klasifikasi yaitu SVM.

1.3 Tujuan dan Manfaat

1.3.1 Tujuan

Berdasarkan dari penelitian yang dilakukan maka adapun tujuan dari penelitian ini adalah :

1. Menggunakan *Random Forest Classifier* sebagai teknik reduksi fitur untuk memilih kumpulan fitur yang digunakan dalam mendeteksi serangan DDoS Pada IPv6.
2. *Support Vector Machine* dapat memanfaatkan hasil dari *Random Forest Classifier* berupa fitur terbaik yang nantinya akan digunakan untuk melatih model klasifikasi.
3. Menganalisa pengaruh teknik pemilihan fitur *Random Forest Classifier* untuk mengidentifikasi fitur yang paling berkontribusi dalam mendeteksi *input traffic anomaly*.

1.3.2 Manfaat

Adapun manfaat dari penulisan tugas akhir ini, yaitu :

1. Dengan menggunakan *Support Vector Machine* sebagai metode dalam mendeteksi serangan DDoS pada IPv6 dapat mengklasifikasikan *traffic input anomaly* pada serangan.
2. Dengan dilakukannya penelitian ini mampu mengindentifikasi fitur penting yang efektif untuk medeteksi serangan DDoS Pada IPv6

1.4 Batasan Masalah

Adapun batasan-batasan masalah dari penyusunan tugas akhir ini, yaitu :

1. Informasi beserta data yang digunakan pada penelitian ini berasal dari dataset yang dibuat sendiri kemudian melalui jurnal - jurnal penelitan yang membahas tentang pendeteksian sebuah serangan DDoS terhadap IPv6.
2. Penelitian ini dilakukan hanya sebatas pendeteksian sebuah serangan DDoS terhadap IPv6.
3. *Output* yang dihasilkan dari penelitian ini seberapa akurat metode *Support Vector Machine* dalam mendeteksi sebuah serangan DDoS terhadap IPv6.

1.5 Sistematika Penelitian

Adapun dalam penyusunan tugas akhir penulis akan disusun secara sistematis dengan cara urutan per-bab. Selanjutnya, di dalam tiap bab itu sendiri berisikan masing - masing *sub bab* yang sebagaimana isinya adalah menjelaskan secara detail dari *sub bab* yang bersangkutan. Secara sistematika penulisan, penyusunan tersebut tersusun sebagai berikut :

BAB I PENDAHULUAN

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

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang komponen *hardware-software* serta *tools* yang digunakan, untuk mendapatkan data, dan penjelasan tentang metode *Support Vector Machine* (SVM) digunakan sebagai prediksi model yang dapat mendeteksi *input traffic anomaly*.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis mengenai langkah- langkah dari metode yang digunakan untuk mencari, mengumpulkan, dan menganalisa dalam penulisan tugas akhir, blok diagram, dan algoritma *flowchart* atau kode semu.

BAB IV PENGUJIAN DAN ANALISA

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

BAB V KESIMPULAN

Bab ini merupakan bab penutup yang berisikan kesimpulan dari pengujian dan analisa data yang dilakukan, dan memberikan saran untuk penelitan lanjutan.

DAFTAR PUSTAKA

[1] O. E. Elejla, M. Anbar, B. Belaton, and B. O. Alijla, “Flow-Based IDS for ICMPv6-Based DDoS Attacks Detection,” *Arab. J. Sci. Eng.*, vol. 43, no. 12, pp. 7757–7775, Dec. 2018, doi: 10.1007/s13369-018-3149-7.

[2] 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, Jul. 2018, doi: 10.1007/s00521-016-2812-8.

[3] Z. Ma and B. Li, “A DDoS attack detection method based on SVM and K-nearest neighbour in SDN environment,” *Int. J. Comput. Sci. Eng.*, vol. 23, no. 3, pp. 224–234, 2020, doi: 10.1504/IJCSE.2020.111431.

[4] 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.

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

[6] 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.

[7] 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, 2019, doi: 10.1016/j.cose.2019.01.002.

[8] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, “An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics,” *Futur. Gener. Comput.*

Syst., vol. 89, pp. 685–697, 2018, doi: 10.1016/j.future.2018.07.017.

[9] 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.

[10] V. Aghaei-Foroushani and A. N. Zincir-Heywood, "Deterministic flow marking for IPv6 traceback (DFM6)," *Proc. 11th Int. Conf. Netw. Serv. Manag. CNSM 2015*, pp. 270–273, 2015, doi: 10.1109/CNSM.2015.7367370.

[11] B. Bouyeddou, B. Kadri, F. Harrou, and Y. Sun, "DDOS-attacks detection using an efficient measurement-based statistical mechanism," *Eng. Sci. Technol. an Int. J.*, vol. 23, no. 4, pp. 870–878, 2020, doi: 10.1016/j.jestch.2020.05.002.

[12] A. Alsadhan *et al.*, "Locally weighted classifiers for detection of neighbor discovery protocol distributed denial-of-service and replayed attacks," *Trans. Emerg. Telecommun. Technol.*, no. June, pp. 1–15, 2019, doi: 10.1002/ett.3700.

[13] F. S. De Lima Filho, F. A. F. Silveira, A. De Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Secur. Commun. Networks*, vol. 2019, 2019, doi: 10.1155/2019/1574749.

[14] G. B. Satrya, R. L. Chandra, and F. A. Yulianto, "The detection of DDOS flooding attack using hybrid analysis in IPv6 networks," *2015 3rd Int. Conf. Inf. Commun. Technol. ICoICT 2015*, pp. 240–244, 2015, doi: 10.1109/ICoICT.2015.7231429.

[15] X. Yang, T. Ma, and Y. Shi, "Typical DoS/DDoS Threats under IPv6," pp. 55–55, 2007, doi: 10.1109/iccgi.2007.61.

[16] K. Alieyan, M. M. Kadhum, M. Anbar, S. U. Rehman, and N. K. A. Alajmi,

"An overview of DDoS attacks based on DNS," *2016 Int. Conf. Inf. Commun. Technol. Converg. ICTC 2016*, pp. 276–280, 2016, doi: 10.1109/ICTC.2016.7763485.

[17] K. Alieyan, M. Anbar, A. Almomani, R. Abdullah, and M. Alauthman, "DNS Features," *2018 Int. Arab Conf. Inf. Technol.*, pp. 1–4, 2018.

[18] L. Hendriks, R. De Oliveira Schmidt, R. Van Rijswijk-Deij, and A. Pras, "On the potential of IPv6 open resolvers for DDoS attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10176 LNCS, pp. 17–29, 2017, doi: 10.1007/978-3-319-54328-4_2.

[19] J. Zhong and X. Chen, "Research on DDoS Attacks in IPv6," *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3424978.3425020.

[20] S. Toklu and M. Şimşek, "Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service (DDoS) Attack Detection and Filtering," *Arab. J. Sci. Eng.*, vol. 43, no. 12, pp. 7923–7931, 2018, doi: 10.1007/s13369-018-3236-9.

[21] F. M. C. Remegio and C. E. Dumdumaya, "Distributed Denial of service attack mitigation and approaches: a literature review," *Int. J. Artif. Intell. Informatics*, vol. 2, no. 2, pp. 86–97, 2022, doi: 10.33292/ijarlit.v2i2.39.

[22] S. Steinke, "Internet Protocol Version 6," *Netw. Tutor.*, pp. 193–196, 2020, doi: 10.1201/9781482280876-47.

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

[24] A. Hamarsheh and Y. Abdalaziz, "Transition to IPv6 Protocol, Where We Are?," *2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019*, no. July 2017, pp. 1–6, 2019, doi: 10.1109/ICCISci.2019.8716482.

[25] B. J. Nikkel, "An introduction to investigating IPv6 networks," *Digit. Investig.*, vol. 4, no. 2, pp. 59–67, 2007, doi: 10.1016/j.diin.2007.06.001.

[26] A. Turiel, “IPv6: New technology, new threats,” *Netw. Secur.*, vol. 2011, no. 8, pp. 13–15, 2011, doi: 10.1016/S1353-4858(11)70085-X.

[27] P. Truchly, L. Danielovič, M. Dukát, and A. Pôbiš, “Educational and simulation portal for Internet protocol version 6,” *ICETA 2015 - 13th IEEE Int. Conf. Emerg. eLearning Technol. Appl. Proc.*, 2016, doi: 10.1109/ICETA.2015.7558520.

[28] H. Iqbal and S. Naaz, “Wireshark as a Tool for Detection of Various LAN Attacks,” *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 833–837, 2019, doi: 10.26438/ijcse/v7i5.833837.

[29] P. Saxena and S. K. Sharma, “Analysis of Network Traffic by using Packet Sniffing Tool: Wireshark,” *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 3, no. 6, pp. 804–808, 2017, [Online]. Available: https://www.academia.edu/35555033/Analysis_of_Network_Traffic_by_using_Packet_Sniffing_Tool_Wireshark.

[30] P. Prathanrat and C. Polprasert, “Performance Prediction of Jupyter Notebook in JupyterHub using Machine Learning,” *2018 Int. Conf. Intell. Informatics Biomed. Sci. ICIIBMS 2018*, vol. 3, pp. 157–162, 2018, doi: 10.1109/ICIIBMS.2018.8550030.

[31] B. M. Randles, I. V. Pasquetto, M. S. Golshan, and C. L. Borgman, “Using the Jupyter Notebook as a Tool for Open Science: An Empirical Study,” *Proc. ACM/IEEE Jt. Conf. Digit. Libr.*, pp. 17–18, 2017, doi: 10.1109/JCDL.2017.7991618.

[32] Z. A. Sunkad and Soujanya, “Feature Selection and Hyperparameter Optimization of SVM for Human Activity Recognition,” *Proc. - 2016 3rd Int. Conf. Soft Comput. Mach. Intell. ISCMI 2016*, pp. 104–109, 2017, doi: 10.1109/ISCMI.2016.30.

[33] R. G. Mantovani, A. L. D. Rossi, E. Alcobaça, J. Vanschoren, and A. C. P. L. F. de Carvalho, “A meta-learning recommender system for hyperparameter tuning: Predicting when tuning improves SVM classifiers,” *Inf. Sci. (Ny).*, vol. 501, pp. 193–221, 2019, doi: 10.1016/j.ins.2019.06.005.

[34] C. A. Pushpam and J. G. Jayanthi, “Research on Feature Selection using SVM,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 4, pp. 7252–7256, 2019, doi: 10.35940/ijrte.d5279.118419.

[35] N. Mehra and S. Gupta, “Maximal margin multi-classifier based on SVM hyperparameter tuning,” *IEEE Int. Conf. Comput. Commun. Control. IC4 2015*, 2016, doi: 10.1109/IC4.2015.7375710.

[36] A. Agarwal, P. Sharma, M. Alshehri, A. A. Mohamed, and O. Alfarraj, “Classification model for accuracy and intrusion detection using machine learning approach,” *PeerJ Comput. Sci.*, vol. 7, pp. 1–22, 2021, doi: 10.7717/PEERJ-CS.437.

[37] 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. (Ny).*, vol. 340–341, pp. 250–261, 2016, doi: 10.1016/j.ins.2016.01.033.