Analisis Serangan DDoS Dengan Menggunakan *Anomaly-Based* IDS Berbasis *Network Behavior Analysis* (NBA)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

Garinnang Baiduri Salasa

09011381823110

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

ANALISIS SERANGAN DDoS DENGAN MENGGUNAKAN *ANOMALY-BASED* IDS BERBASIS *NETWORK BEHAVIOR ANALYSIS* (NBA)

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh

Garinnang Baiduri Salasa

09011381823110

Palembang, 27 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

ii

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 27 Januari 2023

Tim Penguji :

1. **Ketua : Kemahyanto Exaudi, M.T.**
2. **Sekretaris : Adi Hermansyah, M.T.**
3. **Penguji : Huda Ubaya, M.T.**
4. **Pembimbing I : Ahmad Heryanto, M.T.**
5. **Pembimbing II : Tri Wanda Septian, M.Sc.**

Mengetahui, 23/3/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

iii

HALAMAN PERNYATAAN

Yang bertanda di bawah ini :

Nama : Garinnang Baiduri Salasa

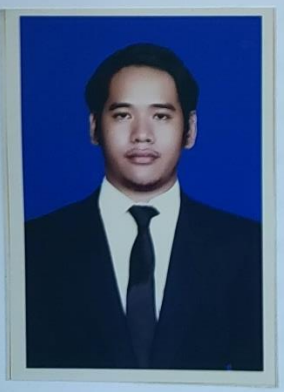
NIM : 09011381823110

Judul : Analisis Serangan DDoS Dengan Menggunakan *Anomaly-Based* IDS Berbasis *Network Behavior Analysis* (NBA).

Hasil Pengecekan Software iThenticate/Turnitin : 20%

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

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, Maret 2023

Garinnang Baiduri Salasa

NIM. 09011381823110

iv

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 "**Analisis Serangan DDoS Dengan Menggunakan Anomaly-Based IDS Berbasis *Network Behavior Analysis* (NBA)**". 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 A. Huzaifa dan Amalinda Fadjari 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 Chendy Maulana dan Muhammad Robby Bahari selaku teman penulis yang telah membantu penulis dalam mengerjakan penelitian ini.
9. Christopher Marlo, M Rifqi Abbiyu Ariq, Budiman Alfian selaku teman yang selalu mendampingi saya baik dari segi logistik maupun moral selama pengerjaan tugas akhir.
10. Teman – teman Sistem Komputer Angkatan 2018 bukit saya lainnya yang selalu menghibur, menemani dan juga memberikan motivasi kepada penulis selama dalam 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 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, 29 Maret 2023

Garinnang Baiduri Salasa
NIM. 09011381823110

DDoS ATTACK ANALYSIS USING ANOMALY-BASED IDS BASED ON NETWORK BEHAVIOR ANALYSIS

Garinnang Baiduri Salasa (09011381823110)
Computer Engineering Departement, Computer Science Faculty, Sriwijaya University
Email : garinnangbs412@gmail.com

ABSTRACT

DDoS assaults pose a serious threat to enterprises, inflicting damage and disruption, thus improving the speed and accuracy of DDoS detection and mitigation is critical. The combination of Network Behavior Analysis (NBA) with the algorithms K-Nearest Neighbor (KNN) and Naive Bayes (NB) was evaluated to detect DDoS attacks (Distributed Denial of Service). Using the CICDDoS2019 dataset, KNN was found to have higher accuracy (99.82%) and better performance metrics than NB (98.02%). The combination of NBA, KNN, and NB provides a powerful defense against DDoS attacks and enables rapid detection and response to potential threats, making it a valuable tool for network administrators and security professionals.

Keywords : DDoS, Machine Learning, Network Behavior Analysis, K-Nearest Neighbor, Naïve Bayes.

Palembang, 29 March 2023

Supervisor	**Co-Supervisor**
Ahmad Heryanto S.Kom, M.T.	**Tri Wanda Septian, M.Sc.**
NIP. 198701222015041002	**NIK. 1901062809890001**

Acknowledged
Head of Computer Systems Departement

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

vii

ANALISIS SERANGAN DDoS DENGAN MENGGUNAKAN ANOMALY-BASED IDS BERBASIS NETWORK BEHAVIOR ANALYSIS (NBA)

Garinnang Baiduri Salasa (09011381823110)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : garinnangbs412@gmail.com

ABSTRAK

Serangan DDoS merupakan ancaman serius bagi perusahaan, menimbulkan kerusakan dan gangguan, sehingga meningkatkan kecepatan dan akurasi deteksi dan mitigasi DDoS sangat penting. Kombinasi Network Behavior Analysis (NBA) dengan algoritma K-Nearest Neighbor (KNN) dan Naive Bayes (NB) dievaluasi untuk mendeteksi serangan DDoS (Distributed Denial of Service). Dengan menggunakan dataset CICDDoS2019, KNN ditemukan memiliki akurasi yang lebih tinggi (99,82%) dan metrik kinerja yang lebih baik daripada NB (98,02%). Kombinasi NBA, KNN, dan NB memberikan pertahanan yang kuat terhadap serangan DDoS dan memungkinkan deteksi dan respons yang cepat terhadap potensi ancaman, menjadikannya alat yang berharga bagi administrator jaringan dan profesional keamanan.

Kata Kunci : DDoS, Machine Learning, Network Behavior Analysis, K-Nearest Neighbor, Naïve Bayes.

Palembang, 9 Maret 2023

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

viii

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Denial of Service (DoS) merupakan metode serangan yang bertujuan untuk mematikan sebuah mesin atau jaringan, membuat pengguna utama tidak dapat mengakses file yang diminta [1]. Bentuk serangan *DoS* yang paling umum ditemui adalah serangan *Distributed Denial of Service.* Menurut Penelitian [2] tujuan dari serangan DDoS antara lain untuk meluapkan target *Host* yang dituju untuk mengganggu *Host* yang jinak. Pada tahun 2015, Kaspersky menemukan sebanyak 50% serangan DDoS disebabkan oleh terlihatnya gangguan dalam *service*, dan 24% sisanya berujung pada *denial of service* seutuhnya [3].

Baru-baru ini, kode sumber dari malware mirai yang terkenal telah bermunculan, berdasarkan dari para ahli bahwa malware tersebut mendeteksi jejaring untuk alat IoT yang tidak terlindungi dengan baik dan menjangkitinya, sehingga mereka dapat dengan mudah meretasnya[4]. Karenanya perlu dilakukan penelitian rinci mengenai pola serangan DDoS ini.

Telah banyak penelitian yang telah dilakukan untuk menganalisa serangan DDoS untuk kedepannya dalam mendeteksi serangan dengan lebih akurat. Salah satu diantara penelitian tersebut yakni dengan melakukan *Network Behavior Analysis* (NBA). NBA sendiri merupakan basis yang bernaung pada tingkah laku dari seberapa signifikan suatu jaringan internet Berdasarkan penelitian [5], [6], dan [7], mereka menyimpulkan bahwa KNN menunjukkan hasil yang begitu signifikan dalam hal akurasi dan kecocokan serangan DDoS sehingga mereka merekomendasikan KNN sebagai alat deteksi serangan yang optimal.

Lain halnya dengan penelitian [8], [9], dan [2], peneliti menggunakan bentuk *Naïve Bayes* dalam mendeteksi serangan DDoS. Dari penelitian tersebut mereka berpendapat bahwa *Naïve Bayes* terbukti tidak kalah saing dengan KNN sehingga para peneliti tersebut berargumen bahwa Naïve Bayes dinilai lebih efektif daripada KNN.

K-Nearest Neighbor sendiri adalah metode pendeteksian yang mengandalkan kedekatan jaringan dalam membuat klasifikasi atau regresi. KNN mampu melakukan prediksi tentang pengelompokan dari sebuah poin data individual. KNN biasanya dipakai sebagai klasifikasi algoritma yang bekerja dari asumsi dimana poin yang sama bisa ditemukan antara satu dan lainnya. KNN terbilang sebagai *Machine Learning* paling mudah dikarenakan mesin ini berdasar pada *Supervised Learning Technique*.

Sedangkan *Naïve Bayes* adalah algoritma *Machine Learning* yang berdasar pada probabilitas theorema Bayes, digunakan dalam tugas klasifikasi yang bervariasi menyesuaikan dengan perintah yang diberikan. *Naïve Bayes* sendiri terbilang sederhana, cepat, akurat dan dapat diandalkan.

Dari penjelasan terkait dua *Machine Learning* tersebut, kita bisa mengetahui kelebihan dari masing-masing mesin baik *K-Nearest Neighbor* maupun *Naïve Bayes*, namun banyak dari penjelasan tersebut masih memiliki kekurangan satu sama lain. Terlebih masih terdapat senjang pendapat terhadap alat mana yang lebih unggul dalam mendeteksi serangan DDoS.

Berdasarkan dari ringkasan yang telah saya simpulkan diatas, bahwasannya didapatkan hasil berupa terdapatnya kesenjangan pendapat perihal alat deteksi mana yang cocok dan ideal untuk mendeteksi serangan DDoS secara optimal, maka dari itu pada penelitian kali ini saya mengangkat topik dengan judul "Analisis Serangan DDoS Dengan Menggunakan Metode *Anomaly-based* IDS Berbasis *Network Behavior Analysis* (NBA)".

1.2 Tujuan dan Manfaat

1.2.1 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu:

1. Mengetahui serangan DDoS dengan deteksi *Anomaly-based* IDS.
2. Membuat analisis serangan DDoS menggunakan basis *Network Behavior Analysis* (NBA).

1.2.2 Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu:

1. Penelitian ini diharapakan dapat membantu peneliti lain dalam menanggulangi serangan DDoS dengan metode *Anomaly-based* yang berbasis *Network Behavior Analysis*.
2. Hasil dari penelitian ini dapat digunakan sebagai bahan informasi dan kajian bagi Fakultas Ilmu Komputer Universitas Sriwijaya dalam pendeteksian serangan DDoS, sehingga dapat mengetahui kapan serangan tersebut dapat terdeteksi secara akurat.

1.3 Perumusan dan Batasan Masalah

1.3.1 Perumusan Masalah

Penelitian ini dilakukan dengan rumusan masalah dengan beberapa point dibawah ini:

1. Bagaimana sebuah serangan DDoS bisa dideteksi dengan metode Anomaly-based IDS?
2. Apakah yang membuat Network Behavior Analysis menjadi patokan dalam mendeteksi serangan DDoS*?*

1.3.2 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu:

1. Informasi beserta data yang digunakan pada penelitian ini sepenuhnya berasal dari jurnal penelitian sebelumnya.
2. Penelitian ini hanya sebatas mendeteksi serangan DDoS dan tidak termasuk langkah pencegahannya.
3. Output yang dihasilkan dari penelitian ini berupa analisis IDS dan solusi sementara dalam pendeteksian DDoS dalam jangka pendek.

1.4 Metodologi Penelitian

Pada tugas akhir ini menggunakan metodelogi sebagai berikut:

1.4.1 Metode Studi Pustaka dan Literatur

Pentingnya metode ini adalah sebagai, menggali informasi yang berkaitan dengan serangan DDoS dengan mencari referensi seperti jurnal ilmiah, dan lain sebagainya yang mendukung penulisan tugas akhir ini

1.4.2 Metode Pembuatan Model

Pada metode ini membuat suatu perancangan pemodelan dengan menggunakan diagram flowchart.

1.4.3 Metode Pengujian

Metode ini mengevaluasi analisis untuk menentukan apakah dapat menghasilkan nilai akurasi yang tinggi atau tidak.

1.4.4 Metode Analisis dan Kesimpulan

Pada tugas akhir ini, hasil pengujian akan diteliti kekurangannya, agar dapat digunakan pada penelitian selanjutnya

1.5 Sistematika Penulisan

Adapun dalam penyusunan tugas akhir penulis akan disusun secara sistematis dengan cara urutan per-bab. Selanjutnya, di dalam tiap bab 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

Pada bagian BAB I akan menjelaskan terhadap sub bab seperti latar belakang, perumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bagian BAB II akan menjelaskan terhadap sub bab seperti penelitian terkait/terdahulu ringkasan hasil kajian literatur, dan landasan teori.

BAB III. METODOLOGI

Pada bagian BAB III akan menjelaskan terhadap sub bab seperti pengumpulan data, lingkungan dan spesifikasi perangkat keras dan perangkat lunak, rancangan blok diagram serta metode dan diagram alir.

BAB IV. ANALISIS DAN HASIL

Pada bagian BAB IV akan menjelaskan terhadap sub bab seperti analisis dari penelitian yang dilakukan serta hasil yang didapatkan dari penelitian tersebut.

BAB V. PENUTUP

Pada bagian BAB V akan menjelaskan terhadap sub bab seperti kesimpulan dan saran.

DAFTAR PUSTAKA

[1] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/COMST.2018.2847722.

[2] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," *J. Netw. Comput. Appl.*, vol. 187, no. May, p. 103108, 2021, doi: 10.1016/j.jnca.2021.103108.

[3] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.

[4] D. K. Sharma *et al.*, "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks," *Ad Hoc Networks*, vol. 121, no. April, p. 102603, 2021, doi: 10.1016/j.adhoc.2021.102603.

[5] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, "Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2297–2307, 2020, doi: 10.1016/j.procs.2020.03.282.

[6] L. Liu, H. Wang, Z. Wu, and M. Yue, "The detection method of low-rate DoS attack based on multi-feature fusion," *Digit. Commun. Networks*, vol. 6, no. 4, pp. 504–513, 2020, doi: 10.1016/j.dcan.2020.04.002.

[7] S. Shanmuga Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, "Machine Learning based DDOS Detection," *2020 Int. Conf. Emerg. Smart Comput. Informatics, ESCI 2020*, pp. 234–237, 2020, doi: 10.1109/ESCI48226.2020.9167642.

[8] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018, doi: 10.1016/j.jocs.2017.03.006.

[9] R. Panigrahi *et al.*, “Intrusion detection in cyber–physical environment using hybrid Naïve Bayes—Decision table and multi-objective evolutionary feature selection,” *Comput. Commun.*, vol. 188, no. September 2021, pp. 133–144, 2022, doi: 10.1016/j.comcom.2022.03.009.

[10] M. A. Lawall, R. A. Shaikh, and S. R. Hassan, “A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing,” in *Procedia Computer Science*, 2021, vol. 182, pp. 13–20, doi: 10.1016/j.procs.2021.02.003.

[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] 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.

[13] 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.

[14] N. V. Patil, C. Rama Krishna, K. Kumar, and S. Behal, “E-Had: A distributed and collaborative detection framework for early detection of DDoS attacks,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2019, doi: 10.1016/j.jksuci.2019.06.016.

[15] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, “Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN,” *Futur. Gener. Comput. Syst.*, vol. 111, pp. 763–779, 2020, doi: 10.1016/j.future.2019.10.015.

[16] N. Z. Bawany and J. A. Shamsi, “SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks,” *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, doi: 10.1016/j.jnca.2019.06.001.

[17] E. M. Bårli, A. Yazidi, E. H. Viedma, and H. Haugerud, “DoS and DDoS

mitigation using Variational Autoencoders," *Comput. Networks*, vol. 199, Nov. 2021, doi: 10.1016/j.comnet.2021.108399.

[18] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101645.

[19] I. Ko, D. Chambers, and E. Barrett, "Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation," *J. Inf. Secur. Appl.*, vol. 55, no. October, p. 102647, 2020, doi: 10.1016/j.jisa.2020.102647.

[20] J. Cui, M. Wang, Y. Luo, and H. Zhong, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 275–283, 2019, doi: 10.1016/j.future.2019.02.037.

[21] X. Liang and T. Znati, "On the performance of intelligent techniques for intensive and stealthy DDos detection," *Comput. Networks*, vol. 164, p. 106906, 2019, doi: 10.1016/j.comnet.2019.106906.

[22] P. D. Bojović, I. Bašičević, S. Ocovaj, and M. Popović, "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method," *Comput. Electr. Eng.*, vol. 73, pp. 84–96, 2019, doi: 10.1016/j.compeleceng.2018.11.004.

[23] B. Kurt, Ç. Yıldız, T. Y. Ceritli, B. Sankur, and A. T. Cemgil, "A Bayesian change point model for detecting SIP-based DDoS attacks," *Digit. Signal Process. A Rev. J.*, vol. 77, pp. 48–62, 2018, doi: 10.1016/j.dsp.2017.10.009.

[24] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, "Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things," *J. Netw. Comput. Appl.*, vol. 130, no. June 2018, pp. 1–13, 2019, doi: 10.1016/j.jnca.2019.01.006.

[25] T. Nitin, S. R. Singh, and P. G. Singh, "Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS)," *ISCA J. Eng. Sci.*, vol. 1, no. 1, pp. 51–56, 2012, [Online]. Available: www.isca.in.

[26] F. C. Morabito, M. Campolo, C. Ieracitano, and N. Mammone, *Deep learning approaches to electrophysiological multivariate time-series analysis*. Elsevier Inc., 2018.