ANALISIS PERBANDINGAN *DETECTION TRAFFIC ANOMALY* SERANGAN DDoS IPv4 ANTARA METODE *NAÏVE BAYES* DAN *SUPPORT VECTOR MACHINE (SVM)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

MUHAMAD CHENDY MAULANA

09011381823112

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

ANALISIS PERBANDINGAN *DETECTION TRAFFIC ANOMALY* SERANGAN DDoS IPv4 DENGAN METODE *NAÏVE BAYES* DAN *SUPPORT VECTOR MACHINE (SVM)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

MUHAMAD CHENDY MAULANA
09011381823112

Palembang, Maret 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing I**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S. Kom, M.T**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Selasa

Tanggal : 7 Maret 2023

Tim Penguji :

1. Ketua : Rossi Passarella, S.T.,M.Eng.

2. Sekertaris : Muhammad Ali Buchari S.Kom., M.T

3. Penguji : Aditya Putra Perdana P, M.T

4. Pembimbing : Ahmad Heryanto, M.T

Mengetahui, 23/3/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhamad Chendy Maulana

NIM : 09011381823112

Judul : Analisis Perbandingan *Detection Traffic Anomaly* Serangan DDoS IPv4 dengan Metode *Naïve Bayes* dan *Support Vector Machine (SVM)*

Hasil Pengecekan Software iThenticate/Turnitin : 15%

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

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

Palembang, Maret 2023

M. Chendy Maulana

NIM. 09011381823112

KATA PENGANTAR

Puji syukur penulis haturkan kehadirat Allah SWT, karna berkat rahmat dan ridho-Nya sehingga peulis dapat menyelesaikan penelitian tugas akhir yang berjudul "**Analisis Perbandingan *Detection Traffic Anomaly* Serangan DDoS IPv4 antara Metode *Naive Bayes* dan *Support Vector Machine* (SVM)".**

Penulis mengucapkan banyak terima kasih kepada seluruh pihak yang telah membantu penulis dalam menyelesaikan skripsi ini, kepada :

1. Allah SWT yang senantiasa telah memberikan rahmat serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan Tugas Akhir ini.
2. Kedua orang tuaku Amril Hadi dan Inem Kasmiati yang selalu memberikan dukungan, motivasi, semangat, dan doa yang selalu menyertai sehingga sampai pada tahap ini.
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 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T., selaku dosen pembimbing yang telah memberikan arahan dalam penelitian serta penyusunan skripsi dan sudah memberikan bimbingan dari awal hingga akhir skripsi ini dapat terselesaikan.
6. Bapak Huda Ubaya, S.T., M.T., selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer penulis saat ini.
7. Yth. Bapak Ibu dosen Program Studi Sistem Komputer Fakultas Ilmu Komputer yang telah mendidik dan membagi ilmu kepada penulis.
8. Mbak Sari Nuzulastri selaku admin jurusan sistem komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.

9. Teman saya Muhammad Wahyu Fadli, Sandika Virgo, dan juga Muhammad Abimanyu Iwari Putra yang pernah membantu penulis dalam masa – masa sulit saat pengerjaan tugas akhir.
10. Budiman Alfian, Aqila Lukman Hakim, dan juga Muhammad Hafiz yang merupakan teman terdekat penulis yang selalu menghibur dalam masa – masa sulit perkuliahan.
11. Teman teman Sistem Komputer angkatan 2018 yang telah memberikan hiburan dan semangat.
12. Adinda Nur Ramadiyah yang selalu meluangkan waktu, memberikan semangat,motivasi,tenaga, dan doa.

Terima kasih kepada semua pihak yang tidak dapat saya sebutkan satu persatu dan untuk orang-orang yang sering bertanya "kapan sempro?", "kapan sidang?", "kapan wisuda?", "kapan nyusul?", dan lain sebagainya, kalian adalah alasanku untuk segera menyelesaikan skripsi ini. Akhir kata, penulis berharap semoga skripsi ini dapat memberikan sumbangan pemikiran yang bermanfaat bagi kita semua dalam pengembangan ilmu pengetahuan. Aamiin.

Palembang, Maret 2023

Penulis

Muhamad Chendy Maulana

NIM. 09011381823112

ANALISIS PERBANDINGAN *DETECTION TRAFFIC ANOMALY* SERANGAN DDoS IPv4 DENGAN METODE *NAÏVE BAYES* DAN *SUPPORT VECTOR MACHINE (SVM)*

MUHAMAD CHENDY MAULANA (09011381823112)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : chendymaulana@gmail.com

ABSTRAK

Anomaly traffic adalah suatu keadaan yang mengakibatkan abnormalitas dalam lalu lintas jaringan. *Anomaly detections* merupakan suatu monitoring untuk memantau pergerakan yang terjadi pada sistem jaringan. *DDoS attack* atau *Distributed Denial of Service* merupakan serangan *cyber* dengan cara mengirimkan *fake traffic* atau lalu lintas palsu ke suatu sistem atau server secara terus menerus. Dampaknya, server tersebut tidak dapat mengatur seluruh *traffic* sehingga menyebabkan *down*. Pada penelitian ini akan dilakukan *detection traffic anomaly* dengan metode *naïve bayes* dan *support vector machine* untuk melihat perbandingan kedua metode yang digunakan dalam deteksi serangan *ddos ipv4*. Didapatkan hasil bahwa dengan penggunaan metode algoritma *Naïve Bayes* menghasilkan nilai *accuracy* 99,68%, *presisi* 99,68%, *recall* 99,68%, dan *F1 score* 99,68% terbukti lebih baik dari pada metode *Support Vector Machine* yang menghasilkan nilai *accuracy* 85,79%, *presisi* 83,79%, *recall* 88,83%, dan *F1 score* 86,24% dalam melakukan *detection traffic anomaly* terhadap paket data serangan *DDoS* dan data normal.

Kata kunci : *Detection Traffic Anomaly, Distributed Denial of Service,Naïve Bayes,Support Vector Machine*

Palembang, 9 Maret 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S. Kom, M.T**
NIP. 196612032006041001	**NIP. 198701222015041002**

COMPARATIVE ANALYSIS OF IPv4 DDoS ATTACK ANOMALY DETECTION TRAFFIC WITH NAIVE BAYES METHOD AND SUPPORT VECTOR MACHINE (SVM)

MUHAMAD CHENDY MAULANA (09011381823112)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : chendymaulana@gmail.com

ABSTRACT

Anomaly traffic is a condition that results in an abnormality in network traffic. Anomaly detections is a monitoring to monitor the movement that occurs in the network system. DDoS attack or Distributed Denial of Service is a cyber attack by continuously sending fake traffic to a system or server. As a result, the server cannot manage all traffic, causing it to go down. In this research, traffic anomaly detection will be carried out using the naïve Bayes method and support vector machine to see a comparison of the two methods used in the detection of IPv4 ddos attacks. The results show that using the Naïve Bayes algorithm method produces an accuracy value of 99.68%, 99.68% precision, 99.68% recall, and 99.68% F1 score which is proven to be better than the Support Vector Machine method which produces an accuracy value of 85 .79%, 83.79% precision, 88.83% recall, and 86.24% F1 score in detecting traffic anomalies against DDoS attack data packets and normal data.

Keywords : *Detection Traffic Anomaly, Distributed Denial of Service,Naïve Bayes,Support Vector Machine*

Palembang, March 2023

Acknowledged,

Head of Computer Systems Department	Supervisor
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S. Kom, M.T**
NIP. 196612032006041001	**NIP. 198701222015041002**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan *Distributed Denial of Service* (DDoS) merupakan serangan *cyber* dengan cara mengirimkan *fake traffic* atau lalu lintas palsu ke suatu sistem atau server secara terus menerus. Dampaknya, server tersebut tidak dapat mengatur seluruh traffic sehingga menyebabkan down[1]. Penyerang meluncurkan sebuah serangan terhadap ketersediaan. Serangan ini sering dilakukan menggunakan banyak sistem membanjiri sistem target dengan besar jumlah lalu lintas.

Deteksi serangan merupakan aspek penting dari *DDoS* pertahanan serangan, dan hasil deteksi dapat memengaruhi keseluruhan kinerja pertahanan serangan. Para penyerang sekarang cenderung menggunakan sumber sebenarnya untuk melakukan serangan *DDoS* dan dapat diluncurkan serangan *DDoS* tingkat rendah dengan mengirimkan tingkat rendah dan berkala aliran serangan, jadi sangat sulit untuk membedakan antara aliran normal dan aliran serangan, sehingga mempengaruhi cepat dan keakuratan deteksi yang sangat sulit. Metode *detection anomaly* adalah digunakan untuk mengidentifikasi pola lalu lintas yang menyimpang dari yang dimodelkan perilaku lalu lintas normal. Anomaly yang teridentifikasi bisa jadi salah satunya serangan atau lalu lintas normal.

Anomaly traffic adalah suatu keadaan yang mengakibatkan abnormalitas dalam lalu lintas jaringan[2]. Kondisi ini bisa mengakibatkan penurunan performansi jaringan sehingga rentannya sebuah jaringan untuk diserang. Dampak dari anomali trafik ini bisa melumpuhkan jaringan, bisa pula disisipi arsip atau file yang membahayakan target dari penyerang. Maka dari itu, perlu dilakukan deteksi terhadap lalu lintas jaringan pada mencegah ataupun mengatasi anomaly didalam lalu lintas jaringan.

Pada penelitian terdahulu yang dilakukan oleh Jieren Cheng[3] dengan judul "***DDoS Attack Detection Using IP Address Feature Interaction***" menjelaskan bahwa

mendeteksi suatu serangan *DDoS* hasil perilaku interaksi aliran serangan *DDoS* dan aliran normal dan karakteristik yang berbeda pada alamat IP dan port mengunakan model deteksi berdasarkan *IAI* oleh pengklasifikasi SVM (*Support Vector Machine*). Yang dimana metode tersebut memanfaatkan IP baru algoritma *Address Interaction Feature* (IAI). Hasil dari eksperimen yang lakukan menunjukan bahwa metode *IAI* dapat secara akurat mengidentifikasi normal mengalir dan tidak akan menyebabkan positif palsu yang tinggi karena besar arus normal kenaikan aliran jaringan latar belakang normal, tingkat deteksi secara bertahap menurun dari 95,8% menjadi 65,1%, tingkat alarm palsu meningkat dari 0,0% menjadi 33,6%, tingkat deteksi rata-rata 10 kelompok adalah 79,7% dan tingkat alarm palsu rata-rata adalah 12,5%. Dengan menggunakan kedua algoritma yang berbeda pada percobaan kali ini terdapat kekurangan yaitu pada frekuensi serangan, mode serangan penyerang, dan mengandalkan jarak dari sensor deteksi serangan. Kemudian juga dengan menggunakan dua metode algoritma ini yaitu menggunakan konsumsi sumber daya yang besar.

Peneliti bernama Ramin Fadaei Fouladi[4] pada penelitiannya dengan judul "***Frequency Based DDoS Attack Detection Approach Using Naive Bayes Classification***" yang mana didalam penelitiannya menggunakan pengklasifikasi *Naive Bayes* dengan dua metode berbasis frekuensi transformasi *Fourier diskrit* dan transformasi *wavelet diskrit* untuk memisahkan antara serangan dan lalu lintas normal. Hasil yang didapat dari penelitian ini dari nilai -17 sebagai nilai ambang batas untuk pengklasifikasi berdasarkan fitur *DFT*, peneliti mencapai tingkat positif palsu dan negatif palsu tentang 15% yang menghasilkan akurasi lebih tinggi sekitar 85% dibandingkan dengan 76% pengklasifikasi berbasis *DWT*. Kekurangan dari penelitian ini adalah ukuran atribut frekuensi lalu lintas.

Penelitian selanjutnya yang dilakukan oleh[5] dengan judul "***Detection of DoS/DDoS attack against HTTP Servers using Naïve Bayesian***" menjelaskan bahwa web server adalah program yang melayani permintaan menggunakan protokol HTTP. Awalnya server web menggunakan statis halaman *Hyper Text Markup Language*

(HTML) untuk disediakan informasi. Namun saat ini server web menyediakan layanan dinamis menggunakan kueri basis data, skrip yang dapat dieksekusi, dll untuk memberikan informasi. Hasil kinerja pengklasifikasi *Naïve Bayesian* dengan metode pra-pemrosesan yang berbeda dievaluasi menggunakan *test bed*. Peneliti menegaskan bahwa *Naïve Bayesian* mengklasifikasikan serangan membaca lambat dengan akurasi 97,82% dan perilaku normal terdeteksi dengan akurasi 96,46%. Diketahui bahwa *Naïve Bayesian* dengan *Numerik Biner* mendeteksi perilaku normal dengan akurasi 99,2% dan *SYN flood* dengan 99,8% akurasi. pengklasifikasi *Naïve Bayesian* saat digunakan metode Diskretisasi; itu mengklasifikasikan perilaku normal dengan akurasi 96,61% dan lambat dengan akurasi 97,15%.

Banyak penelitian menyebutkan bahwa deteksi serangan merupakan aspek penting dari *DDoS* pertahanan serangan, dan hasil deteksi dapat memengaruhi keseluruhan kinerja pertahanan serangan. Para penyerang sekarang cenderung menggunakan sumber sebenarnya untuk melakukan serangan *DDoS* dan dapat diluncurkan serangan *DDoS* tingkat rendah dengan mengirimkan tingkat rendah dan berkala aliran serangan, jadi sangat sulit untuk membedakan antara aliran normal dan aliran serangan, sehingga mempengaruhi cepat dan keakuratan deteksi yang sangat sulit. Berdasarkan uraian diatas maka penulis ingin membandingan pendekatan mana yang lebih baik antara *Naïve Bayes* dan *Support Vector Machine* dalam mendeteksi *traffic anomaly* pada serangan *DDoS*.

1.2 Perumusan Masalah

Penelitian ini dilakukan dengan rumusan masalah dengan beberapa point, 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 *IPv4* dalam rangkaian serangan yang dapat dideteksi. Terdapat solusi untuk mengatasi masalah tersebut yaitu dengan cara

mengoptimalkan klasifikasi agar dapat membedakan antara serangan *IPv4-DDoS* dan *traffic normal* dengan memeriksa fitur *IPv4* dari aliran yang terdeteksi. Selain itu, peneliti merancang suatu sistem pendeteksi anomali *traffic* data pada serangan *DDoS* guna mengetahui antara manakah dari metode *Naïve Bayes* dan *Support Vector Machine* yang lebih baik. Lalu bagaimana cara mendeteksi *anomaly traffic* data pada serangan *DDoS* guna mendapatkan perbandingan dari metode *Naïve Bayes* dan metode *Support Vector Machine* menggunakan kumpulan data yang direpresentasikan menggunakan fitur yang ada. 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 *IPv4*. Terdapat solusi dalam mengatasi permasalahan ini yaitu dengan teknik pemilihan fitur *Random Forest Clasifier* untuk memilih fitur yang terkait dengan serangan *DDoS IPv4* yang akan berdampak *positif* pada akurasi pendeteksian yang kemudian hasil dari fitur dapat digunakan untuk melatih model klasifikasi yaitu *Naïve Bayes* dan *Support Vector Machine*.

1.3 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Penelitian ini dilakukan untuk melihat tingkat perbandingan anatara metode yang digunakan dalam mendeteksi *anomaly traffic* pada serangan *DDoS*.
2. Penelitian ini menggunakan metode *Naïve Bayes* dan metode *Support Vector Machine* untuk melihat perbandingan mendeteksi anomaly *traffic* serangan *DDoS*.
3. *Output* yang dihasilkan dari penelitian ini agar mendapatkan perbandingan dari metode *Support Vector Machine* dan *Naïve Bayes* dalam mendeteksi sebuah serangan *DDoS* terhadap *IPv4*.

1.4 Tujuan

Dari penelitian yang dilakukan maka adapun tujuan dari penelitian penulisan tugas akhir ini, yaitu :

1. Untuk mengimplementasikan metode *Naïve Bayes* dan *Support Vector Machine* dalam medeteksi *traffic anomaly* data serangan *DDoS* dan data normal.

2. Membandingkan mana metode yang lebih baik antara *Naïve bayes* dan *Support Vector Machine* dalam *detection traffic anomaly* pada *DDoS*.

1.5 Manfaat

Adapun manfaat dari penulisan tugas akhir ini, yaitu :

1. Dapat mendeteksi *anomaly traffic* serangan *DDoS* dengan metode *Naïve Bayes*.

2. Dapat mendeteksi *anomaly traffic* serangan *DDoS* dengan metode *Support Vector Machine*.

3. Dapat memberikan informasi mengenai metode *Naïve Bayes* dan *Support Vector Machine* pengaplikasiannya dalam klasifikasi serangan *DDoS*.

1.6 Sistematika Penulisan

Dalam penyusunan tugas akhir penulis akan disusun secara sistematis dengan cara ber ururan per-bab. Selanjutnya, di 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 dalam laporan tugas akhir ini terdiri dari 4 bab antara lain :

BAB I − PENDAHULUAN

Pada bagian **BAB I** berisi penjelaskan mengenai latar belakang masalah, tujuan, manfaat, batasan masalah dan sistematika penulisan.

BAB II − TINJAUAN PUSTAKA

Pada bagian **BAB II** berisi penjelaskan mengenai definisi, tentang komponen hardware-software serta *tools* yang digunakan, untuk mendapatkan data, dan penjelasan tentang metode *Support Vector Machine* dan *Naïve Bayes* digunakan sebagai prediksi model yang dapat mendeteksi input *traffic anomaly*.

BAB III – METODOLOGI PENELITIAN

Pada **BAB III** ini menjelaskan secara sistematis mengenai informasi pengumpulan data, spesifikasi *hardware* dan *software* yang digunakan, serta juga terdapat metode dan *flowchart* yang digunakan dalam penelitian.

BAB IV − ANALIS DAN PEMBAHASAN

Pada bagian **BAB IV** menyajikan dan menganalisis data-data yang didapat dari hasil pengujian.

BAB V − KESIMPULAN DAN SARAN

Dalam **BAB V** ini merupakan bab penutup yang berisikan analisis data yang dilakukan dan kesimpulan dari pengujian, dan memberikan saran untuk penelitan ini.

DAFTAR PUSTAKA

[1] P. Arun Raj Kumar and S. Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems," *Comput. Commun.*, vol. 36, no. 3, pp. 303–319, 2013, doi: 10.1016/j.comcom.2012.09.010.

[2] I. Riadi, R. Umar, and F. D. Aini, "Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (Svm)," *Ilk. J. Ilm.*, vol. 11, no. 1, pp. 17–24, 2019, doi: 10.33096/ilkom.v11i1.361.17-24.

[3] J. Cheng, J. Yin, Y. Liu, Z. Cai, and C. Wu, "DDoS attack detection using IP address feature interaction," *Int. Conf. Intell. Netw. Collab. Syst. INCoS 2009*, pp. 113–118, 2009, doi: 10.1109/INCOS.2009.34.

[4] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Frequency Based DDoS Attack Detection Approach Using Naive Bayes Classification," no. June, 2016.

[5] V. Katkar, A. Zinjade, S. Dalvi, T. Bafna, and R. Mahajan, "Detection of DoS/DDoS attack against HTTP servers using naive Bayesian," *Proc. - 1st Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2015*, pp. 280–285, 2015, doi: 10.1109/ICCUBEA.2015.60.

[6] B. Vrat, N. Aggarwal, and S. Venkatesan, "Anomaly Detection in IPv4 and IPv6 networks using machine learning," *12th IEEE Int. Conf. Electron. Energy, Environ. Commun. Comput. Control (E3-C3), INDICON 2015*, pp. 1–6, 2016, doi: 10.1109/INDICON.2015.7443752.

[7] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, no. Ml, pp. 29–35, 2018, doi: 10.1109/SPW.2018.00013.

[8] W. Hurst, N. Shone, and Q. Monnet, “Predicting the effects of DDoS attacks on a network of critical infrastructures,” *Proc. - 15th IEEE Int. Conf. Comput. Inf. Technol. CIT 2015, 14th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC 2015, 13th IEEE Int. Conf. Dependable, Auton. Se*, pp. 1697–1702, 2015, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.256.

[9] A. A. Amaral, L. S. Mendes, E. H. M. Pena, B. B. Zarpelão, and M. L. Proença, “Network Anomaly Detection by IP Flow Graph Analysis: A DDoS Attack Case Study,” *Proc. - Int. Conf. Chil. Comput. Sci. Soc. SCCC*, vol. 0, pp. 90–94, 2013, doi: 10.1109/SCCC.2013.14.

[10] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, 2008, doi: 10.1016/j.eswa.2007.01.040.

[11] I. Cvitić, D. Peraković, M. Periša, and M. Musa, “Network parameters applicable in detection of infrastructure level DDoS attacks,” *2017 25th Telecommun. Forum, TELFOR 2017 - Proc.*, vol. 2017-Janua, pp. 1–4, 2018, doi: 10.1109/TELFOR.2017.8249347.

[12] M. F. Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. II, no. 9, pp. 3112–3123, 2018.

[13] Y. Gu, K. Li, Z. Guo, and Y. Wang, “Semi-supervised k-means ddos detection method using hybrid feature selection algorithm,” *IEEE Access*, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.

[14] J. Wu, X. Wang, X. Lee, and B. Yan, “Detecting DDoS attack towards DNS server using a neural network classifier,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6354 LNCS, no. PART 3, pp. 118–123, 2010, doi: 10.1007/978-3-642-15825-4_15.

[15] S. Min, D. Seong, J. Hak, and J. Sou, “Detection of DDoS attacks using optimized traffic matrix,” *Comput. Math. with Appl.*, vol. 63, no. 2, pp. 501–510, 2012, doi: 10.1016/j.camwa.2011.08.020.

[16] R. Vijayasarathy, B. Ravindran, and S. V. Raghavan, “A system approach to network modeling for DDoS detection using a Naìve Bayesian classifier,” *2011 3rd Int. Conf. Commun. Syst. Networks, COMSNETS 2011*, 2011, doi: 10.1109/COMSNETS.2011.5716474.

[17] M. Aziz, R. Umar, and F. Ridho, “Implemetasi Jaringan Saraf Tiruan untuk Mendeteksi Serangan DDoS pada Forensik Jaringan,” *QUERY J. Sist. Inf.*, vol. 3, no. 1, pp. 46–52, 2019.

[18] J. David and C. Thomas, “DDoS Attack Detection using Fast Entropy Approach on Flow- Based Network Traffic,” *Procedia - Procedia Comput. Sci.*, vol. 50, pp. 30–36, 2015, doi: 10.1016/j.procs.2015.04.007.

[19] T. Sciences, “ANALYSIS OF THE IoT IMPACT ON VOLUME OF DDoS ATTACKS,” *XXXIII Simp. o novim Tehnol. u poštanskom i Telekomun. saobraćaju – PosTel 2015*, 2015.

[20] Y. Purwanto, Kuspriyanto, Hendrawan, and B. Rahardjo, “Traffic anomaly detection in DDos flooding attack,” *Proc. 2014 8th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2014*, pp. 14–19, 2015, doi: 10.1109/TSSA.2014.7065953.

[21] Q. Ma, C. Sun, B. Cui, and X. Jin, “A novel model for anomaly detection in network traffic based on kernel support vector machine,” *Comput. Secur.*, vol. 104, p. 102215, 2021, doi: 10.1016/j.cose.2021.102215.

[22] H. Nurohman Purwanto, Y., Hafiduddin and H. Nurohman, H., Purwanto, Y., “Anomaly Detection By Self-Similar Analysis,” pp. 1–6, 2015.

[23] O. Babatunde and O. Al-Debagy, “A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6),” *Int. J.*

Comput. Trends Technol., vol. 13, no. 1, pp. 10–13, 2014, doi: 10.14445/22312803/ijctt-v13p103.

[24] 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.

[25] M. I. Fikri, T. S. Sabrila, and Y. Azhar, "Perbandingan Metode Naïve Bayes dan Support Vector Machine pada Analisis Sentimen Twitter," *Smatika J.*, vol. 10, no. 02, pp. 71–76, 2020, doi: 10.32664/smatika.v10i02.455.

[26] T. Ban and D. Inoue, "Feature subset selection by SVM ensemble," *2016 IEEE Symp. Ser. Comput. Intell. SSCI 2016*, 2017, doi: 10.1109/SSCI.2016.7849979.

[27] H. Vhohfwlrq and D. Edvhg, ")Hdwxuh Vhohfwlrq Dojrulwkp Edvhg Rq 690 681," pp. 4113–4116, 2016.

[28] M. Sudarma and D. P. Hostiadi, "KLASIFIKASI PENGGUNAAN PROTOKOL KOMUNIKASI PADA NEWORK TRAFFIC MENGGUNAKAN NAÏVE BAYES SEBAGAI PENENTUAN QoS," *Icsgteis*, no. November, pp. 59–64, 2013, [Online]. Available: https://ojs.unud.ac.id/index.php/prosidingcsgteis2013/article/view/7215.