“ SELEKSI FITUR UNTUK MENEMUKAN POLA FITUR TERBAIK PADA SISTEM PENDETEKSI SERANGAN DDoS DENGAN MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* ”

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar

Sarjana Komputer

OLEH :

Sandika Virgo

09011381823117

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

SELEKSI FITUR UNTUK MENEMUKAN POLA FITUR TERBAIK PADA SISTEM PENDETEKSI SERANGAN DDoS DENGAN MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar

Sarjana Komputer

Oleh

Sandika Virgo

09011381823117

Palembang , 5 Januari 2023

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II 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

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 28 Desember 2022

Tim Penguji :

1. Ketua	**: Sarmayanta Sembiring, M.T.**	( )
2. Sekretaris	**: Adi Hermansyah, M.T.**	( )
3. Penguji	**: Aditya Putra Perdana P, M.T.**	( )
4. Pembimbing I	**: Ahmad Heryanto, M.T.**	( )
5. Pembimbing II	**: Tri Wanda Septian, M.Sc.**	( )

Mengetahui, 5/1/23

Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda di bawah ini :

Nama : Sandika Virgo

NIM : 09011381823117

Judul : Seleksi Fitur Untuk Menemukan Pola Fitur Terbaik Pada Sistem Pendeteksi Serangan DDoS Dengan Menggunakan Metode *Support Vector Machine*.

Hasil Pengecekan Software iThenticate/Turnitin : 9%

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, 09 Januari 2023

Sandika Virgo

NIM. 09011381823117

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas ke hadirat Tuhan Yang Maha Esa, yang atas segala berkat, kasih sayang, serta karunia-Nya penulis dapat menyelesaikan penulisan tugas akhir ini yang berjudul " **Seleksi Fitur Untuk Menemukan Pola Fitur Terbaik Pada Sistem Pendeteksi Serangan DDoS Dengan Menggunakan Metode *Support Vector Machine* ".**

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa dan terima kasih kepada yang terhormat:.

1. Bapak Jaidan Jauhari selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
2. Bapak Dr.Ir.Sukemi,M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer.
3. Bapak Huda Ubaya, M.T. sebagai Pembimbing Akademik Penulis di Jurusan Sistem Komputer..
4. Bapak Ahmad Heryanto, S.Kom, M.T. selaku Dosen Pembimbing I Tugas Akhir dan Bapak Tri Wanda Septian, M.Sc. selaku Dosen Pembimbing II Tugas Akhir .
5. Mbak Sari selaku Administrasi Jurusan Sistem Komputer yang telah membantu melancarkan proses administrasi terkait Tugas Akhir.
6. Kedua orang tua, saudara, dan keluarga besar yang selalu mendoakan dan memberikan motivasi dan *support* dari bantuan material dan moral.
7. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang selalu memberikan semangat dan bantuan yang bermanfaat.
8. Almamater Ilmu Alat Pengabdian.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangat diharapkan penulis agar dapat segera diperbaiki sehingga laporan ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan bacaan bagi yang tertarik dalam penelitian *networking* terutama pada serangan DDoS.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, 04 Januari 2023

Penulis,

Sandika Virgo

NIM. 09011381823117

FEATURE SELECTON TO FIND THE BEST FEATURE SELECTION PATTERN ON THE DDoS ATTACK SYSTEM USING SUPPORT VECTOR MACHINE METHOD

Sandika Virgo (09011381823117)
Computer Engineering Departement, Computer Science Faculty, Sriwijaya University
Email : virgosandika20@gmail.com

ABSTRACT

DDoS is one of the many attacks used by hackers in carrying out cybercrimes. As for knowing attacks detectors, in presenting this research looking for parameters that play a major role in the DDoS dataset, it is necessary to apply a selection feature. In the application of selection using several selection features, namely Random Forest Classifier (RFC), Mutual Information Classifier (MIC), Correlation Based Selection (CBS) and Lasso Regularization Regression (LRR). Then the classification uses the Support Vector Machine (SVM) method, to determine accuracy, precision, recall and F1-score using the confusion matrix technique. In this study using the CIC-IDS2017 dataset, after the research was carried out the Random Forest Classifier selection features became the best selection features.

Keywords : DDoS, Machine Learning, Support Vector Machine, Selection Feature.

Palembang, 5 January 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

FEATURE SELECTON TO FIND THE BEST FEATURE SELECTION PATTERN ON THE DDoS ATTACK SYSTEM USING SUPPORT VECTOR MACHINE METHOD

Sandika Virgo (09011381823117)
Computer Engineering Departement, Computer Science Faculty, Sriwijaya University
Email : virgosandika20@gmail.com

ABSTRACT

DDoS is one of the many attacks used by hackers in carrying out cybercrimes. As for knowing attacks detectors, in presenting this research looking for parameters that play a major role in the DDoS dataset, it is necessary to apply a selection feature. In the application of selection using several selection features, namely Random Forest Classifier (RFC), Mutual Information Classifier (MIC), Correlation Based Selection (CBS) and Lasso Regularization Regression (LRR). Then the classification uses the Support Vector Machine (SVM) method, to determine accuracy, precision, recall and F1-score using the confusion matrix technique. In this study using the CIC-IDS2017 dataset, after the research was carried out the Random Forest Classifier selection features became the best selection features.

Keywords : DDoS, Machine Learning, Support Vector Machine, Selection Feature.

Palembang, 5 January 2023

Supervisor

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

Co-Supervisor

Tri Wanda Septian, M.Sc.
NIK. 1901062809890001

Acknowledged
Head of Computer Systems Departement

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

DAFTAR ISI

LEMBAR PENGESAHAN ..... **ii**
LEMBAR PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
KATA PENGANTAR ..... **v**
ABSTRACT ..... **vii**
ABSTRAK ..... **viii**
DAFTAR ISI ..... **ix**
DAFTAR GAMBAR ..... **xi**
DAFTAR TABEL ..... **xii**
DAFTAR ALGORITMA ..... **xiii**
DAFTAR LAMPIRAN ..... **xiv**
BAB 1 PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Perumusan Masalah 2
1.3 Tujuan 2
1.4 Manfaat 2
1.5 Batasan Masalah 3
1.6 Metodologi Penelitian 3
BAB II TINJAUN PUSTAKA **5**
2.1 Penelitian Terkait 5
2.2 Ringkasan Kajian Terkait 17
2.3 Landasan Teori 25
2.3.1 DDoS 25
2.3.2 Jenis Serangan DDoS 26
2.3.3 Feature Selection 26
2.3.4 Machine Learning 32
2.3.5 Support Vector Machine 33
2.3.6 Confusion Matrix 34
BAB III METODOLOGI PENELITIAN **35**

3.1 Dataset 36
3.2 Topologi Dataset 42
3.3 Software dan Hardware 44
3.4 Pre-Processing 45
3.5 Feature Selection 45
3.6 Perancangan Penelitian 51
BAB 4 PEMBAHASAN DAN HASIL 53
4.1 Pengolahan Dataset 53
4.2 Feature Selection 54
4.3 Support Vector Machine dan Confusion Matrix 71
4.4 Perbandingan Hasil Fitur Seleksi 87
4.5 Uji Coba Svm Pada Perubahan Skenario Parameter 89
4.6 Perbandingan Hasil Perubahan Uji Coba Skenario 95
4.7 Hasil dan Analisa 96
BAB V KESIMPULAN 99
5.1 Kesimpulan 99
5.2 Saran 99
DAFTAR PUSTAKA 100

DAFTAR GAMBAR

Gambar 2.1 Perbandingan linear svm dan polynomial svm 33
Gambar 3.1 Diagram Alir 35
Gambar 3.2 Topologi Dataset 42
Gambar 3.3 Frame feature selection 45
Gambar 3.4 Frame pearson CBS 46
Gambar 3.5 Frame pearson RFC 48
Gambar 3.6 Frame pearson MIC 49
Gambar 3.7 Frame pearson LRR 50
Gambar 3.8 Perancangan penelitian 51
Gambar 4.1 Jumlah baris dan kolom dataset 53
Gambar 4.2 Perbandingan pola serangan 54
Gambar 4.3 Heatmap fitur seleksi CBS 56
Gambar 4.4 Hasil penggunaan RFC 60
Gambar 4.5 Hasil penggunaan MIC 64
Gambar 4.6 Hasil penggunaan LRR 69
Gambar 4.7 Hasil confusion matrix CBS 71
Gambar 4.8 Hasil confusion matrix kernel Rbf pada CBS 72
Gambar 4.9 Hasil confusion matrix poly pada CBS 74
Gambar 4.10 Hasil confusion matrix RFC 75
Gambar 4.11 Hasil confusion matrix Rbf pada RFC 77
Gambar 4.12 Hasil confusion matrix poly pada RFC 78
Gambar 4.13 Hasil confusion matrix LRR 80
Gambar 4.14 Hasil confusion matrix Rbf pada LRR 81
Gambar 4.15 Hasil confusion matrix poly pada LRR 82
Gambar 4.16 Hasil confusion matrix MIC 84
Gambar 4.17 Hasil confusion matrix Rbf pada MIC 85
Gambar 4.18 Hasil confusion matrix poly pada MIC 86
Gambar 4.19 Hasil confusion matrix RFC 89
Gambar 4.20 Hasil confusion matrix MIC 91
Gambar 4.21 Hasil confusion matrix LRR 92
Gambar 4.22 Hasil confusion matrix CBS 94
Gambar 4.23 Grafik hasil nilai perbandingan feature selection 98

DAFTAR TABEL

Tabel 2. 1 Jurnal terkait penelitian 5
Tabel 2.2 Penggunaan fitur dan hasil akurasi KNN 23
Tabel 2.3 Penggunaan fitur dan hasil akurasi NB 23
Tabel 2.4 Penggunaan fitur dan hasil akurasi SVM 24
Tabel 2.5 Penggunaan fitur dan hasil akurasi RFC 24
Tabel 2.6 Penggunaan fitur dan hasil akurasi AN 25
Tabel 3.1 Deskripsi mengenai fitur-fitur dataset 36
Tabel 3.2 Jenis perangkat dalam pembuatan dataset 43
Tabel 3.3 Spesifikasi perangkat keras 44
Tabel 3.4 Spesifikasi perangkat lunak 44
Tabel 4.1 Hasil fitur seleksi berdasarkan output dari variable 57
Tabel 4.2 Hasil fitur seleksi berdasarkan output dari variable 61
Tabel 4.3 Hasil fitur yang tidak memiliki nilai 62
Tabel 4.4 Hasil label fitur seleksi MIC 65
Tabel 4.5 Hasil label fitur MIC yang tidak memiliki nilai 66
Tabel 4.6 Fitur nilai positif 70
Tabel 4.7 Fitur nilai negatif 70
Tabel 4.8 Fitur yang digunakan CBS 71
Tabel 4.9 Fitur yang digunakan RFC 75
Tabel 4.10 Fitur yang digunakan LRL 79
Tabel 4.11 Fitur yang digunakan MIC 83
Tabel 4.12 Perbandingan hasil uji coba svm setiap fitur seleksi 87
Tabel 4.13 Perbandingan hasil uji coba svm menggunakan Rbf 88
Tabel 4.14 Perbandingan hasil uji coba svm menggunakan kernel poly 88
Tabel 4.15 Perubahan parameter RFC 89
Tabel 4.16 Perubahan parameter mutual information 90
Tabel 4.17 Perubahan parameter LRR 92
Tabel 4.18 Perubahan parameter CBS 94
Tabel 4.19 Hasil uji coba svm pada perubahan skenario parameter 95
Tabel 4.20 Hasil uji coba svm dan kernel 97

DAFTAR ALGORITMA

Algoritma 2.1 Pearson correlation based 27
Algoritma 2.2 Ouput variable 27
Algoritma 2.3 feature test 28
Algoritma 2.4 Train_test_split dan Rfc 28
Algoritma 2.5 Output nilai dan parameter 29
Algoritma 2.6 Selectbest dan feature colums 30
Algoritma 2.7 Penggunaan LassoCv 31

DAFTAR LAMPIRAN

Halaman utama dari dataset CIC-IDS2017 103
Halaman download dari dataset CIC-IDS2017 103

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan kemajuan teknologi pada saat ini, yang di bangun pada kehidupan manusia selalu meningkat pada era digital dan perindustrian. Dengan kemajuan teknologi inilah yang membuat maraknya dunia *cyber* semakin tinggi [1]. Serangan tersebut mengacu pada jaringan di internet, banyaknya serangan membuat jumlahnya semakin meningkat dan bermacam macam salah satunya serangan *Distributed Deniel of Service* (DDoS) [2] . Serangan DDoS ialah serangan *cyber* yang dapat menyerang jaringan untuk menghancurkan ketersediaan layanan, dengan cara menyerang secara bersamaan sehingga membuat terjadinya pemalsuan pada jaringan yang banyak hingga jaringan tidak mampu menampung, yang akhirnya membuat server tidak tersedia pada lalu lintas yang sah [1], [2]. Adapun jenis serangan DDoS yang di gunakan *attacker* adalah LDAP, UDP, UDP_Lag, Syn, DNS dan NTP [1]. Serta ada permasalahan dalam seleksi fitur *machine learning*. Tujuan pemilihan fitur ialah untuk memilih fitur yang terbaik berdasarkan kriteria, pemilihan kriteria dapat di kategorikan sebagai metode *filter*, pembungkus, tertanam dari *perspektif* strategi yang mana untuk mengevaluasikan mode dengan fitur yang berbeda sebagai *input* [3].

Pada penelitian [1], mengatakan bahwa serangan DDoS dapat menjadi sebuah masalah seperti dapat menghilangkan penghasilan orang lain, kerusakan dari sebuah *instansi*, dan pencurian. Dengan adanya masalah tersebut peneliti mengusulkan menggunakan pengklasifikasi *Naive Baiyes* dan *algoritma information gain* digunakan untuk mengatasi dalam mengurangi waktu komputasi sehingga dapat meningkatkan secara efisien deteksi DDoS. Adapun hasil yang didapatkan efisiensi dari algoritma *naive bayes* dalam deteksi sebelum dan sesudah penerapan, informasi yang di dapatkan masing-masing adalah 98% dan 99,5% , waktu komputasi juga berkurang sebesar 46,6%.

Pada penelitian [2], menawarkan menggunakan beberapa jenis algoritma dari *machine learning* yaitu *K_nearest_neighbors* (K-NN), *support vector machine* (SVM), *naive bayes* (NB) *decision tree* (DT), *Random Forest* (RD), dan *logistic regression* (LR). Pada pengukurannya mendapatkan hasil percobaan menggunakan beberapa jenis *machine learning* akurasi terbaik pada algoritma *decision tree* dan *random forest* yang mana masing-masing *accuracy* mencapai 99%. Pada *precision* juga mencapai 99% pada kedua metode tersebut, akan tetapi DT lebih baik saat komputasi yang di lakukan karena DF memiliki waktu yaitu 4,53 dan 84,2 detik.

Setelah di uraikan penjelasan di atas maka penulis dapat menyimpulkan untuk judul penelitian tersebut ialah Seleksi Fitur Untuk Menemukan Pola Fitur Terbaik Pada Sistem Pendeteksi Serangan DDoS Dengan Menggunakan Metode *Support Vector Machine*.

1.2 Perumusan Masalah

Adapun rumusan masalah dari penelitian tersebut adalah :

1. Bagaimana menemukan fitur seleksi terbaik pada pendeteksian serangan DDoS pada dataset CIC-IDS2017.
2. Bagaimana pengklasifikasian algoritma *support vector machine* untuk pendeteksi serangan DDoS pada dataset CIC-IDS2017

1.3 Tujuan

Adapun tujuan penulis dari penelitian tersebut adalah :

1. Menemukan seleksi fitur terbaik untuk pendeteksi serangan DDoS pada dataset CIC-IDS2017.
2. Menerapkan algoritm*a support vector machine* pada pendeteksi serangan DDoS pada dataset CIC-IDS2017.
3. Menganalisis keakuratan algoritma *support vector machine* terhadap serangan DDoS pada dataset CIC-IDS2017.

1.4 Manfaat

Adapun manfaat penulis dari penelitian tersebut adalah **:**

1. Dapat mengetahui fitur seleksi terbaik untuk sistem pendeteksi serangan DDoS.
2. Dapat memahami penerapan dari algoritma *support vector machine* pada

pendeteksi serangan DDoS pada dataset CIC-IDS2017.

3. Menjadi literatur untuk melakukan penelitian selanjutnya dimasa yang akan datang.

1.5 Batasan Masalah

Adapun Batasan masalah dari penelitian tersebut adalah :

1. Menggunakan pengklasifikasian algoritma *support vector machine*.
2. Pemilihan fitur seleksi terbaik untuk pendeteksian serangan DDoS pada dataset CIC-IDS2017.

1.6 Metodologi Penelitian

Pada tugas akhir ini menggunakan metodelogi yang mana pada masing-masing di susun berdasarkan sub-bab yang di jelaskan secara teratur dan mengenai apa saja yang akan dilakukan, adapun sistematis tugas akhir sebagai berikut :

BAB 1 PENDAHULUAN

Pada tahap pertama ini sebagai, menggali informasi yang berkaitan dengan serangan DDoS dengan mencari *referensi* seperti buku, jurnal ilmiah, dan lain sebagainya yang mendukung penulisan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Pada tahap kedua ini sebagai langkah-langkah penulis yang di buat berdasarkan masalah yang di cari pada penelitian. Dalam tahap ini penulis melakukan kajian literatur serta mencari landasan terkait pada judul penelitian.

BAB III METODOLOGI PENELITIAN

Pada tahap ketiga ini sebagai tahap pengujian berdasarkan metodologi penelitian yang telah di temukan, sehingga di dapatlah hasil uji yang sesuai dan tepat secara konsep atau yang telah di temukan menerapkan algoritma yang di pakai untuk menentukan perangkat baik *software* maupun *hardware* dalam menulis *code* untuk penerapan penelitian.

BAB IV HASIL DAN ANALISA

Pada tahap ke empat ini sebagai tahap analisis data yang di dapatkan dari pengujian untuk mendapatkan hasil data yang objektif, serta menemukan fitur seleksi yang baik.

BAB V KESIMPULAN DAN SARAN

Pada tahap ke lima ini sebagai tahap di tariknya suatu kesimpulan yang di dapat dari tahapan-tahapan sebelumnya, serta saran untuk di jadikan landasan selanjutnya.

DAFTAR PUSTAKA

[1] N. A. Singh, J. Singh, and T. De, "Distributed denial of service attack detection using naive bayes classifier through info gain feature selection," *ACM International Conference Proceeding Series*, vol. 25-26-Augu, 2016, doi: 10.1145/2980258.2980379.

[2] R. J. Alzahrani and A. Alzahrani, "Security analysis of ddos attacks using machine learning algorithms in networks traffic," *Electronics (Switzerland)*, vol. 10, no. 23, 2021, doi: 10.3390/electronics10232919.

[3] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Comput Secur*, vol. 88, p. 101645, 2020, doi: 10.1016/j.cose.2019.101645.

[4] C. Wang, J. Zheng, and X. Li, "Research on DDoS Attacks Detection Based on RDF-SVM," *Proceedings - 10th International Conference on Intelligent Computation Technology and Automation, ICICTA 2017*, vol. 2017-Octob, pp. 161–165, 2017, doi: 10.1109/ICICTA.2017.43.

[5] A. T. Kyaw, M. Zin Oo, and C. S. Khin, "Machine-Learning Based DDOS Attack Classifier in Software Defined Network," *17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2020*, pp. 431–434, 2020, doi: 10.1109/ECTI-CON49241.2020.9158230.

[6] S. Das, D. Venugopal, S. Shiva, and F. T. Sheldon, "Empirical Evaluation of the Ensemble Framework for Feature Selection in DDoS Attack," *Proceedings - 2020 7th IEEE International Conference on Cyber Security and Cloud Computing and 2020 6th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud-EdgeCom 2020*, no. Ml, pp. 56–61, 2020, doi: 10.1109/CSCloud-EdgeCom49738.2020.00019.

[7] T. Aytaç, M. A. Aydın, and A. H. Zaim, "Detection DDOS attacks using machine learning methods," *Electrica*, vol. 20, no. 2, pp. 159–167, 2020, doi: 10.5152/electrica.2020.20049.

[8] S. Daneshgadeh, T. Kemmerich, T. Ahmed, and N. Baykal, "An Empirical Investigation of DDoS and Flash Event Detection Using Shannon Entropy, KOAD and SVM Combined," *2019 International Conference on Computing, Networking and Communications, ICNC 2019*, pp. 658–662, 2019, doi: 10.1109/ICCNC.2019.8685632.

[9] V. Deepa, K. Muthamil Sudar, and P. Deepalakshmi, "Detection of DDoS attack on SDN control plane using hybrid machine learning techniques," *Proceedings of*

the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018, no. Icssit, pp. 299–303, 2018, doi: 10.1109/ICSSIT.2018.8748836.

[10] D. Li, C. Yu, Q. Zhou, and J. Yu, "Using SVM to Detect DDoS Attack in SDN Network," *IOP Conf Ser Mater Sci Eng*, vol. 466, no. 1, 2018, doi: 10.1088/1757-899X/466/1/012003.

[11] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Syst Appl*, vol. 169, no. April 2020, p. 114520, 2021, doi: 10.1016/j.eswa.2020.114520.

[12] X. Jing, Z. Yan, X. Jiang, and W. Pedrycz, "Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch," *Information Fusion*, vol. 51, pp. 100–113, 2019, doi: 10.1016/j.inffus.2018.10.013.

[13] P. Studi, S. Komputer, F. I. Komputer, and U. Sriwijaya, "Deteksi Serangan Smurf Attack," 2021.

[14] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," *Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems, ICICIS 2019*, pp. 233–238, 2019, doi: 10.1109/ICICIS46948.2019.9014826.

[15] L. Yang and H. Zhao, "DDoS attack identification and defense using SDN based on machine learning method," *Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018*, pp. 174–178, 2019, doi: 10.1109/I-SPAN.2018.00036.

[16] Y. Khosroshahi and E. Ozdemir, "Detection of Sources Being Used in DDoS Attacks," *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*, pp. 163–168, 2019, doi: 10.1109/CSCloud/EdgeCom.2019.000-1.

[17] V. de M. Rios, P. R. M. Inácio, D. Magoni, and M. M. Freire, "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," *Computer Networks*, vol. 186, no. March 2020, p. 107792, 2021, doi: 10.1016/j.comnet.2020.107792.

[18] Q. Li, L. Meng, Y. Zhang, and J. Yan, "DDoS attacks detection using machine learning algorithms," *Communications in Computer and Information Science*, vol. 1009, pp. 205–216, 2019, doi: 10.1007/978-981-13-8138-6_17.

[19] D. Aksu, S. Üstebay, M. A. Aydin, and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature

selection algorithm," *Communications in Computer and Information Science*, vol. 935, pp. 141–149, 2018, doi: 10.1007/978-3-030-00840-6_16.

[20] M. Aamir and S. M. A. Zaidi, "DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation," *Int J Inf Secur*, vol. 18, no. 6, pp. 761–785, 2019, doi: 10.1007/s10207-019-00434-1.

[21] A. Das, Pramod, and B. S. Sunitha, "An Efficient Feature Selection Approach for Intrusion Detection System using Decision Tree," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 2, pp. 646–656, 2022, doi: 10.14569/IJACSA.2022.0130276.

[22] N. Bindra and M. Sood, "Evaluating the impact of feature selection methods on the performance of the machine learning models in detecting DDoS attacks," *Romanian Journal of Information Science and Technology*, vol. 23, no. 3, pp. 250–261, 2020.

[23] K. Mei, M. Tan, Z. Yang, and S. Shi, "Modeling of Feature Selection Based on Random Forest Algorithm and Pearson Correlation Coefficient," *J Phys Conf Ser*, vol. 2219, no. 1, 2022, doi: 10.1088/1742-6596/2219/1/012046.

[24] E. C. Blessie and E. Karthikeyan, "Sigmis: A feature selection algorithm using correlation based method," *J Algorithm Comput Technol*, vol. 6, no. 3, pp. 385–394, 2012, doi: 10.1260/1748-3018.6.3.385.

[25] R. Duangsoithong and T. Windeatt, "Correlation-based and causal feature selection analysis for ensemble classifiers," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5998 LNAI, pp. 25–36, 2010, doi: 10.1007/978-3-642-12159-3_3.

[26] Y. Zhu *et al.*, "Artificial Intelligence Algorithm-Based Lumbar and Spinal MRI for Evaluation of Efficacy of Chinkuei Shin Chewan Decoction on Lumbar Spinal Stenosis," *Contrast Media Mol Imaging*, vol. 2021, 2021, doi: 10.1155/2021/2700452.

[27] P. Waldmann, "On the use of the pearson correlation coefficient for model evaluation in genome-wide prediction," *Front Genet*, vol. 10, no. SEP, pp. 1–4, 2019, doi: 10.3389/fgene.2019.00899.

[28] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, vol. 2018-January, pp. 108–116. doi: 10.5220/0006639801080116.