SELEKSI FITUR UNTUK MENEMUKAN POLA FITUR TERBAIK PADA SISTEM PENDETEKSI SERANGAN DDOS DENGAN MENGGUNAKAN METODE K-NEAREST NEIGHBOR (K-NN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

Ricky Akbar Pratama

09011381823082

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 K-NEAREST NEIGHBOR (K-NN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

Ricky Akbar Pratama
09011381823082

Palembang , 14 Maret 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 : 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, 14/3/23

Ketua Jurusan Sistem Komputer

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda di bawah ini :

Nama : Ricky Akbar Pratama

NIM : 09011381823082

Judul : Seleksi Fitur Untuk Menemukan Pola Fitur Terbaik Pada Sistem Pendeteksi Serangan DDoS Dengan Menggunakan Metode *K-Nearest Neighbor* (K-NN).

Hasil Pengecekan Software iThenticate/Turnitin : 15%

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, 14 Maret 2023

Ricky Akbar Pratama

NIM. 09011381823082

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis panjatkan kepada Allah Subhanahu Wa Ta'ala, atas segala karunia, berkat, dan rahmat-nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul "**Seleksi Fitur Untuk Menemukan Pola Fitur Terbaik Pada Sistem Pendeteksi Serangan DDoS Dengan Menggunakan Metode *K-Nearest Neighbor* (K-NN)**".

Pada penyusunan tugas akhir ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Serta penulis banyak mendapat dukungan dari berbagai pihak dengan memberikan saran, kritik dan semangat. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa dan terimakasih kepada yang terhormat:

1. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakutas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Ahmad Heryanto, S. Kom, M.T. selaku Dosen Pembimbing I Tugas Akhir.
4. Bapak Tri Wanda Septian, M.Sc. selaku Dosen Pembimbing II Tugas Akhir.
5. Ibu Nurul Afifah. M.KOM. selaku Pembimbing Akademik Jurusan Sistem Komputer.
6. Mbak Sari Nuzulastri Anhar Putri selaku Administrator Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberi kemudahan dalam pengurusan administrasi
7. Kedua orang tua berserta keluarga yang selalu mendoakan, memberikan dukungan baik moril maupun materil, serta motivasi dan semangat bagi penulis.
8. Seluruh staff dan pegawai jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh teman-teman dari SK Bukit sebagai teman-teman seperjuangan

dalam mengerjakan tugas akhir.

10. teman-teman SK angkatan 2018 sebagai teman seperjuangan dalam mengerjakan tugas akhir.

Penulis menyadari bahwa tugas akhir ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari sehingga penelitian ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan bacaan bagi yang tertarik dalam penelitian khususnya pada sistem deteksi serangan DDoS.

Akhir kata dengan segala keterbatasan, penulis berharap semoga penelitian ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pemikiran dalam peningkatan mutu pembelajaran dan penelitian.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang,\٩Maret 2023

Penulis,

Ricky Akbar Pratama
NIM. 09011381823082

FEATURE SELECTON TO FIND THE BEST FEATURE SELECTION PATTERN ON THE DDoS ATTACK SYSTEM USING K-NEAREST NEIGHBOR METHOD (KNN)

Ricky Akbar Pratama (09011381823082)
Computer Engineering Departement, Computer Science Faculty, Sriwijaya University
Email : akbarricky048@gmail.com

ABSTRACT

DDoS attacks are one of the main threats to security issues on the internet today which have quite a severe impact. As for knowing the best DDoS attack detection, this study applies several selection features to find the best feature pattern in detecting DDoS attacks using the K-Nearest Neighbor method. 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). Based on the results of the classification using the K-Nearest Neighbor method, the mutual information classifier and random forest classifier that get the highest accuracy and are also the best at reducing features and finding the most relevant feature variables for detecting DDoS attacks.

Keywords : DDoS, Machine Learning, K-nearest neighbor, Feature Selection.

Palembang, 14 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

SELEKSI FITUR UNTUK MENEMUKAN POLA FITUR TERBAIK PADA SISTEM PENDETEKSI SERANGAN DDoS DENGAN MENGGUNAKAN METODE K-NEAREST NEIGHBOR (K-NN)

Ricky Akbar Pratama (09011381823082)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : akbarricky048@gmail.com

ABSTRAK

Serangan DDoS merupakan salah satu ancaman utama dalam masalah keamanan di internet saat ini yang memiliki dampak yang cukup parah. Adapun untuk mengetahui pendeteksian serangan DDoS yang terbaik maka penelitian ini menerapkan beberapa fitur seleksi untuk menemukan pola fitur terbaik dalam mendeteksi serangan DDoS dengan menggunakan metode *K- Nearest Neighbor*. Pada penerapan seleksi menggunakan beberapa fitur seleksi yaitu *Random Forest Classifier* (RFC), *Mutual Information Classifier* (MIC), *Correlation Based Selection* (CBS), dan *Lasso Regularization Regression* (LRR). berdasarkan hasil klasifikasi menggunakan metode *K- Nearest Neighbor* maka yang mendapatkan akurasi tertinggi yaitu fitur seleksi *mutual information* dan *random forest classifier* dan juga menjadi yang terbaik dalam mereduksi fitur serta menemukan variabel fitur yang paling relevan untuk pendeteksian serangan DDoS.

Kata Kunci : DDoS, Machine Learning, K-nearest neighbor, Feature Selection.

Palembang, 14 Maret 2023

Pembimbing I Tugas Akhir	**Pembimbing II 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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan *Distributed Denial of Service* (DDoS) merupakan jenis serangan jaringan yang terus meningkat setiap tahunnya, baik dari segi volume maupun intensitasnya. serangan DDoS merupakan salah satu ancaman utama dalam masalah keamanan di internet saat ini yang memiliki dampak yang cukup parah. *Distributed Denial of Service* (DDoS) adalah teknik yang relatif sederhana akan tetapi sangat kuat dalam melakukan penyerangan terhadap sumber daya Internet dikarenakan Serangan DDoS dengan mudah dapat menghabiskan sumber daya komputasi dan komunikasi korbannya dengan sangat cepat yang bertujuan untuk memberikan gangguan layanan dengan mencoba membatasi akses ke mesin atau layanan dengan merusak layanan itu sendiri [1].

Serangan DDoS menimbulkan ancaman bagi pengguna Internet dan semua infrastruktur yang ada di dalamnya, termasuk *bandwidth*, sumber daya *server*, integritas data, ketersediaan data, dan kerahasiaan data yang tersimpan di server. Hingga saat ini serangan DDoS masih termasuk dalam jenis utama ancaman keamanan siber. Deteksi dini memainkan peran mendasar dalam mencegah dampak fatal serangan DDoS pada sumber daya *server* [2]. Serangan DDoS diatur dengan mengatur jaringan mesin yang terhubung. Mesin-mesin tersebut disebut *zombies* yang merupakan bagian dari jaringan ini yang dikenal sebagai *Botnet*. Mekanisme pengendalian jaringan juga ditetapkan di mana *Command & Control* (C&C) ditugaskan ke sumber daya berkapasitas tinggi khusus yang secara langsung mengeluarkan instruksi atas nama penyerang untuk memberi perintah dan mengambil tanggapan dari sejumlah *zombie* yang digunakan untuk mengirimkan lalu lintas serangan langsung ke target (korban). Mereka juga menyampaikan informasi tentang korban kembali ke penyerang melalui fungsi C&C [3].

Pada penelitian R Alzahrani, A Alzahrani yang berjudul *Security analysis of ddos attacks using machine learning algorithms in networks traffic* menjelaskan bahwa analisis dari kinerja sistem deteksi serangan DDoS menggunakan dataset

CIC-DDoS 2019. pada penelitian ini menggunakan enam jenis algoritma ML seperti K-NN, SVM, NB, DT, RF, dan LR yang mana menghasilkan tikat akurasi sebesar 0.98 menggunakan K-NN, 0.86 menggunakan SVM, 0.45 menggunakan NB, 0.99 menggunakan DT, 0.99 menggunakan RF, dan 0.98 mengunakan LR [4].

Pada penelitian Ming-Yang Su yang berjudul *Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers* dijelaskan bahwa metode untuk *weight features* dari DDoS *attack* dan menganalisis hubungan antara kinerja deteksi dan jumlah fitur. Dengan menggunakan metode klasifikasi K-NN akurasi keseluruhan terbaik adalah 97,42%, yang hanya dipertimbangkan 19 fitur [5]. Pada penelitian A. Kachavimath, S. Nazare, S. Akki yang berjudul *Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics* menjelaskan bahwa deteksi serangan DDoS untuk meningkatkan keamanan jaringan mengunakan *machine learning*. Hasil eksperimen menunjukkan kinerja algoritma *K- Nearest Neighbor* dan *naive bayes* lebih baik dibandingkan dengan model pembelajaran konvensional [6].

Pada penelitiaan berjudul *Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm* menjelaskan bahwa peran dari *feature selection* digunakan untuk mengurangi dimensi dengan memilih fitur terbaik yang menghasilkan peningkatan akurasi pada beberapa metode *machine learning* seperti metode KNN akurasi yang di dapatkan meningkat yaitu menjadi 0,99 % [7].

Dari beberapa penelitian terdahulu tersebut penulis ingin melakukan penelitian dengan menerapkan beberapa fitur seleksi untuk menemukan pola fitur terbaik dalam mendeteksi serangan DDoS dengan menggunakan metode *K-Nearest Neighbor*.

1.2 Tujuan

Berikut ini tujuan dari penelitian tugas akhir ini adalah :

1. Mendeteksi dan mengenali pola fitur terbaik dalam serangan DDoS.
2. Menerapkan algoritma *K-Nearest Neighbor* (KNN) untuk klasifikasi terhadap serangan DDoS.

3. Melakukan fitur seleksi untuk menemukan pola fitur terbaik dalam mendeteksi serangan DDoS.

1.3 Manfaat

Berikut ini Manfaat dari penelitian tugas akhir ini adalah :

1. Dapat mengetahui atau mengenali pola serangan DDoS dari penerapan algoritma *K-Nearest Neighbor* (KNN).
2. Dapat membedakan atau mengklasifikasikan serangan DDoS pada dataset CIC-IDS2017.
3. Dapat mengetahui pola fitur terbaik dari penggunaan fitur seleksi dan algoritma *K-Nearest Neighbor* (KNN) dalam klasifikasi serangan DDoS.

1.4 Rumusan Masalah

Berdasarkan latar belakang diatas terdapat beberapa permasalah yang timbul. maka didapatkan rumusan masalah sebagai berikut :

1. Bagaimana cara mendeteksi dan mengenali pola fitur terbaik dalam serangan DDoS pada dataset CIC-IDS2017 ?
2. Bagaimana cara menemukan teknik fitur seleksi terbaik dari sistem deteksi serangan DDoS dengan metode *K-Nearest Neighbor* (KNN)?
3. Bagaimana cara mengimplementasikan algoritma *K-Nearest Neighbor* (KNN) dalam mendeteksi serangan DDoS ?

1.5 Batasan Masalah

Berdasarkan rumusan masalah diatas, maka didapatkan batasan masalah sebagai berikut :

1. Untuk dataset serangan penelitian ini berfokus pada serangan DDoS.
2. Menggunakan teknik fitur seleksi seperti *Mutual Information, Correlation, Lasso Regularization,* dan *Random Forest Classifier* yang dapat menemukan pola fitur terbaik dari serangan DDoS.
3. Menggunakan algoritma *K-Nearest Neighbor (KNN)* untuk klasifikasi serangan.

1.6 Metodelogi Penelitian

Pada penelitian ini metodologi yang digunakan dalam penelitian tugas akhir akan melalui tahapan-tahapan sebagai berikut :

1. Tahap Pertama (Studi Pustaka)

   Pada tahapan ini merupakan tahap dimana penulis menemukan masalah yang tepat untuk dibahas dalam penelitian. Dengan mencari serta membaca referensi yang memiliki keterkaitan dengan topik tugas akhir seperti jurnal, literatur, buku, akrtikel dan lain-lainya.

2. Tahap Kedua (Perancangan sistem)

   Pada tahap kedua akan membahas mengenai proses dan langkah-langkah yang dibuat berdasarkan perumusan masalah yang dicari pada penelitian yaitu membangun dan menerapkan algoritma yang akan dipakai untuk mengolah data mentah menjadi data bersih yang dapat digunakan untuk penerapan pada penelitian ini.

3. Tahap Ketiga (Pengujian)

   Pada tahap ini membahas pengujian dan penerapan berdasarkan metodologi penelitian yang telah ditentukan, sehingga mendapatkan hasil uji yang tepat dengan konsep yang telah direncanakan serta mendaptkan hasil yang lebih baik dari sebelumnya.

4. Tahap Keempat (Analisa)

   Pada tahap keempat ini akan menganalisis data yang dihasilkan dari proses pengujian dan pengklasifikasian untuk mendapatkan hasil kesimpulan yang objektif.

5. Tahap Kelima (Kesimpulan dan Saran)

   Pada tahapan kelima akan menentukan kesimpulan yang didapat dari tahapan pengujian dan analisa sehingga mendaptkan saran untuk dijadikan landasan penelitian selanjutnya.

1.7 Sistematika Penulisan

Sistematika penulisan ini digunakan untuk mempermudah proses penyusunan tugas akhir serta menjelaskan isi dari tiap bab yang ada pada penelitian ini, maka dibuat suatu sistematika penulisan sebagai berikut :

1. Pendahuluan

   Pada bab ini menjelaskan secara menyeluruh mengenai latar belakang, tujuan, manfaat, rumusan masalah serta batasan masalah, metodologi penelitian, dan sistematika penulisan dengan topik yang diangkat adalah "Seleksi Fitur Untuk Menemukan Pola Fitur Terbaik Pada Sistem Pendeteksi Serangan DDoS Dengan Menggunakan Metode K-NN.

2. Tinjauan Pustaka

   Bab ini berisikan beberapa literatur *review* dari penelitan terkait dengan seleksi fitur, DDoS *attack*, dan algoritma klasifikasi *K-Nearest Neighbor* (K-NN) yang berhubungan secara langsung dengan penelitian sebelumnya.

3. Metodologi Penelitian

   Metodologi penelitian ini menjelaskan proses penelitian yang dilakukan melipuuti penjelasan menyeluruh mengenai tahapan-tahapan dari mempersiapkan data, perancangan sistem, dan penerapan metode penelitian yang telah ditentukan sebelumnya.

4. Pengujian dan Analisa

   Bab ini menjelaskan mengenai hasil klassifikasi yang diperoleh dari pengujian data yang dilakukan kemudian menganalisis hasil dari tiap metode yang diperoleh dari hasil pengujian.

5. Kesimpulan dan Saran

   Pada bab terakhir ini berisi penjelasan mengenai kesimpulan akhir yang diambil dari penelitian yang dilakukan untuk menjawab semua tujuan yang telah ditentukan kemudian menjelaskan saran yang akan digunakan sebagai referensi atau masukan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] C. Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: Classification and state-of-the-art,” *Comput. Networks*, vol. 44, no. 5, pp. 643–666, 2004, doi: 10.1016/j.comnet.2003.10.003.

[2] A. Azhari, A. W. Muhammad, and C. F. M. Foozy, “Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection,” *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 1–8, 2020, doi: 10.29099/ijair.v4i1.156.

[3] 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.

[4] R. J. Alzahrani and A. Alzahrani, “Security analysis of ddos attacks using machine learning algorithms in networks traffic,” *Electron.*, vol. 10, no. 23, 2021, doi: 10.3390/electronics10232919.

[5] M. Y. Su, “Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers,” *Expert Syst. Appl.*, vol. 38, no. 4, pp. 3492–3498, 2011, doi: 10.1016/j.eswa.2010.08.137.

[6] A. V. Kachavimath, S. V. Nazare, and S. S. Akki, “Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics,” *2nd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2020 - Conf. Proc.*, no. Icimia, pp. 711–717, 2020, doi: 10.1109/ICIMIA48430.2020.9074929.

[7] 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,” *Commun. Comput. Inf. Sci.*, vol. 935, pp. 141–149, 2018, doi: 10.1007/978-3-030-00840-6_16.

[8] I. Ramadhan, P. Sukarno, and M. A. Nugroho, “Comparative Analysis of K-Nearest Neighbor and Decision Tree in Detecting Distributed Denial of Service,” *2020 8th Int. Conf. Inf. Commun. Technol. ICoICT 2020*, pp. 16–19, 2020, doi: 10.1109/ICoICT49345.2020.9166380.

[9] A. Maslan, K. M. Bin Mohamad, and F. B. Mohd Foozy, “Feature selection for DDoS detection using classification machine learning techniques,” *IAES Int. J. Artif. Intell.*, vol. 9, no. 1, pp. 137–145, 2020, doi: 10.11591/ijai.v9.i1.pp137-145.

[10] J. Zhang, Q. Liang, R. Jiang, and X. Li, “A feature analysis based identifying scheme using GBDT for DDoS with multiple attack vectors,” *Appl. Sci.*, vol. 9, no. 21, 2019, doi: 10.3390/app9214633.

[11] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, “Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method,” *Symmetry (Basel).*, vol. 14, no. 6, p. 1095, 2022, doi: 10.3390/sym14061095.

[12] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert, and R. Kocaoğlu, “Machine learning approach equipped with neighbourhood component analysis for ddos attack detection in software-defined networking,” *Electron.*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111227.

[13] M. Alkasassbeh, “An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods,” *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 22, pp. 5962–5976, 2017.

[14] M. Aqil, H. Azmi, C. Feresa, M. Foozy, K. Amin, and M. Sukri, “Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms,” vol. 5, no. December, pp. 395–401, 2021.

[15] K. J. Singh and T. De, “Efficient Classification of DDoS Attacks Using an Ensemble Feature Selection Algorithm,” *J. Intell. Syst.*, vol. 29, no. 1, pp. 71–83, 2020, doi: 10.1515/jisys-2017-0472.

[16] C. Wang, H. Yao, and Z. Liu, “An efficient DDoS detection based on SU-Genetic feature selection,” *Cluster Comput.*, vol. 22, pp. 2505–2515, 2019, doi: 10.1007/s10586-018-2275-z.

[17] D. Alghazzawi, O. Bamasaq, H. Ullah, and M. Z. Asghar, “Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection,” *Appl. Sci.*, vol. 11, no. 24, 2021, doi: 10.3390/app112411634.

[18] N. A. Singh, J. Singh, and T. De, “Distributed denial of service attack

detection using naive bayes classifier through info gain feature selection," *ACM Int. Conf. Proceeding Ser.*, vol. 25-26-Augu, 2016, doi: 10.1145/2980258.2980379.

[19] S. Nandi, S. Phadikar, and K. Majumder, "Detection of DDoS Attack and Classification Using a Hybrid Approach," *ISEA-ISAP 2020 - Proc. 3rd ISEA Int. Conf. Secur. Priv. 2020*, pp. 41–47, 2020, doi: 10.1109/ISEA-ISAP49340.2020.234999.

[20] G. Lucky, F. Jjunju, and A. Marshall, "A Lightweight Decision-Tree Algorithm for detecting DDoS flooding attacks," *Proc. - Companion 2020 IEEE 20th Int. Conf. Softw. Qual. Reliab. Secur. QRS-C 2020*, pp. 382–389, 2020, doi: 10.1109/QRS-C51114.2020.00072.

[21] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models," *Sustain.*, vol. 12, no. 3, 2020, doi: 10.3390/su12031035.

[22] 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.

[23] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the SYN Flood DoS Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 8, pp. 15–11, 2013, doi: 10.5815/ijcnis.2013.08.01.

[24] A. Singh and D. Juneja, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks," *Int. J. Eng. Sci. Technol.*, vol. 2, no. 8, pp. 3405–3411, 2010.

[25] P. Prajapati, N. Patel, and P. Shah, "A review of recent detection methods for HTTP ddos attacks," *Int. J. Sci. Technol. Res.*, vol. 8, no. 12, pp. 1693–1696, 2019.

[26] U. M. Khaire and R. Dhanalakshmi, "Stability of feature selection algorithm: A review," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1060–1073, 2022, doi: 10.1016/j.jksuci.2019.06.012.

[27] B. Remeseiro and V. Bolon-Canedo, "A review of feature selection methods in medical applications," *Comput. Biol. Med.*, vol. 112, no. May, pp. 25–29, 2019, doi: 10.1016/j.compbiomed.2019.103375.

[28] L. Yu and H. Liu, “Feature Selection for High-Dimensional Data: A Fast Correlation-Based Filter Solution,” *Proceedings, Twent. Int. Conf. Mach. Learn.*, vol. 2, pp. 856–863, 2003.

[29] B. Khelil, A. Kachouri, M. Ben Messaoud, and H. Ghariani, “P Wave Analysis in ECG Signals using Correlation for Arrhythmias Detection P Wave Analysis in ECG Signals using Correlation for Arrhythmias Detection,” no. January, 2007.

[30] J. R. Vergara and P. A. Estévez, “A review of feature selection methods based on mutual information,” *Neural Comput. Appl.*, vol. 24, no. 1, pp. 175–186, 2014, doi: 10.1007/s00521-013-1368-0.

[31] F. Amiri, M. Rezaei Yousefi, C. Lucas, A. Shakery, and N. Yazdani, “Mutual information-based feature selection for intrusion detection systems Fatemeh,” *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1184–1199, 2011, doi: 10.1016/j.jnca.2011.01.002.

[32] N. Kwak and C. H. Choi, “Input feature selection by mutual information based on Parzen window,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 12, pp. 1667–1671, 2002, doi: 10.1109/TPAMI.2002.1114861.

[33] D. Petkovic, R. Altman, M. Wong, and A. Vigil, “Improving the explainability of Random Forest classifier – User centered approach,” *Pacific Symp. Biocomput.*, vol. 0, no. 212669, pp. 204–215, 2018, doi: 10.1142/9789813235533_0019.

[34] M. Pal, “Random forest classifier for remote sensing classification,” *Int. J. Remote Sens.*, vol. 26, no. 1, pp. 217–222, 2005, doi: 10.1080/01431160412331269698.

[35] F. Emmert-Streib and M. Dehmer, “High-Dimensional LASSO-Based Computational Regression Models: Regularization, Shrinkage, and Selection,” *Mach. Learn. Knowl. Extr.*, vol. 1, no. 1, pp. 359–383, 2019, doi: 10.3390/make1010021.

[36] T. Wang, “A combined model for short-term wind speed forecasting based on empirical mode decomposition, feature selection, support vector regression and crossvalidated lasso,” *PeerJ Comput. Sci.*, vol. 7, pp. 1–23, 2021, doi: 10.7717/peerj-cs.732.

[37] S. S. Dash, S. K. Nayak, and D. Mishra, “A review on machine learning algorithms,” *Smart Innov. Syst. Technol.*, vol. 153, no. October, pp. 495–507, 2021, doi: 10.1007/978-981-15-6202-0_51.

[38] I. H. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions,” *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–21, 2021, doi: 10.1007/s42979-021-00592-x.

[39] H. A. Abu Alfeilat *et al.*, “Effects of Distance Measure Choice on K-Nearest Neighbor Classifier Performance: A Review,” *Big Data*, vol. 7, no. 4, pp. 221–248, 2019, doi: 10.1089/big.2018.0175.

[40] G. Farahani, “Feature Selection Based on Cross-Correlation for the Intrusion Detection System,” *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8875404.

[41] C. Nguyen, Y. Wang, and H. N. Nguyen, “Random forest classifier combined with feature selection for breast cancer diagnosis and prognostic,” *J. Biomed. Sci. Eng.*, vol. 06, no. 05, pp. 551–560, 2013, doi: 10.4236/jbise.2013.65070.

[42] R. Wazirali, “An Improved Intrusion Detection System Based on KNN Hyperparameter Tuning and Cross-Validation,” *Arab. J. Sci. Eng.*, vol. 45, no. 12, pp. 10859–10873, 2020, doi: 10.1007/s13369-020-04907-7.