DETEKSI SERANGAN DDOS DENGAN INTRUSION DETECTION SYSTEM MENGGUNAKAN METODE BIDIRECTIONAL RNN

TUGAS AKHIR

Oleh :

JEPI SUJANA

09011281823061

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

DETEKSI SERANGAN DDOS DENGAN INTRUSION DETECTION SYSTEM MENGGUNAKAN METODE BIDIRECTIONAL RNN

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh

JEPI SUJANA

09011281823061

Indralaya, 5 Januari 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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Jumat

Tanggal : 23 Desember 2022

Tim Penguji :

1. **Ketua : Ahmad Zarkasi, M.T.**
2. **Sekretaris : Nurul Afifah, M.Kom.**
3. **Penguji : Aditya Putra Perdana Prasetyo, M.T.**
4. **Pembimbing : Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama **: Jepi Sujana**

NIM **: 09011281823061**

Judul **: Deteksi Serangan DDoS Dengan Intrusion Detection System Menggunakan Metode Bidirectional RNN**

Hasil Pengecekan Software iThenticate/Turnitin : 14%

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

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

Indralaya, 5 Januari 2023

Jepi Sujana

NIM.09011281823061

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan atas kehadirat Allah SWT yang telah memberikan segala karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini dengan judul **"Deteksi Serangan DDoS Dengan Intrusion Detection System Menggunakan Metode Bidirectional RNN"**.

Penulis berharap agar laporan ini bermanfaat bagi banyak pihak, serta menjadi salah satu sumber bacaan atau referensi bagi peneliti lain yang tertarik dalam bidang keamanan jaringan komputer.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada berbagai pihak yang telah terlibat atas ide dan saran, serta bantuannya dalam menyelesaikan penulisan Tugas Akhir ini. Oleh karena itu penulis ingin mengucapkan rasa syukur dan terima kasih kepada yang terhormat :

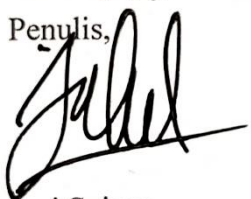
1. Tuhan yang Maha Esa Allah SWT, yang telah memberikan rahmat serta karunia-Nya sehingga saya dapat menyelesaikan penulisan Tugas Akhir ini dengan baik.
2. Kedua orang tua dan adik serta keluarga saya tercinta yang telah memberikan doa, nasihat, motivasi, dan dukungannya baik dari segi moril, materil maupun spiritual selama ini.
3. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Ahmad Fali Oklilas, M.T. selaku Dosen Pembimbing Akademik.
6. Bapak Ahmad Heryanto, S.Kom., M.T selaku Dosen pembimbing Tugas Akhir saya yang telah memberikan kritik, saran, dan motivasi terbaik untuk kebaikan serta kemajuan dalam menyelesaikan Tugas Akhir ini.
7. Mbak Renny Virgasari, S.E. selaku admin jurusan Sistem Komputer yang telah membantu saya dalam menyelesaikan urusan administrasi Tugas Akhir ini.

8. Agung Al Hafizin, Ahmad Afidin, Jumhadi, Rani Octaviani, M Taufik, M Alfat Hayatur Rizon, Rizki Angga Pratama, kepada teman-teman yang ada di Lab Jarkom dan Comnets yang telah membantu saya dalam melakukan penulisan akhir ini.
9. Mochammad Rafii Nanda W, Dwi Lingga Hanayuda, Daffa Bima Perdana, dan Bima Gusti Syauqi sebagai teman seperjuangan yang telah berjuang bersama-sama dalam suka dan duka.
10. Dimas Aditya Kristianto, Ades Harafi Duri, Alifah Fidela, Samuel Benedict, Prazna Paramitha Avi, Tri Putri, Hanna Pertiwi dan Rizki Valen Mafaza yang telah membantu dan memberikan semangat.
11. Teman-teman SK B 2018 Indralaya yang telah memberikan dukungan dan semangat.
12. Teman-teman seperjuangan dari jurusan Sistem Komputer yang tidak bisa saya sebutkan satu-persatu.
13. Semua pihak yang telah membantu dan mendukung.

Dalam penyusunan Tugas Akhir ini saya menyadari sepenuhnya bahwa laporan ini masih memiliki banyak kekurangan, oleh karena itu saya mengharapkan kritik dan saran dari semua pihak yang berkenan agar menjadi bahan evaluasi dan menjadi lebih baik lagi.

Akhir kata penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Indralaya, 5 Januari 2023
Penulis,



Jepi Sujana
NIM. 09011281823061

DDOS ATTACK DETECTION WITH INTRUSION DETECTION SYSTEM USING BIDIRECTIONAL RNN METHOD

JEPI SUJANA (09011281823061)
Computer Engineering Department, Computer Science Faculty, Sriwijaya University
Email : jepisujana@gmail.com

ABSTRACT

DDoS attacks can cause targeted servers to become slow and web server services unavailable, but DDoS attacks are difficult to detect in a network because their traffic patterns are similar to those of legitimate clients, because attackers emulate their attack traffic among legitimate traffic to hide their attacks. In this study, datasets originating from CSE-CIC-IDS 2018 were used. There are three objectives in this study. The first is the implementation of the Corelation-based Feature Selection (CFS) feature in order to obtain important features during the attack detection process. The second is the application of the Bidirectional RNN method to detect DDoS attacks. The third is knowing the results of DDoS attack detection performance seen from the results of the values for accuracy, precision, sensitivity, specificity, F1-Score, BAAC and MMC. The deep learning method used is Bidirectional RNN, which is a branch of RNN which can duplicate the RNN processing chain so that the input can be processed in the order of the backward layer and the forward layer so that it is possible to provide an increase in high accuracy results. This research has three benefits, the first is providing optimization in terms of computation time, the second is applying the Bidirectional RNN method to detect DDoS attacks, and the third is providing the best performance when the detection process is using the Bidirectional RNN method. This research was conducted by training the CSE-CIC-IDS 2018 dataset on machine learning by tuning hyper parameters and comparing the ratios of different training data and test data so as to produce the best evaluation value with an accuracy value of 99.9954%, 99.9905% recall, 100% specificity, 100% precision, F1-Score 99.9954%, and performance BACC 99.9954%, and MCC 99.9908%.

Keywords *: DDoS, RNN, Bidirectional RNN, CFS, CSE-CIC-IDS 2018 Datasets.*

Palembang, 5 January 2023

Acknowledge,

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

DETEKSI SERANGAN DDOS DENGAN INTRUSION DETECTION SYSTEM MENGGUNAKAN METODE BIDIRECTIONAL RNN

JEPI SUJANA (09011281823061)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
, Email : jepisujana@gmail.com

ABSTRAK

Serangan DDoS dapat menyebabkan server yang telah ditargetkan menjadi lambat dan layanan web server tidak tersedia, tetapi serangan DDoS sulit untuk di deteksi dalam jaringan karena pola lalu lintasnya mirip dengan klien yang sah, karena penyerang meniru lalu lintas serangan mereka di antara lalu lintas yang sah untuk menyembunyikan serangan mereka. Dalam penelitian ini digunakan dataset yang berasal dari CSE-CIC-IDS 2018. Terdapat tiga tujuan dalam penelitian ini yang pertama penerapan fitur *Corelation-based Feature Selection* (CFS) agar didapatkan fitur penting saat proses deteksi serangan. Kedua penerapan metode *Bidirectional RNN* untuk mendeteksi serangan DDoS. Ketiga mengetahui hasil performa deteksi serangan DDoS dilihat dari hasil nilai akurasi, presisi, sensitivitas, spesifitas, F1-Score, BAAC dan MMC. Adapun metode *deep learning* yang digunakan adalah *Bidirectional RNN* merupakan cabang dari RNN di mana dapat menggandakan rantai pemrosesan RNN sehingga inputnya dapat diproses dalam urutan lapisan *backward* dan lapisan *forward* sehingga memungkinkan memberikan peningkatan hasil akurasi yang tinggi. Penelitian ini memiliki tiga manfaat, yang pertama memberikan pengoptimalan dari segi waktu komputasi, kedua menerapkan metode *Bidirectional RNN* untuk melakukan deteksi serangan DDoS, dan yang ketiga memberikan performa terbaik saat proses deteksi menggunakan metode *Bidirectional RNN*. Penelitian ini dilakukan dengan cara *training* dataset CSE-CIC-IDS 2018 pada *machine learning* dengan melakukan *tuning hyper parameter* serta melakukan perbandingan rasio data latih dan data uji yang berbeda sehingga menghasilkan nilai evaluasi terbaik dengan nilai akurasi 99.9954%, recall 99.9905%, spesifitas 100%, presisi 100%, F1-Score 99.9954%, dan performa BACC 99.9954%, serta MCC 99.9908%.

Kata Kunci : DDoS, RNN, *Bidirectional* RNN, CFS, Dataset CSE-CIC-IDS 2018.

Palembang, 5 Januari 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**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Distributed Denial of Service (DDoS) adalah suatu bentuk serangan terbaru dari *Denial of Service* (DoS)[1], yang membuat lalu lintas normal jaringan dan server yang telah ditargetkan menjadi lambat. Serangan ini dibagi menjadi dua, pertama serangan DDoS menyebabkan gangguan pada konektivitas pengguna yang sah dikarenakan kehabisan *bandwidth*, sehingga mengurangi kapasitas penggunaan sumber daya jaringan disebut serangan pada lapisan jaringan (*network layer attack*). Sedangkan serangan yang membanjiri sumber daya server (misalnya CPU, memori, soket) disebut serangan lapisan aplikasi (*application layer attack*)[2], dalam serangan ini penyerang mencoba membuat sumber daya atau layanan menjadi tidak tersedia bagi pengguna yang sah[3]. Serangan DDoS berbasis IPv4 masih sangat dominan dikarenakan sederhananya perutean internet dan arsitektur dalam pengalamatan, sehingga penyerang dapat mengeksploitasi celah yang ada kemudian membuat beban yang meningkat pada penyedia layanan internet (ISP) dan operator pusat data[4]. Serangan DDoS dapat menyebabkan layanan web server tidak tersedia, tetapi serangan DDoS sulit untuk di deteksi dalam jaringan karena pola lalu lintasnya mirip dengan klien yang sah[5].

Dalam konteks serangan DDoS volumetrik, alamat sumber paket yang masuk akan diacak (dipalsukan), dan paket tersebut berasal dari kumpulan *host* atau penyedia layanan besar yang rentan disusupi. Salah satu masalah utama untuk metode deteksi DDoS adalah sulitnya membedakan paket serangan DDoS dari paket yang sah, karena penyerang meniru lalu lintas serangan mereka di antara lalu lintas yang sah untuk menyembunyikan serangan mereka. Hal ini membuat serangan DDoS menjadi ancaman yang sangat serius bagi pengguna komputer[6]. DDoS mewakili ancaman siber berorientasi jaringan kritis, yang trennya terus meningkat selama dekade terakhir. Sebagai contoh, serangan DDoS yang menargetkan Amazon AWS pada Q1 tahun 2020 dilaporkan memiliki volume puncak 2,3 Tbps[7]. *Distributed Denial of Service* (DDoS) telah menjadi salah

satu serangan selama beberapa dekade terakhir membuat pengguna yang sah tidak dapat mengakses layanan, lalu penyerang akan melumpuhkan target atau layanan.

Untuk melindungi sebuah sistem dan juga jaringan komputer dari berbagai macam serangan, maka perlu digunakan sebuah sistem deteksi serangan yaitu *Intrusion Detection System* (IDS). IDS merupakan suatu sistem perangkat keras atau perangkat lunak yang berfungsi untuk mengidentifikasi tindakan jahat pada suatu sistem komputer agar keamanan sistem memungkinkan untuk dipertahankan. Tujuan dari IDS untuk mengidentifikasi berbagai jenis trafik jaringan yang berbahaya dan penggunaan komputer yang mana tidak dapat di identifikasi oleh firewall tradisional[8]. Meskipun Intrusion Detection System (IDS) memiliki peran yang penting dalam mendeteksi potensi serangan, arus lalu lintas yang padat menyebabkan tantangan teknis tersendiri terkait dengan pemantauan dan pendeteksian aktivitas jaringan[9].

Terdapat dua pendekatan utama dari IDS, yang pertama IDS berbasis anomali di mana membandingkan perilaku normal aplikasi yang diamati untuk diidentifikasi terhadap adanya perilaku menyimpang yang signifikan, yang kedua IDS berbasis *signature* yang mana akan melakukan suatu pengawasan kepada paket pada jaringan dan melakukan suatu perbandingan kepada paket tersebut memakai *database* dengan semua perilaku *malware* yang diketahui (*malware signatures*)[10]. Terdapat beberapa kelemahan dari IDS yang pertama ketidakmampuan dalam menganalisis trafik dengan kecepatan dan volume yang tinggi, sehingga mengarah ke deteksi secara non-realtime, tidak mendukung IP versi 6.0 dan trafik terenkripsi[11]. berdasarkan penelitian terkait[11] terdapat tiga teknik yang digunakan berdasarkan pengumpulan informasi dan suplai data input, yang pertama *Host-based Intrusion Detection System* (HIDS), yang kedua *Network-based Intrusion Detection System* (NIDS), dan yang ketiga *Distributed Intrusion Detection System* (DIDS).

Recurrent Neural Networks (RNN) atau jaringan saraf berulang merupakan suatu jenis arsitektur jaringan saraf tiruan yang prosesnya melakukan pemanggilan secara berulang-ulang guna memproses data masukan yang biasanya merupakan data sekuensial. RNN mempunyai keterbatasan yang memproses input

dalam urutan temporal yang ketat yang artinya input saat ini memiliki konteks input sebelumnya namun tidak untuk prediksi masa depan. Sedangkan *Bidirectional Recurrent Neural Networks* (BRNN) dapat menggandakan rantai pemrosesan RNN sehingga inputnya dapat diproses dalam urutan waktu maju dan mundur. BRNN dapat dilatih tanpa batasan menggunakan informasi input hingga kerangka masa depan yang telah ditentukan dari sebelumnya. Ini dicapai dengan melatihnya secara bersamaan dalam arah waktu positif dan negatif[12].

Bidirectional Recurrent Neural Networks berfokus kepada konteks sebelum dan sesudah, sehingga dapat menggunakan lebih banyak informasi agar memberikan nilai yang lebih baik. Secara struktural, BRNN terdiri dari dua RNN yang berlawanan arah dengan kedua RNN terhubung ke lapisan output yang sama[13]. *Bidirectional Recurrent Neural Networks* terdiri dari unit LSTM dan GRU. Lapisan pertama dua arah terdiri dari LSTM yang merambat maju (*forward-propagation*) dan GRU yang merambat mundur(*back-propagation*), sehingga lapisan kedua memiliki komposisi dua arah yang berlawanan[14]. Dalam proses pelatihan BRNN, arah yang berbeda dipelajari secara mandiri, kemudian jalur maju dan mundur digabungkan agar lebih mengintegrasikan urutan dari fitur maju dan mundur[15].

Dalam penelitian sebelumnya[16], Implementasi dari sistem deteksi serangan DDOS IoT menggunakan *Machine learning*. Dalam penelitian tersebut terdapat empat jenis serangan DDoS yaitu sensor data Flood, ICMP Flood, SYN Flood, dan UDP Flood. Berdasarkan hasil dari percobaan penelitian tersebut didapatkan nilai dari Akurasi sebesar 97.39%, Presisi sebesar 97.38%, Recall sebesar 97.39%, dan F1-Score sebesar 97.33% dari segi kemampuan dalam melakukan deteksi serangan DDoS.

Dalam penelitian sebelumnya[17], Identifikasi serangan DDoS menggunakan *Deep Learning*. Berdasarkan hasil penelitian tersebut terdapat berbagai jenis metode yang dipakai dalam melakukan percobaan, yang pertama *Random Forest* didapatkan nilai Akurasi 96.627%, Presisi 95.532%, Recall 94.893%, dan F1-Score 93.698%, metode yang kedua yaitu CNNLSTM didapatkan nilai Akurasi 95.896%, Presisi 97.534%, Recall 94.208%, dan F1-

Score 95.831%, lalu metode yang ketiga yaitu LSTM didapatkan nilai Akurasi 97.606%, Presisi 97.832%, Recall 97.387%, dan F1-Score 97.601%, dari segi kemampuan dalam melakukan deteksi serangan DDoS.

Berdasarkan dari hasil yang diperoleh beberapa penelitian terkait di atas, maka dalam penelitian ini akan digunakan metode *Bidirectional Recurrent Neural Networks* (BRNN) untuk melakukan deteksi pada serangan DDoS. Dengan memakai dataset dari CIC-IDS-2018, agar memperoleh hasil prediksi yang terbaik dalam melakukan pendeteksian serangan.

1.2 Rumusan Masalah

Di bawah ini merupakan rumusan masalah yang akan dibahas untuk implementasi pada tugas akhir ini, yaitu sebagai berikut:

1. Bagaimana penerapan dari seleksi fitur agar didapatkan fitur penting pada deteksi serangan DDoS?
2. Bagaimana cara dari deteksi serangan DDoS dengan penerapan metode *Bidirectional* RNN?
3. Bagaimana kinerja hasil dari deteksi dengan metode *Bidirectional* RNN terhadap nilai akurasi, presisi, sensitivitas, spesifitas, F1-Score, BAAC dan MMC?

1.3 Batasan Masalah

Berikut ini merupakan batasan masalah dari tugas akhir ini, yaitu:

1. Penelitian ini menggunakan data dari *University of New Brunswick* (UNB) yaitu (CSE-CIC-IDS2018).
2. Penelitian ini sebatas mendeteksi serangan DDoS dengan IDS menggunakan metode *Bidirectional* RNN.
3. Output yang dihasilkan dari penelitian ini berupa nilai akurasi yang digunakan sebagai tolak ukur untuk melihat tingkat kecocokan author dengan label.

1.4 Tujuan Penelitian

Berikut ini merupakan tujuan dari penulisan tugas akhir ini, yaitu:

1. Penerapan seleksi pada fitur *Corelation-based Feature Selection* (CFS) agar didapatkan fitur yang penting saat proses deteksi serangan DDoS.
2. Penerapan metode *Bidirectional* RNN yang digunakan untuk mendeteksi serangan DDoS.
3. Dapat mengukur hasil dari kinerja terhadap nilai akurasi, presisi, sensitivitas, spesifitas, F1-Score, BAAC dan MMC.

1.5 Manfaat Penelitian

Berikut ini merupakan merupakan manfaat dari penelitian tugas akhir ini, yaitu:

1. Pengoptimalan dari segi waktu dalam proses komputasi.
2. Dapat menerapkan metode *Bidirectional* RNN untuk melakukan deteksi serangan DDoS.
3. Dapat memberikan performa terbaik saat proses deteksi menggunakan metode *Bidirectional* RNN.

1.6 Metodologi Penelitian

Dalam melakukan penelitian ini akan melewati beberapa metodologi, yang meliputi:

1. Metode Literatur dan Metode Studi Pustaka

   Ditahap ini penulis akan melakukan pencarian berbagai informasi tentang sistem deteksi serangan memakai metode *Bidirectional Recurrent Neural Networks* melalui berbagai macam artikel-artikel terkait, jurnal ilmiah, internet, dan buku yang dapat mendukung dalam penulisan Tugas Akhir ini.

2. Metode Konsultasi

   Pada metode ini, akan dilakukan konsultasi dengan pihak-pihak terkait, yang memiliki wawasan serta pengetahuan yang baik dalam mengatasi permasalahan pada saat penulisan tugas akhir.

3. Metode Pengumpulan Data

   Dalam fase ini dilakukan pengumpulan data terkait dengan serangan *Distributed Denial of Service* (DDoS), dan sistem deteksi intrusi (IDS).

4. Metode Pengujian

   Dalam tahap ini akan dilakukan perancangan sistem yang digunakan untuk melatih agar mendapatkan hasil dari deteksi serangan DDoS.

5. Metode Analisa dan Penarikan Kesimpulan

   Hasil yang didapat dari pengujian tugas akhir ini akan dilakukan analisa dari proses deteksi serangan dan akan ditarik beberapa kesimpulan dari penelitian ini.

1.7 Sistematika Penulisan

Berikut ini merupakan sistematika penulisan dari penelitian tugas akhir yaitu:

BAB I PENDAHULUAN

Di bab I ini penelitian akan terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan metodologi penelitian, serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Di bab II akan terdiri tentang penjelasan mengenai teori-teori utama tentang *Bidirectional Recurrent Neural Networks* (BRNN), *Distributed Denial of Service* (DDoS), dan teori-teori lain yang memiliki hubungan dengan penelitian Tugas Akhir

BAB III. METODOLOGI PENELITIAN

Metodologi penelitian ini akan terdiri dari proses penelitian yang dilakukan, pembuatan rancangan dari sistem deteksi serangan, serta penerapan dari proyek penelitian tugas akhir tersebut.

BAB IV. HASIL DAN ANALISIS PENELITIAN

Hasil dan analisis penelitian akan terdiri dari proses penelitian, dan analisa terhadap hasil data set menggunakan metode *Bidirectional Recurrent Neural Networks*.

BAB V. KESIMPULAN DAN SARAN

Pada bab ini akan dilakukan penarikan beberapa kesimpulan dari penjelasan yang ada di bab sebelumnya serta diberikan saran yang dapat membangun guna penelitian selanjutnya.

DAFTAR PUSTAKA

[1] A. B. M. A. Al Islam and T. Sabrina, "Detection of various denial of service and distributed denial of service attacks using RNN ensemble," *ICCIT 2009 - Proc. 2009 12th Int. Conf. Comput. Inf. Technol.*, no. Iccit, pp. 603–608, 2009, doi: 10.1109/ICCIT.2009.5407308.

[2] A. Sharma and A. Bhasin, "Critical Investigation of Denial of Service and Distributed Denial of Service Models and Tools," *Proc. - IEEE 2018 Int. Conf. Adv. Comput. Commun. Control Networking, ICACCCN 2018*, pp. 546–550, 2018, doi: 10.1109/ICACCCN.2018.8748468.

[3] B. Kumar Joshi, N. Joshi, and M. Chandra Joshi, "Early Detection of Distributed Denial of Service Attack in Era of Software-Defined Network," *2018 11th Int. Conf. Contemp. Comput. IC3 2018*, pp. 1–3, 2018, doi: 10.1109/IC3.2018.8530546.

[4] D. Salopek, M. Zec, M. Mikuc, and V. Vasic, "Surgical DDoS Filtering with Fast LPM," *IEEE Access*, vol. 10, pp. 4200–4208, 2022, doi: 10.1109/ACCESS.2022.3140522.

[5] K. Hong, Y. Kim, H. Choi, and J. Park, "SDN-Assisted Slow HTTP DDoS Attack Defense Method," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 688–691, 2018, doi: 10.1109/LCOMM.2017.2766636.

[6] A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Commun. Lett.*, vol. 13, no. 9, pp. 717–719, 2009, doi: 10.1109/LCOMM.2009.090615.

[7] I. Cvitic, D. Perakovic, B. B. Gupta, and K. K. R. Choo, "Boosting-Based DDoS Detection in Internet of Things Systems," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2109–2123,

2022, doi: 10.1109/JIOT.2021.3090909.

[8] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

[9] J. E. Varghese and B. Muniyal, “An Efficient IDS Framework for DDoS Attacks in SDN Environment,” *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[10] F. J. Mora-Gimeno, H. Mora-Mora, B. Volckaert, and A. Atrey, “Intrusion detection system based on integrated system calls graph and neural networks,” *IEEE Access*, vol. 9, pp. 9822–9833, 2021, doi: 10.1109/ACCESS.2021.3049249.

[11] H. Jadidoleslamy, “Weaknesses, Vulnerabilities And Elusion Strategies Against Intrusion Detection Systems,” *Int. J. Comput. Sci. Eng. Surv.*, vol. 3, no. 4, pp. 15–25, 2012, doi: 10.5121/ijcses.2012.3402.

[12] M. Schuster and K. K. Paliwal, “Bidirectional Recurrent Neural Networks,” *IEEE Trans. Signal Process.*, vol. 45, no. 11, pp. 2673–2681, 1997, doi: 10.1016/s1634-6939(13)59289-1.

[13] H. Bohan and B. Yun, “Traffic flow prediction based on BRNN,” *ICEIEC 2019 - Proc. 2019 IEEE 9th Int. Conf. Electron. Inf. Emerg. Commun.*, pp. 320–323, 2019, doi: 10.1109/ICEIEC.2019.8784513.

[14] X. Tang, Y. Dai, Q. Liu, X. Dang, and J. Xu, “Application of Bidirectional Recurrent Neural Network Combined with Deep Belief Network in Short-Term Load Forecasting,” *IEEE Access*, vol. 7, pp. 160660–160670, 2019, doi: 10.1109/ACCESS.2019.2950957.

[15] Y. Xu, X. Yan, Y. Wu, Y. Hu, W. Liang, and J. Zhang, “Hierarchical Bidirectional RNN for Safety-Enhanced B5G

Heterogeneous Networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2946–2957, 2021, doi: 10.1109/TNSE.2021.3055762.

[16] Y. Chen, J. Sheu, Y. Kuo, and N. Van Cuong, "Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning," pp. 122–127, 2020.

[17] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," *2017 IEEE Int. Conf. Smart Comput. SMARTCOMP 2017*, pp. 1–8, 2017, doi: 10.1109/SMARTCOMP.2017.7946998.

[18] J. Halladay *et al.*, "Detection and Characterization of DDoS Attacks Using Time-Based Features," *IEEE Access*, vol. 10, pp. 49794–49807, 2022, doi: 10.1109/ACCESS.2022.3173319.

[19] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A New Framework for DDoS Attack Detection and Defense in SDN Environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020, doi: 10.1109/ACCESS.2020.3021435.

[20] Ismail *et al.*, "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443–21454, 2022, doi: 10.1109/ACCESS.2022.3152577.

[21] S. Nayyar, S. Arora, and M. Singh, "Recurrent Neural Network Based Intrusion Detection System," *Proc. 2020 IEEE Int. Conf. Commun. Signal Process. ICCSP 2020*, pp. 136–140, 2020, doi: 10.1109/ICCSP48568.2020.9182099.

[22] Y. Fu, F. Lou, F. Meng, Z. Tian, H. Zhang, and F. Jiang, "An intelligent network attack detection method based on RNN," *Proc. - 2018 IEEE 3rd Int. Conf. Data Sci. Cyberspace, DSC 2018*, pp. 483–489, 2018, doi: 10.1109/DSC.2018.00078.

[23] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," *Proc. - 21st IEEE Int. Symp. a World Wireless, Mob.*

Multimed. Networks, WoWMoM 2020, pp. 391–396, 2020, doi: 10.1109/WoWMoM49955.2020.00072.

[24] D. Erhan and E. Anarim, "Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm," *IEEE Access*, vol. 8, pp. 118912–118923, 2020, doi: 10.1109/ACCESS.2020.3005781.

[25] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[26] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 602–622, 2016, doi: 10.1109/COMST.2015.2487361.

[27] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An Intra-and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract," *IEEE Access*, vol. 7, pp. 98893–98907, 2019, doi: 10.1109/ACCESS.2019.2930715.

[28] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810–146821, 2021, doi: 10.1109/ACCESS.2021.3123791.

[29] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.

[30] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward

generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-Janua, no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[31] A. Habibi Lashkari, G. Draper Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Tor Traffic using Time based Features," in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017, pp. 253–262, doi: 10.5220/0006105602530262.

[32] S. Chormunge and S. Jena, "Correlation based feature selection with clustering for high dimensional data," *J. Electr. Syst. Inf. Technol.*, vol. 5, no. 3, pp. 542–549, Dec. 2018, doi: 10.1016/j.jesit.2017.06.004.

[33] S. H. Moon and Y. H. Kim, "An improved forecast of precipitation type using correlation-based feature selection and multinomial logistic regression," *Atmos. Res.*, vol. 240, no. February, p. 104928, 2020, doi: 10.1016/j.atmosres.2020.104928.

[34] Y. Pristyanto, S. Adi, and A. Sunyoto, "The effect of feature selection on classification algorithms in credit approval," *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 451–456, 2019, doi: 10.1109/ICOIACT46704.2019.8938523.

[35] N. P. and K. M. Te-Shun Chou, Kang K. Yen, Jun Luo, "CORRELATION-BASED FEATURE SELECTION FOR INTRUSION DETECTION DESIGN Te-Shun Chou, Kang K. Yen, and Jun Luo," *Mil. Commun. Conf.*, pp. 1–7, 2007.

[36] A. C. Siregar and B. Ceasar Octariadi, "Feature Selection for Sambas Traditional Fabric 'Kain Lunggi' Using Correlation-Based Featured Selection (CFS)," *Proc. 2019 Int. Conf. Data Softw. Eng. ICoDSE 2019*, pp. 0–4, 2019, doi: 10.1109/ICoDSE48700.2019.9092731.

[37] X. Xu, H. Li, W. Xu, Z. Liu, L. Yao, and F. Dai, “Artificial intelligence for edge service optimization in Internet of Vehicles: A survey,” *Tsinghua Sci. Technol.*, vol. 27, no. 2, pp. 270–287, 2022, doi: 10.26599/TST.2020.9010025.

[38] S. A. Hassan, S. Akbar, A. Rehman, T. Saba, H. Kolivand, and S. A. Bahaj, “Recent Developments in Detection of Central Serous Retinopathy Through Imaging and Artificial Intelligence Techniques&x2013;A Review,” *IEEE Access*, vol. 9, pp. 168731–168748, 2021, doi: 10.1109/ACCESS.2021.3108395.

[39] M. Nazar, M. M. Alam, E. Yafi, and M. M. Su’Ud, “A Systematic Review of Human-Computer Interaction and Explainable Artificial Intelligence in Healthcare with Artificial Intelligence Techniques,” *IEEE Access*, vol. 9, pp. 153316–153348, 2021, doi: 10.1109/ACCESS.2021.3127881.

[40] IBM Cloud Education, “What is deep learning?,” *IBM*, 2020. https://www.ibm.com/cloud/learn/deep-learning (accessed Oct. 15, 2022).

[41] IBM Cloud Education, “What are Recurrent Neural Networks?,” *IBM*, 2020. https://www.ibm.com/cloud/learn/recurrent-neural-networks (accessed Oct. 25, 2022).

[42] K. S. Germain and F. Kragh, “Channel Prediction and Transmitter Authentication with Adversarially-Trained Recurrent Neural Networks,” *IEEE Open J. Commun. Soc.*, vol. 2, no. March, pp. 964–974, 2021, doi: 10.1109/OJCOMS.2021.3072569.

[43] DIVE INTO DEEP LEARNING, “Bidirectional Recurrent Neural Networks,” *DIVE INTO DEEP LEARNING*. https://d2l.ai/chapter_recurrent-modern/bi-rnn.html (accessed Oct. 26, 2022).

[44] A. Alsirhani, S. Sampalli, and P. Bodorik, “DDoS Detection System: Using a Set of Classification Algorithms Controlled by

Fuzzy Logic System in Apache Spark," *IEEE Trans. Netw. Serv. Manag.*, vol. PP, no. c, p. 1, 2019, doi: 10.1109/TNSM.2019.2929425.

[45] L. Frassineti, C. Barba, F. Melani, F. Piras, R. Guerrini, and C. Manfredi, "Automatic detection and sonification of nonmotor generalized onset epileptic seizures: Preliminary results," *Brain Res.*, vol. 1721, p. 146341, Oct. 2019, doi: 10.1016/j.brainres.2019.146341.

[46] M. Kabir, S. Ahmad, M. Iqbal, Z. N. Khan Swati, Z. Liu, and D.-J. Yu, "Improving prediction of extracellular matrix proteins using evolutionary information via a grey system model and asymmetric under-sampling technique," *Chemom. Intell. Lab. Syst.*, vol. 174, pp. 22–32, Mar. 2018, doi: 10.1016/j.chemolab.2018.01.004.

[47] M. Bach, A. Werner, J. Żywiec, and W. Pluskiewicz, "The study of under- and over-sampling methods' utility in analysis of highly imbalanced data on osteoporosis," *Inf. Sci. (Ny).*, vol. 384, pp. 174–190, Apr. 2017, doi: 10.1016/j.ins.2016.09.038.

[48] D. Ding, S. Han, H. Zhang, Y. He, and Y. Li, "Predictive biomarkers of colorectal cancer," *Comput. Biol. Chem.*, vol. 83, p. 107106, Dec. 2019, doi: 10.1016/j.compbiolchem.2019.107106.

[49] S. Su, Y. Sun, X. Gao, J. Qiu, and Z. Tian, "A Correlation-Change Based Feature Selection Method for IoT Equipment Anomaly Detection," *Appl. Sci.*, vol. 9, no. 3, p. 437, Jan. 2019, doi: 10.3390/app9030437.

[50] M. A. Deif, A. A. A. Solyman, M. A. Kamarposhti, S. S. Band, and R. E. Hammam, "A deep bidirectional recurrent neural network for identification of SARS-CoV-2 from viral genome sequences," *Math. Biosci. Eng.*, vol. 18, no. 6, pp. 8933–8950, 2021, doi: 10.3934/mbe.2021440.

[51] E. M. Hassib, A. I. El-Desouky, L. M. Labib, and E. S. M. El-kenawy, “WOA + BRNN: An imbalanced big data classification framework using Whale optimization and deep neural network,” *Soft Comput.*, vol. 24, no. 8, pp. 5573–5592, 2020, doi: 10.1007/s00500-019-03901-y.