PENERAPAN *INTRUSION DETECTION SYSTEM* DENGAN MENGGUNAKAN *GATED RECURRENT UNIT* (GRU) DALAM MENDETEKSI SERANGAN DDOS

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

DAFFA TEDI AGUSTIANSYAH

09011181924005

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

PENERAPAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN *GATED RECURRENT UNIT* (GRU) DALAM MENDETEKSI SERANGAN DDOS

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH

DAFFA TEDI AGUSTIANSYAH
09011181924005

Indralaya, Juli 2023

Mengetahui,

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

AUTHENTICATION PAGE

IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING A GATED RECURRENT UNIT (GRU) IN DETECTING DDOS ATTACKS

FINAL TASK

Submitted To Fulfill One Of The Requirements

To Obtain A Bachelor's Degree In Computer Science

By

DAFFA TEDI AGUSTIANSYAH

09011181924005

Indralaya, July 2023

Acknowledge,

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari: Selasa

Tanggal: 18 Juli 2023

Tim Penguji:

1. Ketua Sidang : Dr. Ahmad Zarkasi, M.T.
2. Sekretaris Sidang : Nurul Afifah, M.Kom.
3. Penguji Sidang : Huda Ubaya, M.T.
4. Pembimbing : Ahmad Heryanto, S.Kom., M.T.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Daffa Tedi Agustiansyah

NIM : 09011181924005

Program Studi : Sistem Komputer

Judul : Penerapan *Intrusion Detection System* menggunakan *Gated Recurrent Unit* (GRU) dalam mendeteksi serangan DDoS

Hasil pengecekan *Software Ithentivate/Turnitin* : 15%

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 tidak dipaksakan

Indralaya, Juli 2023

Penulis

Daffa Tedi Agustiansyah

NIM : 09011181924005

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan atas kehadirat llah SWT yang telah memberikan segala karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini dengan judul **"Penerapan *Intrusion Detection System* menggunakan *Gated Recurrent Unit* (GRU) dalam mendeteksi serangan DDoS"**.

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:

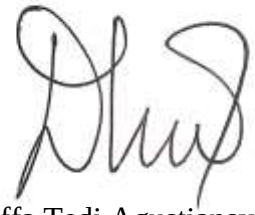
1. Tuhan yang Maha Esa Allah SWT, yang telah memberikan rahmat serta karunia-Nya sehingga saya dapat menyelesaikan penulisan Tugas Akhir ini dengan baik.
2. Kedua orang tua, kakak, dan adik serta keluarga saya tercinta yang telah memberikan doa, nasihat, motivasi, dan dukungannya baik dari segi moral, 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 dan Dosen Pembimbing Akademik
5. 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.
6. Semua pihak yang telah membantu

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 baha 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, Juli 2023

Penulis,



Daffa Tedi Agustiansyah

NIM. 09011181924005

PENERAPAN *INTRUSION DETECTION SYSTEM* DENGAN MENGGUNAKAN *GATED RECURRENT UNIT* (GRU) DALAM MENDETEKSI SERANGAN DDOS

DAFFA TEDI AGUSTIANSYAH (09011181924005)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : daffatediagustiansyah@gmail.com

ABSTRAK

Distributed Denial of Service atau biasa disingkat DDoS merupakan serangan yang biasa digunakan oleh *hacker* untuk mengehntikan *user* (pengguna) sah mengakses layanan jaringan tertentu dan terus mengirimkan lalu lintas ke sistem target secara terus-menerus. Serangan DDoS biasanya dilakukan dalam dua fase yaitu fase intuisi dimana penyerang membuat pengaturan peluncuran serangan dengan membuat *botnet* yang merupakan jaringan perangkat yang terinfeksi atau berbahaya dan fase kedua, pengaturan pada *botnet* akan dipicu untuk menyerang jaringan target. Metode yang digunakan pada penelitian adalah *Gated Recurrent Unit* (GRU). Kelebihan dari GRU adalah model GRU merupakan jenis RNN lanjutan lainnya yang membutuhkan sedikit waktu untuk dilatih karena kesederhanaan struktur gerbangnya. Penelitian dilakukan dengan mendeteksi 2 kelas serangan yaitu serangan DDoS dan serangan *Benign* dengan hasil validasi mulai dari 10% hingga 90% data training, terhadap *hyper parameter* jumlah *Layer* dan *Node*, aktivasi *tanh* dan *softmax*, *learning rate*, *batch size*, *optimizer*, dan *loss*. Berdasarkan pengujian yang telah dilakukan, hasil terbaik didapat pada data training 70% dan data training 30% dengan tingkat *akurasi* 99,9995%, *recall* 100%, *sensitivitas* 99,9990%, *presisi* 100%, *F1-score* 99,9994%.

Kata Kunci: *Intrusion Detection System, Distributed Denial of Service, Deep Learning, Gated Recurrent Unit, Correlation-based Feature Selection.*

Mengetahui

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

IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING THE GATED RECURRENT UNIT (GRU) IN DETECTING DDOS ATTACKS

DAFFA TEDI AGUSTIANSYAH (09011181924005)

Computer Engineering Department, Computer Science Faculty, Sriwijaya University

Email : daffatediagustiansyah@gmail.com

ABSTRACT

Distributed Denial of Service or commonly abbreviated as DDoS is an attack commonly used by hackers to stop legitimate users from accessing certain network services and continue to send traffic to the target system continuously. DDoS attacks are usually carried out in two phases, namely the intuition phase where the attacker makes arrangements to launch the attack by creating a botnet which is a network of infected or malicious devices and the second phase, the settings on the botnet will be triggered to attack the target network. The method used in this research is the Gated Recurrent Unit (GRU). The advantage of GRU is that the GRU model is another advanced type of RNN that requires less time to train due to the simplicity of its gate structure. The research was conducted by detecting 2 classes of attacks, namely DDoS attacks and Benign attacks with validation results ranging from 10% to 90% of training data, on the hyper parameter number of Layers and Nodes, tanh and softmax activation, learning rate, batch size, optimizer, and loss. Based on the tests that have been carried out, the best results are obtained on 70% training data and 30% training data with an accuracy rate of 99.9995%, 100% recall, 99.9990% sensitivity, 100% precision, F1-score 99.9994%.

Keywords: *Intrusion Detection System, Distributed Denial of Service, Deep Learning, Gated Recurrent Unit, Correlation-based Feature Selection.*

Acknowledge,

Head of Computer System Deparment	**Supervisor**
Dr. Ir. 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

Terdapat 5 alasan utama seorang penyerang (*attacker*) memulai serangan yaitu keuntungan finansial, balas dendam (*revenge*), keyakinan ideologis, tantangan intelektual, dan perang *cyber* dengan cara meluncurkan serangan dapat bervariasi dari satu penyerang ke penyerang lainnya dan menganggu sistem yang ditargetkan adalah salah satu tujuan serangan pada dunia *cyber* [2][3][4]. Dari hal tersebut, niat untuk melancarkan serangan dapat bervariasi dari penyerang ke penyerang. Karena efek serangan ini meningkat, sangat penting untuk mendeteksi dan mencegah serangan sejak dini sebelum mencapai target. Diantara serangan-serangan tersebut adalah *Distributed Denial of Service* (DDoS) yang biasa digunakan *hacker* untuk menghentikan *user* (pengguna) sah mengakses layanan jaringan tertentu dan terus mengirimkan lalu lintas ke sistem target secara terus-menerus [2][5]. Serangan DDoS biasanya dilaksanakan dalam 2 fase yaitu fase intusi dimana penyerang membuat pengaturan peluncuran serangan dengan membuat *botnet* yang merupakan jaringan perangkat yang terinfeksi atau berbahaya (menggunakan alat DDoS di beberapa host jaringan). Fase kedua, pengaturan pada *botnet* akan dipicu untuk menyerang jaringan target [2].

Serangan DDoS mampu melumpuhkan *server* dengan membanjiri lalu lintas jaringan dengan mengakibatkan *down*. Serangan DDoS merupakan Teknik yang paling populer dan menjadi senjata pilihan *hacker* karena telah terbukti menjadi ancaman di internet, serangan ini telah ada sejak tahun 1990 [3]. Serangan DDoS, yang merupakan salah satu serangan paling berbahaya, dapat membanjiri jaringan *cloud* dengan lalu lintas yang tidak diinginkan dan menutup sumber daya *cloud* untuk pengguna *cloud*. Keamanan sistem *cloud* menjadi sangat penting seiring dengan meningkatnya serangan terhadap sistem tersebut [2].

Serangan DDoS ini dapat diklasifikasikan sebagai serangan *flooding* dan serangan *logical*. Serangan *SYN flooding*, serangan *ICMP*, dan serangan

UDP flooding adalah beberapa jenis serangan *flooding* [4]. *Ping of death*, serangan *teardrop*, dan serangan *land* adalah beberapa jenis serangan *logical* [4]. Serangan *UDP flooding* sering digunakan untuk serangan DDoS bandwith besar, dan serangan *SYN flooding* bekerja dengan membuat koneksi setengah terbuka. Dalam jenis serangan ini, Ketika sistem korban menerima paket SYN dari *port* terbuka, penyerang mencoba membangun koneksi dengan merespons dengan SYN-ACK. Selama *SYN flooding*, penyerang tidak menanggapi paket SYN-ACK. Dalam serangan ini, koneksi yang ditargetkan tetap setengah terbuka sampai batas waktu berakhir. Jenis serangan ini berfokus pada *server* dan dilakukan menggunakan paket TCP. Dalam serangan seperti itu, yang menyebabkan konsekuensi serius, sumber daya dikonsumsi sepenuhnya dan *server* terkunci. Serangan UDP Flood adalah jenis DDOS yang menargetkan protokol UDP [4].

Berbagai peneliti di dunia menggunakan mekanisme pembelajaran machine learning seperti *Support Vector Machine* (SVM), *K-Nearest Neighbor* (KNN), *Artificial Neural Network* (ANN), *Random Forest*, dan lainnya. Begitu juga dengan metode seperti *Logistic Regression* dan *Gaussian* model yang mana akurasi terbaik yang dilaporkan sebesar 84% [6][7][8].

Metode *Intrusion Detection System* (IDS) menggunakan pembelajaran *machine learning* telah dipelajari oleh banyak peneliti, namun teknik ini biasanya dipertimbangkan kembali tentang cara memberi label pada dataset training yang sangat penting untuk keakuratan model deteksi. Dan peneliti juga perlu mempertimbangkan sumber daya komputasi dan penyimpanan yang dikonsumsi oleh model training atau testing [7]. Karena itulah, disini saya menggunakan metode *Gated Recurrent Unit* (GRU). GRU merupakan salah satu metode *dari Recurrent Neural Network* (RNN) yang memiliki sumber daya komputasi dan penyimpanan yang sedikit dan biasa digunakan untuk meningkatkan akurasi deteksi dan mengurangi *False Alarm Rate* (FAR) [8].

Pada penelitian [4] menggunakan LSTM-CLOUD untuk mendeteksi dan mencegah serangan DDoS di jaringan *cloud* publik. Sistem LSTM-CLOUD terdiri dari 2 modul yaitu deteksi dan pertahanan. Fungsi dari modul pertama

sistem ditentukan sebagai pendeteksi terjadinya serangan DDoS dengan menggunakan *Deep Learning Long Short Term Memory* (LSTM). Fungsi modul kedua sistem ditentukan sebagai pengaktifan mekanisme pertahanan. Eksperimen menunjukkan bahwa akurasi model deteksi menggunakan LSTM adalah 99,83%.

Pada penelitian [5] menggabungkan pemilihan fitur sekuensial dengan *Multilayer Perceptron* (MLP) untuk memilih fitur optimal selama fase training dan merancang mekanisme feedback untuk merekonstruksi deteksi saat mendeteksi kesalah yang cukup besar. hasilnya menunjukkan bahwa metode peneliti dapat menghasilkan kinerja deteksi yang sebanding dan mengoreksi deteksi ketika kinerjanya buruk.

Pada penelitian [2] menggunakan pendekatan supervised learning yaitu *Logistic Regression* (LR), *Decision Tree* (DT), *Gradient boost* (GB), *K-nearest neighbor* (KNN), dan *Support Vector Machine* (SVM). Semua penelitian ini dievaluasi pada dataset CIC-DDOS2019 dan hasil penelitian menunjukkan bahwa model GB berkinerja baik dibandingkan dengan metode lainnya dengan akurasi 99,97%.

Pada penelitian [9] menggunakan berbagai macam model berdasarkan *Deep Neural Network* (DNN) seperti *Convolutional Neural Network* (CNN), dan *Long Short Term Memory* (LSTM). Peneliti menggunakan dataset CIC-DDOS2019 untuk menguji model yang disarankan dan mendapat hasil akurasi sebesar 99,99 % dan 99,30% dengan menggunakan model berbasis CNN.

Berdasarkan dari penelitian-penelitian yang terkait, maka penelitian ini akan menggunakan metode *Gated Recurrent Unit* (GRU) untuk mendeteksi serangan *Distributed Denial of Service* (DDoS) dengan menggunakan dataset CIC-DDOS2019. Hasil prediksi yang bagus tergantung dari tingat kesalahannya, yaitu semakin kecil error maka semakin tepat metode tersebut dalam prediksi.

1.2. Perumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana cara mendeteksi serangan DDoS dengan menggunakan metode GRU?
2. Fitur-fitur penting apa saja yang digunakan untuk mendeteksi serangan DDoS?
3. Bagaimana hasil kinerja deteksi GRU mempengaruhi nilai akurasi, sensitivitas, spesifikasi, presisi, F1-Score, BACC, dan MCC?

1.3. Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Serangan yang digunakan pada penelitian ini adalah serangan DDoS
2. Metode yang digunakan untuk penelitian ini adalah *Gated Recurrent Unit* (GRU)
3. Dataset yang digunakan pada penelitian ini adalah CIC-DDoS2019

1.4. Tujuan Penelitian

Penelitian ini memiliki tujuan sebagai berikut :

1. Membuat model untuk penerapan *Intrusion Detection System* dalam mendeteksi serangan DDoS menggunakan *Gated Recurrent Unit* (GRU).
2. Mengetahui seberapa akurat model *Gated Recurrent Unit* dalam mendeteksi serangan DDoS.
3. Menerapkan Pemilihan Fitur berbasis Korelasi (CFS) untuk memperoleh fitur-fitur penting dalam mendeteksi serangan DDoS.

1.5. Manfaat Penelitian

Adapun manfaat dalam penelitian ini adalah sebagai berikut:

1. Untuk mendapatkan hasil performa model *Gated Recurrent Unit* dalam mendeteksi serangan NTP-DDoS.

2. Untuk mengembangkan hasil perfoma model *Gated Recurrent Unit* menjadi performa terbaik dalam skripsi ini.

1.6. Metodologi Penelitian

Di bawah ini merupakan tahapan metodologi dalam penulisan skripsi ini, sebagai berikut:

1. Metode Studi Pustaka dan Studi Literatur

   Dalam metode ini, peneliti mencari informasi mengenai klasifikasi dan pendeteksian serangan DDoS dengan menggunakan metode GRU (*Gated Recurrent Unit*) melalui beberapa materi pembelajaran dari buku, jurnal, internet, dan artikel yang berhubungan dengan penulisan skripsi ini.

2. Metode Konsultasi

   Pada metode ini, peneliti melakukan konsultasi dengan pihak yang mempunyai pengetahuan dan pemahaman terhadap skripsi ini untuk mengatasi masalah-masalah yang sedang dihadapi.

3. Metode Pengumpulan Data

   Pada metode ini, peneliti mengumpulkan data yang berhubungan dengan serangan DDoS, *Intrusion Detection System* (IDS), serta klasifikasi dan deteksi serangan DDoS.

4. Metode Pengujian

   Dalam metode ini, akan dilakukan pembuatan rancangan sistem yang digunakan untuk mendapatkan hasil dari klasifikasi dan deteksi serngan dengan melatih model *Gated Recurrent Unit* (GRU).

5. Metode Analisis dan Penarikan Kesimpulan

   Setelah mendapatkan hasil dari metode pengujian pada skripsi ini, selanjutnya hasil dari proses klasifikasi dan deteksi serangan tersebut akan dianalisis dan dibuat kesimpulan pada penelitian ini.

1.7. Sistematika Penulisan

Berikut sistematika penulisan dalam penelitian ini adalah:

BAB I PENDAHULUAN

Pada Bab I penelitian ini, mencantumkan latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bab II penelitian ini, mencantumkan penjelasan dari teori-teori yang berkaitan dengan DDoS, GRU (*Gated Recurrent Unit*), dan teori-teori lainnya yang berkaitan dengan penelitian skripsi.

BAB III METODOLOGI

Pada Bab III penelitian ini, mencantumkan tahapan-tahapan penelitian yang dilakukan berupa proses perancangan model sistem klasifikasi dan deteksi serangan yang digunakan pada skripsi ini.

BAB IV HASIL DAN PEMBAHASAN

Pada Bab IV penelitian ini, mencantumkan proses tahapan-tahapan penelitian dengan analisis dari hasil klasifikasi dan deteksi serangan pada dataset dengan menggunakan metode GRU (*Gated Recurrent Unit*).

BAB V KESIMPULAN DAN SARAN

Pada Bab V penelitian ini, mencantumkan beberapa kesimpulan yang ditarik oleh peneliti dari hasil penjelasan dari bab-bab sebelumnya dan memberikan saran yang nantinya akan digunakan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] P. Lou, Y. Yang, and J. Yan, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” *ACM Int. Conf. Proceeding Ser.*, no. Cic, pp. 70–75, 2019, doi: 10.1145/3340997.3341005.

[2] R. K. Batchu and H. Seetha, “A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning,” *Comput. Networks*, vol. 200, no. September, p. 108498, 2021, doi: 10.1016/j.comnet.2021.108498.

[3] M. A. Ridho and M. Arman, “Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan,” *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[4] H. Aydın, Z. Orman, and M. A. Aydın, “A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment,” *Comput. Secur.*, vol. 118, 2022, doi: 10.1016/j.cose.2022.102725.

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

[6] E. E. Abdallah, W. Eleisah, and A. F. Otoom, “Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey,” *Procedia Comput. Sci.*, vol. 201, no. C, pp. 205–212, 2022, doi: 10.1016/j.procs.2022.03.029.

[7] X. K. Li, W. Chen, Q. Zhang, and L. Wu, “Building Auto-Encoder Intrusion Detection System based on random forest feature selection,” *Comput. Secur.*, vol. 95, p. 101851, 2020, doi: 10.1016/j.cose.2020.101851.

[8] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, “Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks,” *2018 4th IEEE Conf. Netw. Softwarization Work. NetSoft 2018*, no. NetSoft, pp. 462–469, 2018, doi: 10.1109/NETSOFT.2018.8460090.

[9] D. Akgun, S. Hizal, and U. Cavusoglu, “A new DDoS attacks intrusion detection model based on deep learning for cybersecurity,” *Comput. Secur.*, vol. 118, p. 102748, 2022, doi: 10.1016/j.cose.2022.102748.

[10] U. Sabeel, S. S. Heydari, K. Elgazzar, and K. El-Khatib, “Building an Intrusion Detection System to Detect Atypical Cyberattack Flows,” *IEEE Access*, vol. 9, pp. 94352–94370, 2021, doi: 10.1109/ACCESS.2021.3093830.

[11] T. Kim and W. Pak, “Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System,” *IEEE Access*, vol. 9, pp. 83806–83817, 2021, doi: 10.1109/ACCESS.2021.3087201.

[12] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset,” *IEEE Access*, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[13] C. Xu, J. Shen, X. Du, and F. Zhang, “An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units,” *IEEE Access*, vol. 6, pp. 48697–48707, 2018, doi: 10.1109/ACCESS.2018.2867564.

[14] M. V. O. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença, “A GRU deep learning system against attacks in software defined networks,” *J. Netw. Comput. Appl.*, vol. 177, no. December 2020, p. 102942, 2021, doi: 10.1016/j.jnca.2020.102942.

[15] B. Yan and G. Han, “LA-GRU: Building Combined Intrusion Detection Model Based on Imbalanced Learning and Gated Recurrent Unit Neural Network,” *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/6026878.

[16] J. Zhang, Y. Ling, X. Fu, X. Yang, G. Xiong, and R. Zhang, “Model of the intrusion detection system based on the integration of spatial-temporal features,” *Comput. Secur.*, vol. 89, p. 101681, 2020, doi: 10.1016/j.cose.2019.101681.

[17] R. V. Mendonca *et al.*, “Intrusion Detection System Based on Fast

Hierarchical Deep Convolutional Neural Network," *IEEE Access*, vol. 9, pp. 61024–61034, 2021, doi: 10.1109/ACCESS.2021.3074664.

[18] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," *Comput. Commun.*, vol. 199, no. October 2022, pp. 113–125, 2023, doi: 10.1016/j.comcom.2022.12.010.

[19] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with naïve Bayes feature embedding," *Comput. Secur.*, vol. 103, p. 102158, 2021, doi: 10.1016/j.cose.2020.102158.

[20] N. Gupta, V. Jindal, and P. Bedi, "LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system," *Comput. Networks*, vol. 192, no. December 2020, p. 108076, 2021, doi: 10.1016/j.comnet.2021.108076.

[21] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," *Comput. Secur.*, vol. 103, 2021, doi: 10.1016/j.cose.2021.102177.

[22] 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.

[23] M. A. Khan, M. R. Karim, and Y. Kim, "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network," *Symmetry (Basel).*, vol. 11, no. 4, 2019, doi: 10.3390/sym11040583.

[24] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS.2018.2869577.

[25] V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," *Comput.*

Networks, vol. 136, pp. 37–50, 2018, doi: 10.1016/j.comnet.2018.02.028.

[26] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença, "Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic," *Expert Syst. Appl.*, vol. 92, pp. 390–402, 2018, doi: 10.1016/j.eswa.2017.09.013.

[27] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection," *Comput. Secur.*, vol. 77, pp. 304–314, 2018, doi: 10.1016/j.cose.2018.04.010.

[28] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[29] O. Thorat, N. Parekh, and R. Mangrulkar, "TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100048, 2021, doi: 10.1016/j.jjimei.2021.100048.

[30] J. Chris, J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 10, pp. 9608–9613, 2019.

[31] 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.

[32] 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.

[33] M. Firdausy Al Fitri and L. Adelia Putri Siregar, “Literatur Review Deteksi Serangan DDos Mengggunakan Teknik Pendekatan Deep Learning,” *J. Inform. dan Sist. Inf.*, vol. 2, no. 3, pp. 2722–130, 2022, [Online]. Available: https://www.scopus.com/.

[34] 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, 2018, doi: 10.1016/j.jesit.2017.06.004.

[35] N. Gopika and A. E. A. Meena Kowshalaya, “Correlation Based Feature Selection Algorithm for Machine Learning,” *Proc. 3rd Int. Conf. Commun. Electron. Syst. ICCES 2018*, no. Icces, pp. 692–695, 2018, doi: 10.1109/CESYS.2018.8723980.

[36] Y. Tao, J. Li, and J. Xu, “Multi-label Feature Selection Method via Maximizing Correlation-based Criterion with Mutation Binary Bat Algorithm,” *Proc. Int. Jt. Conf. Neural Networks*, 2020, doi: 10.1109/IJCNN48605.2020.9207541.

[37] 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.

[38] T. Djatna and Y. Morimoto, “Pembandingan Stabilitas Algoritma Seleksi Fitur Menggunakan Transformasi Ranking Normal,” *J. Ilm. Ilmu Komput.*, vol. 6, no. 2, p. 245006, 2008.

[39] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” *Comput. Networks*, vol. 174, no. October 2019, 2020, doi: 10.1016/j.comnet.2020.107247.

[40] S. ur Rehman *et al.*, “DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU),” *Futur. Gener. Comput. Syst.*, vol. 118, pp. 453–466, 2021, doi: 10.1016/j.future.2021.01.022.

[41] S. M. Kasongo and Y. Sun, “A Deep Gated Recurrent Unit based model for wireless intrusion detection system,” *ICT Express*, vol. 7, no. 1, pp. 81–87, 2021, doi: 10.1016/j.icte.2020.03.002.

[42] A. S. Alshra’A, A. Farhat, and J. Seitz, “Deep Learning Algorithms for Detecting Denial of Service Attacks in Software-Defined Networks,” *Procedia Comput. Sci.*, vol. 191, no. 2019, pp. 254–263, 2021, doi: 10.1016/j.procs.2021.07.032.

[43] 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, 2019, doi: 10.3390/app9030437.

[44] R. Dey and F. M. Salemt, “Gate-variants of Gated Recurrent Unit (GRU) neural networks,” *Midwest Symp. Circuits Syst.*, vol. 2017-Augus, no. 2, pp. 1597–1600, 2017, doi: 10.1109/MWSCAS.2017.8053243.

[45] 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.

[46] T. Yang, Y. Hou, Y. Liu, F. Zhai, and R. Niu, “WPD-ResNeSt: Substation station level network anomaly traffic detection based on deep transfer learning,” *CSEE J. Power Energy Syst.*, 2021, doi: 10.17775/cseejpes.2020.02850.

[47] A. R. Gad, A. A. Nashat, and T. M. Barkat, “Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset,” *IEEE Access*, vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.

[48] D. Stiawan *et al.*, “An Approach for Optimizing Ensemble Intrusion Detection Systems,” *IEEE Access*, vol. 9, pp. 6930–6947, 2021, doi: 10.1109/ACCESS.2020.3046246.

[49] M. Artur, “Review the performance of the Bernoulli Naïve Bayes Classifier

in Intrusion Detection Systems using Recursive Feature Elimination with Cross-validated selection of the best number of features," *Procedia Comput. Sci.*, vol. 190, no. 2019, pp. 564–570, 2021, doi: 10.1016/j.procs.2021.06.066.

[50] S. Behera, A. Pradhan, and R. Dash, "Deep Neural Network Architecture for Anomaly Based Intrusion Detection System," *2018 5th Int. Conf. Signal Process. Integr. Networks, SPIN 2018*, pp. 270–274, 2018, doi: 10.1109/SPIN.2018.8474162.

[51] Y. W. Chen, J. P. Sheu, Y. C. Kuo, and N. Van Cuong, "Design and implementation of IoT DDoS attacks detection system based on machine learning," *2020 Eur. Conf. Networks Commun. EuCNC 2020*, pp. 122–127, 2020, doi: 10.1109/EuCNC48522.2020.9200909.