SISTEM KLASIFIKASI SERANGAN DDOS *HTTP FLOOD* DENGAN METODE *LONG SHORT TERM MEMORY* (LSTM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

AHMAD AFIDIN

09011281722067

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

SISTEM KLASIFIKASI SERANGAN DDOS *HTTP FLOOD* DENGAN METODE *LONG SHORT TERM MEMORY* (LSTM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

AHMAD AFIDIN

09011281722067

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

SISTEM KLASIFIKASI SERANGAN DDOS HTTP FLOOD DENGAN METODE LONG SHORT TERM MEMORY (LSTM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

AHMAD AFIDIN

09011281722067

Indralaya, Juni 2021

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Deris Stiawan, M.T., Ph.D.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 17 Juni 2021

Tim Penguji :

1. Ketua Sidang : Ahmad Fali Oklilas, M.T. (.....)
2. Sekretaris Sidang : Tri Wanda Septian, S.Kom., M.Sc. (.....)
3. Penguji Sidang : Sarmayanta Sembiring, S.SI., M.T. (.....)
4. Pembimbing I : Deris Stiawan, M.T., Ph.D. (.....)
5. Pembimbing II : Ahmad Heryanto, S.Kom., M.T. (.....)

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: **Ahmad Afidin**
Nim	: 09011281722067
Program Studi	: Sistem Komputer
Judul Penelitian	: Sistem Klasifikasi Serangan DDoS HTTP Flood Dengan Metode *Long Short Term Memory* (LSTM)

Hasil Pengecekan *Software iThenticate/Turnitin* : 14 %

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

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

Indralaya, Juni 2021

Ahmad Afidin

Nim. 09011281722067

HALAMAN PERSEMBAHAN

"Tetap Bersyukur Dengan Apapun Yang Didapatkan, Karena Itulah Takdir Yang Tuhan Tentukan Untuk Kita"

"Kita Tidak Akan Berpindah Tempat Jika Kita Tidak Bargerak, Gapai Semua Hal Yang Kita Inginkan Dengan Memulai Satu Langkah Kecil Dari Diri Kita Sendiri"

"Barangsiapa bertakwa kepada Allah niscaya Dia akan membukakan jalan keluar baginya, dan Dia memberinya rezeki dari arah yang tidak disangka-sangkanya. Dan barangsiapa bertawakal kepada Allah, niscaya Allah akan mencukupkan (keperluan)nya. Sesungguhnya Allah melaksanakan urusan-Nya. Sungguh, Allah telah mengadakan ketentuan bagi setiap sesuatu
(Qs. At-Thalaq: 2-3)"

"Tugas Akhir ini saya persembahkan untuk kedua orang tua saya yang tercinta, yang telah memberikan dukungan penuh untuk saya, yang mempertaruhkan segala hidupnya untuk saya dan yang senantiasa memberikan semangat serta do'a yang tidak pernah putus sehingga semua nya dapat berjalan dengan apa yang di harapkan"

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul **"Sistem Klasifikasi Serangan DDoS *HTTP Flood* dengan metode *Long Short Term Memory* (LSTM)"**.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusun Proposal Tugas Akhir ini :

- Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan baik dan lancar.
- Orang tua saya tercinta yang telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih untuk segala do'a, motivasi dan dukungannya baik moril, materil maupun spritual selama ini.
- Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Deris Stiawan, M.T, Ph.D., selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

- Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Ahmad Fali Oklilas, M.T._selaku Pembimbing Akademik Jurusan Sistem Komputer.
- Mbak Nurul Afifah, S.Kom., M.Kom. yang telah membantu membimbing dalam menyelesaikan tugas akhir
- Mbak Renny Virgasari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
- Meutia Zamieyus, Tia Hermita, Febi Rusmiati, Lisa Melinda, Agung Setiawan, Amartya Bimantara, M Taufiq Qurahman, Abdi Bimantara dan Teman-teman seperjuangan Tim Grub Riset Comnets yang lainnya yang telah banyak membantu.
- RoomMate Bima Pratama Anom dan Rahmat Syauqi Islami yang selalu memberi semangat, dukungan serta selalu menemani hari-hari penulis dalam menyelesaikan Tugas Akhir.
- Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga proposal tugas akhir ini bermanfaat dan berguna bagi khalayak.

Indralaya, Juni 2021

Penulis,

Klasifikasi Serangan DDoS HTTP Flood Dengan Metode Long Short Term Memory (LSTM)

Ahmad Afidin (09011281722067)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : aafidin145@gmail.com

Abstract

Distributed Denial of Service (DDoS) merupakan serangan yang dapat mengganggu lalu lintas sebuah jaringan dengan memanfaatkan mesin zombie yang dikendalikan oleh penyerang. Serangan *HTTP Flood* dilakukan dengan mengeksploitasi permintaan *HTTP GET* dan *HTTP POST* ke target yang diserang. Pada penelitian ini menggunakan dataset CSE-CIC-IDS 2018 yang berasal dari *University Of New Brunswick* (UNB). Digunakan algoritma seleksi fitur *Correlation-based Feature Selection* (CFS) untuk mendapatkan fitur penting pada proses klasifikasi. Selain itu, digunakan algoritma *Long Short Term Memory* (LSTM) untuk mengklasifikasikan serangan *DDoS HTTP Flood*. Hasil pada penelitian ini menunjukkan bahwa *Long Short Term Memory* (LSTM) dengan memanfaatkan algoritma fitur seleksi *Correlation-based Feature Selection* (CFS) dapat melakukan klasifikasi serangan DDoS HTTP Flood dengan cukup baik dengan hasil akurasi sebesar 99.97%, sensitivitas sebesar 99.96%, spesifitas sebesar 99.95%, presisi sebesar 99,91%, F1-Score sebesar 99.93%.

Keywords : *DDoS, HTTP Flood, Correlation-based Feature Selection* (CFS), *Long Short Term Memory* (LSTM)

Pembimbing I Tugas Akhir

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Pembimbing II Tugas Akhir

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

Ketua Jurusan Sistem Komputer

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

Klasifikasi Serangan DDoS HTTP Flood Dengan Metode Long Short Term Memory (LSTM)

Ahmad Afidin (09011281722067)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : aafidin145@gmail.com

Abstract

Distributed Denial of Service (DDoS) merupakan serangan yang dapat mengganggu lalu lintas sebuah jaringan dengan memanfaatkan mesin zombie yang dikendalikan oleh penyerang. Serangan *HTTP Flood* dilakukan dengan mengeksploitasi permintaan *HTTP GET* dan *HTTP POST* ke target yang diserang. Pada penelitian ini menggunakan dataset CSE-CIC-IDS 2018 yang berasal dari *University Of New Brunswick* (UNB). Digunakan algoritma seleksi fitur *Correlation-based Feature Selection* (CFS) untuk mendapatkan fitur penting pada proses klasifikasi. Selain itu, digunakan algoritma *Long Short Term Memory* (LSTM) untuk mengklasifikasikan serangan *DDoS HTTP Flood*. Hasil pada penelitian ini menunjukkan bahwa *Long Short Term Memory* (LSTM) dengan memanfaatkan algoritma fitur seleksi *Correlation-based Feature Selection* (CFS) dapat melakukan klasifikasi serangan DDoS HTTP Flood dengan cukup baik dengan hasil akurasi sebesar 99.97%, sensitivitas sebesar 99.96%, spesifitas sebesar 99.95%, presisi sebesar 99,91%, F1-Score sebesar 99.93%.

Keywords : *DDoS, HTTP Flood, Correlation-based Feature Selection* (CFS), *Long Short Term Memory* (LSTM)

Pembimbing I Tugas Akhir

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Pembimbing II Tugas Akhir

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

Ketua Jurusan Sistem Komputer

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

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Distributed Denial of Service (DDoS) merupakan bentuk lain dari serangan *Denial of Service* (DoS) yang mengganggu lalu lintas normal server, layanan atau jaringan yang ditargetkan dengan membanjiri lalu lintas internet pada target. Serangan DDoS memanfaatkan sejumlah mesin yang di eksploitasi untuk melakukan serangan DDoS [1]. Dalam serangan DDoS penyerang memanfaatkan mesin bot atau juga sering disebut mesin *zombie*, penyerang bisa memanfaatkan ribuan mesin bot yang biasanya terdiri dari komputer yang terinfeksi malware. Program yang berjalan pada latar belakang pada ribuan mesin bot tersebut akan mengirim permintaan koneksi ke server yang ingin diserang, sehingga membuat server tersebut tidak dapat di gunakan [2]. Serangan DDoS merupakan serangan yang cukup popular dikalangan *hacker*. Selain itu serangan DDoS memiliki banyak jenis. DDoS memiliki konsep yang sederhana, yaitu membuat lalu lintas sebuah server berjalan dengan beban yang berat sehingga server tidak dapat menampung lagi koneksi dari user lain[3].

Serangan *HTTP Flood* merupakan salah satu jenis serangan DDoS yang cukup berbahaya. Serangan *HTTP Flood* dilakukan dengan cara mengeksploitasi permintaan *HTTP GET* dan *HTTP POST* ke target yang berupa web server ataupun aplikasi. Serangan *HTTP Flood* sangat sulit dibedakan karena serangan ini menggunakan permintaan URL yang standar [4].

Pada penelitian [5] melakukan deteksi dan klasifikasi serangan *HTTP FLOOD*. Digunakan *Bat algorithm* untuk melakukan deteksi dan klasifikasi serangan dengan rata-rata performa yang didapatkan mencapai 94%. Pada penelitian tersebut digunakan dataset CAIDA 2017. Dari penelitian ini dijelaskan bahwa performa akurasi yang di dapatkan dapat ditingkatkan lagi pada penelitian selanjutnya dengan menggunakan pendekatan metode yang berbeda.

Pada penelitian [6] menyajikan sistem deteksi dan klasifikasi trafik serangan DDoS dengan menggunakan pendekatan *Deep Learning* dengan metode *Convolutional Neural Network* (CNN). Penelitian tersebut menggunakan dataset NSL-KDD dan dataset *realtime.* Berdasarkan hasil penelitian mengungkapkan bahwa kinerja akurasi yang di dapatkan cukup baik namun karena metode yang digunakan merupakan metode dengan masukan data citra maka komputasi pada proses klasifikasi sangat lamban.

Pada penelitian [7] digunakan metode deteksi serangan menggunakan *Long Short Term Memory-Recrurent Nueral Network* (LSTM-RNN). Pada penelitian ini digunakan dataset NSL-KDD dan didapatkan performa akurasi yang cukup baik namun masih bisa ditingkatkan kembali.

Pada penelitian [8] dilakukan deteksi serangan *hybrid* dengan menggunakan metode RNN dan menggunakan dataset NSL-KDD. Pada penelitian ini didapatkan performa akurasi yang cukup baik namun parameter yang digunakan untuk mempresentasikan hasil klasifikasi masih terbilang sedikit.

Berdasarkan beberapa penjelasan diatas mengenai penelitian terkait dengan hasil dan penjelasan masing-masing, maka penelitian ini mengusulkan untuk melakukan klasifikasi serangan *HTTP Flood* dengan menggunakan metode *Long Short Term Momory* (LSTM) dan akan digunakan dataset CSE-CIC-IDS 2018.

1.2. Rumusan Masalah

Berikut rumusan masalah pada tugas akhir ini, yaitu :

1. Bagaimana menerapkan seleksi fitur untuk mendapatkan fitur penting pada proses klasifikasi serangan DDoS *HTTP Flood* ?.
2. Bagaimana mengklasifikasikan serangan DDoS *HTTP Flood* ?.
3. Bagaimana pengaruh hasil performa pada klasifikasi dengan metode LSTM terhadap nilai akurasi, spesifitas, sensitivitas, presisi, F1-Score, BACC dan MCC ?.

1.3. Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Metode yang digunakan hanya berfokus pada klasifikasi serangan DDoS *HTTP Flood.*
2. Hasil performa dari *Long Short Term Memory* .
3. Tidak melakukan pencegahan terhadap serangan DDoS *HTTP Flood.*

1.4. Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Menerapkan seleksi fitur *Corelation-based Feature Selection* (CFS) untuk mendapatkan fitur penting pada proses klasifikasi serangan DDoS *HTTP Flood.*

2. Menerapkan metode *Long Short Term Momory* untuk mengklasifikasikan serangan DDoS *HTTP Flood.*

3. Mengukur hasil performa akurasi, spesifitas, sensitivitas, presisi, F1-Score, BACC dan MCC.

1.5. Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1. Mengoptimalkan waktu pada proses komputasi..
2. Dapat menerapkan metode *Long Short Term Memory* dalam mengklasifikasikan serangan DDoS *HTTP Flood.*

3. Mendapatkan performa terbaik pada proses klasifikasi dengan metode LSTM.

1.6. Metodologi Penelitian

Pada penelitian ini melewati beberapa tahapan metodologi yang meliputi :

1. Metode Studi Pustaka dan Literature

   Dalam tahap ini, penulis mencari informasi tentang sistem klasifikasi serangan dengan metode *Long Short Term Memory* melalui beberapa media pembelajaran jurnal ilmiah, buku, internet, serta artikel-artikel terkait yang mendukung dalam penulisan Tugas Akhir ini.

2. Metode Konsultasi

   Pada metode ini melakukan konsultasi kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penulisan tugas akhir.

3. Metode Pengumpulan data

   Dalam tahap ini dilakukan pengambilan data yang berkaitan dengan serangan DDoS *HTTP Flood* , sistem deteksi intrusi, dan klasifikasi serangan.

4. Metode Pengujian

   Pada tahap ini akan dilakukan perancangan sistem yang dapat dilakukan untuk melatih dan mendapatkan hasil klasifikasi serangan DDoS *HTTP Flood.*

5. Metode Analisa dan Kesimpulan

   Hasil dari pengujian pada tugas akhir ini akan menganalisa hasil dari proses klasifikasi dan membuat bebapa kesimpulan dari penelitian ini.

1.7. Sistematika Penulisan

Dibawah ini merupakan sistematika penulisan penelitian Tugas Akhir adalah sebagai berikut:

BAB I. PENDAHULUAN

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

BAB II. TINJAUAN PUSTAKA

Pada bab II ini terdiri penjelasan teori-teori dasar tentang *Long Short Term memory*, DDoS *HTTP Flood* serta teori lain yang berhubungan dengan penelitian Tugas Akhir.

BAB III. METODOLOGI

Pada bab III ini terdiri dari proses penelitian dilakukan dan perancangan sistem klasifikasi serta penerapan metode penelitian Tugas Akhir.

BAB IV. HASIL DAN ANALISIS

Pada bab IV ini terdiri dari proses penelitian, serta analisa hasil performa perbandingan dua dataset yang menggunakan metode *Long Short Term Memory* .

BAB V. KESIMPULAN DAN SARAN

Pada bab V ini akan ditarik beberapa kesimpulan dari hasil penjelasan di bab sebelumnya serta memberikan saran yang membangun untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] 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.

[2] K. Y. Nikolskaya, S. A. Ivanov, V. A. Golodov, A. V. Minbaleev, and G. D. Asyaev, "Review of modern DDoS-attacks, methods and means of counteraction," *Proc. 2017 Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2017*, vol. 2, pp. 87–89, 2017, doi: 10.1109/ITMQIS.2017.8085769.

[3] R. R. Zebari, S. R. M. Zeebaree, and K. Jacksi, "Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers," *ICOASE 2018 - Int. Conf. Adv. Sci. Eng.*, pp. 156–161, 2018, doi: 10.1109/ICOASE.2018.8548783.

[4] P. V. Razumov *et al.*, "Developing of Algorithm of HTTP FLOOD DDoS Protection," *ICCAIS 2020 - 3rd Int. Conf. Comput. Appl. Inf. Secur.*, 2020, doi: 10.1109/ICCAIS48893.2020.9096870.

[5] I. Sreeram and V. P. K. Vuppala, "HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm," *Appl. Comput. Informatics*, vol. 15, no. 1, pp. 59–66, 2019, doi: 10.1016/j.aci.2017.10.003.

[6] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," *Proc. - 2019 IEEE 9th Int. Conf. Intell. Comput. Inf. Syst. ICICIS 2019*, pp. 233–238, 2019, doi: 10.1109/ICICIS46948.2019.9014826.

[7] F. Meng, Y. Fu, F. Lou, and Z. Chen, "An effective network attack detection method based on kernel PCA and LSTM-RNN," *2017 Int. Conf. Comput. Syst. Electron. Control. ICCSEC 2017*, pp. 568–572, 2018, doi: 10.1109/ICCSEC.2017.8447022.

[8] 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.

[9] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, “Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection,” *IEEE Access*, vol. 6, no. May, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.

[10] M. M. U. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, “A few-shot deep learning approach for improved intrusion detection,” *2017 IEEE 8th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2017*, vol. 2018-Janua, pp. 1–7, 2018, doi: 10.1109/UEMCON.2017.8249084.

[11] W. Wang, X. Du, and N. A. Wang, “Building a Cloud IDS Using an Efficient Feature Selection Method and SVM,” *IEEE Access*, vol. 7, pp. 1345–1354, 2019, doi: 10.1109/ACCESS.2018.2883142.

[12] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, “Intrusion detection based on K-Means clustering and Naïve Bayes classification,” *2011 7th Int. Conf. Inf. Technol. Asia Emerg. Converg. Singul. Forms - Proc. CITA’11*, 2011, doi: 10.1109/CITA.2011.5999520.

[13] M. A. M. Hasan, M. Nasser, S. Ahmad, and K. I. Molla, “Feature Selection for Intrusion Detection Using Random Forest,” *J. Inf. Secur.*, vol. 07, no. 03, pp. 129–140, 2016, doi: 10.4236/jis.2016.73009.

[14] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, “Using Deep Learning Techniques for Network Intrusion Detection,” *2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020*, pp. 171–176, 2020, doi: 10.1109/ICIoT48696.2020.9089524.

[15] T.-H. Lee, L.-H. Chang, and C.-W. Syu, “Deep Learning Enabled Intrusion Detection and Prevention System over SDN Networks,” *2020 IEEE Int. Conf. Commun. Work. (ICC Work.*, vol. 7-11 June, pp. 1–6, 2020, doi:

10.1109/iccworkshops49005.2020.9145085.

[16] R. H. Hwang, M. C. Peng, C. W. Huang, P. C. Lin, and V. L. Nguyen, “An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection,” *IEEE Access*, vol. 8, pp. 30387–30399, 2020, doi: 10.1109/ACCESS.2020.2973023.

[17] S. Nayyar, S. Arora, and M. Singh, “Recurrent Neural Network Based Intrusion Detection System,” *IEEE Access*, pp. 136–140, 2020, doi: 10.1007/springerreference_12231.

[18] X. Zhang, J. Ran, and J. Mi, “An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic,” *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2019*, pp. 456–460, 2019, doi: 10.1109/ICCSNT47585.2019.8962490.

[19] R. Nakamura, Y. Sekiya, D. Miyamoto, K. Okada, and T. Ishihara, “Malicious Host Detection by Imaging SYN Packets and A Neural Network,” *2018 Int. Symp. Networks, Comput. Commun. ISNCC 2018*, 2018, doi: 10.1109/ISNCC.2018.8530964.

[20] 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.

[21] 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.

[22] N. Agrawal and S. Tapaswi, “Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3769–3795, 2019, doi: 10.1109/COMST.2019.2934468.

[23] A. N. Viet, L. P. Van, H. A. N. Minh, H. D. Xuan, N. P. Ngoc, and T. N. Huu, “Mitigating HTTP GET flooding attacks in SDN using NetFPGA-

based OpenFlow switch," *ECTI-CON 2017 - 2017 14th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, pp. 660–663, 2017, doi: 10.1109/ECTICon.2017.8096324.

[24] 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.

[25] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," *ICISSP 2017 - Proc. 3rd Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2017-Janua, no. Cic, pp. 253–262, 2017, doi: 10.5220/0006105602530262.

[26] 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. October 2019, p. 104928, 2020, doi: 10.1016/j.atmosres.2020.104928.

[27] 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.

[28] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Phys. Commun.*, vol. 42, p. 101157, 2020, doi: 10.1016/j.phycom.2020.101157.

[29] S. Ameur, A. Ben Khalifa, and M. S. Bouhlel, "A novel hybrid bidirectional unidirectional LSTM network for dynamic hand gesture recognition with Leap Motion," *Entertain. Comput.*, vol. 35, no. January, p. 100373, 2020, doi: 10.1016/j.entcom.2020.100373.

[30] 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, no. June, 2019, doi: 10.1016/j.brainres.2019.146341.

[31] 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, no. July 2017, pp. 22–32, 2018, doi: 10.1016/j.chemolab.2018.01.004.

[32] 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, 2017, doi: 10.1016/j.ins.2016.09.038.

[33] D. Ding, S. Han, H. Zhang, Y. He, and Y. Li, "Predictive biomarkers of colorectal cancer," *Comput. Biol. Chem.*, vol. 83, no. August, 2019, doi: 10.1016/j.compbiolchem.2019.107106.

[34] 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.

[35] V. Kanimozhi and D. T. P. Jacob, "Calibration of Various Optimized Machine Learning Classifiers in Network Intrusion Detection System on the Realistic Cyber Dataset Cse-Cic-Ids2018 Using Cloud Computing," *Int. J. Eng. Appl. Sci. Technol.*, vol. 04, no. 06, pp. 209–213, 2019, doi: 10.33564/ijeast.2019.v04i06.036.