ENHANCED STACKED PADA *LONG SHORT-TERM MEMORY* UNTUK MENINGKATKAN KEMAMPUAN KLASIFIKASI SERANGAN DDOS PADA *DATASET* CICDDOS 2019

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

CATURNING ANJARWATI

09011281823056

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2022

LEMBAR PENGESAHAN

***ENHANCED STACKED* PADA *LONG SHORT-TERM MEMORY* UNTUK MENINGKATKAN KEMAMPUAN KLASIFIKASI SERANGAN DDOS PADA *DATASET* CICDDOS 2019**

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh :

Caturning Anjarwati

09011281823056

Indralaya, 16 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**

AUTHENTICATION PAGE

***ENHANCED STACKED* ON *LONG SHORT-TERM MEMORY* TO IMPROVE THE CLASSIFICATION CAPABILITY OF DDOS ATTACK ON THE CICDDOS 2019 DATASET**

SKRIPSI

Submitted to Complete One of the
Conditions Obtaining Strata 1 Degree

By :
Caturning Anjarwati
09011281823056

Indralaya, 16 January 2023

Acknowledge,

Head of Computer System Departement	Final Project Advisor
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto. S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Senin

Tanggal : 26 Desember 2022

Tim Penguji :

1. **Ketua** : **Dr. Ir. H. Sukemi, M.T.**
2. **Sekretaris** : **Nurul Afifah, M.Kom.**
3. **Penguji** : **Huda Ubaya, S.T., M.T.**
4. **Pendamping I** : **Ahmad Heryanto, M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Caturning Anjarwati
NIM	: 09011281823056
Judul	: Enhanced Stacked Pada Long Short-Term Memory Untuk Meningkatkan Kemampuan Klasifikasi Serangan DdoS Pada Dataset CICDDoS 2019

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 tidak dipaksakan.

Indralaya, Januari 2023

Caturning Anjarwati

09011281823056

KATA PENGANTAR

Assalamualaikum Warahmatullah Wabarakatu

Puji syukur penulis panjatkan kepada Allah SWT, atas limpahannikmat, rahmat, serta hiday-nya sehingga penulisdapat menyelesaikan penyusunan tugas akhir ini yang berjudul "**Enhanced Stacked Pada *Long Short-Term Memory* Untuk Meningkatkan Kemampuan Klasifikasi Serangan *DDoS* Pada Dataset CICDDoS 2019"**

Dalam proposal ini penulis menjelaskan mengenai klasifikasi serangan DDoS dengan menggunakan metode LSTM beserta dengan data-data hasil penelitian yang saya lakukan. Harapan saya laporan ini bermanfaat bagi banyak pihak, serta menjadi salah satu sumber bacaan atau referensi bagi pembaca, akademisi dan peneliti lainnya.

Pada kesempatan ini penulis ingin mengucapkan rasa terima kasih kepada beberapa pihaak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini. Oleh Karena itu, penulis ingin mengucapkan rasa syukur kepeda Allah SWT dan terimakasih kepada yang terhormat:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam melaksanakan tugas akhir.
2. Orang tua dan keluarga besar tercinta yang telah memberikan do'a dan dukungan baik secara moril maupun materil.
3. Yang terhormat, bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Yang terhormat, Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Yang terhormat, Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

6. Yang terhotmat, Bapak Fali Oklilas, M.T. selaku Pembimbing Akademik Jurusan Sistem Komputer.
7. Mbk Reni selaku Admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
8. Kepada Kak Sandi Nopriansyah. S.Kom. selaku kakak tingkat yang memberikan referensi serta arahannya. Agung Al Hafidzin. S.kom., Jumhadi. S.Kom., Rani Octaviani. S.Kom., Hanna Pertiwi dan Tri Putri Rahmadani sebagai teman seperjuangan yang baik dan saling mendukung satu sama lain sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik.
9. Terkhusus kepada Muhammad Yasin yang selalu meluangkan waktu dan memberikan dukungan serta menyemangati penulis dalam menyelesaikan tugas akhir.
10. Semua pihak yang telah membantu.

Penulis menyadari bahwa penelitian ini masih jauh dari kata sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan sarapan yang bersifat membangun agar lebih baik dikemudian hari. Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua.

Wassalamualaikum Warahmatullahi Wabarakatuh

Indralaya, Januari 2023

Caturning Anjarwati

NIM: 09011281823056

vi

HALAMAN PERSEMBAHAN

Skripsi saya yang berjudul "*Enhanced Stacked* pada *Long Short Term Memory* untuk meningkatkan kemampuan klasifikasi serangan DDoS pada dataset CICDDoS 2019", saya persembahkan untuk:

- Orang tua saya tercinta
- Pasangan saya tercinta
- Dosen Pembimbing
- Dosen Penguji
- Seluruh Dosen dan Staf jurusan Sistem Komputer
- Teman-teman satu angkatan Sistem Komputer 2018
- Teman-teman Sistem Komputer kelas B angkatan 2018
- Adik-adik tingkat jurusan Sistem Komputer

Semoga bermanfaat dan menjadi referensi bagi para pembaca sekalian.

ENHANCED STACKED ON *LONG SHORT-TERM MEMORY* TO IMPROVE THE CLASSIFICATION CAPABILITY OF DDOS ATTACK ON THE CICDDOS 2019 DATASET

CATURNING ANJARWATI (09011281823056)

Computer Egineering Departement, Computer Science Faculty,

Sriwijaya Univercity

Email : anjarwati130400@gmail.com

ABSTRACT

Distributed Denial Of Service (DDoS) attacks are a type of cyber attack against websites. DDoS is marked by the amount of fake traffic that floods the server, system or internet network. As a result, the target website cannot be accessed because it is unable to manage too much traffic entering the server. There are three objectives in this research, including building a Long Shoer Term Memory Stacked model to classify DDoS attacks on network traffic records with the CICDDoS 2019 dataset. The second is to test the model in terms of time and resources needed when compared to existing models. The three produce the model with the best performance in the best performance in the classification of DDoS attacks. The Deep Learning method used is the BI-Directional LSTM method which is a branch of LSTM which has the advantage of having 2 layers, namely the forward layer and the backward layer so that it allows additional information enhancement and improves memory capabilities. This research was conducted by training the CIC-DDoS 2019 dataset on machine learning with the provision of tuning hyperparameters and comparing results with different ratios of training data and test data so that the best evaluation results were obtained with an accuracy value of 98.16%, precision 96.93 %, recall 99.39%, specificity 96.99% and f1 score 98.14%.

INDEX TERMS DDoS, LSTM, CIC-DDoS-2019 Dataset.

Acknowledge,

Head of Computer System Departement	**Final Project Advisor**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto. S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

ENHANCED STACKED PADA LONG SHORT TERM MEMORY UNTUK MENINGKATKAN KEMAMPUAN KLASIFIKASI SERANGAN DDOS PADA DATASET CICDDOS 2019

CATURNING ANJARWATI (09011281823056)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer,

Universitas Sriwijaya

Email : anjarwati130400@gmail.com

ABSTRAK

Serangan Distributed Denial Of Service (DDoS) merupakan salah satu jenis serangan cyber terhadap situs web. DDoS ditandai dengn banyaknya fake traffic yang membanjiri server, system atau jaringan internet. Akibatnya, website target tidak bsa diakses karena tidak mampu mengelola traffic yang terlalu banyak masuk ke dalam server. Terdapat tiga tujuam dalam penelitian ini antara lain membangun model Long Shoer Term Memory Stacked untuk melakukan klasifikasi serangan DDoS pada rekam traffic jaringan dengan dataset CICDDoS 2019. Kedua menguji model dalam segi waktu dan resource yang dibuthkan apabila dibandingkan dengan model-model yang telah ada sebelumnya. Ketiga menghasilkan model dengan kinerj terbaik dalam kinerja terbaik dalam klasifikasi serangan DDoS. Adapun metode Deep Learning yang dipakai adalah memakai metode BI-Directional LSTM yang merupakan cabang dari LSTM yang memiliki kelebihan memiliki 2 lapisan yaitu lapisan forward dan lapisan backward sehingga memungkinkan peningkatan informasi tambahan dan meningkatkan kemampuan memori. Penelitian ini dilakukan dengan mentraining dataset CIC-DDoS 2019 pada machine learning dengan ketentuan melakukan tuning hyperparameter serta melakukan perbandingan hasil dengan variasi rasio data training dan data uji yang berbeda sehingga didapatkan hasil evaluasi terbaik dengan nilai akurasi akurasi 98,16%, presisi 96,93%, recall 99,39%, spesifitas 96,99% dan score f1 98,14%.

Kata Kunci : DDoS, LSTM, Dataset CIC-DDOS-2019.

Mengetahui,

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

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.2. Latar Belakang

Semakin meningkatnya kebutuhan manusia dalam penggunaan komputer saat ini mengakibatkan semakin dibutuhkannya pelayanan yang mumpu untuk memenuhi kebutuhan tersebut [1]. Salah satu bentuk layanan yang menjadi kebutuhan penting dalam penggunaan komputer adalah layanan keamanan, seperti deteksi intruksi atau serangan [2]. Ada banyak jenis serangan yang biasa dilakukan oleh *hacker* agar dapat masuk kedalam sistem komputer, bentuk serangan *Distributed denial-of-service* (DDoS) merupakan jenis serangan yang sering digunakan oleh *hacker* [1].

DDoS merupakan teknik yang paling popular yang terlah terbukti memberikan ancaman di internet sejak tahun 1990 [3]. Bahkan pada tahun 2018, serangan DDoS ditetapkan sebagai bentuk serangan yang paling sering terjadi di dunia maya dan serangan yang paling popular [2]. Serangan ini memungkinkan pengguna mengalami kerugian yang besar dengan cara mengirimkan jumlah permintaan yang besar kepada target dengan tujuan menolak permintaan normal dan menurunkan kualitas layanan [4]. Oleh sebab itu, guna meningkatkan keamanan sistem suatu komputer dibutuhkan suatu solusi untuk mempelajari tipe serangan ini agar sistem dapat memberikan penanganan yang tepat dan efisien.

Hingga saat ini berbagai studi telah dilakukan guna mempelajari bentuk-bentuk serangan DDoS yang telah menyerang sistem. Berbagai penelitian deteksi serangan DDoS telah berhasil mengembangkan berbagai teknik dan metode. Pada penelitian [5] dihasilkan suatu solusi deteksi DDoS dengan menggunakan teknik entropy dengan membandingkan alamat IP sumber dengan alamat IP tujuan. Penelitian tersebut mampu mendeteksi serangan DDoS secara efisien. Penelitian [6] mengusulkan model *time series* dengan menggunakan algoritma ARIMA dan *chaotic system* yang mana mampu mengklasifikasikan serangan hingga mencapai 99,5%. Kedua penelitian tersebut masih menggunakan teknik konvensional sehingga memiliki kelemahan dalam proses komputasi dan masih terpengaruhnya hasil model berdasarkan fitur data yang dimasukkan.

Selain metode konvensional, sekarang ini penelitian terhadap serangan DDoS mulai menggunakan metode *machine learning*. Metode ini terbukti memberikan performa komputasi yang lebih baik dan efisien apabila dibandingkan dengan metode konvensional, akan tetapi performa model yang dihasilkan tetap berdasarkan fitur yang dimasukkan. Hal ini tampak di beberapa penelitian seperti pada penelitan [5], [7], [8]. Penelitian [5] melakukan deteksi DDoS dengan teknik SVM-RIPPER yang mampu menghasilkan *alert cluster* dalam deteksi serangan DDoS. Penelitian [8] mampu melakukan deteksi serangan DDoS yang bersifat serangan jenis baru dengan akurasi yang cukup baik. Penelitian [7] mengaplikasikan *Artificial Neural Network* (ANN) untuk mendeteksi DDoS dengan karakteristik fitur khusus dan mampu mendeteksi dengan tingkat akurasi hingga 98%.

Walaupun metode *machine learning* telah menunjukkan hasil yang signifikan, metode-metode ini masih memiliki kekurangan dalam fitur masukkan yang dimasukkan. Oleh sebab itu deperlukan suatu solusi yang dapat memudahkan dalam proses klasifikasi serangan tanpa harus menyeleksi fitur masukkan secara manual. Salah satu metode yang dapat digunakan adalah dengan menggunakan *Deep Learning. Deep Learning* merupakan metode yang sedang banyak digunakan sekarang ini. Salah satu metode yang banyak dimanfaatkan dalam deteksi maupun klasifikasi adalah pendekatan *time-based* seperti RNN, LSTM, dan GRU [9]–[13]. Beberapa penelitian seperti [9], [11], [13], [10] yang menggunakan LSTM memiliki hasil yang baik dengan tingkat rata-rata akurasi mencapai 99%. Pada beberapa penelitian menyarankan adanya bentuk *deep* dan *light-weight* DL sebagai upaya untuk meningkatan performa dari model yang telah diuji sebelumnya [10], [12], [13].

Long Short Term Memory (LSTM) merupakan variasi dari *Recurren Neural Network* (RNN). LSTM dapat mempelajari pola panjang dari data berurutan karena mencegah situasi vanishing gradient. LSTM pertama kali dikenalkan oleh Hochreiter dan Schmidhuber dan kemungkinan dikembangkan pada tahun 2000 oleh Schmidhuber . RNN menggunakan koneksi berulang dalam loop, yang memungkinkan informasi tetap ada. LSTM diciptakan dengan tujuan mengatasi masalah hidden layer[13].

Stacked adalah kumpulan elemen-elemen data yang disimpan dalam satu laju linear, yang hanya boleh diakses dari data teratas. *Stacked* merupakan struktur data yang meniru bagaimana proses menyimpan dan mengambil suatu data pada suatu tumpukkan data. Dapat dikatakan bahwa proses menyimpan data disebut push dan proses mengambil data disebut pop dari suatu tumpukkan yang selalu dilakukan pada bagian atas tumpukkan atau *stacked* sehingga terjadi urutan yang artinya, data yang terakhir disimpan adalah data yang pertama harus diambil karena data tersebut yang berada pada urutan teratas dari tumpukkan[14].

Stacked LSTM adalah salah satu bentuk bentuk *Deep Learning*. Pada *Stacked* LSTM lapisan LSTM akan terus ditambahkan *(deepening*) hingga memperoleh kinerja akurasi yang diinginkan [14], [15]. *Stacked* LSTM menggunakan hierarki jaringan LSTM untuk memetakan urutan data ke urutan ruang lainya. *Stacked* LSTM digunakan untuk mendeteksi serangan agar dapat ditangani dengan baik. *Enhanced Stacked* sendiri memiliki arti penumpukkan yang ditingkatkan. Dengan demikian, *Enhanced Stacked* sebagai metode referensi merupakan alternative yang memungkinkan, yang memiliki keuntungan berjalan lebih cepat[15].

Oleh sebab itu, pada penelitian ini akan dilakukan klasifikasi terhadap serangan DDoS dengan menggunakan salah satu metode Deep Learning yaitu LSTM (*Long Short Term Memory)*. Pada penelitian ini lapisan LSTM akan menjadi parameter pengujian sehingga lapisan LSTM akan terus ditambahkan hingga memperoleh kinerja maksimum yang mana metode ini disebut dengan *Stacked* LSTM. Pelatihan dan pengujian model akan dilakukan terhadap *dataset* CICDDoS 2019.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang dijelaskan, maka perumusan masalah yang akan dibahas adalah sebagai berikut :

1. Bagaimana membangun model LSTM *Stacked* untuk melakukan klasifikasi serangan DDoS pada rekaman trafik jaringan dengan *dataset* CICDDoS 2019 ?

2. Bagaimana kinerja model yang dihasilkan saat melakukan klasifikasi dari segi waktu dan *resource* yang dibutuhkan dibandingkan dengan penelitian yang telah ada?
3. Bagaimana performa model yang dihasilkan saat melakukan klasifikasi serangan DDoS?

1.3. Batasan Masalah

Berikut batasan masalah pada Tugas Akhir ini, yaitu :

1. Penelitian ini menggunakan data CICDDoS 2019 dari Universitas of New Brunswick (UNB).
2. Bentuk serangan DDoS yang digunakan pada penelitian ini adalah PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, SNMP, SSDP, dan WebDDoS.
3. Klasifikasi serangan DDoS akan dilakukan oleh model *Stacked* LSTM.
4. Parameter yang akan diuji pada penelitian ini adalah jumlah lapisan LSTM yang akan memberikan kinerja maksimum.
5. *Hyperparameter* yang akan di-*tuning* pada model dengan jumlah lapisan LSTM terbaik adalah *learning rate, epoch,* dan *batch size*.
6. Evaluasi kinerja model akan dibandingan berdasarkan penelitian *literatur review* pada model dengan pengujian terhadap *dataset* yang sama.

1.4. Tujuan

Tujuan yang akan dicapai dari penelitian ini adalah sebagai berikut :

1. Membangun model *Long Short Term Memory Stacked* untuk melakukan klasifikasi serangan DDoS pada rekaman trafik jaringan dengan *dataset* CICDDoS 2019.
2. Menguji model dalam segi waktu dan *resource* yang dibutuhkan apabila dibandingkan dengan model-model yang telah ada sebelumnya.
3. Menghasilkan model dengan kinerja terbaik dalam klasifikasi serangan DDoS.

1.5. Sistematika Penulisan

Sistematika yang akan digunakan dalam penulisan tugas akhir adalah sebagai berikut :

BAB I PENDAHULUAN

Bab pertama akan memaparkan sistematis mengenai latar belakang, tujuan penelitian, rumusan masalah, serta bentuk sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab kedua akan menjelaskan teori-teori yang akan menjadi landasan ide dari penelitian ini. Dasar teori yang akan dibahas pada bab ini adalah literatur mengenai DDoS, *Long Short Term Memory Stacked* dan performa validasi.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan proses dan rangkaian kegiatan dalam penelitian. Penelitian akan dimulai dari persiapan data, pembagian data latih dan data uji, pengujian model *stacked* LSTM, dan validasi performa.

BAB IV HASIL DAN ANALISIS

Bab ini akan memaparkan hasil pengujian yang diperoleh dan mennganalisa hasil penelitian yang telah dilakukan.

BAB V KESIMPULAN

Bab ini akan menampung simpulan dari hasil keseluruhan penelitian dan analisa terhadap penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *AITI*, vol. 17, no. 2 SE-Articles, Feb. 2021, doi: https://doi.org/10.24246/aiti.v17i2.143-158.

[2] K. Kurniabudi, A. Harris, and A. Rahim, "Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest," *Techno.Com*, vol. 19, no. 1, pp. 56–66, 2020, doi: 10.33633/tc.v19i1.2860.

[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] A. W. Muhammad, "Analisis Statistik Log Jaringan Untuk Deteksi Serangan Ddos Berbasis Neural Network," *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 220–225, 2016, doi: 10.33096/ilkom.v8i3.76.220-225.

[5] X. Ma and Y. Chen, "DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 114–117, 2014, doi: 10.1109/LCOMM.2013.112613.132275.

[6] S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, "A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 700–703, 2016, doi: 10.1109/LCOMM.2016.2517622.

[7] A. Saied, R. E. Overill, and T. Radzik, "Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept BT - Highlights of Practical Applications of Heterogeneous Multi-Agent Systems. The PAAMS Collection," 2014, pp. 309–320.

[8] T. Zhao, D. C.-T. Lo, and K. Qian, "A Neural-Network Based DDoS Detection System Using Hadoop and HBase," in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace*

Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, 2015, pp. 1326–1331, doi: 10.1109/HPCC-CSS-ICESS.2015.38.

[9] 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.

[10] 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.

[11] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS attack detection using deep learning and IDS," *Int. Arab J. Inf. Technol.*, vol. 17, no. 4A Special Issue, pp. 655–661, 2020, doi: 10.34028/iajit/17/4A/10.

[12] X. Liang and T. Znati, "A Long Short-Term Memory Enabled Framework for DDoS Detection," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013450.

[13] S. Sumathi, R. Rajesh, and S. Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection," *J. Sensors*, vol. 2022, 2022, doi: 10.1155/2022/8530312.

[14] R. U. Khan, X. Zhang, R. Kumar, A. Sharif, N. A. Golilarz, and M. Alazab, "An Adaptive Multi-Layer Botnet Detection Technique Using Machine Learning Classifiers," *Appl. Sci. 2019, Vol. 9, Page 2375*, vol. 9, no. 11, p. 2375, Jun. 2019, doi: 10.3390/APP9112375.

[15] N. Kathirkamanathan, B. Thevarasa, G. Mahadevan, N. Skandhakumar, and N. Kuruwitaarachchi, "Prevention of DDoS Attacks Targeting Financial Services using Supervised Machine Learning and Stacked LSTM," in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, 2022, pp. 1–5, doi: 10.1109/I2CT54291.2022.9825228.

[16] 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.

[17] A. Chartuni and J. Márquez, “Multi-classifier of ddos attacks in computer networks built on neural networks,” *Appl. Sci.*, vol. 11, no. 22, 2021, doi: 10.3390/app112210609.

[18] Y. Li and Y. Lu, “LSTM-BA: DDoS Detection approach combining LSTM and bayes,” *Proc. - 2019 7th Int. Conf. Adv. Cloud Big Data, CBD 2019*, no. 61702267, pp. 180–185, 2019, doi: 10.1109/CBD.2019.00041.

[19] A. Zainudin, L. A. C. Ahakonye, R. Akter, D. S. Kim, and J. M. Lee, “An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks,” *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2022.3196942.

[20] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, “A Multi-Classifier for DDoS Attacks Using Stacking Ensemble Deep Neural Network,” *2022 Int. Wirel. Commun. Mob. Comput. IWCMC 2022*, pp. 1125–1130, 2022, doi: 10.1109/IWCMC55113.2022.9824189.

[21] S. Geges and W. Wibisono, “Client Puzzle,” vol. 67, no. penceghan, pp. 53–67, 2015, [Online]. Available: [1] Abliz, Mehmud, and Taieb Znati. ?A Guided Tour Puzzle For Denial Of Service Prevention?. 2009 Annual Computer Security Applications Confer- ence (2009): n. pag.

[22] P. Koopman, J. Sung, C. Dingman, D. Siewiorek, and T. Marz, “Comparing operating systems using robustness benchmarks,” in *Proceedings of SRDS’97: 16th IEEE Symposium on Reliable Distributed Systems*, 1997, pp. 72–79, doi: 10.1109/RELDIS.1997.632800.

[23] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, “Distributed denial of service attacks,” in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics. “cybernetics evolving to systems, humans, organizations, and their complex interactions”*

(cat. no.0, 2000, vol. 3, pp. 2275–2280 vol.3, doi: 10.1109/ICSMC.2000.886455.

[24] 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.

[25] S. J. Russell and P. Norvig, *Artificial Intelligence A Modern Approach*, 3rd Editia., vol. 56, no. 1. New Jersey: Pearson Education, Inc., 1988.

[26] Cholissodin, I. and Soebroto, A. A. and Hasanah, U. and Febiola, Y. Inggiroebroto, and A. Andy, *AI , MACHINE LEARNING & DEEP LEARNING (Teori & Implementasi)*, 1.01. Malang: Dosen Pengampu MK Stream Data Science FILKOM UB, 2020.

[27] P. Ongsulee, "Artificial intelligence, machine learning and deep learning," *Int. Conf. ICT Knowl. Eng.*, pp. 1–6, 2018, doi: 10.1109/ICTKE.2017.8259629.

[28] A. Roihan, P. A. Sunarya, and A. S. Rafika, "Pemanfaatan Machine Learning dalam Berbagai Bidang: Review paper," *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 5, no. 1, pp. 75–82, 2020, doi: 10.31294/ijcit.v5i1.7951.

[29] T. M. Mitchell, *Machine Learning*, vol. 1. McGraw-Hill Science/Engineering/Math, 1997.

[30] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.

[31] J. M. Czum, "Dive Into Deep Learning," *J. Am. Coll. Radiol.*, vol. 17, no. 5, pp. 637–638, 2020, doi: 10.1016/j.jacr.2020.02.005.

[32] J. Díaz-Ramírez, "Machine Learning and Deep Learning," *Ingeniare*, vol. 29, no. 2, pp. 182–183, 2021, doi: 10.4067/S0718-33052021000200180.

[33] P. A. Miceli, W. D. Blair, and M. M. Brown, *Isolating Random and Bias Covariances in Tracks*. 2018.

[34] H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” 2019, doi: 10.3390/app9204396.

[35] M. Verleysen, U. catholique de Louvain, and K. U. Leuven, *Proceedings*. Ciaco, 2015.

[36] S. Atef and A. B. Eltawil, “Assessment of stacked unidirectional and bidirectional long short-term memory networks for electricity load forecasting,” *Electr. Power Syst. Res.*, vol. 187, p. 106489, Oct. 2020, doi: 10.1016/J.EPSR.2020.106489.

[37] A. Sahar and D. Han, “An LSTM-based indoor positioning method using Wi-Fi signals,” *ACM Int. Conf. Proceeding Ser.*, no. January, 2018, doi: 10.1145/3271553.3271566.

[38] Z. Karevan, “Spatio-temporal Stacked LSTM for Temperature Prediction in Weather Forecasting.”

[39] K. M. Ting, “Confusion Matrix,” 2010.

[40] “(PDF) Confusion Matrix.” https://www.researchgate.net/publication/355096788_Confusion_Matrix (accessed Aug. 29, 2022).

[41] A. N. Jahromi, S. Hashemi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “An Enhanced Stacked LSTM Method with No Random Initialization for Malware Threat Hunting in Safety and Time-Critical Systems,” *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 4, no. 5, pp. 630–640, 2020, doi: 10.1109/TETCI.2019.2910243.

[42] J. Yao and M. Shepperd, “Assessing software defection prediction performance: Why using the Matthews correlation coefficient matters,” *ACM Int. Conf. Proceeding Ser.*, pp. 120–129, 2020, doi: 10.1145/3383219.3383232.