KLASIFIKASI SERANGAN *BOTNET* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY STACKED*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

HANNA PERTIWI
09011281823037

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2022

HALAMAN PENGESAHAN

KLASIFIKASI SERANGAN *BOTNET* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY STACKED*

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh :

HANNA PERTIWI
09011281823037

Palembang, Desember 2022

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

CLASSIFICATION OF BOTNET ATTACKS ON INTRUSION DETECTION SYSTEM USING THE LONG SHORT TERM MEMORY STACKED METHOD

FINAL TASK

Submitted to Complete One of the
Conditions Obtaining Strata 1 Degree

By

HANNA PERTIWI
09011281823037

Palembang, December 2022

Acknowledge,

Head of Computer System Department	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 : 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, 4/1/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Hanna Pertiwi

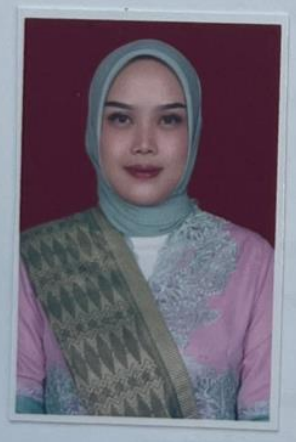
NIM : 09011281823037

Judul : Klasifikasi Serangan *Botnet* Pada *Intrusion Detection System* Menggunakan Metode *Long Short Term Memory Stacked*

Hasil Pengecekan Software iThenticate/Turnitin : 7%

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.



Palembang, Desember 2022

Hanna Pertiwi

NIM.09011281823037

KATA PENGANTAR

Puji syukur kepada Allah SWT atas rahmat-Nya sehingga penulis diberi kesempatan untuk menyelesaikan Tugas Akhir yang berjudul **"Klasifikasi Serangan *Botnet* Pada *Intrusion Detection System* Menggunakan Metode *Long Short Term Memory Stacked".*** Pada kesempatan ini, penulis menyampaikan rasa terima kasih kepada semua pihak yang telah membantu dan mendukung sehingga dapat memberikan dorongan kepada penulis dalam penyelesaian Tugas Akhir ini.

Oleh karena itu, penulis mengucapkan rasa terima kasih kepada:

- Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan tugas akhir ini dengan baik.

- Kedua Orang Tua yang terus memberikan do'a restu dan dukungan selama menempuh perkuliahan serta kedua adik saya yang selalu memberikan energi positif kepada saya.

- Yang terhormat, Bapak Jaidan Jauhari, S.Pd.,M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

- Yang terhormat, Bapak Dr.Ir.H. Sukemi.,M.T. selaku ketua jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

- Yang terhormat, Bapak Ahmad Heryanto, S.Kom.,M.T. selaku Dosen Pembimbing Tugas Akhir.

- Yang terhormat, Bapak Rossi Passarella, M.ENG selaku Pembimbing Akademik Jurusan Sistem Komputer.

- Mbak Reni selaku admin jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

- Kepada Tri Putri Rahmadani, Caturning Anjarwati, Berby Febriana Audrey, Rani Octaviani, Prazna Paramitha Avi, Dita Rizky, Feni Fadilah, Jumhadi, Yusdi, Taufik, Dimas.

- Terkhusus kepada Agus Tomy yang selalu mendukung dan memberi semangat saya dalam menyelesaikan tugas akhir.

- Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.

- Semua pihak yang telah membantu.

Penulis menyadari bahwa dalam penulisan Tugas Akhir ini masih banyak terdapat kekurangan, oleh karena itu seluruh saran dan kritik sangatlah berguna untuk menjadi bahan evaluasi bagi penulis.

Indralaya, Desember 2022

Penulis

Hanna Pertiwi

NIM.09011281823037

CLASSIFICATION OF BOTNET ATTACKS ON INTRUSION DETECTION SYSTEM USING THE LONG SHORT TERM MEMORY STACKED METHOD

HANNA PERTIWI
Computer Engineering Department, Computer Science Faculty, Sriwijaya University

Email : hannapertiwi961@gmail.com

ABSTRACT

Botnets are one of the most serious threats to the internet because they are able to provide a platform that can be distributed to illegal activities such as various attacks on the internet. One of the capabilities of a botnet that differentiates it from other malware is that it can be controlled remotely by a bootmaster under a command and control channel (C&C) channel infrastructure. There are two objectives in this research, among others, to build a model for the Stacked LSTM method to classify Botnet attack forms on IDS traffic based on the 2018 CIC-IDS dataset. Second, produce the model with the best performance. Therefore, to overcome the previous problem, the deep learning method was used. The Deep Learning method used is the Stacked LSTM method which is a branch of LSTM. In this study, the Principal Component Analysis (PCA) technique was used to reduce dimensions and training time efficiency, the Synthetic Minority Over-Sampling Technique (SMOTE) technique was also applied to balance the dataset to be processed, then Hyperparameter Tuning was applied to see the best parameters to be applied. on research models. Research validation was carried out 5 times in the study. The best validation results from the overall results were at 90% training data and 10% testing data where in this study the results obtained were 99.46% accuracy points, 99.86% recall, 99.06% specificity, 99.07% precision, and F1 score 99.46%.

***Keywords** : Botnet, Stacked LSTM, PCA, SMOTE, CIC-IDS-2018 Datasets*

Acknowledge,

Head of Computer System Department

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

Final Project Advisor

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

KLASIFIKASI SERANGAN *BOTNET* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY STACKED*

HANNA PERTIWI
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : hannapertiwi961@gmail.com

ABSTRACT

Botnet menjadi salah satu ancaman paling serius terhadap internet karena botnet mampu menyediakan *platform* yang dapat didistribusikan pada kegiatan ilegal seperti berbagai serangan di internet. Salah satu kemampuan botnet yang membedakannya dengan malware yang lain adalah botnet dapat dikendalikan dari jauh oleh seorang *bootmaster* dibawah infrastruktur *command and control channel* (C&C) *channel*. Terdapat dua tujuan dalam Penelitian ini antara lain untuk Membangun model metode Stacked LSTM untuk melakukan klasifikasi bentuk serangan Botnet pada trafik IDS dengan berdasarkan dataset CIC-IDS 2018. Kedua Menghasilkan model dengan performa terbaik. Oleh karena itu untuk mengatasi masalah sebelumnya digunakan metode deep learning. Adapun metode Deep Learning yang dipakai adalah memakai metode Stacked LSTM yang merupakan cabang dari LSTM. Dalam penelitian ini menggunakan teknik Principal Component Analysis (PCA) untuk mereduksi dimensi dan juga efisiensi waktu pelatihan, diterapkan juga teknik Synthetic Minority Over-Sampling Technique (SMOTE) untuk menyeimbangkan dataset yang akan diolah, lalu diterapkan Tuning Hyperparameter untuk melihat parameter terbaik yang akan diterapkan pada model penelitian. Validasi penelitian dilakukan sebanyak 5 kali dalam penelitian. Hasil Validasi terbaik dari keseluruhan hasil yaitu pada 90% data training dan 10% data testing dimana pada penelitian ini didapatkan hasil poin akurasi akurasi 99.46%, recall 99.86%, spesifitas 99.06%, presisi 99.07%, dan F1 score 99.46%.

***Kata Kunci** : Botnet, Stacked LSTM, PCA, SMOTE, CIC-IDS-2018 Datasets*

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

Halaman

HALAMAN PENGESAHAN ..... **i**
AUTHENTICATION PAGE ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
KATA PENGANTAR ..... **v**
ABSTRACT ..... **vii**
ABSTRAK ..... **viii**
DAFTAR ISI ..... **ix**
DAFTAR GAMBAR ..... **xii**
DAFTAR TABEL ..... **xiv**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Perumusan Masalah 3
1.3. Batasan Masalah 3
1.4. Tujuan 3
1.5. Sistematika Penulisan 3
BAB II TINJAUAN PUSTAKA **5**
2.1. Penelitian Terdahulu 5
2.2. Penelitian Terkait 15
2.3. Malware 18
2.4. Botnet 19
2.5. Intrusion Detection System (IDS) 20
2.6. Deep Learning (DL) 22
2.7. Long Short-Term Memory (LSTM) 22
2.8. Confusion Matrix 25

BAB III METODOLOGI PENELITIAN 28

3.1. Pendahuluan 28

3.2. Kerangka Kerja 28

3.3. Dataset 30

3.4. Persiapan Data 35

3.5. Pembagian Data Uji dan Latih 36

3.6. *Stacked Long Short Term Memory* 36

3.7. Skenario Penelitian 39

3.8. Validasi Performa Model 40

BAB IV HASIL DAN ANALISIS 41

4.1 Pendahuluan 41

4.2 Hasil Ekstraksi Dataset 41

4.3 Seleksi Fitur PCA 43

4.4 Hyperparameter LSTM *Stacked* 44

4.5 Tuning Hyperparameter LSTM *Stacked* 44

4.5.1 Hyperparameter Utama 47

4.6 Hasil Klasifikasi 47

4.7 Validasi Hasil Klasifikasi 48

4.8 Validasi Hasil Rasio Data 50:50 49

4.9 Validasi Hasil Rasio Data 60:10 51

4.10 Validasi Hasil Rasio Data 70:30 54

4.11 Validasi Hasil Rasio Data 80:20 57

4.12 Validasi Hasil Rasio Data 90:10 60

4.13 Analisis Validasi BACC dan MCC 61

4.14 Perbandingan Penelitian Terdahulu 65

BAB V KESIMPULAN 67

5.1 Kesimpulan 67

5.2 Saran……67

DAFTAR PUSTAKA 68

DAFTAR GAMBAR

Halaman

Gambar 2.1 Timeline Penelitian Terkait 18
Gambar 2.2 Siklus Hidup Botnet [44] 19
Gambar 2.3 Komponen Kerja Sebuah IDS [45] 17
Gambar 2.4 (a) Arsitektur Long Short-term Memory, (b) *Stacked* LSTM [50] 21
Gambar 3.1 Metodologi Penelitian 29
Gambar 3.2 Perbandingan Total Data 26
Gambar 3.3 Rancangan Arsitektur *Stacked* LSTM 37
Gambar 3.4 Struktur Hirerarki *Stacked* LSTM 38
Gambar 3.5 Arsitektur LSTM 39
Gambar 3.6 Flowchart Metode Stacked LSTM 42
Gambar 4.1 Data Berformat .pcap 42
Gambar 4.2 Hasil ekstraksi data 42
Gambar 4.3 Proses ekstraksi data 43
Gambar 4.4 Data PCA 44
Gambar 4.5 Analisis hasil klasifikasi 48
Gambar 4.6 Grafik loss rasio data 50:50 49
Gambar 4.7 Grafik Akurasi rasio data 50:50 49
Gambar 4.8 ROC Curve rasio data 50:50 51
Gambar 4.9 Grafik loss rasio data 60:10 52
Gambar 4.10 Grafik Akurasi rasio data 60:10 52
Gambar 4.11 ROC Curve rasio data 60:10 54
Gambar 4.12 Grafik loss rasio data 70:30 55
Gambar 4.13 Grafik Akurasi rasio data 70:30 55
Gambar 4.14 ROC Curve rasio data 70:30 57
Gambar 4.15 Grafik loss rasio data 80:20 58
Gambar 4.16 Grafik Akurasi rasio data 80:20 58
Gambar 4.17 ROC Curve rasio data 80:20 60
Gambar 4.18 Grafik loss rasio data 90:10 61
Gambar 4.19 Grafik Akurasi rasio data 90:10 61
Gambar 4.20 ROC Curve rasio data 90:10 63

Gambar 4.21 Analisis BACC dan MCC 64

DAFTAR TABEL

Halaman

Tabel 2.1 Penelitian Terdahulu 5
Tabel 2.2 Penelitian Terkait 16
Tabel 2.3 Perbandingan Formula LSTM dan *Stacked* LSTM [52] 24
Tabel 2.4 *Confussion Matrix* 25
Tabel 3.1 Daftar Bentuk Penyerangan dan Durasi Penyerangan 30
Tabel 3.2 Fitur Trafik Network *Dataset* CSE-CIC-2018 31
Tabel 3.3 Persebaran Banyak Skenario Serangan 35
Tabel 3.4 Jumlah Pembagian Data Latih dan Data Uji 36
Tabel 3.5 Spesifikasi Perangkat Keras 39
Tabel 3.6 Skenario Penelitian 39
Tabel 4.1 Unit node tuning hyperparameter 45
Tabel 4.2 Dropout tuning *hyperparamete*r 45
Tabel 4.3 Learning rate tuning *hyperparameter* 46
Tabel 4.4 Batch size tuning *hyperparameter* 46
Tabel 4.5 *Hyperparameter* utama 47
Tabel 4.6 Confusion matrix rasio data 50:50 50
Tabel 4.7 Hasil performa klasifikasi rasio data 50:50 50
Tabel 4.8 Confusion matrix rasio data 60:40 53
Tabel 4.9 Hasil performa klasifikasi rasio data 60:40 53
Tabel 4.10 Confusion matrix rasio data 70:30 56
Tabel 4.11 Hasil performa klasifikasi rasio data 70:30 56
Tabel 4.12 Confusion matrix rasio data 80:20 59
Tabel 4.13 Hasil performa klasifikasi rasio data 80:20 59
Tabel 4.14 Confusion matrix rasio data 90:10 62
Tabel 4.15 Hasil performa klasifikasi rasio data 90:10 62
Tabel 4.16 Hasil Validasi BACC dan MCC 63
Tabel 4.17 Hasil Perbandingan Penelitian Terdahulu 65

DAFTAR LAMPIRAN

Lampiran 1. Form Perbaikan
Lampiran 2. Cek Plagiat

BAB I

PENDAHULUAN

1.1. Latar Belakang

Dalam konteks serangan, botnet umumnya dimanfaakan sebagai alat untuk menganggu pekerjaan operasi normal atau untuk degradasi layanan keseuruhan dari sisem target [1]. Botnet terdiri dari tiga komponen yaitu *Botmaster*, *Command and Control* (C&C) Server, dan *bot*. C&C adalah server pusat yang digunakan untuk merekam atau mengendalikan suatu komputer yang telah terinfeksi. Oleh sebab itu, Botnet memungkinkan untuk dikendalikan oleh penyerang dari jarak jauh untuk melakukan berbagai serangan jaringan. [2]

Dalam beberapa tahun kebelakang banyak penelitian yang dilakukan untuk melakukan deteksi maupun klasifikasi terhadap serangan *botnet*. Pada [3], [4], deteksi serangan *botnet* dilakukan dengan menggunakan *supervised* machine learning. Beberapa *machine learning* yang digunakan adalah *Naïve Bayesian*, *Bayesian Network*, dan *Decission Tree*. Algortima *supervised learning* dapat diimplementasikan secara efisien terhadap klasifikasi serangan. Akan tetapi, terhadap beberapa pendekatan ini, pendekatan ini masih belum teralu baik dalam melakukan klasifikasi dikarenakan model yang dihasilkan hanya berfokus dalam melakukan deteksi seragan botnet hanya berdasarkan trafik TCP saja sehingga tidak mumpuni dalam melakukan klasifkasi terhadap fitur masukkan lainnya [4].

Pada beberapa penelitian dengan metode *machine learning* lainnya [5]–[7], berbagai pendekatan *machine learning* dilakukan berdasarkan analisis trafik dengan berbabagai metode. Pada [6], analisis trafik diakukan berdasarkan fitur *host-based* dan *flow-based* dengan menggunakan *Nearest Neighbors*, *Naive Bayesian*, *Support Vector Machine* (SVM), *Artificial Neural Networks* (ANN), dan *Gaussian-based classifier.* Berdasarkan hasil penelitian tersebut, SVM menghasilkan kinerja yang baik dengan tangkat akurasi 97% akan tetapi kelemahan dari metode ini adalah tidak dilakukannya uji terhadap waktu pendeteksian dan implementasi model untuk melakukan klasifikasi terhadap

botnet secara umum. Pada penelitian [8], tidak berbeda jauh dengan penelitian sebelumnya, klasifikasi dilakukan dengan skala besar terhadap *Netflow* yang diserang maupun tidak. Akan tetapi performanya masih belum baik (70% akurasi) dan model sangat terpengaruh berdasarkan pola fitur yang dimasukkan sehingga tidak bisa melakukan klasifikasi seluruh jenis serangan.

Selama ini telah banyak dilakukan penelitian untuk melakukan deteksi terhadap serangan Botnet akan tetapi belum banyak penelitian yang melakukan klasifikasi terhadap serangan Botnet. Pada penelitian [3]–[13], klasifikasi terhadap serangan Botnet masih banyak menggunakan metode *machine learning*. Penggunaan metode *machine learning* dalam klasifikasi serangan Botnet masih memiliki kelemahan. Kelemahan yang menjadi faktor terbesar dalam beberapa penelitian tersebut adalah pemilihan fitur yang akan dipelajari oleh model. Laju revolusi bentuk serangan Botnet yang begitu cepat mengakibatkan semakin banyak pula fitur yang dapat menjadi indikasi serangan Botnet. Salah satu metode yang dapat menjadi penyelesaian masalah ini adalah metode Deep Learning [9], [10], [13], [14].

Beberapa penelitian dengan menggunakan *deep learning* telah mulai dilakukan sejak tahun 2018 sehingga terdapat beberapa metode yang telah diteliti hingga saat ini. Salah satu pendekatan yang paling banyak digunakan dan dikembangkan dalam deteksi dan klasifikasi serangan Botnet adalah dengan menggunakan *Deep Neural Network* (DNN) [15]–[17]. Pada [15], [17], dijabarkan bahwa hasil dengan menggunakan DNN menghasilkan performa yang sangat baik dengan memanfaatkan *head packet* dan *timestamp* dari paket sebagai fitur masukkan yang mana diambil dari *raw data* secara otomatis oleh DNN. Peneliti tersebut menekankan bahwa performa sistem masih dapat ditingkatkan dengan memanfaatkan aspek lainnya.

Oleh sebab itu, klasifikasi serangan Botnet pada Trafik dalam *Intrusion Detection System* (IDS) pada penelitian ini akan memanfaatkan metode *deep learning* dalam implementasinya Dalam peneltian ini akan dilakukan peningkatan performa model klasifikasi pada [17] dengan memanfaatkan arsitektur DNN lainnya. Arsitektur yang akan digunakan adalah *Long Short-Term Memory*

Stacked yang mana peningkaan dari DNN yang menghilangkan kemungkinan *gradients descent* dan *gradient explosion* [18].

1.2. Perumusan Masalah

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

1. Bagaimana membangun model *Stacked Long Short Term Memory* untuk melakukan klasifikasi serangan Botnet pada rekaman trafik IDS pada *dataset* CSE-CIC-IDS 2018?
2. Bagaimana performa yang dihasilkan dapat melebihi hasil dengan menggunakan metode machine learning?

1.3. Batasan Masalah

Berikut batasan masalah pada Tugas Akhir ini, yaitu :

1. Penelitian ini menggunakan data CSE-CIC-IDS 2018 dari Universitas of New Brunswick (UNB).
2. Penelitian ini merupakan simulasi program dengan menggunakan Bahasa pemrograman *Python*.

1.4. Tujuan

Tujuan yang akan dicapai dari penelitian ini adalah sebagai berikut :

1. Membangun model *Long Short Term Memory Stacked* untuk melakukan klasifikasi bentuk serangan Botnet pada trafik IDS dengan berdasarkan *dataset* CSE-CIC-IDS 2018 dari Universitas of New Brunswick (UNB).
2. Menghasilkan model dengan performa terbaik.

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 dasar yang akan menjadi landasan dari penelitian ini. Dasar teori yang akan dibahas pada bab ini adalah literatur mengenai *malware, botnet, Intrusion Detection System, 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,

BAB IV HASIL DAN ANALISIS

Bab ini akan memaparkan hasil pengujian yang diperoleh dan menjelaskan Analisa terhadap hasil penelitian yang telah dilakukan.

BAB V KESIMPULAN

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

DAFTAR PUSTAKA

[1] N. I. Putri, R. Komalasari, and Z. Munawar, "PENTINGNYA KEAMANAN DATA DALAM INTELIJEN BISNIS," *J-SIKA|Jurnal Sist. Inf. Karya Anak Bangsa* , vol. 2, no. 02, pp. 41–48, 2020, Accessed: Sep. 19, 2022. [Online]. Available: https://ejournal.unibba.ac.id/index.php/j-sika/article/view/381.

[2] D. N. Fuadin, "Deteksi Botnet Menggunakan Naïve Bayes," *Thesis*, 2017.

[3] M. Stevanovic and J. Pedersen, "Machine learning for identifying botnet network traffic," *Forskningsbasen.Deff.Dk*, 2013, [Online]. Available: http://forskningsbasen.deff.dk/Share.external?sp=S12d2f5d1-eba2-45f7-bc2a-cc7487941bd7&sp=Saau.

[4] M. Stevanovic, J. M. Pedersen, M. Stevanovic, and J. M. Pedersen, "On the use of machine learning for identifying botnet network traffic," *J. Cyber Secur. Mobil.*, vol. 4, no. 2, pp. 1–32, Jan. 2016, doi: 10.13052/JCSM2245-1439.421.

[5] L. Bilge, D. Balzarotti, W. Robertson, E. Kirda, and C. Kruegel, "Disclosure: Detecting botnet command and control servers through large-scale NetFlow analysis," *ACM Int. Conf. Proceeding Ser.*, pp. 129–138, 2012, doi: 10.1145/2420950.2420969.

[6] S. Saad *et al.*, "Detecting P2P botnets through network behavior analysis and machine learning," *2011 9th Annu. Int. Conf. Privacy, Secur. Trust. PST 2011*, pp. 174–180, 2011, doi: 10.1109/PST.2011.5971980.

[7] "DGA Botnet Detection Using Supervised Learning Methods | Proceedings of the Eighth International Symposium on Information and Communication Technology." https://dl.acm.org/doi/abs/10.1145/3155133.3155166 (accessed Sep. 19, 2022).

[8] M. Stevanovic and J. M. Pedersen, "An efficient flow-based botnet detection using supervised machine learning," *2014 Int. Conf. Comput. Netw. Commun. ICNC 2014*, pp. 797–801, 2014, doi: 10.1109/ICCNC.2014.6785439.

[9] M. Yusof, M. M. Saudi, and F. Ridzuan, “Mobile botnet classification by using hybrid analysis,” *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 103–108, 2018, doi: 10.14419/IJET.V7I4.15.21429.

[10] G. Fedynyshyn, M. C. Chuah, and G. Tan, “Detection and classification of different botnet C&C channels,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6906 LNCS, pp. 228–242, 2011, doi: 10.1007/978-3-642-23496-5_17/COVER/.

[11] N. S. Raghava, D. Sahgal, and S. Chandna, “Classification of Botnet detection based on botnet architechture,” *Proc. - Int. Conf. Commun. Syst. Netw. Technol. CSNT 2012*, pp. 569–572, 2012, doi: 10.1109/CSNT.2012.128.

[12] M. Stevanovic and J. M. Pedersen, “An analysis of network traffic classification for botnet detection,” pp. 1–8, Dec. 2015, doi: 10.1109/CYBERSA.2015.7361120.

[13] Y. Xiao, J. Liu, K. Ghaboosi, H. Deng, and J. Zhang, “Botnet: Classification, attacks, detection, tracing, and preventive measures,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2009, 2009, doi: 10.1155/2009/692654.

[14] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, “Deep learning-based classification model for botnet attack detection,” *J. Ambient Intell. Humaniz. Comput. 2020 137*, vol. 13, no. 7, pp. 3457–3466, Mar. 2020, doi: 10.1007/S12652-020-01848-9.

[15] M. Shahhosseini, H. Mashayekhi, and M. Rezvani, “A Deep Learning Approach for Botnet Detection Using Raw Network Traffic Data,” *J. Netw. Syst. Manag.*, vol. 30, no. 3, pp. 1–23, 2022, doi: 10.1007/s10922-022-09655-7.

[16] Q. Li, F. Wang, J. Wang, and W. Li, “LSTM-Based SQL Injection Detection Method for Intelligent Transportation System,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4182–4191, May 2019, doi: 10.1109/TVT.2019.2893675.

[17] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, K. Anoh, and A. A.

Atayero, “SMOTE-DRNN: A Deep Learning Algorithm for Botnet Detection in the Internet-of-Things Networks,” *Sensors 2021, Vol. 21, Page 2985*, vol. 21, no. 9, p. 2985, Apr. 2021, doi: 10.3390/S21092985.

[18] 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.

[19] D. Liu, Y. Li, Y. Hu, and Z. Liang, “A P2P-botnet detection model and algorithms based on network streams analysis,” *2010 Int. Conf. Futur. Inf. Technol. Manag. Eng. FITME 2010*, vol. 1, pp. 55–58, 2010, doi: 10.1109/FITME.2010.5655788.

[20] W. H. Liao and C. C. Chang, “Peer to peer botnet detection using data mining scheme,” *Int. Conf. Internet Technol. Appl. ITAP 2010 - Proc.*, 2010, doi: 10.1109/ITAPP.2010.5566407.

[21] X. Yu, X. Dong, G. Yu, Y. Qin, and D. Yue, “Data-adaptive clustering analysis for online botnet detection,” *3rd Int. Jt. Conf. Comput. Sci. Optim. CSO 2010 Theor. Dev. Eng. Pract.*, vol. 1, pp. 456–460, 2010, doi: 10.1109/CSO.2010.214.

[22] C. Langin, H. Zhou, S. Rahimi, B. Gupta, M. Zargham, and M. R. Sayeh, “A self-organizing map and its modeling for discovering malignant network traffic,” *2009 IEEE Symp. Comput. Intell. Cyber Secur. CICS 2009 - Proc.*, 2009, doi: 10.1109/CICYBS.2009.4925099.

[23] H. Choi and H. Lee, “Identifying botnets by capturing group activities in DNS traffic,” *Comput. Networks*, vol. 56, no. 1, pp. 20–33, Jan. 2012, doi: 10.1016/J.COMNET.2011.07.018.

[24] F. Sanchez, Z. Duan, and Y. Dong, “Blocking spam by separating end-user machines from legitimate mail server machines,” *ACM Int. Conf. Proceeding Ser.*, pp. 116–124, 2011, doi: 10.1145/2030376.2030390.

[25] W. Lu, G. Rammidi, and A. A. Ghorbani, “Clustering botnet communication traffic based on n-gram feature selection,” *Comput.*

Commun., vol. 34, no. 3, pp. 502–514, Mar. 2011, doi: 10.1016/J.COMCOM.2010.04.007.

[26] S. C. Chen, Y. R. Chen, and W. G. Tzeng, "Effective Botnet Detection Through Neural Networks on Convolutional Features," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 372–378, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00062.

[27] M. Debashi and P. Vickers, "Sonification of Network Traffic for Detecting and Learning about Botnet Behavior," *IEEE Access*, vol. 6, pp. 33826–33839, 2018, doi: 10.1109/ACCESS.2018.2847349.

[28] A. Al-Nawasrah, A. Al-Momani, F. Meziane, and M. Alauthman, "Fast flux botnet detection framework using adaptive dynamic evolving spiking neural network algorithm," *2018 9th Int. Conf. Inf. Commun. Syst. ICICS 2018*, vol. 2018-Janua, pp. 7–11, 2018, doi: 10.1109/IACS.2018.8355433.

[29] H. Dhayal and J. Kumar, "Estrategias de detección de Botnet y Botnet P2P: una revisión," *2018 Int. Conf. Commun. Signal Process.*, pp. 1077–1082, 2018.

[30] E. B. Beigi, H. H. Jazi, N. Stakhanova, and A. A. Ghorbani, "Towards effective feature selection in machine learning-based botnet detection approaches," *2014 IEEE Conf. Commun. Netw. Secur. CNS 2014*, pp. 247–255, 2014, doi: 10.1109/CNS.2014.6997492.

[31] M. I. Hossain, S. Eshrak, M. J. Auvik, S. F. Nasim, R. Rab, and A. Rahman, "Efficient Feature Selection for Detecting Botnets Based on Network Traffic and Behavior Analysis," in *7th International Conference on Networking, Systems and Security*, 2020, pp. 56–62, doi: 10.1145/3428363.3428378.

[32] W. N. H. Ibrahim *et al.*, "Multilayer Framework for Botnet Detection Using Machine Learning Algorithms," *IEEE Access*, vol. 9, pp. 48753–48768, 2021, doi: 10.1109/ACCESS.2021.3060778.

[33] 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, Jun. 2021, doi: 10.1016/j.comnet.2021.108076.

[34] C. Yin, Y. Zhu, S. Liu, J. Fei, and H. Zhang, "An enhancing framework for botnet detection using generative adversarial networks," in *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, May 2018, pp. 228–234, doi: 10.1109/ICAIBD.2018.8396200.

[35] P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, "Using a Long Short-Term Memory Recurrent Neural Network (LSTM-RNN) to Classify Network Attacks," *Information*, vol. 11, no. 5, p. 243, May 2020, doi: 10.3390/info11050243.

[36] A. Pektaş and T. Acarman, "Botnet detection based on network flow summary and deep learning," *Int. J. Netw. Manag.*, vol. 28, no. 6, pp. 1–15, 2018, doi: 10.1002/nem.2039.

[37] J. van Roosmalen, H. Vranken, and M. van Eekelen, "Applying Deep Learning on Packet Flows for Botnet Detection," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018, pp. 1629–1636, doi: 10.1145/3167132.3167306.

[38] W. C. Shi and H. M. Sun, "DeepBot: a time-based botnet detection with deep learning," *Soft Comput. 2020 2421*, vol. 24, no. 21, pp. 16605–16616, May 2020, doi: 10.1007/S00500-020-04963-Z.

[39] R. Vinayakumar, K. P. Soman, P. Poornachandran, M. Alazab, and A. Jolfaei, "DBD: Deep learning DGA-based botnet detection," *Adv. Sci. Technol. Secur. Appl.*, pp. 127–149, 2019, doi: 10.1007/978-3-030-13057-2_6/COVER.

[40] B. Nugraha, A. Nambiar, and T. Bauschert, "Performance Evaluation of Botnet Detection using Deep Learning Techniques," *Proc. 11th Int. Conf. Netw. Futur. NoF 2020*, pp. 141–149, Oct. 2020, doi: 10.1109/NOF50125.2020.9249198.

[41] W. Yustanti, R. Bisma, A. Qoiriah, and A. Prihanto, *Keamanan Sistem Informasi*. Zifatama Jawara.

[42] F. Sulianta, *101 Masalah Malware \& Penanganannya*. Penerbit Andi.

[43] T. W. W. & A. Sanjaya, “Studi sistem keamanan komputer,” *J. Artif.*, vol. 2, no. 2, pp. 70–77, 2008.

[44] A. Nugraha and F. A. Rafrastara, “Taxonomy Botnet Dan Studi Kasus: Conficker,” *Semin. Nas. Teknol. Inf. Komun. Terap. 2011*, vol. 1, no. Semantik, 2011.

[45] J. Gondohanindijo, “Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System),” *Semarang*, vol. 2, pp. 46–54, 2011.

[46] I. Cholissodin, A. A. Soebroto, U. Hasanah, and Y. I. Febiola, “AI, Machine Learning & Deep Learning.” Fakultas Ilmu Komputer, Universitas Brawijaya, Malang, 2020.

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

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

[49] 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.

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

[51] 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.

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

[53] C. Yin, Y. Zhu, S. Liu, J. Fei, and H. Zhang, “An enhancing framework for botnet detection using generative adversarial networks,” in *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 2018, pp. 228–234, doi: 10.1109/ICAIBD.2018.8396200.