Pengoptimalan *Long Short-Term Memory (LSTM)* dengan *Autoencoder* untuk mendeteksi *Botnet*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Strata 1

OLEH :
Marcho Hardrian
09011381722132

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2023

Pengoptimalan *Long Short-Term Memory (LSTM)* dengan *Autoencoder* untuk mendeteksi *Botnet*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Strata 1

OLEH :
Marcho Hardrian
09011381722132

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

PENGOPTIMALAN *LONG SHORT-TERM MEMORY (LSTM)* DENGAN *AUTOENCODER* UNTUK MENDETEKSI BOTNET

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Jenjang S-1

Oleh :

MARCHO HARDRIAN
09011381722132

Palembang, 12 Januari 2023

Mengetahui,

Ketua Jurusan Sistem Komputer

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

Pembimbing Tugas Akhir

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari Rabu

Tanggal 7 Desember 2022

Tim Penguji:

1. **Ketua Sidang** : **Sarmayanta Sembiring, M.T.** _____
2. **Sekretaris Sidang** : **Aditya Putra Perdana P, M.T.** _____
3. **Penguji Sidang** : **Kemahyanto Exaudi, M.T.** _____
4. **Pembimbing** : **Ahmad Heryanto, M.T.** _____

Mengetahui, 13/1/22
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda yangan dibawah ini:

Nama : Marcho Hardrian
NIM : 09011381722132
Judul : Pengoptimalan Long Short-Term Memory (LSTM) dengan Autoencoder untuk mendeteksi Botnet

Hasil pengecekan *Software iThentivate/Turnitin* : 19%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atauplagiat 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.

Palembang, Januari 2023

Marcho Hardrian
NIM.09011381722132

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan yang maha esa, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan proposal tugas akhir ini dengan judul "**Pengoptimalan *Long Short-Term Memory* (LSTM) dengan *Autoencoder* untuk mendeteksi Botnet**".

Dalam laporan ini penulis menjelaskan mengenai proses system deteksi dengan menggunakan metode *Long Short-Term Memory* (LSTM). Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak,dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti di keamanan jaringan komputer.

Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan yang maha esa dan terimakasih kepada yang terhormat :

1. Keluargaku tercinta, yang selalu ada dan tidak pernah lelah dalam mendidik serta memberikan dukungan baik secara moril maupun materil kepada penulis sehingga dapat menyelesaikan proposal tugas akhir ini.

2. Bapak Dr.Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

3. Bapak Dr.Ir.Sukemi, M.T. selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya

4. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing Tugas Akhir penulis sekaligus Dosen Pembimbing Akademik di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

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

6. Teman teman yang telah sangat membantu saya dalam proses pengerjaam dan penulisan Tugas Akhir ini.

7. Seluruh teman-teman seperjuangan terkhusus angkatan 2017 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang tidak dapat saya sebutkan satu persatu.

8. Almamater

Penulis menyadari bahwa Laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, 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.

Palembang, Januari 2023

Penulis

PENGOPTIMALAN *LONG SHORT-TERM MEMORY* (LSTM) DENGAN *AUTOENCODER* UNTUK MENDETEKSI *BOTNET*

Marcho Hardrian (09011381722132)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, UniversitasSriwijaya

Email: marchohardrian@gmail.com

ABSTRAK

Botnet merupakan sekumpulan program yang telah terinfeksi oleh malware dan terhubung kedalam jaringan internet yang telah dikendalikan oleh pihak tertentu. Dengan menggunakan Long Short-Term Memory (LSTM) dapat membantu mendeteksi data serangan botnet. LSTM, dapat mengembalikan akurasi atau Confusion Matrix yang lebih baik. Sebelum memasuki proses deteksi, data terlebih dahulu melewati proses Autoencoder. Proses Autoencoder digunakan agar data yang digunakan semakin kecil dan mengakibatkan proses komputansi lebih efisien. Berdasarkan hasil penelitian yang telah dilakukan, algoritma Long Short Term-Memory (LSTM) berhasil diterapkan dalam sistem pendeteksi serangan botnet, dengan hasil terbaik didapatkan nilai akurasi sebesar 99.86 %, spesifisitas sebesar 99.88 %, nilai sensitivitas sebesar 99.86 %, nilai presisi sebesar 99.95%, serta nilai f1-score sebesar 99.90%.

Kata Kunci : *Botnet, Malware, Long Short-Term Memory* (LSTM), *Autoencoder, Confusion Matrix*

Palembang, 17 Januari 2023

Pembimbing Tugas Akhir

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

PENGOPTIMALAN *LONG SHORT-TERM MEMORY* (LSTM) DENGAN *AUTOENCODER* UNTUK MENDETEKSI *BOTNET*

Marcho Hardrian (09011381722132)

Departement of Computer Engineering, Faculty of Computer Science,

Sriwijaya University

Email: marchohardrian@gmail.com

ABSTRACT

Botnet is a group of programs that have been infected by malware and connected to the internet network that has been controlled by certain parties. Using Long Short-Term Memory (LSTM) can help detect botnet attack data. LSTM, can return better accuracy or better Confusion Matrix. Before entering the detection process, the data first goes through the autoencoder process. The Autoencoder process is used so that the data used is smaller and results in a more efficient computing process. Based on the results of the research that has been done, the Long Short Term-Memory (LSTM) was successfully applied in the Botnet attack detection system, with the best results obtained an accuracy value of 99.86%, a specificity of 99.88%, a sensitivity value of 99.86%, a precision value of 99.95%, and the f1-score is 99.90%.

Keywords : *Botnet, Malware, Long Short-Term Memory* (LSTM), *Autoencoder, Confusion Matrix*

Palembang, 7 Januari 2023

Pembimbing Tugas Akhir

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Botnet merupakan sekumpulan program yang telah terinfeksi oleh malware dan terhubung kedalam jaringan internet yang telah dikendalikan oleh pihak tertentu. *Botnet* sendiri merupakan singkatan dari *robot* dan *network*.[1] Pihak tertentu yang mengendalikan *botnet* disebut sebagai *botmaster*. *Botnet* dibuat untuk menginfeksi komputer tanpa sepengetahuan atau persetujuan pemiliknya misalnya, mengirimkan virus sebagai lampiran email. Setelah komputer terinfeksi dengan perangkat lunak *bot*, komputer akan menghubungi *botmaster*. *Botmaster* kemudian dapat mengirim perintah ke *bot* untuk melakukan tugas (berbahaya) yang akan merugikan pengguna komputer lain. *Botmaster* sendiri dapat mengendalikan banyak *botnet* yang berjumlah ribuan atau bahkan jutaan *bot*, seperti *botnet BredoLab* yang diperkirakan memiliki 30 juta *bot*[2].

Terdapat banyak sekali jenis *botnet* yang telah ditemukan akhir-akhir tahun ini. Jenis-jenis *botnet* tersebut umumnya terdiri dari *mirai, zeus, ares* serta *bashlite* [3]. Hal ini menandakan bahwa penyebaran *botnet* semakin banyak dimana-mana. Sistem keamanan yang memadai akan sangat dibutuhkan untuk meminimalisir penyebaran *botnet*. Pada penelitian yang dilakukan sebelumnya[4] membahas megenai proses mendeteksi dua jenis *bashlite* dan *mirai*. *Long Short Term Memory* (LSTM) digunakan pada penelitian tersebut guna membantu mendeteksi data serangan *botnet*. Penelitian tersebut mendapatkan nilai akurasi tertinggi sebesar 90%.

Pada penelitian lain[5] *Neural Network* (Bi-LSTM RNN), bersama dengan *Word Embedding* untuk mendeteksi botnet, dibandingkan dengan LSTM-RNN untuk memastikan apakah pengumpulan informasi dari masa lalu dan masa depan yang digunakan oleh Bi-LSTM RNN, dapat mengembalikan akurasi atau matriks konfusi yang lebih baik. Kedua model mengembalikan akurasi tinggi dan matriks

konfusi rendah untuk empat vektor serangan yang digunakan oleh malware *botnet* mirai. Hasil yang didapatkan untuk mirai, udp, dan dns cukup bagus dengan akurasi validasi 99%, 98%, 98% dan 0,000809, 0,125630, 0,116453 matriks konfusi validasi masing-masing.

Penelitian lain juga membahas mengenai deteksi botnet. Penelitian tersebut menggunakan proses reduksi dimensi data (*autoencoder*)[3]. *Autoencoder* berguna untuk meminimalisir penggunaan memori dalam proses deteksi, sehingga menghasilkan system deteksi yang lebih efisien.Penelitian tersebut berhasil mendapatkan hasil yang cukup bagus, dimana nilai *false positif* yang cukup rendah.

Dari beberapa penjelasan sebelumnya, penelitian ini akan menggunakan LSTM untuk mendeteksi data *botnet.* Dimana sebelum memasuki proses deteksi, data terlebih dahulu melewati proses *autoencoder*. Proses *autoencoder* digunakan agar data yang digunakan semakin kecil dan mengakibatkan proses komputansi lebih efisien.

1.2. Perumusan dan Batasan Masalah

1.2.1. Perumusan Masalah

Rumusan Masalah yang diambil dari tugas akhir ini adalah :

1. Bagaimana menerapkan sistem deteksi botnet menggunakan algoritma *Long Short Term-Memory* (LSTM)?

2. Bagaimana meningkatkan hasil performa deteksi menggunakan algoritma autoencoder dalam sistem pendeteksian serangan Botnet ?

1.2.2. Batasan Masalah

Berikut batasan masalah pada Tugas Akhir ini, yaitu :

1. Dataset yang digunakan pada penelitian ini berasal *CIC IDS 2018.*
2. Proses deteksi yang dilakukan menggunakan algoritma *Long Short Term-Memory* (LSTM)
3. Proses Reduksi dimensi dataset menggunakan algoritma *autoencoder*
4. Analisa data botnet menggunakan proses *Static Analysis*
5. Dalam penelitian ini tidak membahas bagaimana cara mencegah serangan botnet

1.3. Tujuan dan Manfaat

1.3.1. Tujuan

Tujuan dari penulisan Tugas Akhir ini, yaitu :

1. Menerapkan algoritma *Long Short Term-Memory* (LSTM) dalam sistem pendeteksi serangan botnet
2. Berhasil meningkatkan hasil performa melalui proses reduksi dimensi data menggunakan algoritma autoencoder.

1.3.2. Manfaat

Hasil yang didapatkan dari penelitian ini dapat menjadi landasan dalam pengembangan lebih lanjut mengenai system deteksi *botnet* menggunakan LSTM. Selain itu manfaat dari penelitian ini secara praktis sebagai berikut :

1. Dapat mendeteksi *botnet* dengan menggunakan metode LSTM.

2. *Autoencoder* sangat berpengaruh dalam peningkatan kinerjasistem deteksi *botnet* berbasis LSTM.

3. Hasil yang didapatkan dari penelitian ini dapat menjadi referensi untuk meningkatkan nilai akuras dalam sistem deteksi botnet menggunakan algoritma LSTM.

1.4. Metodologi Penelitian

Pada Tugas Akhir ini, metodologi yang digunakan adalah sebagai berikut :

1.4.1. Tahap Pertama (Persiapan data)

Tahap ini ialah tahap yang dilakukan setelah masalah yang dibahas telah sesuai dan relevan diangkat sebagai penelitian. Pada tahap ini diharuskan untuk membaca literature yang sesuai dengan topik penelitian dan mencari dataset yang akan digunakan.

1.4.2. Tahap Kedua (Pengolahan data)

Pada tahap ini membahas mengenai proses bagaimana mengolah suatu data mentah menjadi data siap olah, memvisualisasikan data, serta melakukan proses reduksi dimensi data dengan menggunakan *autoencoder*.

1.4.3. Tahap Ketiga (Deteksi)

Pada tahap ini dilakukanlah proses pendeteksian data botnet dan data normal dengan menggunakan LSTM. Setelah proses deteksi selesai, dilanjutkan pada proses validasi dengan menggunakan beberapa parameter pengujian.

1.4.4. Tahap Keempat (Analisis)

Setelah mendapatkan data dari tahap pengklasifikasian, maka langkah selanjutnya adalah melakukan analisis terhapada hasil yang telah didapatkan sebelumnya sehingga didapatkan hasil yang objektif.

1.5. Sistematika Penulisan

Dalam mempermudah penyusunan Tugas Akhir ini dan juga membuat isi dari setiap bab yang ada pada Tugas Akhir ini lebih jelas, maka dibuat sistematika penulisan sebagai berikut :

BAB I – PENDAHULUAN

Pada bab ini menjelasakan mengenai latar belakang,perumusan masalah, batasan masalah, tujuan dan manfaat dari topik yang diangkat berupa sistem klasifikasi *botnet* menggunakan algoritma LSTM.

BAB II – TINJAUAN PUSTAKA

Pada bab ini berisikan beberapa *literature riview* yang berhubungan dengan masalah deteksi *botnet* dengan menggunakan LSTM yang mengacu pada beberapa penelitian sebelumnya.

BAB III – METODOLOGI

Pada bab ini menjelasakan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan-tahapan yang dilakukan untuk mempersiapkan data *botnet* dan normal, Penerapan LSTM serta model yang digunakan sehingga tujuan dari penulis tercapai.

BAB IV – HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan hasil yang telah diperoleh padatahap sebelumnya, data yang diuji akan dianalisa menggunakan berbagai macam teknik serta validasi hasil.

BAB V – KESIMPULAN DAN SARAN

Pada bab ini menjelaskan kesimpulan dan hasil yang diperoleh, serta merupakan jawaban yang diperoleh daritujuan yang ingin dicapai.

DAFTAR PUSTAKA

[1] S. Shaposhnikov, Sankt-Peterburgskiĭ gosudarstvennyĭ ėlektrotekhnicheskiĭ universitet "LĖTI," Nat͡sional′nyĭ issledovatel′skiĭ universitet "MIĖT" (Russia), Institute of Electrical and Electronics Engineers, Institute of Electrical and Electronics Engineers, and Institute of Electrical and Electronics Engineers., *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) : January 29 - February 01, 2018, St. Petersburg and Moscow, Russia*.

[2] V. Kanimozhi and Dr. 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," *International Journal of Engineering Applied Sciences and Technology*, vol. 04, no. 06, pp. 209–213, 2019, doi: 10.33564/ijeast.2019.v04i06.036.

[3] Y. Meidan *et al.*, "N-BaIoT-Network-based detection of IoT botnet attacks using deep *autoencoder*s," *IEEE Pervasive Comput*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.

[4] H. Alkahtani and T. H. H. Aldhyani, "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/3806459.

[5] C. D. McDermott, F. Majdani, and A. v. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *Proceedings of the International Joint Conference on Neural Networks*, vol. 2018-July, pp. 1–8, 2018, doi: 10.1109/IJCNN.2018.8489489.

[6] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, vol. 2018-January, pp. 108–116. doi: 10.5220/0006639801080116.

[7] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–15, Aug. 2020, doi: 10.3390/s20164372.

[8] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks," *IEEE Internet Things J*, vol. 8, no. 6, pp. 4944–4956, Mar. 2021, doi: 10.1109/JIOT.2020.3034156.

[9] S. I. Popoola, “Federated Deep Learning for Botnet Attack Detection in IoT Networks.”

[10] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, “MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network,” *ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy*, no. February, pp. 207–218, 2020, doi: 10.5220/0009187802070218.

[11] H. T. Nguyen, Q. D. Ngo, and V. H. Le, “A novel graph-based approach for IoT botnet detection,” *Int J Inf Secur*, vol. 19, no. 5, pp. 567–577, Oct. 2020, doi: 10.1007/s10207-019-00475-6.

[12] IEEE Computational Intelligence Society, International Neural Network Society, and Institute of Electrical and Electronics Engineers, *2018 International Joint Conference on Neural Networks (IJCNN) : 2018 proceedings.*

[13] M. M. Rasheed, A. K. Faieq, and A. A. Hashim, “Android Botnet Detection Using Machine Learning,” *Ingénierie des systèmes d information*, vol. 25, no. 1, pp. 127–130, 2020, doi: 10.18280/isi.250117.

[14] H. Bah\csi, S. Nõmm, and F. B. la Torre, “Dimensionality reduction for machine learning based iot botnet detection,” in *2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, 2018, pp. 1857–1862.

[15] A. A. Ahmed, “Botnet Detection Using a Feed-Forward Backpropagation Artificial Neural Network,” in *International Conference on Computational Intelligence in Information System*, 2018, pp. 24–35.

[16] I. Apostol, M. Preda, C. Nila, and I. Bica, “Iot botnet anomaly detection using unsupervised deep learning,” *Electronics (Switzerland)*, vol. 10, no. 16, Aug. 2021, doi: 10.3390/electronics10161876.

[17] M. M. Salim, S. K. Singh, and J. H. Park, “Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks,” *Appl Soft Comput*, vol. 113, Dec. 2021, doi: 10.1016/j.asoc.2021.107859.

[18] W. C. Shi and H. M. Sun, “DeepBot: a time-based botnet detection with deep learning,” *Soft comput*, vol. 24, no. 21, pp. 16605–16616, Nov. 2020, doi: 10.1007/s00500-020-04963-z.

[19] O. Kompougias *et al.*, “IoT Botnet Detection on Flow Data using *Autoencoder*s.”

[20] S. I. Popoola, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Gui, “Stacked recurrent neural network for botnet detection in smart homes,” *Computers and Electrical Engineering*, vol. 92, Jun. 2021, doi: 10.1016/j.compeleceng.2021.107039.

[21] R. Biswas and S. Roy, “Botnet traffic identification using neural networks,” *Multimed Tools Appl*, vol. 80, no. 16, pp. 24147–24171, Jul. 2021, doi: 10.1007/s11042-021-10765-8.

[22] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "BoTShark: A deep learning approach for botnet traffic detection," in *Advances in Information Security*, vol. 70, Springer New York LLC, 2018, pp. 137–153. doi: 10.1007/978-3-319-73951-9_7.

[23] P. Wurzinger, L. Bilge, T. Holz, J. Goebel, C. Kruegel, and E. Kirda, "Automatically generating models for botnet detection," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5789 LNCS, pp. 232–249, 2009, doi: 10.1007/978-3-642-04444-1_15.

[24] N. S. Raghava, D. Sahgal, and S. Chandna, "Classification of Botnet detection based on botnet architechture," *Proceedings - International Conference on Communication Systems and Network Technologies, CSNT 2012*, pp. 569–572, 2012, doi: 10.1109/CSNT.2012.128.

[25] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, vol. 2018-January, no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[26] V. Kanimozhi and T. Prem Jacob, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019*, pp. 33–36, 2019, doi: 10.1109/ICCSP.2019.8698029.

[27] H. Wang, R. Czerminski, and A. C. Jamieson, "Neural Networks and Deep Learning," *The Machine Age of Customer Insight*, pp. 91–101, 2021, doi: 10.1108/978-1-83909-694-520211010.

[28] T. Katte-Bangayya and M. Vinicius, "Recurrent Neural Network and its Various Architecture Types Cite this paper Related papers A Survey on Parallel Processing in a CPU-GPU Collaborat ive Environment Using Ant Colony Opt … Research and Scient ific Innovat ion Societ y RSIS Int ernat ional A Crit ical Review of Recurrent Neural Net works for Sequence Learning Recurrent Neural Network and its Various Architecture Types Trupti Katte," 2018. [Online]. Available: www.rsisinternational.org

[29] P. TS and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448–454, 2021, doi: 10.1016/j.gltp.2021.08.017.

[30] N. I. Widiastuti, "Deep Learning--Now and Next in Text Mining and Natural Language Processing," in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 407, no. 1, p. 12114.

[31] N. K. Manaswi, “RNN and LSTM,” in *Deep Learning with Applications Using Python*, Apress, 2018, pp. 115–126. doi: 10.1007/978-1-4842-3516-4_9.

[32] S. Siami-Namini, N. Tavakoli, and A. S. Namin, “The performance of LSTM and BiLSTM in forecasting time series,” in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 3285–3292.

[33] H. M. Lynn, S. B. Pan, and P. Kim, “A deep bidirectional GRU network model for biometric electrocardiogram classification based on recurrent neural networks,” *IEEE Access*, vol. 7, pp. 145395–145405, 2019.

[34] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, “Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks,” *IEEE Internet Things J*, vol. 8, no. 6, pp. 4944–4956, 2021, doi: 10.1109/JIOT.2020.3034156.

[35] F. O. Catak and A. F. Mustacoglu, “Distributed denial of service attack detection using *autoencoder* and deep neural networks,” *Journal of Intelligent and Fuzzy Systems*, vol. 37, no. 3, pp. 3969–3979, 2019, doi: 10.3233/JIFS-190159.

[36] A. Naway and Y. Li, “Android Malware Detection Using *Autoencoder*,” pp. 1–9, 2019, [Online]. Available: http://arxiv.org/abs/1901.07315

[37] H. Abdel-Jaber, D. Devassy, A. al Salam, L. Hidaytallah, and M. El-Amir, “A Review of Deep Learning Algorithms and Their Applications in Healthcare,” *Algorithms*, vol. 15, no. 2. MDPI, Feb. 01, 2022. doi: 10.3390/a15020071.

[38] F. O. Catak and A. F. Mustacoglu, “Distributed denial of service attack detection using *autoencoder* and deep neural networks,” *Journal of Intelligent and Fuzzy Systems*, vol. 37, no. 3, pp. 3969–3979, 2019, doi: 10.3233/JIFS-190159.

[39] D. Stiawan, A. Heriyanto, Kurniabudi, B. Purnama, Darmawijaya, Samsuryadi, R. Budiarto “Network anomaly detection research: a survey” *Indonesian Journal of Electrical Engineering and Informatics*, vol. 7, no. 1, pp. 37-50, 2019.