PEMBAHARUAN SISTEM DETEKSI SERANGAN PORTSCAN BERBASIS LSTM DENGAN PENGIMPLENTASIAN ALGORITMA *UNIDIRECTIONAL LSTM* (UNI-LSTM)

SKRIPSI

Oleh :

WILDA SEPTRIYANTI

09011381924101

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

PEMBAHARUAN SISTEM DETEKSI SERANGAN PORTSCAN BERBASIS LSTM DENGAN PENGIMPLEMENTASIAN ALGORITMA *UNIDIRECTONAL LSTM* (UNI-LSTM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memproleh Gelar Sarjana Komputer

Oleh
WILDA SEPTRIYANTI
09011381924101

Indralaya, 16 Oktober 2023
Mengetahui,

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

AUTHENTICATION PAGE

UPDATED LSTM-BASED PORTSCAN ATTACK DETECTION SYSTEM WITH IMPLEMENTATION OF UNIDIRECTIONAL LSTM ALGORITHM (UNI-LSTM)

FINAL TASK

Submitted To Fulfill One Of The Requirements To

Obtain A Bachelor's Degree In Computer Sciene

By

Wilda Septriyanti
09011381924101

Indralaya, 16 Oktober 2023

Acknowledge

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

Telah diuji dan lulus pada

Hari : Senin

Tanggal : 02 Oktober 2023

Tim Penguji :

1. Ketua : Dr. Ahmad Zarkasi, M.T.

2. Sekretaris : Nurul Afifah, M.Kom.

3. Penguji : Ahmad Fali Oklilas, M.T

4. Pembimbing : Ahmad Heryanto, S.Kom., M.T

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 19661203200604100

HALAMAN PERNYATAAN

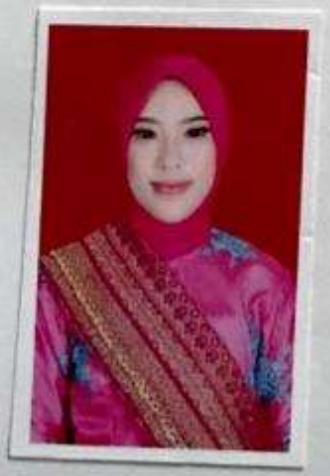
Yang bertanda tangan di bawah ini:

Nama	: Wilda Septriyanti
Nim	: 09011381924101
Judul	: Pembaharuan Sistem Deteksi Serangan Portscan berbasis LSTM dengan Pengimplementasian Algoritma Unidirectional LSTM (Uni LSTM)

Hasil Pengecekan Software Ithenticate/Turnitin : 16%

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

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



Indralaya, 13 Oktober 2023

Wilda Septriyanti

09011381924101

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan atas kehadirat Allah SWT yang telah memberikan Rahmat, Hidayah, dan Karunia-Nya kepada penulis sehingga dapat menyelesaikan penyusunan Tugas Akhir dengan judul **"Pembaharuan Sistem Deteksi Serangan PortScan Berbasis LSTM dengan pengimplementasian Algoritma Unidirectional LSTM (Uni-LSTM)".**

Penulis menyadari dalam penyusunan Tugas Akhir ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak yang telah memberikan ide dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini, penulis ingin mengucapkan rasa syukur kepasa Allah SWT dan terima kasih kepada yang terhormat:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini dengan baik dan lancer.
2. Kedua orang tua yang sangat penulis cintai Ayahanda Rohim dan Ibunda Patimah yang telah memberikan kasih sayang dan selalu mendoakan yang terbaik untuk penulis, serta motivasi dan dukungannya baik moral, material maupun spiritual.
3. Kakak tercinta Willy Agustian, Yudi Saputra dan Ayuk tersayang Widya Astuti serta Ikhwan Taqy Athallah yang telah memberikan semangat dan doanya selalu untuk penulis untuk mencapai impian.
4. Bapak Prof. Dr. Erwin, S.Si., M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M. T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto, S. Kom, M.T., selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya untuk membimbing serta

memberikan saran dan motivasi yang terbaik untuk penulis dalam menyelesaikan Tugas Akhir.

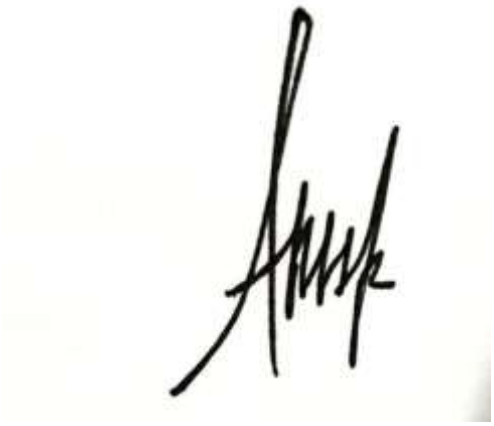
7. Bapak Prof. Dr. Ir Bambang Tutuko, M. T. selaku Pembimbing Akademik yang telah mengizinkan penulis melaksanakan kerja praktek dan yang telah membimbing serta memberikan penulis banyak ilmu
8. Untuk Keluarga besar yang telah memberikan banyak dukungan
9. Kepada temanku Rianti Agustina dan Risti Auliah Utami yang selalu ada dan siap membantu
10. Kepada Septianti yang telah siap selalu direpotkan
11. Terima kasih kepada Agi Reksana yang telah mensuport

Dalam penulisan Tugas Akhir ini penulis menyadari penuh bahwa masih banyak kekurangan dalam Tugas Akhir ini, baik dari segi materi maupun penyajian. Oleh karena itu penulis mengharapkan kritik dan saran dari semua pihak yang berkenan agar menjadi bahan evaluasi dan menjadi lebih baik lagi.

Wassalamualaikum Warahmatullahi Wabarakatuh

Indralaya, 13 Oktober 2023

Penulis,



Wilda Septriyanti

NIM. 09011381924101

PEMBAHARUAN SISTEM DETEKSI SERANGAN PORTSCAN BERBASIS LSTM DENGAN PENGIMPLEMENTASIAN ALGORITMA UNIDIRECTIONAL LSTM (UNI LSTM)

WILDA SEPTRIYANTI (09011381924101)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : wseptriyanti@gmail.com

ABSTRAK

Serangan Port Scanning adalah salah satu serangan yang cukup berbahaya, teknik ini dapat memetakan karakteristik, mendeteksi port yang terbuka bahkan mendapatkan informasi penting pada suatu jaringan atau host untuk kemudian diteruskan ke serangan lebih lanjut. Upaya untuk melindungi sistem keamanan jaringan terhadap serangan PortScan, maka dibutuhkan sistem serangan seperti Intrusion Detection System (IDS). Metode yang digunakan dalam penelitian ini adalah Unidirectional LSTM adalah salah satu jenis arsitektur jaringan saraf rekuren (RNN) yang digunakan untuk memproses data berurutan, seperti teks, waktu berjalan, atau data deret waktu. Penelitian ini menggunakan dua jenis serangan yaitu serangan FTP dan SSH Bruteforce yang diambil dari dataset CIC-IDS 2018. Pada tiap-tiap uji coba diperoleh nilai dari performa akurasi dengan hasil validasi menggunakan data latih 40% dan data uji 60% didapatkan nilai akurasi sebesar 99.50%, hasil validasi menggunakan data latih 50% dan data uji 50% didapatkan nilai akurasi sebesar 99.57%,

Kata Kunci : *Serangan PortScan, Instrusion Detection Sistem, Dataset CIC-IDS 2018, Unidirectional Long Short Term Memory*

UPDATED LSTM-BASED PORTSCAN ATTACK DETECTION SYSTEM WITH IMPLEMENTATION OF UNIDIRECTIONAL LSTM ALGORITHM (UNI-LSTM)

WILDA SEPTRIYANTI (09011381924101)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : wseptriyanti@gmail.com

ABSTRACT

Port Scanning attacks are quite dangerous attacks, this technique can map characteristics, detect open ports and even obtain important information on a network or host to then forward to further attacks. In an effort to protect the network security system against PortScan attacks, an attack system such as an Intrusion Detection System (IDS) is needed. The method used in this research is Unidirectional LSTM, which is a type of recurrent neural network (RNN) architecture used to process sequential data, such as text, running time, or time series data. This research uses two types of attacks, namely FTP and SSH Bruteforce attacks taken from the 2018 CIC-IDS dataset. In each trial, accuracy performance values were obtained with validation results using 40% training data and 60% test data, obtaining an accuracy value of 99.50. %, validation results using 50% training data and 50% test data obtained an accuracy value of 99.57%,

Keywords : *PortScan Attack, Intrusion Detection System, CIC-IDS 2018 Dataset, Unidirectional Long Short Term Memory*

DAFTAR ISI

xi

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Port Scanning atau pemindaian port merupakan kegiatan yang dilakukan oleh penyerang siber untuk mengumpulkan informasi tentang sistem target. Metode ini digunakan untuk mengidentifikasi port yang terbuka pada sistem atau jaringan yang dituju. Dalam konteks keamanan komputer, Port Scanning dapat digunakan oleh penyerang untuk menemukan kerentanan atau celah keamanan yang dapat mereka manfaatkan untuk melakukan serangan yang lebih serius.[1].

Dalam upaya melawan serangan Port Scanning, telah dikembangkan berbagai metode pendeteksian yang dapat membantu mengidentifikasi aktivitas tersebut. Salah satu metode yang digunakan adalah Unidirectional LSTM (Long Short-Term Memory), yang merupakan teknik pemodelan dan prediksi data yang telah terbukti berhasil dalam berbagai bidang, termasuk pengenalan pola dan pemrosesan bahasa alami.

Pada penelitian ini, peneliti akan melakukan pengambilan dataset dengan membuat skenario sendiri. Setelah itu, dataset akan melalui proses ekstraksi fitur. Tujuan dari ekstraksi fitur adalah untuk mengubah file .pcap menjadi file .csv. Penggunaan file .csv mempermudah peneliti dalam mengidentifikasi pola dari serangan stealh scan.

Dalam penelitian sebelumnya[2] peneliti menggunakan metode machine learning. Hasil dari percobaan penelitian tersebut menunjukkan akurasi sebesar 97,80% dan 69,79%.

Dalam penelitian sebelumnya yang dilakukan oleh[3], dilakukan uji klasifikasi menggunakan perangkat lunak WEKA dan menerapkan metode Naïve Bayes. Hasil dari uji tersebut menunjukkan akurasi sebesar 86,2% dengan nilai rata-rata Precision sebesar 0,885, Recall sebesar 0,862, dan F-measure sebesar 0,849. Hasil ini menunjukkan bahwa penerapan metode Naïve Bayes berhasil dalam mengklasifikasikan potensi serangan berdasarkan teknik Port Scanning.

Pada penelitian[4] yang melakukan pengujian sistem IDS menggunakan metode Naïve Bayes sebanyak 10 kali. Hasil dari penelitian tersebut menunjukkan

bahwa akurasi Naïve Bayes dalam deteksi dan pengklasifikasian berdasarkan jenis serangan adalah sebagai berikut: untuk jenis serangan FIN scan sebesar 99,04%, jenis serangan NULL scan sebesar 98,94%, jenis serangan XMAS scan sebesar 99,13%, dan jenis serangan all out attack sebesar 99,10%.

Metode Unidirectional LSTM menggunakan jaringan saraf rekuren (RNN) yang memiliki kemampuan untuk "mengingat" informasi sebelumnya dan mengambil keputusan berdasarkan urutan data yang diberikan. Dalam konteks Port Scanning, Unidirectional LSTM dapat digunakan untuk menganalisis pola-pola karakteristik dari aktivitas pemindaian port yang mencurigakan.

Dengan menerapkan Unidirectional LSTM pada data lalu lintas jaringan, dapat dilakukan analisis secara real-time untuk mendeteksi adanya Port Scanning. Model LSTM dapat dilatih menggunakan data riwayat Port Scanning yang diketahui, sehingga dapat mempelajari pola-pola khas dari aktivitas tersebut. Setelah dilatih, model tersebut dapat digunakan untuk memonitor lalu lintas jaringan secara kontinu dan mendeteksi adanya tanda-tanda Port Scanning yang mencurigakan.

Dengan menerapkan metode Unidirectional LSTM untuk pendeteksian Port Scanning, diharapkan dapat meningkatkan efektivitas dan efisiensi dalam mengidentifikasi serangan tersebut. Pendekatan ini dapat membantu organisasi dan penyedia layanan untuk melindungi jaringan mereka dari ancaman keamanan yang diakibatkan oleh aktivitas Port Scanning.

1.2 Rumusan Masalah

Berikut ini rumusan masalah yang akan akan dibahas untuk implementasi dalam tugas akhir ini, yakni :

1. Bagaimana penerapan dari seleksi fitur agar bisa menadapatkan fitur penting pada deteksi serangan PortScanning.
2. Bagaimana cara supaya bisa mendeteksi serangan PortScanning dengan menerapkan metode Unidirectional LSTM.
3. Bagaimana hasil kinerja dari deteksi *Unidirectional* LSTM terhadap nilai – nilai dari *akurasi, recall, spesifitas, presisi, F1-Score, BACC* dan *MCC.*

1.3 Batasan Masalah

Berikut ini merupakan batasan masalah dari Tugas Akhir ini :

1. Pendeteksian ini hanya difokuskan pada serangan Port Scanning.
2. Penelitian ini hanya menggunakan program bahasa python.
3. Saat ini peneliti menggunakan data dari *University of New Brunswick* (UNB) yaitu (CSE-CIC-IDS2018).

1.4 Tujuan Penelitian

Berikut ini merupakan tujuan penelitian dari Tugas Akhir ini :

1. Penerapan Corelation-based Feature Selection (CFS) pada seleksi fitur dalam pendeteksian serangan Port Scanning guna untuk mendapatkan fitur terbaik.
2. Penerapan metode Unidirectional LSTM yang digunakan untuk mendeteksi serangan Port Scanning.
3. Mengukur hasil dari kinerja mengenai nilai *akurasi recall, spesifitas, presisi , F1-Score, BACC, dan MMC.*

1.5 Manfaat Penelitian

Berikut adalah manfaat penelitian dari Tugas Akhir ini, yakni :

1. Optimalisasi dari segi waktu dalam proses komputasi.
2. Bisa menerapkan metode Unidirectional LSTM untuk melakukan pendeteksian serangan Port Scanning.
3. Memberikan performa yang baik saat proses deteksi dari metode Unidirectional LSTM.

1.6 Metode Penelitian

Dalam melakukan penelitian penulis akan melewati beberapa tahapan metodologi, yaitu meliput :

1. Metode Studi Literatur dan Studi Pustaka

   Pada tahapan in penulis melakukan pencarian untuk menemukan berbagai informasi tentang sebuah sistem pendeteksian serangan menggunakan metode Unidirectional LSTM melalui berbagai macam artikel, jurnal ilmiah, internet dan buku yang terkait mendukung

penulisan Tugas Akhir ini.

2. Metode Konsultasi

   Pada langkah ini akan diadakan konsultasi kepada pihak yang memiliki wawasan luas, pengetahuan dan pemahaman yang baik dalam mengatasi masalah pada saat penulisan Tugas Akhir.

3. Metode Pengumpulan Data

   Pada metode ini akan dilakuan pengumpulan data terkait dengan Port Scanning dan sistem deteksi instrusi (IDS).

4. Metode Pengujian

   Dalam fase ini dilakukan perancangan sistem yang akan digunakan untuk melatih supaya mendapatkan hasil dari pendeteksian serangan Port Scanning.

5. Metode Analisa dan Penarikan Kesimpulan

   Dalam tahap ini akan melakukan analisa dari sebuah proses pendeteksian serangan dan menarik beberapa kesimpulan dari penelitian ini.

1.7 Sistem Penulisan

Berikut merupakan sistematika penulisan dari penelitian Tugas Akhir yang meliputi :

BAB I PENDAHULUAN

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

BAB II. TINJAUAN PUSTAKA

Di bab ini menjelaskan teori-teori utama tentang Unidirectional LSTM, Port Scanning dan teori lain yang memiliki keterkaitan dengan penulisan Tugas Akhir ini.

BAB III. METODOLOGI PENELITIAN

Metodologi Penelitian ini terdiri dari proses penelitian yang kita lakukan, pembuatan rancangan dari sebuah sistem deteksi serangan, serta

penerapan metode penelitian akhir untuk proyek tersebut.

BAB IV. HASIL DAN ANALISIS PENELITIAN

Bab ini terdiri dari proses penelitian serta analisa hasil data set menggunakan metode Unidirectional Long Short Term Memory (UniLSTM).

BAB V. KESIMPULAN DAN SARAN

Bab ini adalah bab terakhir dalam penulisan Tugas Akhir, pada bab ini akan ditarik beberapa kesimpulan dari penjelasan yang telah dibahas pada bab sebelumnya, serta memberikan saran yang dapat membangun untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] M. R. Id, D. Landes, and A. Hotho, "Detection of slow port scans in flow-based network traffic," pp. 1–18, 2018.

[2] D. Aksu and M. A. Aydin, "International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings," *Int. Congr. Big Data, Deep Learn. Fight. Cyber Terror. IBIGDELFT 2018 - Proc.*, pp. 77–80, 2019.

[3] D. K. NURILAHI, R. MUNADI, S. SYAHRIAL, and A. BAHRI, "Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 10, no. 2, p. 309, 2022, doi: 10.26760/elkomika.v10i2.309.

[4] J. Chandra, H. Hermanto, and A. Rahman, "Deteksi Serangan Port Scanning Menggunakan Algoritma Naive Bayes," *Julyxxxx*, vol. x, No.x, no. x, pp. 1–5, 2021.

[5] S. K. Wanjau and G. M. Wambugu, "SSH-Brute Force Attack Detection Model based on Deep Learning," vol. 10, no. 01, pp. 42–50, 2021.

[6] A. Coluccia, A. Fascista, and G. Ricci, "A KNN-Based Radar Detector for Coherent Targets in Non-Gaussian Noise," *IEEE Signal Process. Lett.*, vol. 28, pp. 778–782, 2021, doi: 10.1109/LSP.2021.3071972.

[7] L. Dong *et al.*, "Very High Resolution Remote Sensing Imagery Classification Using a Fusion of Random Forest and Deep Learning Technique-Subtropical Area for Example," *IEEE J.*

Sel. Top. Appl. Earth Obs. Remote Sens., vol. 13, pp. 113–128, 2020, doi: 10.1109/JSTARS.2019.2953234.

[8] I. G. and Y. B. and A. Courville, "Deep learning 简介 一 、 什么是 Deep Learning ？," *Nature*, vol. 29, no. 7553, pp. 1–73, 2016, [Online]. Available: http://deeplearning.net/.

[9] G. Feng, B. Li, M. Yang, and Z. Yan, "V-CNN: Data Visualizing based Convolutional Neural Network," *2018 IEEE Int. Conf. Signal Process. Commun. Comput. ICSPCC 2018*, 2018, doi: 10.1109/ICSPCC.2018.8567781.

[10] "Deep_Learning-Based_Intrusion_Detection_With_Adversaries.pdf." .

[11] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," *2016 Int. Conf. Platf. Technol. Serv. PlatCon 2016 - Proc.*, 2016, doi: 10.1109/PlatCon.2016.7456805.

[12] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, no. c, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[13] C. H. Lee, Y. Y. Su, Y. C. Lin, and S. J. Lee, "Machine learning based network intrusion detection," *2017 2nd IEEE Int. Conf. Comput. Intell. Appl. ICCIA 2017*, vol. 2017-Janua, pp. 79–83, 2017, doi: 10.1109/CIAPP.2017.8167184.

[14] M. Assefi, E. Behravesh, G. Liu, and A. P. Tafti, "Big data machine learning using apache spark MLlib," *Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017*, vol. 2018-Janua, pp. 3492–3498, 2017, doi: 10.1109/BigData.2017.8258338.

[15] S. N. Nguyen, V. Q. Nguyen, J. Choi, and K. Kim, "Design and implementation of intrusion detection system using convolutional neural network for DoS detection," *ACM Int. Conf. Proceeding Ser.*, pp. 34–38, 2018, doi: 10.1145/3184066.3184089.

[16] S. Naseer *et al.*, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231–48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[17] K. Özkan, Ş. Işik, and Y. Kartal, "Evaluation of convolutional neural network features for malware detection," *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/ISDFS.2018.8355390.

[18] 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.

[19] S. Althubiti, W. Nick, J. Mason, X. Yuan, and A. Esterline, "Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2018-April, pp. 1–5, 2018, doi: 10.1109/SECON.2018.8478898.

[20] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, no. DL, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[21] 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.

[22] 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. 2020 - Proc.*, pp. 2–7, 2020, doi: 10.1109/ICCWorkshops49005.2020.9145085.

[23] M. Haggag, M. M. Tantawy, and M. M. S. El-Soudani, "Implementing a deep learning model for intrusion detection on apache spark platform," *IEEE Access*, vol. 8, no. 1, pp. 163660–163672, 2020, doi: 10.1109/ACCESS.2020.3019931.

[24] 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," *Inf.*, vol. 11, no. 5, pp. 1–21, 2020, doi: 10.3390/INFO11050243.

[25] Q. Zhou and D. Pezaros, "Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection -- An Analysis on CIC-AWS-2018 dataset," no. July, 2019, [Online]. Available: http://arxiv.org/abs/1905.03685.

[26] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "SSH and FTP brute-force attacks detection in computer networks: Lstm and machine learning approaches," *2020 5th Int. Conf. Comput. Commun. Syst. ICCCS 2020*, pp. 491–497, 2020, doi: 10.1109/ICCCS49078.2020.9118459.

[27] H. Hou *et al.*, "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," *IEEE Access*, vol. 8, pp. 90907–90913, 2020, doi: 10.1109/ACCESS.2020.2983953.

[28] 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, 2020, doi: 10.1109/NoF50125.2020.9249198.
[29] J. E. Varghese and B. Muniyal, “An Efficient IDS Framework for DDoS Attacks in SDN Environment,” *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.
[30] M. Dabbagh, A. J. Ghandour, K. Fawaz, W. El-Hajj, and H. Hajj, “Slow port scanning detection,” *Proc. 2011 7th Int. Conf. Inf. Assur. Secur. IAS 2011*, pp. 228–233, 2011, doi: 10.1109/ISIAS.2011.6122824.
[31] U. Kanlayasiri, “A Rule-based Approach for Port Scanning Detection,” *Proc. 23rd ...*, 2000, [Online]. Available: ftp://158.42.249.231/viejo/pub/doc/ids/A_Rule-based_Approach_for_PortScanning_Detection.pdf.
[32] 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.
[33] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.
[34] Y. Chen, Y. Xu, and H. Cheng, “Traffic Flow Prediction Based on GM-RBF,” *Lect. Notes Electr. Eng.*, vol. 944, pp. 413–425, 2023, doi: 10.1007/978-981-19-5615-7_29.
[35] A. C. Siregar and B. Ceasar Octariadi, “Feature Selection for Sambas Traditional Fabric ‘Kain Lunggi’ Using Correlation-Based Featured Selection (CFS),” *Proc. 2019 Int. Conf. Data Softw. Eng. ICoDSE 2019*, pp. 0–4, 2019, doi: 10.1109/ICoDSE48700.2019.9092731.
[36] A. Science and I. Corporation, “Un cor rec t ed Pro o Un cor rec t Pro o,” 2019, doi: 10.1162/neco.
[37] R. C. Staudemeyer and E. R. Morris, “Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks,” no. September, 2019, [Online]. Available: http://arxiv.org/abs/1909.09586.
[38] R. D. W. Santosa, M. A. Bijaksana, and A. Romadhony, “Implementasi Algoritma Long Short-Term Memory (LSTM) untuk Mendeteksi Penggunaan Kalimat Abusive Pada Teks Bahasa Indonesia,” *e-Proceeding Eng.*, vol. 8, no. 1, pp. 691–

702, 2021.
[39] 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.
[40] 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. July, 2019, doi: 10.1016/j.brainres.2019.146341.
[41] 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. December 2017, pp. 22–32, 2018, doi: 10.1016/j.chemolab.2018.01.004.
[42] 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.
[43] D. Ding, S. Han, H. Zhang, Y. He, and Y. Li, “Predictive biomarkers of colorectal cancer,” *Comput. Biol. Chem.*, vol. 83, 2019, doi: 10.1016/j.compbiolchem.2019.107106.
[44] T. Elmasri, N. Samir, M. Mashaly, and Y. Atef, “Evaluation of CICIDS2017 with qualitative comparison of machine learning algorithm,” *Proc. - 2020 IEEE Cloud Summit, Cloud Summit 2020*, pp. 46–51, 2020, doi: 10.1109/IEEECloudSummit48914.2020.00013.