KLASIFIKASI SERANGAN DDOS PADA *APACHE SPARK* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY*

TUGAS AKHIR

OLEH :

DWI LINGGA HANAYUDA

09011281823051

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

KLASIFIKASI SERANGAN DDOS PADA *APACHE SPARK* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

DWI LINGGA HANAYUDA

09011281823051

Indralaya, Juli 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir,
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19661203200641001	**NIP. 198701222015041002**

AUTHENTICATION PAGE

CLASSIFICATION OF DDOS ATTACKS ON APACHE SPARK USING LONG SHORT-TERM MEMORY METHOD

FINAL TASK

Submitted To Fulfill One Of The Requirements

To Obtain A Bachelor's Degree In Computer Science

By :

DWI LINGGA HANAYUDA

09011281823051

Indralaya, Juli 2023

Acknowledge,

Head of Computer System Departmen	***Final Project Advisor***
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19661203200641001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 18 Juli 2023

Tim Penguji:

1. **Ketua Sidang : Dr. Ahmad Zarkasi, M.T.**
2. **Sekretaris Sidang : Nurul Afifah, M.Kom.**
3. **Penguji Sidang : Huda Ubaya, M.T.**
4. **Pembimbing : Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

iv

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Dwi Lingga Hanayuda

NIM : 09011281823051

Program Studi : Sistem Komputer

Judul : Klasifikasi Serangan DDoS Pada *Apache Spark* Menggunakan Metode *Long Short Term Memory*

Hasil Pengecekan Software *iThenticate/Turnitin* : 13%

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

Demikian, pernyatan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Indralaya, Juli 2023

Dwi Lingga Hanayuda

NIM. 09011281823051

v

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh.

Puji dan syukur atas kehadiran Allah Subhanahu Wa ta'ala yang telah memberikan rahmat dan hidayah-Nya lah sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini yang berjudul "**Klasifikasi Serangan DDoS pada *Apache Spark* menggunakan Metode *Long Short Term Memory***".

Pada kesempatan ini penulis mengucapkan terima kasih kepada pihak yang telah memberikan bantuan, dorongan, motivasi, semangat dan bimbingan dalam menyelesaikan penyusunan Tugas Akhir ini. Penulis mengucapkan terima kasih kepada :

1. Allah Subhanahu Wa ta'ala yang memberikan rahmat dan hidayah-Nya serta nikmat yang tak terhitung.
2. Kedua orangtua penulis dan saudara yang telah membantu.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya untuk membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulisan dalam menyelesaikan Tugas Akhir ini.
5. Bapak Ahmad Fali Oklilas, M.T. selaku Dosen Pembimbing Akademik.
6. Mbak Renny selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
7. Mochammad Rafii Nanda Wicaksana, Jepi Sujana, Bima Gusti Syauqi, Daffa Bima Perdana, M Taufik, Agung Al hafizin, Jumhadi dan teman lainnya selaku rekan yang membantu menyusun dan menyelesaikan penulisan Tugas Akhir ini.
8. Rixza Deviantiwi Putri AS selaku support system yang terus memberikan dukungan dengan tulus untuk berjuang menyelesaikan skripsi ini hingga tuntas.

Dalam penyusunan Tugas Akhir ini penulis menyadari sepenuhnya masih jauh dari kata sempurna, oleh karena itu penulis mengharapkan saran dan kritik dari semua pihak yang berkenan agar menjadi bahan evaluasi yang lebih baik lagi.

Akhir kata saya harap semoga Laporan Tugas Akhir ini dapat bermanfaat serta dapat menambah pengetahuan dan wawasan bagi yang membutuhkannya.

Wassalamualakum Warahmatullahi Wabarakatuh

Indralaya, Juli 2023

Penulis,

Dwi Lingga Hanayuda.

NIM. 09011281823051

KLASIFIKASI SERANGAN DDOS PADA *APACHE SPARK* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY*

Dwi Lingga Hanayuda (09011281823051)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : 09011281823051@student.unsri.ac.id

ABSTRAK

Serangan *Distributed Denial-of-Service* (DDoS) merupakan ancaman serius bagi infrastruktur jaringan komputer. *Apache Spark*, sebagai platform pemrosesan data terdistribusi yang populer, penting untuk mengembangkan metode yang efektif untuk mengklasifikasikan serangan DDoS pada *Apache Spark* guna meningkatkan keamanan sistem. Dalam penelitian ini, kami mengusulkan pendekatan klasifikasi menggunakan metode *Long-Short Term Memory* (LSTM), pra-pemrosesan data dengan normalisasi dan pemisahan dataset menjadi data latih dan data uji. Membangun model LSTM dengan menggunakan arsitektur yang telah dioptimalkan. Model dilatih menggunakan data latih dan kemudian diuji dengan menggunakan data uji untuk mengklasifikasikan serangan DDoS. Penelitian ini menggunakan dataset CIC-IDS2018. Hasil eksperimen menunjukkan bahwa metode LSTM memberikan kinerja yang baik dalam mengklasifikasikan serangan DDoS pada Apache Spark. Model LSTM mencapai tingkat akurasi yang tinggi dan memiliki nilai pengukuran evaluasi lainnya, seperti presisi, *recall,* dan *F1-score* yang baik. Dengan demikian, metode LSTM dapat menjadi solusi yang efektif untuk mengamankan *Apache Spark* dari serangan DDoS.

Kata Kunci : *Distributed Denial of Service*, LSTM, *Apache Spark*, Keamanan Sistem.

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir,**
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19661203200641001	**NIP. 198701222015041002**

viii

CLASSIFICATION OF DDOS ATTACKS ON APACHE SPARK USING LONG SHORT-TERM MEMORY METHOD

Dwi Lingga Hanayuda (09011281823051)
Department of Computer System, Computer Science Faculty, Sriwijaya University

Email : 09011281823051@student.unsri.ac.id

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks pose a serious threat to computer network infrastructures. Apache Spark, as a popular distributed data processing platform, requires effective methods to classify DDoS attacks on Apache Spark in order to enhance system security. In this research, we propose a classification approach using the Long-Short Term Memory (LSTM) method, data preprocessing with normalization, and dataset separation into training and testing data. We construct an optimized LSTM model architecture, which is trained using the training data and tested using the testing data to classify DDoS attacks. The CIC-IDS2018 dataset is used in this study. The experimental results demonstrate that the LSTM method achieves good performance in classifying DDoS attacks on Apache Spark. The LSTM model achieves high accuracy and exhibits good evaluation metrics such as precision, recall, and F1-score. Thus, the LSTM method can serve as an effective solution for securing Apache Spark against DDoS attacks.

Keywords *: Distributed Denial of Service*, LSTM, *Apache Spark, System Security.*

Acknowledge,

Head of Computer System Deparment	***Final Project Advisor***
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19661203200641001	**NIP. 198701222015041002**

ix

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Distributed Denial of Service (DDoS) adalah salah satu jenis serangan jaringan yang membuat layanan atau situs web tidak dapat diakses oleh pengguna yang sah. Serangan ini menggunakan banyak sumber serangan yang berasal dari berbagai lokasi, yang bertujuan untuk membuat sistem target tidak dapat memproses permintaan yang benar. Tujuan DDoS adalah menghabiskan sumber daya dari host korban untuk menghentikan layanan[1]. Serangan DDoS dapat membuat situs web dan layanan online mengalami downtime dan kehilangan pendapatan, sehingga menjadi masalah yang serius bagi industri teknologi informasi.

Saat ini, serangan DDoS telah menjadi sangat dinamis dan canggih, karena mereka diluncurkan dalam berbagai pola, mempersulit solusi statis untuk dideteksi dan pencegahan akses resmi ke *resources*[2]. DDoS sering digunakan untuk melakukan serangan keamanan jaringan, dan memiliki berbagai jenis, seperti UDP Flood, ICMP Flood, SYN Flood, dan HTTP Flood. Serangan DDoS juga dapat menggunakan malware yang menginfeksi komputer-komputer individu dan menggunakan mereka sebagai sumber serangan, yang disebut sebagai botnet.

Mendeteksi DDoS dapat dilakukan dengan menggunakan data mining untuk menganalisis karakteristik serangan seperti pada. Parameter yang digunakan adalah entropi sumber IP, entropi nomor port, entropi jenis paket, rata-rata setiap jenis paket, dan jumlah paket[3]. Pentingnya deteksi dan mitigasi serangan DDoS sangat meningkat dengan adanya peningkatan akses internet dan popularitas layanan online. Oleh karena itu, sangat penting bagi industri teknologi informasi untuk memahami dan memantau serangan DDoS, serta memiliki solusi yang efektif untuk melindungi sistem dari serangan tersebut

Terdapat banyak metode dan alat untuk melakukan serangan DDoS. Secara tradisional, serangan DDoS seperti ICMP flooding, SYN flooding dan UDP flooding dilakukan pada *layer network* dan *layer transport*. Akibat yang ditimbulkan dari serangan DDoS menyebabkan kerugian yang besar sehingga menjadi suatu masalah serius dan dikatakan sebagai pelanggaran terhadap kebijakan penggunaan internet. Serangan ini biasanya akan menyerang aktifitas yang terjadi pada internet seperti pada website, bisnis, dan kompetisi game. Pada tahun 2015, serangan DDoS menyerang *Github*, yang merupakan penyedia layanan berbasis cloud yang berdampak pada layanan selama seminggu dan pada tahun 2016 terjadi hal yang sama pada perusahaan *Dyn*, yang menyediakan layanan server DNS sehingga hal ini berdampak pada *Netflix* dan *Spotify*[4].

Dikarenakan hal tersebut, deteksi serangan DDoS menjadi yang pertama dan yang paling penting untuk melawan serangan DDoS. Terdapat dua teknik untuk mendeteksi DDoS yaitu dengan deteksi penyalahgunaan dan deteksi anomali. Teknik deteksi penyalahgunaan yaitu mendeteksi serangan dengan membandingkan aktivitas jaringan tujuan saat ini dengan karakteristik serangan yang telah diketahui. Tetapi cara ini sulit untuk mendeteksi serangan baru. Oleh karena itu, teknik deteksi anomali digunakan untuk mendeteksi serangan yang belum diketahui dengan membandingkan aktivitas jaringan tujuan saat ini dengan aktivitas normal yang telah ditetapkan. Dasar untuk melakukan pendekatan deteksi yaitu menggunakan *machine learning* untuk membuat model aktivitas normal dan membandingkannya dengan aktivitas baru. Model *deep learning* diusulkan untuk memecahkan masalah yang terkait dengan ketidakcukupan metode berbasis pengambilan sampel yang digunakan dalam keamanan jaringan pada tahap awal jaringan iot software-defined networking (SDN)[5].

Pada [1], [2], dan [5] telah melakukan penelitian DDoS pada *Apache Spark* dengan hasil yang cukup bagus pada penelitian[1] menggunakan Neural-Network yang memberikan akurasi lebih rendah daripada[2] yang mana memberikan akurasi sedikit lebih tinggi pada pendeteksian serangan DDoS. Pada [6] dengan menggunakan Apache Kafka dan Spark streaming, analisis prediksi *traffic* secara *real-time* data dilakukan dan kinerja model yang baik diamati dalam menganalisis

data. Hasilnya menunjukkan jika *Apache Spark* lebih baik digunakan untuk memproses big data. Pada penelitian kali ini menggunakan metode LSTM yang mana metode ini lebih unggul karena LSTM memiliki kemampuan mempelajari hubungan jarak jauh dalam suatu data sequence, LSTM menggunakan struktur jaringan yang memungkinkan model untuk mengingat informasi sebelumnya dan memutuskan apakah dan bagaimana informasi tersebut akan disimpan dan dilupakan dalam pengambilan keputusan selanjutnya.

Long Short-Term Memory (LSTM) adalah jenis arsitektur jaringan saraf tiruan yang dapat digunakan untuk memproses data sequentional, seperti waktu series, bahasa, dan audio. *Long Short-Term Memory* (LSTM) adalah jenis khusus Recurrent Neural Networks (RNN). LSTM di perkenalkan oleh Hochreiter dan Hochreiter pada tahun 1997[7].

LSTM memiliki kemampuan untuk mengingat informasi dalam jangka panjang, yang membuatnya sangat cocok untuk aplikasi pembelajaran mesin yang membutuhkan memori jangka panjang. LSTM mengintegrasikan memori jangka panjang ke dalam arsitektur jaringan saraf tiruan, yang memungkinkan jaringan untuk mengingat informasi yang diperoleh dari masa lalu dan mempengaruhi pemrosesan informasi saat ini. Hal ini membuat LSTM sangat efektif untuk memproses data yang memiliki dependensi waktu, seperti data waktu series atau data bahasa.

Pada LSTM terdapat sebuah model jaringan saraf yang digunakan untuk memproses data yang memiliki dependensi waktu atau urutan[8]. Sedangkan, *Apache Spark* adalah sebuah framework pemrosesan data terdistribusi yang dapat digunakan untuk memproses data dalam skala besar. Kedua teknologi ini dapat digunakan bersama-sama untuk memproses data besar yang memiliki dependensi waktu. *Apache Spark* dapat digunakan untuk mengelola dan mengakses data secara terdistribusi.

Dalam skripsi ini, akan dibahas tentang klasifikasi serangan DDoS pada *Apache Spark* menggunakan metode LSTM. Diharapkan hasil dari penelitian ini dapat memberikan kontribusi dan solusi dalam memproteksi infrastruktur jaringan dari serangan DDoS yang semakin kompleks dan memanfaatkan skala besar data

dalam lingkungan *Apache Spark*. Untuk meningkatkan performa model yang telah dibuat dan maka dari itu penulis mengusulkan judul penelitian klasifikasi serangan DDoS dengan menggunakan metode *Long Short-Term Memory* pada *Apache Spark*.

1.2 Perumusan Masalah

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

1. Bagaimana membangun simulasi program untuk mengenali dan mengklasifikasikan serangan dari DDoS pada *Apache Spark*?
2. Bagaimana model tersebut dapat menghitung akurasi deteksi serangan DDoS pada *Apache Spark* menggunakan metode Long Short-Term Memory?

1.3 Tujuan

Adapun tujuan dari penulisan Tugas Akhir ini antara lain :

1) Membangun simulasi program untuk mengenali dan mendeteksi pola serangan dari DDoS pada *Apache Spark*.
2) Menghitung akurasi, presisi, *recall*, dan F1 Score dari deteksi serangan DDoS pada *Apache Spark* menggunakan metode Long Short -Term Memory.
3) Mampu memproses data yang besar dan kompleks secara terdistribusi, sehingga dapat mengoptimalkan waktu dan sumber daya yang digunakan dalam proses klasifikasi.

1.4 Manfaat

Manfaat dari penulisan Tugas Akhir ini, antara lain :

1. Mendeteksi serangan DDoS pada lalu lintas jaringan.
2. Dapat menerangkan proses terjadinya penyerangan yang dilakukan oleh pelaku pada sistem korban.
3. Memungkinkan pengolahan data yang lebih efisien dan cepat
4. LSTM dapat meningkatkan akurasi dalam memprediksi data yang kompleks dan mempertahankan informasi yang penting dalam data.

5. Dapat membantu mengurangi waktu dan biaya yang diperlukan dalam mendeteksi serangan DDoS dengan menggunakan *Apache Spark*.

1.5 Batasan Masalah

Batasan Masalah pada Tugas Akhir ini, antara lain :

1. Penelitian ini menggunakan data dari *University of New Brunswick* (UNB).
2. Hasil dari penelitian ini berupa nilai akurasi, presisi, *recall*, dan F1 Score yang digunakan sebagai acuan untuk melihat tingkat kecocokan author dengan label.
3. Metode LSTM digunakan hanya pada tahap klasifikasi serangan DDoS, sehingga tidak membahas mengenai deteksi serangan DDoS.

1.6 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.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan proses dan rangkaian kegiatan dalam penelitian.

BAB IV HASIL DAN ANALISIS

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

BAB V KESIMPULAN

Bab ini akan memaparkan kesimpulan sementara dari hasil yang telah didapat dari penelitian.

DAFTAR PUSTAKA

[1] C.-J. Hsieh and T.-Y. Chan, “Detection DDoS Attacks Based on Neural-Network Using Apache Spark,” pp. 1–4, 2016, doi: 10.1109/ICASI.2016.7539833.

[2] A. Alsirhani, S. Sampalli, and P. Bodorik, “DDoS Detection System: Utilizing Gradient Boosting Algorithm and Apache Spark,” *Can. Conf. Electr. Comput. Eng.*, vol. 2018-May, pp. 1–6, 2018, doi: 10.1109/CCECE.2018.8447671.

[3] M. Aziz, R. Umar, and F. Ridho, “Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan,” *J. Sist. Inf.*, vol. 5341, no. April, pp. 2579–5341, 2019.

[4] A. E. Cil, K. Yildiz, and A. Buldu, “Detection of DDoS attacks with feed forward based deep neural network model,” *Expert Syst. Appl.*, vol. 169, no. December 2020, p. 114520, 2021, doi: 10.1016/j.eswa.2020.114520.

[5] A. Alsirhani, S. Sampalli, and P. Bodorik, “DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark,” *IEEE Trans. Netw. Serv. Manag.*, vol. PP, no. c, p. 1, 2019, doi: 10.1109/TNSM.2019.2929425.

[6] G. M. D’Silva, A. Khan, Gaurav, and S. Bari, “Real-time processing of IoT events with historic data using Apache Kafka and Apache Spark with dashing framework,” *RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc.*, vol. 2018-Janua, pp. 1804–1809, 2017, doi: 10.1109/RTEICT.2017.8256910.

[7] 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.

[8] T. Ali, J. Ali, and M. M. T. Jawhar, “Detecting network attacks Model

based on a long short-term memory (LSTM),” vol. 4, no. 8, pp. 64–71, 2022.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] S. Pande, A. Khamparia, D. Gupta, and D. N. H. Thanh, *DDOS Detection Using Machine Learning Technique*, vol. 921. Springer Singapore, 2021.

[15] 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.

[16] W. Huang, X. Peng, Z. Shi, and Y. Ma, “Adversarial Attack against LSTM-based DDoS Intrusion Detection System,” *Proc. - Int. Conf. Tools with Artif. Intell. ICTAI*, vol. 2020-Novem, pp. 686–693, 2020, doi: 10.1109/ICTAI50040.2020.00110.

[17] 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.

[18] L. Chen, Y. Zhang, Q. Zhao, G. Geng, and Z. Yan, “Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark,” *Procedia Comput. Sci.*, vol. 134, pp. 310–315, 2018, doi: 10.1016/j.procs.2018.07.177.

[19] 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.

[20] P. H. Pwint and T. Shwe, “Network Traffic Anomaly Detection based on Apache Spark,” *2019 Int. Conf. Adv. Inf. Technol. ICAIT 2019*, pp. 222–226, 2019, doi: 10.1109/AITC.2019.8920897.

[21] S. Gumaste, D. G. Narayan, S. Shinde, and K. Amit, “Detection of DDoS attacks in openstack-based private cloud using Apache Spark,” *J. Telecommun. Inf. Technol.*, vol. 2020, no. 4, pp. 62–71, 2020, doi: 10.26636/JTIT.2020.146120.

[22] M. Aamir and S. M. Ali Zaidi, “Clustering based semi-supervised machine learning for DDoS attack classification,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 4, pp. 436–446, 2021, doi: 10.1016/j.jksuci.2019.02.003.

[23] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, “Automated DDOS attack detection in software defined networking,” *J. Netw. Comput.*

Appl., vol. 187, no. March, p. 103108, 2021, doi: 10.1016/j.jnca.2021.103108.

[24] Y. Sudriani, I. Ridwansyah, and H. A Rustini, "Long short term memory (LSTM) recurrent neural network (RNN) for discharge level prediction and forecast in Cimandiri river, Indonesia," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 299, no. 1, 2019, doi: 10.1088/1755-1315/299/1/012037.

[25] M. Wildan, P. Aldi, and A. Aditsania, "Analisis dan Implementasi Long Short Term Memory Neural Network untuk Prediksi Harga Bitcoin," *e-Proceeding Eng.*, vol. 5, no. 2, pp. 3548–3555, 2018.