# KLASIFIKASI MALWARE TROJAN HORSE MENGGUNAKAN METODE LONG SHORT TERM MEMORY (LSTM)

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat**
**Memperoleh Gelar Sarjana Komputer**


**OLEH :**

**MUHAMMAD RAMADHANIL**

**09011382025101**



**JURUSAN SISTEM KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS SRIWIJAYA**


**2025**

# LEMBAR PENGESAHAN

## KLASIFIKASI MALWARE TROJAN HORSE MENGGUNAKAN METODE LONG SHORT TERM MEMORY (LSTM)

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat**
**Memperoleh Gelar Sarjana Komputer (S1)**

**Oleh**

**Muhammad Ramadhanil**

**09011382025101**

**Palembang, 28 Januari 2025**

**Mengetahui,**

| Pembimbing I Tugas Akhir | Pembimbing II Tugas Akhir |
|---|---|
| **Prof. Ir. Deris Stiawan, M.T., Ph.D** | **Nurul Afifah, M.Kom** |
| **NIP. 197806172006041002** | **NIP. 199211102023212049** |

**Ketua Jurusan Sistem Komputer**

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

# VALIDITY SHEET

## TROJAN HORSE MALWARE CLASSIFICATION USING THE LONG SHORT TERM MEMORY (LSTM) METHOD

**THESIS**

**Submitted to complete one of the requirements**
**Obtain a Bachelor's Degree in Computer (S1)**

**By**

**Muhammad Ramadhanil**

**09011382025101**

**Palembang, 20 Januari 2025**

**Mengetahui,**

| Pembimbing I Tugas Akhir | Pembimbing II Tugas Akhir |
|---|---|
| **Prof. Ir. Deris Stiawan, M.T., Ph.D** | **Nurul Afifah, M.Kom** |
| **NIP. 197806172006041002** | **NIP. 199211102023212049** |

**Ketua Jurusan Sistem Komputer**

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

# HALAMAN PERSETUJUAN

**Telah diuji dan lulus pada :**

**Hari** : **Senin**

**Tanggal** : **23 Desember 2024**

**Tim Penguji :**

1. **Ketua** : **Kemahyanto Exaudi, S.Kom., M.T.**
2. **Penguji** : **Ahmad Heryanto, S.Kom., M.T.**
3. **Pembimbing I** : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II** : **Nurul Afifah, M.Kom**

**Mengetahui,** 20/1/25

**Ketua Jurusan Sistem Komputer**

**Dr. Ir. Sukemi, M.T.**

**NIP. 196612032006041001**

# HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Ramadhanil

NIM : 09011382025101

Judul : Klasifikasi Malware Trojan Horse Menggunakan Metode Long Short Term Memory (LSTM)

Hasil pengecekan Plagiat/Turnitin: 12%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa paksaan dari pihak manapun.

Palembang, Januari 2025


Muhammad Ramadhanil

NIM. 09011382025101

# KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur Alhamdullilah penulis ucapkan kehadirat Allah SWT karena rahmat dan karunia-Nya penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul "**Klasifikasi Malware Trojan Horse Menggunakan Metode Long Short-Term Memory (LSTM)**".

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

1. Allah SWT yang telah memberikan berkah serta nikmat Kesehatan dan kesempatan sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan baik dan lancar.
2. Kedua Orang tua dan keluarga yang sangat penulis sayangi, yang telah membesarkan, mendukung, dan mendidik penulis dengan kasih sayang. Terima kasih untuk segala do'a, motivasi dan dukungannya baik moril, materil maupun spiritual selama ini.
3. Bapak Prof. Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom, M.T sebagai Dosen Pembimbing Akademik.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D., IPU., ASEAN ENG. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya untuk membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.
7. Ibu Nurul Afifah, M.Kom sebagai dosen pembimbing II yang telah memberikan bimbingan dan saran selama penulis menyelesaikan Tugas Akhir ini.

8. Mbak Sari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
9. Teman- teman satu kelompok riset yang selalu memberi solusi dan semangat, Indah Ria Andina, Viginita Putri Lestari dan Riski Wahyuni.
10. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa laporan tugas akhir ini masih sangat jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan penulis agar penulisan laporan ini dapat menjadi lebih baik lagi dan dapat dijadikan sumber referensi yang bermanfaat dan berguna untuk khalayak.

Akhir kata penulis mengharapkan agar laporan tugas akhir ini dapat menghasilkan sesuatu yang bermanfaat, khususnya bagi Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Wassalamu'alaikum Warahmatullah Wabarakatuh.

Palembang, Januari 2025
Penulis,

**Muhammad Ramadhanil**
NIM. 09011382025101

# KLASIFIKASI MALWARE TROJAN HORSE MENGGUNAKAN METODE LONG SHORT TERM MEMORY (LSTM)

**MUHAMMAD RAMADHANIL (09011382025101)**
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: danielsiregar131201@gmail.com

## ABSTRAK

Trojan horse merupakan serangan cyber yang dilakukan dengan menyamar atau menyusup didalam sistem melalui program atau file yang tampak normal dan tidak berbahaya. Trojan horse dapat memperoleh akses yang tidak sah ke dalam sistem komputer yang memungkinkan hacker melakukan berbagai jenis serangan dan mencuri informasi pribadi pengguna dengan mengendalikan sistem dari jarak jauh. Selain itu, kemajuan teknologi dan teknik serangan cyber terus memperluas fungsionalitas dan kemampuan Trojan, sehingga semakin sulit dideteksi dan dikalahkan. Oleh karena itu, penelitian ini mengusulkan menggunakan metode Long Short-Term Memory (LSTM) yang merupakan teknologi kecerdasan buatan bagian dari neural network yang telah menjadi pendekatan yang efektif dan canggih dalam menghadapi ancaman cyber yang terus berkembang khususnya pada trojan horse. Penelitian ini menggunakan dataset sebanyak 31.265 yang berasal dari CIC-MalMem-2022. Hasil penelitian menunjukkan bahwa model LSTM mampu mencapai akurasi sebesar 99%. Hasil ini mengidentifikasi bahwa model LSTM memiliki kinerja yang dapat diandalkan dalam melakukan klasifikasi.

***Kata Kunci:*** *Long Short-Term Memory (LSTM), Trojan Horse, Resampling Data*

**KLASIFIKASI MALWARE TROJAN HORSE MENGGUNAKAN METODE LONG SHORT TERM MEMORY (LSTM)**

**MUHAMMAD RAMADHANIL (09011382025101)**
Department of Computer System, Computer Science Faculty
Sriwijaya University
Email: danielsiregar131201@gmail.com

## ABSTRACT

Trojan horse is a cyber attack that is carried out by disguising or infiltrating a system through programs or files that appear normal and harmless. Trojan horses can gain unauthorized access into computer systems allowing hackers to carry out various types of attacks and steal users' personal information by taking control of the system remotely. In addition, advances in cyber attack technology and techniques continue to expand the functionality and capabilities of Trojans, making them increasingly difficult to detect and defeat. Therefore, this study proposes to use the Long Short-Term Memory (LSTM) method which is an artificial intelligence technology part of neural networks that has become an effective and sophisticated approach in dealing with cyber threats that continue to grow, especially in trojan horses. This study uses a dataset of 31,265 from CIC-MalMem-2022. The results show that the LSTM model is able to achieve an accuracy of 99%. These results identify that the LSTM model has reliable performance in performing classification.

***Keywords:*** *Long Short-Term Memory (LSTM), Trojan Horse, Resampling Data*

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Malware telah menjadi topik hangat di bidang cyber security sejak kemunculannya pada tahun 1980an. Malware merupakan perangkat lunak berbahaya yang digunakan hacker untuk merugikan sistem dan user melalui berbagai aktivitas kriminal. Seiring dengan kemajuan teknologi dan akses internet, malware juga terus berkembang dan hacker memiliki kemampuan untuk menghindari metode pendeteksian yang membuat proses deteksi malware menjadi rumit [1]. Malware mempunyai keragaman kategori dan kelompok malware yang berbeda, termasuk *Worm, Virus, Bot, Botnet, Trojan, Ransomware, Spyware*, dan *Rootkit* [1].

Trojan horse merupakan serangan *cyber* yang dilakukan dengan menyamar atau menyusup didalam sistem melalui program atau file yang tampak normal dan tidak berbahaya. Trojan horse dapat memperoleh akses tidak sah ke sistem computer yang memungkinkan penyerang atau *hacker* melakukan berbagai jenis serangan dan mencuri informasi pribadi pengguna [2]. Hacker menggunakan *trojan horse* untuk berbagai tujuan, termasuk mencuri data, menghancurkan integritas sistem, dan mengendalikan sistem dari jarak jauh. Selain itu, kemajuan teknologi dan teknik serangan siber terus memperluas fungsionalitas dan kemampuan Trojan, sehingga semakin sulit dideteksi dan dikalahkan.

Oleh karena itu, untuk menghadapi ancaman cyber yang terus berkembang khususnya pada trojan horse dibutuhkan pendekatan keamanan yang lebih canggih. Penelitian tugas akhir ini mengusulkan menggunakan metode Long Short-Term Memory (LSTM) yang merupakan teknologi kecerdasan buatan yang termasuk dalam *neural network*. Long Short-Term Memory (LSTM) telah menjadi pendekatan yang efektif dalam mendeteksi dan melawan ancaman ini.

LSTM (*Long Short-Term Memory*) merupakan salah satu jenis arsitektur dalam jaringan saraf tiruan (neural network), yang khusus dirancang untuk

menangani masalah ketergantungan temporal panjang. LSTM merupakan pengembangan dari jenis Recurrent Neural Netwok (RNN) yang memiliki keunggulan dalam mengatasi masalah "vanishing gradient" yang sering dihadapi oleh RNN. Metode LSTM dapat memahami dan menyimpan informasi dalam jangka waktu yang lama membuat metode ini dapat mengatasi klasifikasi dengan pola temporal yang kompleks, seperti deteksi *trojan horse*.

Menurut Widi [3] dalam penelitiannya mengenai “Klasifikasi Judul Berita Clickbait menggunakan RNN-LSTM”, analisis metode memiliki ketepatan akurasi sebesar 79% dalam melakukan klasifikasi judul berita clickbait. Dataset yang digunakan pada penelitian ini berasal dari jurnal yang berisi 15000 yang telah dianotasi antara clickbait dan non clickbait, data non clickbait berjumlah 8700 dan clickbait berjumlah 6300 [3].

Menurut David [4] dalam penelitiannya mengenai “Klasifikasi Sentimen Ulasan Makanan Amazon Dengan Bidirectional LSTM”, analisis metode memiliki ketepatan akurasi sebesar 93% dalam melakukan klasifikasi sentimen konsumen pada makanan. Dataset yang digunakan pada penelitian ini berasal dari Kanggle yang berisi 568.454 ulasan dari Amazon Fine Food [4].

Menurut Akmal [5] dalam penelitiannya mengenai “Klasifikasi Pelanggaran Undang-Undang ITE pada Twitter Menggunakan LSTM dan BiLSTM”, analisis metode memiliki ketepatan akurasi sebesar 98%. Dataset yang digunakan pada penelitian ini menggunakan teknik scrapping menggunakan Twitter API dengan memanfaatkan library tweepy untuk mengakses data tweet [5].

Penelitian menggunakan dataset yang tidakseimbang antara data benign dan data malware, oleh karena itu penggunaan teknik Random oversampling dapat mengatasi masalah data yang tidak seimbang, terutama dalam kelas minoritasnya jauh lebih rendah dibandingkan kelas mayoritas. Tujuan utama dari random oversampling adalah untuk mengatasi ketidakseimbangan kelas dengan cara menggandakan atau menduplikasi sampel yang ada secara acak untuk menambah jumlah sampel pada kelas minoritas.

Dari penjelasan diatas, penulis akan melakukan Klasifikasi Trojan Horse menggunakan dataset yang berasal dari *Canadian Institute for Cyber Security* (CIC) yaitu CIC-MalMem-2022. Adapun judul penelitian tugas akhir yang dilakukan yaitu "**Klasifikasi Malware Trojan Horse Menggunakan Metode Long Short-Term Memory (LSTM)**".

## 1.2 Rumusan Masalah

Berdasarkan latar belakang penelitian diatas, rumusan masalah yang akan dibahas pada penelitian ini adalah:

1. Bagaimana cara mengatasi dataset CIC-MalMem-2022 yang tidak seimbang dalam klasifikasi Malware Trojan Horse?
2. Bagaimana cara melakukan klasifikasi Malware Trojan Horse?
3. Bagaimana performa evaluasi model LSTM dalam melakukan klasifikasi Trojan Horse?

## 1.3 Batasan Masalah

Berdasarkan latar belakang penelitian diatas, batasan masalah yang akan dibahas pada penelitian ini adalah:

1. Dataset yang digunakan dalam penelitian berasal dari *Canadian Institute for Cyber Security* (CIC) yaitu CIC-MalMem-2022.
2. Malware yang digunakan dalam penelitian ini yaitu Trojan Horse.
3. Teknik Random Oversampling untuk mengatasi dataset yang tidak seimbang.
4. Metode yang digunakan dalam penelitian adalah Long Short-Term Memory (LSTM).

## 1.4 Tujuan Penelitian

Berdasarkan latar belakang penelitian diatas, berikut ini tujuan dari penelitian tugas akhir yang diakukan:

1. Menerapkan teknik Random Oversampling untuk mengatasi dataset yang tidak seimbang dalam klasifikasi Malware Trojan Horse.
2. Menerapkan metode Long Short-Term Memory (LSTM) untuk mengatasi klasifikasi trojan horse pada dataset CIC-MalMem-2022.
3. Menerapkan Confusion Matrix untuk mengevaluasi performa model Long Short-Term Memory (LSTM).

## 1.5 Manfaat Penelitian

Berikut ini beberapa manfaat penelitian tugas akhir yang dilakukan yaitu:

1. Penerapan random oversampling dapat menyeimbangkan antara kelas mayoritas dan kelas minoritas.
2. Penerapan metode Long Short-Term Memory (LSTM) dapat meningkatkan akurasi dalam klasifikasi malware trojan horse.
3. Penerapan Confusion Matrix dapat mengetahui hasil performa klasifikasi metode Long Short-Term Memory (LSTM).

## 1.6 Metodologi Penelitian

Berikut ini merupakan beberapa metodologi penelitian tugas akhir yang dilakukan yaitu:

1. Metode Studi Pustaka (Literature)

   Metode ini dilakukan dengan cara mencari dan mengumpulkan referensi yang berupa literature yang terdapat pada buku dan website internet mengenai Trojan Horse, Long Short-Term Memory (LSTM), imbalance dataset, evaluasi performa klasifikasi model dan lainnya yang dibutuhkan dalam penelitian.
2. Metode Pengumpulan Data

   Metode ini dilakukan dengan mengumpulkan dataset, yang mana dalam penelitian ini penulis menggunakan dataset berasal dari *Canadian Institute for Cyber Security* (CIC) yaitu CIC-MalMem-2022.

3. Metode Pengolahan Data

   Metode ini dilakukan dengan menganalisis dataset terlebih dahulu sebelum mengolah dataset. Dataset yang diperoleh merupakan dataset imbalance sehingga diperlukan teknik penyeimbangan data. Pada penelitian ini teknik penyeimbangan data dilakukan dengan teknik Random Oversampling.

4. Metode Analisa

   Metode ini dilakukan dengan menganalisa hasil dari pengolahan data yang kemudian divalidasi untuk mendapatkan hal-hal penting yang akan digunakan untuk dijadikan kesimpulan.

5. Metode Kesimpulan dan Saran

   Metode ini adalah metode terakhir yang dilakukan setelah mendapat hal-hal penting yang kemudian akan menjadi kesimpulan pada penelitian tugas akhir ini serta saran yang dapat dijadikan referensi bagi yang tertarik untuk meneliti lebih lanjut.

## 1.7 Sistematika Penulisan

Berikut ini merupakan sistematika yang digunakan dalam penulisan tugas akhir agar mendeskripsikan bab – bab yang terdapat dalam tugas akhir yang dilakukan:

**BAB I. PENDAHULUAN**

Bab ini akan menjelaskan mengenai Latar Belakang penelitian, Tujuan penelitian, Manfaat penelitian, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penulisan tugas akhir.

**BAB II. TINJAUAN PUSTAKA**

Bab ini berisi dasar teori dari penelitian terkait dengan trojan horse, proses analisis dataset, teknik Random Oversampling, klasifikasi dengan mengunakan metode *Long Short-Term Memory* (LSTM), dan hal-hal yang berkaitan langsung dengan penelitian.

**BAB III. METODELOGI**

Bab ini akan menjelaskan mengenai langkah-langkah (metodologi) penelitian, diagram alur (*flow chart*) dalam setiap tahap perancangan sistem pada tugas akhir.

**BAB IV. ANALISA DAN PEMBAHASAN**

Bab ini akan menjelaskan mengenai hasil dari pengolahan data yang telah dilakukan, dari hasil tersebut akan dilakukan analisa agar mendapatkan data yang akurat. Analisa dilakukan menggunakan *Confusion Matrix*.

**BAB V. KESIMPULAN DAN TINDAK LANJUT**

Bab ini berisi hasil kesimpulan yang didapat dari penelitian yang telah dilakukan. Dan saran yang diharapkan dapat membuat penelitian ini dikembangkan lebih baik.

# DAFTAR PUSTAKA


[1] T. Carrier, P. Victor, A. Tekeoglu, and A. Habibi Lashkari, "Detecting Obfuscated Malware using Memory Feature Engineering," *Int. Conf. Inf. Syst. Secur. Priv.*, no. Icissp, pp. 177–188, 2022, doi: 10.5220/0010908200003120.

[2] A. M. Abuzaid, M. M. Saudi, B. M. Taib, and Z. H. Abdullah, "An Efficient Trojan Horse Classification (ETC)," *IJCSI Int. J. Comput. Sci. Issues*, vol. 10, no. Issue 2, No 3, pp. 96–104, 2013, [Online]. Available: http://ijcsi.org/papers/IJCSI-10-2-3-96-104.pdf%5Cnwww.IJCSI.org

[3] W. Afandi, S. N. Saputro, A. M. Kusumaningrum, H. Adriansyah, M. H. Kafabi, and S. Sudianto, "Klasifikasi Judul Berita Clickbait menggunakan RNN-LSTM," *J. Inform. J. Pengemb. IT*, vol. 7, no. 2, pp. 85–89, 2022, doi: 10.30591/jpit.v7i2.3401.

[4] D. J. M. Pasaribu, K. Kusrini, and S. Sudarmawan, "Peningkatan Akurasi Klasifikasi Sentimen Ulasan Makanan Amazon dengan Bidirectional LSTM dan Bert Embedding," *Inspir. J. Teknol. Inf. dan Komun.*, vol. 10, no. 1, 2020, doi: 10.35585/inspir.v10i1.2568.

[5] A. P. Hesaputra, "Klasifikasi Pelanggaran Undang-Undang ITE pada Twitter Menggunakan LSTM dan BiLSTM," *Univ. Islam Indones.*, p. 7.

[6] A. Rajabi, B. Ramasubramanian, and R. Poovendran, "Trojan Horse Training for Breaking Defenses against Backdoor Attacks in Deep Learning," no. ML, 2022, [Online]. Available: http://arxiv.org/abs/2203.15506

[7] E. D. O. Andrade, J. Viterbo, C. N. Vasconcelos, J. Guérin, and F. C. Bernardini, "A model based on LSTM neural networks to identify five different types of malware," in *Procedia Computer Science*, 2019, vol. 159, pp. 182–191. doi: 10.1016/j.procs.2019.09.173.

[8] K. N. K. Thapa and N. Duraipandian, "Malicious Traffic classification Using Long Short-Term Memory (LSTM) Model," *Wirel. Pers. Commun.*, vol.

119, no. 3, pp. 2707–2724, 2021, doi: 10.1007/s11277-021-08359-6.

[9] R. D. Maddineni and C. D. Deepak, “Consistent Interpretation of Ensemble Classifiers in Trojan-Horse Detection,” *IEEE Access*, vol. 11, no. June, pp. 70930–70946, 2023, doi: 10.1109/ACCESS.2023.3294282.

[10] Y. Gao, C. Xu, D. Wang, S. Chen, D. C. Ranasinghe, and S. Nepal, “StriP: A defence against trojan attacks on deep neural networks,” in *ACM International Conference Proceeding Series*, 2019, pp. 113–125. doi: 10.1145/3359789.3359790.

[11] O. Aslan and R. Samet, “A Comprehensive Review on Malware Detection Approaches,” *IEEE Access*, vol. 8. IEEE, pp. 6249–6271, 2020. doi: 10.1109/ACCESS.2019.2963724.

[12] R. Pascanu, J. W. Stokes, and O. M. Way, “MALWARE CLASSIFICATION WITH RECURRENT NETWORKS,” *Univ. Montr. Canada*, pp. 1916–1920, 2015.

[13] K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles, “Understanding and mitigating banking trojans: From Zeus to emotet,” *Proc. 2021 IEEE Int. Conf. Cyber Secur. Resilience, CSR 2021*, no. July, pp. 121–128, 2021, doi: 10.1109/CSR51186.2021.9527960.

[14] J. Magee, “IoT Architecture Security and Proposal for Semi-Markov Chain IDS,” *Hampt. Univ.*, p. 8, 2019, [Online]. Available: https://par.nsf.gov/servlets/purl/10344951

[15] University of New Brunswick, “Canadian Institute for Cyber Security (CIC),” *Dataset*, [Online]. Available: https://www.unb.ca/cic/datasets/malmem-2022.html

[16] A. Ambarwari, Q. Jafar Adrian, and Y. Herdiyeni, “Analysis of the Effect of Data Scaling on the Performance of the Machine Learning Algorithm for Plant Identification,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 1, pp. 117–122, 2020, doi: 10.29207/resti.v4i1.1517.

[17] L. G. Aug, “LSTM-Based Forecasting Model for GRACE Accelerometer

Data," pp. 1–12, 2019.

[18] S. Diantika, "Penerapan Teknik Random Oversampling Untuk Mengatasi Imbalance Class Dalam Klasifikasi Website Phishing Menggunakan Algoritma Lightgbm," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 1, pp. 19–25, 2023, doi: 10.36040/jati.v7i1.6006.

[19] M. S. Shelke, P. R. Deshmukh, and P. V. K. Shandilya, "A Review on Imbalanced Data Handling Using Undersampling and Oversampling Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 4, pp. 444–449, 2017, doi: 10.23883/ijrter.2017.3168.0uwxm.

[20] A. S. Bayangkari Karno, "Analisis Data Time Series Menggunakan LSTM (Long Short Term Memory) Dan ARIMA (Autocorrelation Integrated Moving Average) Dalam Bahasa Python.," *Ultim. InfoSys J. Ilmu Sist. Inf.*, vol. 11, no. 1, pp. 1–7, 2020, doi: 10.31937/si.v9i1.1223.

[21] Yudi Widhiyasana, Transmissia Semiawan, Ilham Gibran Achmad Mudzakir, and Muhammad Randi Noor, "Penerapan Convolutional Long Short-Term Memory untuk Klasifikasi Teks Berita Bahasa Indonesia," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 10, no. 4, pp. 354–361, 2021, doi: 10.22146/jnteti.v10i4.2438.

[22] F. N. Fajri and S. Syaiful, "Klasifikasi Nama Paket Pengadaan Menggunakan Long Short-Term Memory (LSTM) Pada Data Pengadaan," *Build. Informatics, Technol. Sci.*, vol. 4, no. 3, pp. 1625–1633, 2022, doi: 10.47065/bits.v4i3.2635.

[23] M. Rizki, S. Basuki, and Y. Azhar, "Implementasi Deep Learning Menggunakan Arsitektur Long Short Term Memory(LSTM) Untuk Prediksi Curah Hujan Kota Malang," *J. Repos.*, vol. 2, no. 3, pp. 331–338, 2020, doi: 10.22219/repositor.v2i3.470.

[24] L. Wiranda and M. Sadikin, "Penerapan Long Short Term Memory Pada Data Time Series Untuk Memprediksi Penjualan Produk Pt. Metiska Farma," *J. Nas. Pendidik. Tek. Inform.*, vol. 8, no. 3, pp. 184–196, 2019.

[25] T. B. Sianturi, I. Cholissodin, and N. Yudistira, “Penerapan Algoritma Long Short-Term Memory ( LSTM ) berbasis Multi Fungsi Aktivasi Terbobot dalam Prediksi Harga Ethereum,” vol. 7, no. 3, pp. 1101–1107, 2023.

[26] R. Akbar, R. Santoso, and B. Warsito, “Prediksi Tingkat Temperatur Kota Semarang Menggunakan Metode Long Short-Term Memory (Lstm),” *J. Gaussian*, vol. 11, no. 4, pp. 572–579, 2023, doi: 10.14710/j.gauss.11.4.572-579.

[27] E. Spam *et al.*, “Performance Comparison of Anti-Spam Technology Using Confusion Matrix Classification Performance Comparison of Anti-Spam Technology Using Confusion Matrix Classification”, doi: 10.1088/1757-899X/879/1/012076.

[28] G. Budiprasetyo, M. Hani’ah, and D. Z. Aflah, “Prediksi Harga Saham Syariah Menggunakan Algoritma Long Short-Term Memory (LSTM),” *J. Nas. Teknol. dan Sist. Inf.*, vol. 8, no. 3, pp. 164–172, 2023, doi: 10.25077/teknosi.v8i3.2022.164-172.

[29] I. G. T. Isa and B. Junedi, “Hyperparameter Tuning Epoch dalam Meningkatkan Akurasi Data Latih dan Data Validasi pada Citra Pengendara,” *Pros. Sains Nas. dan Teknol.*, vol. 12, no. 1, p. 231, 2022, doi: 10.36499/psnst.v12i1.6697.