KLASIFIKASI DETEKSI MALWARE MENGGUNAKAN DEEP NEURAL NETWORK (DNN)

Laporan Tugas Akhir

Diajukan Untuk Memenuhi

Persyaratan Guna Meraih Gelar Sarjana

Informatika Universitas Muhammadiyah Malang

Mahardhika Yudha Pratama (201910370311127)

Bidang Minat

(Jaringan)

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2025

LEMBAR PERSETUJUAN

KLASIFIKASI DETEKSI MALWARE MENGGUNAKAN METODE DEEP NEURAL NETWORK (DNN)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui
Malang 06 November 2025

Dosen pembimbing 1	Dosen Pembimbing 2
Zamah Sari, S, T, M.T	**Christian Sri Kusuma Aditya, S.kom, M.Kom**
NIDN. 0708087701	**NIDN. 0727029101**

LEMBAR PERYATAAN

Yang bertanda tangan di bawah ini :

NAMA : **Mahardhika Yudha Pratama**

NIM : **201910370311127**

FAK/JUR : **Teknik Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul " **KLASIFIKASI DETEKSI MALWARE MENGGUNAKAN METODE DEEP NEURAL NETWORK (DNN)"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya orang tulis orang lain. Baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat peryataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala benyuk resiko/sanksi yang berlaku.

Mengetahui
Dosen Pembimbing 1

Zamah Sari, S. T, M.T
NIDN. 0708087701

Malang,06 November 2025
Yang Membuat pernytaan ini

Mahardhika Yudha Pratama
201910370311127

Dosen Pembimbing 2

Christian Sri Kusuma Aditya, S,Kom, M.Kom
NIDN. 0727029101

LEMBAR PENGESAHAN

KLASIFIKASI DETEKSI MALWARE MENGGUNAKAN DEEP NEURAL NETWORK (DNN)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Informatika Universitas Muhammadiyah Malang

Disusun oleh

Mahardhika Yudha Pratama

201910370311127

Tugas Akhir Ini Telah Di Uji Dan Dinyatakan Lulus Melalui Sidang Majelis Penguji Pada

Tanggal 3 Oktober 2025

Menyetujui

Dosen Penguji 1	Dosen Penguji 2
Ir. Wildan Suharso S.Kom.,M.Kom	**Bashor Fauzan MuthohirinS.Kom.,M.Kom**
NIP.10817030596PNS.	**NIP.20230126071994PNS.**

Mengetahui,

Ketua Jurusan Informatika

Dr. Ir. Agus Eko Minarno, S.Kom., M.Kom., IPM.

NIP. 10814100540PNS.

ABSTRAK

Penelitian tentang klasifikasi deteksi malware menggunakan Jaringan Saraf Tiruan Dalam (Deep Neural Network/DNN). Dengan meningkatnya ancaman siber, seperti laporan Check Point Research yang mencatat peningkatan serangan siber sebesar 30% pada tahun 2024, dan biaya pelanggaran data rata-rata mencapai USD 4,88 juta menurut IBM, deteksi malware menjadi krusial. Penelitian ini bertujuan untuk menguji efektivitas DNN dalam mendeteksi dan mengklasifikasikan berbagai jenis malware, termasuk varian baru dan zero-day, serta membandingkan performanya dengan metode berbasis tanda tangan dan pembelajaran mesin lainnya. Dataset yang digunakan terdiri dari 10.868 sampel, dengan 9.339 malware dan 1.529 benign, mencakup fitur seperti entropi bagian, panggilan API, dan impor DLL. Hasil penelitian menunjukkan bahwa model DNN berbasis LSTM mencapai akurasi 98,84%, presisi 99,44%, recall 99,27%, dan F1-score 99,36%. Penelitian ini menunjukkan bahwa DNN menawarkan pendekatan yang lebih adaptif dibandingkan metode tradisional dalam menghadapi ancaman malware yang terus berkembang.

Kata kunci— Malware, Deteksi Malware, Jaringan Saraf Tiruan Dalam, Long Short-Term Memory, Keamanan Siber

ABSTRACT

Research on Malware Detection Classification Using Deep Neural Networks (DNN). With the rising threat of cyberattacks—such as the 30% increase in global cyber incidents reported by Check Point Research in 2024, and the average cost of a data breach reaching USD 4.88 million according to IBM—malware detection has become crucial. This study aims to examine the effectiveness of DNN in detecting and classifying various types of malware, including new variants and zero-day threats, as well as comparing its performance with signature-based methods and other machine learning approaches. The dataset used consists of 10,868 samples, including 9,339 malware and 1,529 benign files, covering features such as section entropy, API calls, and DLL imports. The results show that the LSTM-based DNN model achieved an accuracy of 98.84%, precision of 99.44%, recall of 99.27%, and F1-score of 99.36%. This research demonstrates that DNN provides a more adaptive approach compared to traditional methods in addressing the evolving challenges of malware threats.

Keywords— Malware, Malware Detection, Deep Neural Network, Long Short-Term Memory, Cybersecurity

LEMBAR PERSEMBAHAN

Puji syukur penulis panjatkan ke hadirat Allah SWT. atas segala limpahan rahmat, karunia, serta petunjuk-Nya yang tiada henti. Berkat kasih sayang dan pertolongan-Nya, penulis akhirnya dapat menyelesaikan Tugas Akhir ini sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Malang.

Dalam kesempatan ini, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Bapak/Ibu Dekan Fakultas Teknik Universitas Muhammadiyah Malang, atas segala fasilitas, dukungan, serta kesempatan, yang telah diberikan kepada penulis untuk menempuh pendidikan di lingkungan akademik yang kondusif dan inspiratif.
2. Bapak Hariyady, S.Kom., M.T. serta Dosen Program Studi Informatika atas segala bimbingan akademik, kebijakan, dan arahannya yang membantu kelancaran proses studi penulis hingga tahap akhir.
3. Bapak Zamah Sari, S.T., M.T. selaku dosen pembimbing pertama tugas akhir, yang telah meluangkan waktu, tenaga, dan pikiran untuk membimbing, memberikan masukan, serta mengarahkan penulis dengan penuh kesabaran dan ketulusan selama proses penyusunan tugas akhir ini berlangsung.
4. Bapak Christian Sri Kusuma Aditya, S.Kom., M.Kom., selaku dosen pembimbing kedua tugas akhir, yang telah meluangkan waktu, tenaga, dan pikiran untuk membimbing, memberikan masukan, serta mengarahkan penulis dengan penuh kesabaran dan ketulusan selama proses penyusunan tugas akhir ini berlangsung.
5. Untuk Ibu dan Ayah yang selalu membuatku termotivasi dan selalu menyirami kasih sayang, selalu mendoakanku, selalu menasehatiku menjadi lebih baik. Terima kasih Ibu..Terimah kasih Ayah atas semua yang telah engkau berikan semoga diberi kesehatan dan panjang umur agar dapat menemani langkah kecilku bersama adik-adikku tercinta Iput dan Salsa menuju kesuksesan.

6. Sahabat dan Teman Tersayang, tanpa semangat, dukungan dan bantuan kalian semua tak kan mungkin aku sampai disini, terimakasih untuk canda tawa, tangis, dan perjuangan yang kita lewati bersama dan terimakasih untuk kenangan manis yang telah mengukir selama ini. Dengan perjuangan dan kebersamaan kita pasti bisa! Semangat
7. Kepada teman-teman Informatika angkatan 2019 terima kasih karena telah berperan banyak memberikan pengalaman dan pembelajaran selama masa perkuliahan, see you on top, guys.
8. Terima kasih kepada diri sendiri, atas keteguhan hati, semangat untuk terus belajar, dan keberanian untuk tidak menyerah meski kondisi tersulit sekalipun. Terima kasih telah bertahan sejauh ini dan terus melangkah meski terkadang jalan terasa berat.

Akhir kata, penulis berharap Tugas Akhir ini dapat memberikan manfaat bagi semua pihak yang berkepentingan dan menjadi awal untuk berkarya dan berkontribusi lebih luas di masa mendatang.

Malang, 18 september 2025

Mahardhika Yudha. P

DAFTAR ISI

DAFTAR TABEL

UNIVERSITAS MUHAMMADIYAH MALANG

DAFTAR GAMBAR

UNIVERSITAS MUHAMMADIYAH MALANG

DAFTAR PUSTAKA

[1] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023, doi: 10.33701/jk.v5i1.3208.

[2] A. Wibowo, *"Internet of Things (IoT) dalam Ekonomi dan Bisnis Digital." Penerbit Yayasan Prima Agus Teknik*. 2023. [Online]. Available: https://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/436/461

[3] V. R. Sianipar and H. Pangaribuan, "Analisis Dan Deteksi Malware Pada Protokol Jaringan Menggunakan Metode Malware Analisis Dinamis Dan Malware Analisis Statis," *Comput. Sci. Ind. Eng.*, vol. 9, no. 6, 2023, doi: 10.33884/comasiejournal.v9i6.7833.

[4] T. G. Laksana and S. Mulyani, "FAKTOR – FAKTOR MENDASAR KEJAHATAN SIBER TERHADAP KEMANUSIAAN," vol. 11, pp. 136–160, 2024, doi: 10.25105/prio.v11i2.18960.

[5] C. Supriyanto, F. A. Rafrastara, A. Amiral, and ..., "Malware Detection Using K-Nearest Neighbor Algorithm and Feature Selection," *J. Media Inform. Budidarma*, vol. 8, pp. 412–420, 2024, doi: 10.30865/mib.v8i1.6970.

[6] E. L. Tjiong, "Pendeteksi Malware Javascript Menggunakan Fitur Semantik Program," *JSR Jar. Sist. Inf. Robot.*, vol. 7, no. 1, pp. 111–116, 2023, doi: 10.58486/jsr.v7i1.228.

[7] G. R. Kanagachidambaresan, A. Ruwali, D. Banerjee, and K. B. Prakash, "Klasifikasi Malware Menggunakan MetodeRecurrent Neural Network," *EAI/Springer Innov. Commun. Comput.*, vol. 23, no. 3, pp. 53–61, 2021.

[8] R. Firdaus, "Prediksi Indeks Harga Produsen Pertanian Karet Di Indonesia Menggunakan Metode LSTM," *J. Fasilkom*, vol. 13, no. 01, pp. 1–6, 2023, doi: 10.37859/jf.v13i01.4851.

[9] Géron, A. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow*. O'Reilly Media.

[10] Joseph Teguh Santoso, *Keamanan Siber Perusahaan*. 2020. [Online]. Available: https://www.pertamina.com/id/keamanan-siber-perusahaan%0Ahttps://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/458

[11] K. Lee, C. Choi, D. H. Shin, and H. S. Kim, "Prediction of heavy rain damage using deep learning," *Water (Switzerland)*, vol. 12, no. 7, pp. 1–18, 2020, doi: 10.3390/w12071942.

[12] B. Purnama, E. A. Winarto, S. Shairuppdin, and ..., "Deteksi Malware Ransomware Menggunakan Deep Neural Network," *JEPIN (Jurnal Edukasi …*, vol. 10, no. 1, pp. 8–12, 2024, [Online]. Available: https://jurnal.untan.ac.id/index.php/jepin/article/view/68492

[13] I. M. M. Matin, M. Agustin, B. Sugiarto, and A. N. Asri, "Deteksi Malware Menggunakan Machine Learning Dengan Metode Ensemble," *Pros. Sains Nas. dan Teknol.*, vol. 13, no. 1, p. 265, 2023, doi: 10.36499/psnst.v13i1.9224.

[14] R. B. Hadiprakoso, N. Qomariasih, and R. N. Yasa, "Identifikasi Malware Android Menggunakan Pendekatan Analisis Hibrid Dengan Deep Learning," *J. Teknol. Inf. Univ. Lambung Mangkurat*, vol. 6, no. 2, pp. 77–84, 2021, doi: 10.20527/jtiulm.v6i2.82.

[15] A. Lozano-Diez, R. Zazo, D. T. Toledano, and J. Gonzalez-Rodriguez, "An analysis of the influence of deep neural network (DNN) topology in bottleneck feature based language recognition," *PLoS One*, vol. 12, no. 8, pp. 1–22, 2017, doi: 10.1371/journal.pone.0182580.

[16] K. C. Laudon and J. P. Laudon, *Managing Information Systems: Managing the Digital Firm*. 2014.

[17] T. Hunter Team and S. Endpoint Security, "The Ransomware Threat Landscape: What to Expect in 2022," 2022.

[18] A. H. Muhammad, B. Sugiantoro, A. Luthfi, M. Teknik, I. Universitas, and I. Indonesia, "ETODE KLASIFIKASI DAN ANALISIS KARAKTERISTIK MALWARE MENGGUNAKAN KONSEP ONTOLOGI," *Teknomatika*, vol. 9, no. 1, pp. 15–28, 2024.

[19] L. N. Adenansi, Retno, "MALWARE DYNAMIC," *Educ. Inf. Commun. Technol.*, vol. 1, pp. 37–43, 2017.

[20] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017.

[21] K. Z. Ansyafa, M. Fajarudin, M. Fadhil, and S. N. Neyman, "Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 10, 2024, doi: 10.47134/pjise.v1i4.2641.

[22] V. U. Putri, E. B. Cahyono, and Y. Azhar, "Deteksi Botnet Pada Passive DNS Dengan Menggunakan Metode K Nearest Neighbor," *J. Repos.*, vol. 2, no. 12, pp. 1631–1638, 2020, doi: 10.22219/repositor.v2i12.450.

[23] billy, febrielo hanielus, caezario talumepa Saefullah Asep, "[149-157]+Perancangan+Keylogger+Berbasis+Spyware+untuk+Memonitoring+Aktivitas+Penggguna+Smartphone+Menggunakan+Aplikasi+Smart+Keylogger," *Pros. SNATIF*, vol. 4, no. September, pp. 149–157, 2023.

[24] V. Kumar, "Signature Based Intrusion Detection System Using SNORT," *Int. J. Comput. Appl. Inf. Technol. - IJCAIT*, vol. I, no. Iii, pp. 35–41, 2012, [Online]. Available: http://ijcait.com/IJCAIT/index.php/www-ijcs/article/view/171

[25] B. Gdowski, R. Kościej, and M. Niemiec, "Heuristic-based Intrusion Detection Functionality in a Snort Environment," *Inf. Secur. An Int. J.*, vol. 50, no. September, pp. 23–36, 2021, doi: 10.11610/isij.5010.

[26] A. F. Muhtadi and A. Almaarif, "Analysis of Malware Impact on Network Traffic using Behavior-based Detection Technique," *Int. J. Adv. Data Inf. Syst.*, vol. 1, no. 1, pp. 17–25, 2020, doi: 10.25008/ijadis.v1i1.14.

[27] F. A. Vadhil, M. L. Salihi, and M. F. Nanne, "Machine learning-based intrusion detection system for detecting web attacks," *IAES Int. J. Artif. Intell.*, vol. 13, no. 1, pp. 711–721, 2024, doi: 10.11591/ijai.v13.i1.pp711-721.

[28] WikiStat, "Neural Networks and Introduction to Deep Learning," *WikiStat*, pp. 1–17, 2015, [Online]. Available: http://klab.tch.harvard.edu/academia/classes/BAI/pdfs/intro-deep-

learning.pdf

[29] A. I. Georgevici and M. Terblanche, “Neural networks and deep learning: a brief introduction,” *Intensive Care Med.*, vol. 45, no. 5, pp. 712–714, 2019, doi: 10.1007/s00134-019-05537-w.

[30] E. Jawad, “the Deep Neural Network-a Review,” *Ijrdo -Journal Math.*, vol. 9, no. 9, pp. 1–5, 2023, doi: 10.53555/m.v9i9.5842.

[31] D. Raabe, “Deep Neural Networks,” *Comput. Sci. Sport*, no. December, pp. 177–184, 2024, doi: 10.1007/978-3-662-68313-2_21.

[32] C. C. Aggarwal, “Training Deep Neural Networks,” *Neural Networks Deep Learn.*, pp. 105–167, 2018, doi: 10.1007/978-3-319-94463-0_3.

[33] E. P. Cynthia and E. Ismanto, “Memprediksi Ketersediaan Komoditi Pangan Provinsi Riau,” *J. Teknol. Dan Sist. Inf. Univrab*, vol. 2, no. 2, pp. 196–209, 2017.

[34] S. R. Dubey, S. K. Singh, and B. B. Chaudhuri, “Activation functions in deep learning: A comprehensive survey and benchmark,” *Neurocomputing*, vol. 503, pp. 92–108, 2022, doi: 10.1016/j.neucom.2022.06.111.

[35] A. Nader and D. Azar, “Evolution of Activation Functions: An Empirical Investigation,” *ACM Trans. Evol. Learn. Optim.*, vol. 1, no. 2, pp. 1–26, 2021, doi: 10.1145/3464384.

[36] F. T. Admojo and Y. I. Sulistya, “Analisis Performa Algoritma Stochastic Gradient Descent (SGD) Dalam Mengklasifikasi Tahu Berformalin,” *Indones. J. Data Sci.*, vol. 3, no. 1, pp. 1–8, 2022, doi: 10.56705/ijodas.v3i1.42.

[37] T. Sakshi, “Activation functions in Neural Networks - GeeksforGeeks,” no. March, 2023.

[38] P. N. Rena, *ENERAPAN METODE CONVOLUTIONAL NEURAL NETWORK PADA PENDETEKSI GAMBAR NOTASI BALOK*. 2019.

[39] J. N. Semendawai, D. Stiawan, and I. Pahendra, “Klasifikasi Shellcode dengan Machine Learning Berbasis Klasifikasi Biner,” vol. 5, no. 9, pp. 1514–1526, 2024.

[40] Z. Muhammad, J. Nafis, R. Nazilla, R. Nugraha, and S. Uyun, “erbandingan Algoritma Decision Tree dan K-Nearest Neighbor untuk Klasifikasi,” vol. 13, pp. 245–252, 2024, doi: 10.34010/komputika.v13i2.12609.

[41] E. Ferdiana Sari and Ekohardi, “Penerapan Github Sebagai Media E-Learning Untuk Mengetahui Keefektifan Kolaborasi Project Pada Mata Pelajaran Pemrograman Web Dan Perangkat Bergerak Di Smk Negeri 2 Surabaya,” *It-Edu*, vol. 06, no. 2, pp. 14–22, 2021.

[42] S. Hidayatulloh, “Optimalisasi Github Untuk Software Project Management Dengan Memanfaatkan Notifikasi Sms,” *J. Inform.*, vol. 2, no. 1, pp. 198–204, 2016, doi: 10.31311/ji.v2i1.64.

[43] I. Wicaksono, J. S. Komputer, F. I. Komputer, and U. Sriwijaya, “DETEKSI MALWARE ANDROID DENGAN METODE REVERSE ENGINEERING,” 2024.

[44] N. Naik *et al.*, “Embedded YARA rules: strengthening YARA rules utilising fuzzy hashing and fuzzy rules for malware analysis,” *Complex Intell. Syst.*, vol. 7, no. 2, pp. 687–702, 2021,

doi: 10.1007/s40747-020-00233-5.

[45] I. Prabakaran *et al.*, "Gaussian mixture models for probabilistic classification of breast cancer," *Cancer Res.*, vol. 79, no. 13, pp. 3492–3502, 2019, doi: 10.1158/0008-5472.CAN-19-0573.

[46] N. Suhermi, S. Suhartono, I. M. G. M. Dana, and D. D. Prastyo, "Pemilihan Arsitektur Terbaik pada Model Deep Learning Melalui Pendekatan Desain Eksperimen untuk Peramalan Deret Waktu Nonlinier," *Stat. J. Theor. Stat. Its Appl.*, vol. 18, no. 2, pp. 153–159, 2019, doi: 10.29313/jstat.v18i2.4545.

[47] R. T. Amdani, S. T. Hafidudin, and M. Iqbal, "Analysis and Detection of Malware Poison Ivy With Malware Dynamic Analysis Method and Malware Static Analysis," *J. Elektro Telekomun. Terap. Anal.*, vol. 7, no. 2, pp. 178–191, 2021.

[48] S. C. Dewi, H. Bunyamin, and S. Budi, "Penerapan Data Science pada Analisis Data Acara TV dan Film pada Aplikasi Layanan Streaming," *J. Strateg.*, vol. 4, no. 1, pp. 125–133, 2022.

[49] E. V. Tjahjadi and B. Santoso, "Klasifikasi Malware Menggunakan Teknik Machine Learning," *J. Ilm. Ilmu Komput.*, vol. 2, no. 1, pp. 60–70, 2023.

[50] R. A. Sari, P. S. Informatika, F. Teknik, and U. M. Makassar, "ANALISIS KESESUAIAN KONTEKS SARAN DAN," 2024.

[51] D. Satria Yudha Kartika and H. Maulana, "Preprosesing dan normalisasi pada dataset kupu-kupu untuk ekstraksi fitur warna, bentuk dan tekstur," *J. Comput. Electron. Telecommun.*, vol. 1, no. 2, pp. 1–8, 2021, doi: 10.52435/complete.v1i2.76.

[52] N. K. Verma and A. Salour, "Feature extraction," *Stud. Syst. Decis. Control*, vol. 256, pp. 121–173, 2020, doi: 10.1007/978-981-15-0512-6_4.

[53] Gde Agung Brahmana Suryanegara, Adiwijaya, and Mahendra Dwifebri Purbolaksono, "Peningkatan Hasil Klasifikasi pada Algoritma Random Forest untuk Deteksi Pasien Penderita Diabetes Menggunakan Metode Normalisasi," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 114–122, 2021, doi: 10.29207/resti.v5i1.2880.

[54] R. BAGASKARA and S. Nurmaini, "Perancangan Sistem Deteksi Malware Menggunakan Metode Deep Neural Network," 2019, [Online]. Available: https://repository.unsri.ac.id/897/

[55] J. Baek and Y. Choi, "Deep neural network for predicting ore production by truck-haulage systems in open-pit mines," *Appl. Sci.*, vol. 10, no. 5, 2020, doi: 10.3390/app10051657.

[56] A. chandra Saputra, "Penentuan Parameter Learning Rate Selama Pembelajaran Jaringan Syaraf Tiruan Backpropagation Menggunakan Algoritma Genetika," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 14, no. 2, pp. 202–212, 2020, doi: 10.47111/jti.v14i2.1141.

[57] 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.

[58] L. Yosia Wibowo, N. Annisa, P. Ananda Khairunnisa, V. Handrianus Pranatawijaya, and R. Priskila, "Implementasi Long Short-Term Memory Dalam Analisis Sentimen Pengguna

Aplikasi Twitter Yang Mengandung Ujaran Kebencian," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 3, pp. 3170–3174, 2024, doi: 10.36040/jati.v8i3.9654.

[59] M. Kamal Wisyaldin, G. Maya Luciana, H. Pariaman, and P. Pembangkitan Jawa Bali, "Pendekatan Long Short-Term Memory untuk Memprediksi Kondisi Motor 10 kV pada PLTU Batubara," *Kilat*, vol. 9, no. 2, pp. 311–318, 2020, [Online]. Available: https://doi.org/10.33322/kilat.v9i2.997

[60] L. Kristiana and D. Miyanto, "Penambahan Parameter PM2.5 dalam Prediksi Kualitas Udara : Long Short Term Memory," *Multimed. Artif. Intell. Netw. Database*, vol. 8, no. 2, pp. 188–202, 2023.

[61] E. Raff, J. Sylvester, and C. Nicholas, "Learning the PE header, malware detection with minimal domain knowledge," *AISec 2017 - Proc. 10th ACM Work. Artif. Intell. Secur. co-located with CCS 2017*, pp. 121–132, 2017, doi: 10.1145/3128572.3140442.

[62] Y. Wang, W., Zhu, M., Zeng, X., Ye, X., Sheng, Y., & Hou, "End-to-End Encrypted Traffic Classification With One-Dimensional Convolution Neural Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 14(1), no. 110–120, 2019.

[63] A. T. N. Hartono and H. D. Purnomo, "Pengembangan Stochastic Gradient Descent dengan Penambahan Variabel Tetap," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 7, no. 3, pp. 359–367, 2023, doi: 10.35870/jtik.v7i3.840.

[64] Schultz, M. G., Eskin, E., Zadok, E., & Stolfo, S. J. (2001). Data mining methods for detection of new malicious executables. *IEEE Symposium on Security and Privacy*.

[65] Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. *Australasian Joint Conference on Artificial Intelligence*.

[66] Islam, R., Tian, R., Batten, L., & Versteeg, S. (2013). Classification of malware based on integrated dynamic and static features. *Journal of Network and Computer Applications*, 36(2), 646–656.

[67] A. Alhussain, Z. Almubaid, H. Mahgoub, and M. El-Baz, "A Malware Obfuscation AI Technique to Evade Antivirus Detection in Counter Forensic Domain," *ResearchGate*, 2020.

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Mahardhika Yudha Pratama

NIM : 201910370311127

Judul TA : Klasifikasi Deteksi Malware Menggunakan Metode Deep Neural Network (DNN)

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	8%
2.	Bab 2 – Daftar Pustaka	25 %	9%
3.	Bab 3 – Analisis dan Perancangan	25 %	11%
4.	Bab 4 – Implementasi dan Pengujian	15 %	13%
5.	Bab 5 – Kesimpulan dan Saran	5 %	0%
6.	Makalah Tugas Akhir	20%	19%

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

(Viola Emylia)