KLASIFIKASI MALWARE PDF MENGGUNAKAN DEEP NEURAL NETWORK PADA LAYANAN GARUDA KEMENDIKBUD SEBAGAI AGREGATOR NASIONAL

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu
Syarat Memperoleh Gelar Sarjana

Oleh :

RISKY WAHYUNI

09011382025158

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

KLASIFIKASI MALWARE PDF MENGGUNAKAN DEEP NEURAL NETWORK PADA LAYANAN GARUDA KEMENDIKBUD SEBAGAI AGREGATOR NASIONAL

Skripsi

Program Studi Sistem Komputer

Jenjang S1

Oleh:

RISKY WAHYUNI

09011382025158

Palembang, 26 Agustus 2024

Pembimbing I	Pembimbing II
Prof. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP. 197806172006041002	**NIP. 199211102023212049**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

AUTHENTICATION PAGE

PDF MALWARE CLASSIFICATION USING DEEP NEURAL NETWORK ON GARUDA KEMENDIKBUD SERVICE AS A NATIONAL AGGREGATOR

THESIS

Dept. of Computer System

Bachelor's Degree

By:

RISKY WAHYUNI

09011382025158

Palembang, 26 August 2024

Supervisor	Co-Supervisor
Prof. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP. 197806172006041002	**NIP. 199211102023212049**

Acknowledge, 26/8/24

Head Of Computer Systems Departement

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah di uji dan lulus pada:

Hari : Selasa

Tanggal : 24 Juli 2024

Tim Penguji :

1. **Ketua : Aditya Putra Perdana Prasetyo, M.T.**
2. **Sekretaris : Iman Saladin B. Azhar, M.MSI.**
3. **Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II : Nurul Afifah, M.Kom.**
5. **Penguji : Huda Ubaya, S.T., M.T.**

Mengetahui, 16/8/24
Ketua Jurusan Sistem Komputer

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

Halaman Pernyataan

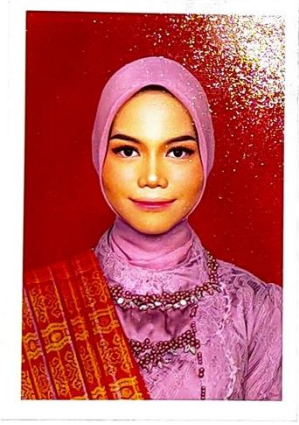
Yang Bertanda Tangan Dibawah Ini:

Nama	:	Risky Wahyuni
Nim	:	09011382025158
Judul	:	Klasifikasi Malware PDF Menggunakan Deep Network Pada Layanan Garuda Kemendikbud Sebagai Agregator Nasional.

Hasil Pengecekan Software *Thenticate/Turnitin*: 2%

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

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



Palembang, 23 Agustus 2024

Risky Wahyuni
Nim. 09011382025158

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh dengan Rahmat dan berkah Allah SWT beserta kedamaianya.

Puji syukur kehadirat Allah SWT, penulis memohon kepada Allah SWT agar dapat menyelesaikan proposal tugas akhir ini yang berjudul **"Klasifikasi Malware PDF Menggunakan Deep Neural Network Pada Layanan GARUDA Kemendikbud Sebagai Agregator Nasional"**

Penulis ingin menyampaikan penghargaan atas pemikiran, saran, dan bantuan yang telah diberikan dalam penyusunan tugas akhir ini. Sehubungan dengan hal tersebut, penulis mengucapkan puji syukur kepada Allah SWT dan yang mulia :

1. Ayahanda Sunardi, yang selalu menjadi panutanku. Ibunda Murtika, malaikat pelindung yang tak pernah lelah mencintaiku. Kalian berdua telah memberikan segalanya untukku, dari kasih sayang yang tulus hingga dukungan yang tak pernah putus. Setiap tetes keringat dan air mata yang kalian curahkan untukku adalah bukti cinta yang tak terhingga. Semoga penulis bisa membahagiakan kalian dan membuat kalian bangga.
2. Bapak Prof Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Prof. Deris Stiawan, M.T., Ph.D., IPU., ASEAN Eng. selaku Dosen Pembimbing I Tugas Akhir yang berkenan meluangkan waktu dalam membimbing, memberikan saran dan motivasi untuk penulis dalam menyelesaikan tugas akhir ini.
5. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir yang berkenan meluangkan waktu dalam membimbing, memberikan saran dan motivasi untuk penulis dalam menyelesaikan tugas akhir ini.
6. Bapak Muhammad Ali Buchari, M.T. selaku Dosen Pembimbing

Akademik.

7. Mba Sari Admin Jurusan Sistem Komputer yang telah membantu dalam mengelola seluruh berkas administrasi.
8. Indra Wikcaksono, yang selalu mendukung penulis pada hari yang tidak mudah selama proses pengerjaan skripsi, terimakasih telah mendengarkan keluh kesah penulis dan berkontrubusi banyak, Terimakasih telah menjadi bagian perjalanan penulis.
9. Teruntuk sahabat, Mayin, Anngun, dinoy, ridoks, depoy, Terimakasih telah menjadi sahabat yang baik, mari tetap bersama meski menjalani hidup masing masing, mari bertemu dan bercerita banyak hal, mari untuk selalu tetap saling menyangi dan selalu mendukung dalam segala hal yang baik.
10. Virginita, Indah, Krisna, Nisa, Cytia, dan Vanesa selaku sahabat yang selalu memberi semangat serta dukungannya. Sehat selaluuu guys ehehe
11. Risky Wahyuni, diri saya sendiri apresiasi sebesar besarnya karna telah bertanggung jawab meyelesaikan skripsi ini, terimakasih karna tidak menyerah dan menikmati setiap prosesnya.
12. Teman-teman seperjuangan SK Unggulan 20
13. Dan semua pihak yang tidak dapat disebutkan satu persatu.
14. Almamater.

penulis berharap semoga laporan tugas akhir ini dapat memberikan manfaat bagi kita semua, khususnya bagi mahasiswa fakultas ilmu komputer universitas sriwijaya, baik secara langsung maupun tidak langsung sebagai kontribusi dalam meningkatkan taraf hidup pengajaran dan penelitian.

Palembang, Agustus 2024
Penulis,

Risky Wahyuni
NIM. 09011382025158

KLASIFIKASI MALWARE PDF MENGGUNAKAN DEEP NEURAL NETWORK PADA LAYANAN GARUDA KEMENDIKBUD SEBAGAI AGREGATOR NASIONAL

Risky Wahyuni (09011382025158)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : riskywahyuni2502@gmail.com

ABSTRAK

Gerba Rujukan Digital (GARUDA) merupakan repositori yang mengelola berbagai karya ilmiah Indonesia, artikel yang tersedia pada repositori GARUDA diterbitkan dalam format PDF yang rentan terhadap serangan malware sehingga membuka peluang bagi *hacker* untuk melakukan kejahatan dengan mencuri data pribadi, merusak file, atau mengambil kendali sistem tanpa izin. Oleh karena itu, penelitian berfokus untuk membedakan file PDF yang aman dengan file PDF berbahaya (*Malware*) penulis akan mengekstrak metadata dari setiap file PDF menggunakan PDFiD, metadata tersebut sebagai ciri (fitur) untuk melakukan klasifikasi *multiclass* dengan menggunakan metode *Deep Neural Network*. Tujuannya adalah untuk mengklasifikasikan file PDF menjadi tiga kategori benign, *malware html, malware PDF.* Evaluasi model pada penelitian ini menggunakan *confusion matrix* dengan menghitung nilai akuras, presisi, racall, dan f1-score, pada penelitian ini melakukan 5 kali skenario pengujian dengan tujuan untuk membadingkan hasil terbaik hyperparameter tunning dari 5 skenario, sehingga didapat hasil terbaik pada scenario 4 dengan nilai akurasi 99.45%, presisi 100%, *recall* 98.36% serta *f1-score* 99.17%.

Kata kunci : PDF Malware, PDFiD, *Multiclass, Deep Neural Network.*

PDF MALWARE CLASSIFICATION USING DEEP NEURAL NETWORK ON GARUDA KEMENDIKBUD SERVICE AS A NATIONAL AGGREGATOR

Risky Wahyuni (09011382025158)
Dept. of Computer System, Faculty of Computer Science, Universitas Sriwijaya
Email : riskywahyuni2502@gmail.com

ABSTRACK

Gerba Rujukan Digital (GARUDA) is a repository that manages various Indonesian scientific works, articles available in the GARUDA repository are published in PDF format which is vulnerable to malware attacks thus opening up opportunities for hackers to commit crimes by stealing personal data, damaging files, or taking control of the system without permission. Therefore, the research focuses on distinguishing safe PDF files from malicious PDF files (Malware) The author will extract metadata from each PDF file using PDFiD, the metadata as a feature to perform multiclass classification using the Deep Neural Network method. The goal is to classify PDF files into three categories benign, html malware, PDF malware. Evaluation of the model in this study using confusion matrix by calculating the value of accuracy, precision, recall, and f1-score, in this study conducted 5 times the test scenario with the aim of comparing the best results of hyperparameter tuning from 5 scenarios, so that the best results were obtained in scenario 4 with an accuracy value of 99.45%, precision 100%, recall 98.36% and f1-score 99.17%.

Keywords: PDF Malware, PDFiD, Multiclass, Deep Neural Network.

DAFTAR ISI

DAFTAR GAMBAR

HALAMAN

DAFTAR TABEL

HALAMAN

BAB I
PENDAHALUAN

1.1 Latar Belakang

Gerba Rujukan digital atau dikenal dengan GARUDA merupakan repositori yang menjadi sumber kumpulan informasi beragam seperti karya tulis ilmiah, tugas akhir mahasiswa, rangkuman studi, matematika, ilmu komputer dan berbagai materi lainnya, seluruh karya yang dikumpulkan direpositori GARUDA merupakan hasil karya anak bangsa Indonesia yang dikelola oleh kementrian ristek dan teknologi (KEMENDIKBUD DIKTI). GARUDA menyediakan lebih dari sajuta publikasi dan jurnal, ada lebih dari 40 bidang yang berbeda mulai dari astronomi, ilmu sosial, hingga Pendidikan [1]. Namun sama seperti platform umumnya, GARUDA juga memiliki risiko keamanan terutama terkait serangan siber. Artikel yang tersedia pada repositori ini diterbitkan dalam format PDF yang rentan terhadap serangan malware sehingga membuka peluang bagi *hacker* untuk melakukan kejahatan dengan mencuri data pribadi, merusak file, atau mengambil kendali sistem tanpa izin. Malware ini bisa menyebar melalui email, situs web, atau perangkat penyimpanan portable [2], Hacker dapat memodifikasi file PDF dengan menyuntikkan muatan berbahaya melalui objek lain dan kompleksitas format PDF untuk menyembunyikan konten berbahaya**.** Contohnya, serangan berbasis JavaScript menyuntikkan kode di berbagai lokasi dalam file untuk menipu pendeteksi, hacker juga menggunakan teknik pengelakan fitur untuk membuat varian malware PDF yang tidak terdeteksi oleh pengklasifikasi yang ada [3].

Dengan demikian penggunaan Deep Neural Network merupakan langkah penting dalam meningkatkan keamanan sistem terhadap ancaman malware, Deep Neural Network sangat akurat dalam menentukan kebenaran dalam malware dengan klasifikasi, terutama saat data tidak seimbang deep neural network mampu memberikan kinerja yang unggul dalam mempelajari fitur secara otomatis untuk menyelesaikan masalah kompleks seperti klasifikasi gambar, teks, dan audio dengan mengahsilkan akurasi yang tinggi. Dalam beberapa tahun terakhir deep neural network telah menjadi salah satu

algoritma paling kuat dan efisien diberbagai bidang termasuk dalam mengklasifikasi malware [4].

Penelitian [5] menggunakan dataset yang terdiri dari 7414 file, dengan 3707 file malware dan 3707 file jinak. Dataset tersebut dilabeli sebagai X dan Y. Penelitian ini mengembangkan model Deep Neural Network (DNN) yang menunjukkan performa terbaik dibandingkan dengan teknik klasifikasi lainnya, serta mampu mengatasi masalah ketidakseimbangan dan overfitting data. Hasil penelitian menunjukkan bahwa model DNN dapat mengklasifikasikan perangkat lunak berbahaya dengan tingkat presisi, akurasi, dan recall yang tinggi, dengan akurasi mencapai 99,42%.

Penelitian [6] menggunakan 1,1 juta sampel malware windows dari koleksi EMBER untuk mengembangkan algoritme deteksi berbasis biner dan tanda tangan dengan deep neural network dan hasilnya menunjukkan akurasi pengujian sebesar 98,53%, mengatasi ketidak seimbangan data antara dataset kecil dan besar. Kesimpulannya, pendekatan deep learning ini dapat menjadi mesin algoritma utama untuk melindungi perangkat digital dari malware dan meningkatkan keamanan siber secara keseluruhan.

Penelitian [7] dataset 10.070 sampel, terdiri dari 3.961 sampel jinak dan 6.109 sampel berbahaya. sampel berbahaya dikumpulkan dari VirusTotal. Kumpulan data tersebut dipisahkan menjadi kumpulan data pelatihan A dan pengujian B. Studi ini bertujuan untuk mengklasifikasikan sampel malware sebagai benign atau malicious menggunakan metode deep learning, terutama CNN-BiLSTM, dengan fokus pada keberhasilan deteksi malware, ketahanan terhadap perubahan konsep, obfuscation packing, dan serangan adversarial. Hasil eksperimen menunjukkan bahwa metode yang diusulkan efektif dalam mendeteksi malware, terutama dalam menghadapi sampel malware yang lebih baru. Model-model yang diuji, seperti CNN-LSTM dan CNN-BiLSTM, menunjukkan kinerja yang baik dalam deteksi malware, dengan CNN-BiLSTM memiliki akurasi tertinggi dalam validasi silang. Metode yang diusulkan juga terbukti lebih tahan terhadap interferensi packing dan serangan adversarial dibandingkan dengan metode berbasis panggilan API Akurasi

tertinggi yang dicapai adalah 95.7% oleh model CNN-BiLSTM pada panjang input 2 juta.

Penelitian ini bertujuan untuk mengindetifikasi malware dalam file PDF menggunakan karateristik khusus dari file PDF GARUDA. karakteristik pada PDF ini dieksekusi menggunakan *pdfid.py* untuk mengetahui dataframenya dan digunakan sebagai dataset untuk melatih model *Deep Neural Network* kemudian dilakukan klasifikasi dan analisis terhadap file PDF yang terindikasi mengadung malware. Sehingga pada Tugas akhir ini penulis akan melakukan penelitian dengan judul **"***Klasifikasi Malware PDF Menggunakan Deep Neural Network Pada Layanan GARUDA Kemendikbud Sebagai Agregator Nasional*"

1.2 Perumusan Masalah

1. Bagaimana proses ekstraksi file dataset PDF GARUDA sebelum di proses menjadi dataset?
2. Bagaimana pengaruh *Random Oversampling* sebagai metode resampling untuk menangani masalah data imbalance pdf malware GARUDA?
3. Bagaimana model *Deep Neural Networks* digunakan untuk mengklasifikasi PDF malware GARUDA?

1.3 Tujuan

Adapun tujuan pada penulisan penelitian ini adalah :

1. Mengekstraksi dataset file PDF Malware GARUDA Menggunakan teknik analisis malware yaitu analisis statis.
2. Menerapkan teknik Random Oversampling pada dataset yang tidak seimbang untuk proses klasifikasi malware PDF.
3. Melakukan evaluasi performa deep neural network dalam klasifikasi serangan file PDF Malware.

1.4 Manfaat

Adapun manfaat pada penulisan penelitian ini adalah :

1. Dataset GARUDA memberikan bahan uji beragam untuk mengembangkan dan mengevaluasi algoritma analisis malware berbasis analisis statis.

2. Memberikan Solusi untuk mengatasi ketidakseimbangan data pada dataset GARUDA, sehingga klasifikasi terhadap serangan file PDF menjadi lebih akurat.
3. Mengevaluasi seberapa baik performa model deep neural networks dalam mengkalasifikasi file PDF GARUDA dengan memeberikan akurasi yang baik.

1.5 Batasan Masalah

Adapun manfaat pada penulisan penelitian ini adalah :

1. Berfokus pada Teknik ekstraksi yang khusus diterapakn pada dataset file pdf garuda.
2. Khusus mengimplentasi random oversampling pada satu model klasifikas yaitu deep neural network.
3. Tidak melibatkan penggunaan metrik lainnya, evaluasi model deep neural network hanya menggunakan matrik evaluasi umum accuracy, precision, recall dan f1-score.
4. Tidak ada pembahasan mengenai upaya untuk mencegah serangan malware pdf.

1.6 Metodologi Penelitian

Dalam penelitian tugas akhir ini akan dilakukan serangkaian tahapan dengan menerapakan metologi sebagai berikut :

1. Pada tahap ini, penelitian dimulai dengan mengkaji literatur yang relvan sesuai dengan penelitian sebelumnya seperti artikel, makalah, jurnal terkait topik yang sama pada klasifikasi malware pdf menggunakan deep neural network.
2. Tahap perancangan sistem

   Tahap ini mencakup pemilihan perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian.
3. Tahap pengujian

   Tahap pengujuan dilakukan menggunakan parameter yang telah ditentukan sesuai dengan batasan masalah.
4. Tahap hasil dan Analisa

Hasil dari pengujian dianalisa untuk mengevalusi kelebihan dan kekuranganya dengan demikian anlisa ini dapat menghasilkan Kesimpulan dan saran sebagai referensi pada penelitian selanjutnya.

5. Tahap kesimpulan dan saran

   Pada tahap akhir ini penulis Menyusun Kesimpulan dari seluruh kegiatan tugas akhir pada penelitian ini, penulis juga akan memberikan saran untuk penelitian yang akan dating.

1.7 Sistematika Penulisan

Berikut ini merupakan sistematika yang digunakan dalam penulisan tugas akhir, yang mendeskripsikan bab-bab yang terdapata dalam tugas akhir :

BAB I **PENDAHULUAN**

Pada BAB I, akan membahas mengenai latar belakang, tujuan penelitian, manfaat penelitian, rumusan masalah, batasan masalah, metologi penelitian dan sistematika penulisan.

BAB II **TINJAUAN PUSAKA**

Pada BAB II, mengkaji literatur yang relvan sesuai dengan penelitian sebelumnya seperti artikel, makalah, jurnal terkait topik yang sama pada klasifikasi malware pdf menggunakan deep neural network.

BAB III **METOLOGI PENELITIA**

Pada BAB III, akan menguraikan tahapan tahapan yang dilakukan dalam penelitian tugas akhir ini, serta menjelaskan rancangan sistem yang digunkan.

BAB I V **HASIL DAN ANALISA**

Pada BAB IV, akan menyajikan hasil dari penelitian pada klasifikasi malware pdf menggunakan deep neural network, dengan memberikan Analisa dari algoritma yang digunakan.

BAB V **PENDAHULUAN**

Pada BAB V, berisi Kesimpulan berdasarkan hasil penelitian yang telah dicapai, serta memberikan saran untuk pengembangan lebih lanjut dalam penelitian mendatang.

DAFTAR PUSTAKA

[1] R. Wahyudin, "Garba Rujukan Digital," vol. 10, no. 1, pp. 62–63, 2010, [Online]. Available: http://garuda.ristekbrin.go.id/documents/detail/480401

[2] C. Liu *et al.*, "A novel adversarial example detection method for malicious PDFs using multiple mutated classifiers," *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301124, 2021, doi: 10.1016/j.fsidi.2021.301124.

[3] H. Bae, Y. Lee, Y. Kim, U. Hwang, S. Yoon, and Y. Paek, "Learn2Evade: Learning-Based Generative Model for Evading PDF Malware Classifiers," *IEEE Trans. Artif. Intell.*, vol. 2, no. 4, pp. 299–313, 2021, doi: 10.1109/tai.2021.3103139.

[4] E. Mbunge, B. Muchemwa, J. Batani, and N. Mbuyisa, "A review of deep learning models to detect malware in Android applications," *Cyber Secur. Appl.*, vol. 1, no. April 2022, p. 100014, 2023, doi: 10.1016/j.csa.2023.100014.

[5] N. Afifah and D. Stiawan, "The Implementation of Deep Neural Networks Algorithm for Malware Classification," *Comput. Eng. Appl. J.*, vol. 8, no. 3, pp. 189–202, 2019, doi: 10.18495/comengapp.v8i3.294.

[6] U. Divakarla, K. H. K. Reddy, and K. Chandrasekaran, "A Novel Approach towards Windows Malware Detection System Using Deep Neural Networks," *Procedia Comput. Sci.*, vol. 215, no. 2022, pp. 148–157, 2022, doi: 10.1016/j.procs.2022.12.017.

[7] W. Qiang, L. Yang, and H. Jin, "Efficient and Robust Malware Detection Based on Control Flow Traces Using Deep Neural Networks," *Comput. Secur.*, vol. 122, p. 102871, 2022, doi: 10.1016/j.cose.2022.102871.

[8] Y. Li, Y. Wang, Y. Wang, L. Ke, and Y. an Tan, "A feature-vector generative adversarial network for evading PDF malware classifiers," *Inf. Sci. (Ny).*, vol. 523, pp. 38–48, 2020, doi: 10.1016/j.ins.2020.02.075.

[9] D. Gibert, J. Planes, C. Mateu, and Q. Le, "Fusing feature engineering and

deep learning: A case study for malware classification," *Expert Syst. Appl.*, vol. 207, no. April 2021, p. 117957, 2022, doi: 10.1016/j.eswa.2022.117957.

[10] T. Tsafrir, A. Cohen, E. Nir, and N. Nissim, "Efficient feature extraction methodologies for unknown MP4-Malware detection using Machine learning algorithms," *Expert Syst. Appl.*, vol. 219, no. May 2022, p. 119615, 2023, doi: 10.1016/j.eswa.2023.119615.

[11] X. Ling *et al.*, "Adversarial attacks against Windows PE malware detection: A survey of the state-of-the-art," *Comput. Secur.*, vol. 128, p. 103134, 2023, doi: 10.1016/j.cose.2023.103134.

[12] A. Charim, S. Basuki, and D. R. Akbi, "Detect Malware in Portable Document Format Files (PDF) Using Support Vector Machine and Random Decision Forest," *J. Online Inform.*, vol. 3, no. 2, p. 99, 2019, doi: 10.15575/join.v3i2.196.

[13] A. Syukron and A. Subekti, "Penerapan Metode Random Over-Under Sampling dan Random Forest Untuk Klasifikasi Penilaian Kredit," *J. Inform.*, vol. 5, no. 2, pp. 175–185, 2018, doi: 10.31311/ji.v5i2.4158.

[14] E. M. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb, "MalDozer: Automatic framework for android malware detection using deep learning," *DFRWS 2018 EU - Proc. 5th Annu. DFRWS Eur.*, vol. 24, pp. S48–S59, 2018, doi: 10.1016/j.diin.2018.01.007.

[15] N. Verbiest, E. Ramentol, C. Cornelis, and F. Herrera, "Preprocessing noisy imbalanced datasets using SMOTE enhanced with fuzzy rough prototype selection," *Appl. Soft Comput. J.*, vol. 22, pp. 511–517, 2014, doi: 10.1016/j.asoc.2014.05.023.

[16] N. H. Latifah, A. Silvia, E. Prihatini, S. Nurmaini, and I. Yani, "Swarm Intelligent in Bio-Inspired Perspective: A Summary," *Comput. Eng. Appl. J.*, vol. 7, no. 2, pp. 105–120, 2018, doi: 10.18495/comengapp.v7i2.255.

[17] Wirogatama, "Arsitektur Neural Network," *Archit. Neural Netw.*, pp. 181–

211, 2019.

[18] “Knowledge is Power in Four Dimensions: Models to Forecast Future Paradigm,” *Knowledge is Power in Four Dimensions: Models to Forecast Future Paradigm*. 2022. doi: 10.1016/c2021-0-02583-9.

[19] B. A. B. Ii and P. J. Komputer, “LANDASAN TEORI 1 . Local area network (LAN),” pp. 5–29, 2013, [Online]. Available: https://repository.bsi.ac.id/index.php/unduh/item/2416/file_10-babII-landasan-teori.pdf

[20] T. Wongvorachan, S. He, and O. Bulut, “A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining,” *Information*, vol. 14, p. 54, Jan. 2023, doi: 10.3390/info14010054.

[21] M.-C. Popescu, V. Balas, L. Perescu-Popescu, and N. Mastorakis, “Multilayer perceptron and neural networks,” *WSEAS Trans. Circuits Syst.*, vol. 8, Jul. 2009.