IMPLEMENTASI FITUR SELEKSI PADA MALWARE DENGAN DEEP NEURAL NETWORK

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

AHMAD NAUFAL IRFAN
090113817221

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2023

LEMBAR PENGESAHAN

IMPLEMENTASI FITUR SELEKSI PADA MALWARE DENGAN DEEP NEURAL NETWORK

TUGAS AKHIR

Diajukan untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

AHMAD NAUFAL IRFAN

09011381722102

Palembang, 31 Juli 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T. 9/8/23	Ahmad Heryanto, S.Kom., M.T
NIP. 196612032006041001	NIP. 198701222015041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Senin

Tanggal : 31 Juli 2023

Tim Penguji:

1. **Ketua Sidang** : **Rossi Passarella, S.T. M.Eng**
2. **Sekretaris Sidang** : **Muhammad Ali Buchari, S.Kom., M.T.**
3. **Penguji Sidang** : **Dr. Ir. H. Sukemi, M.T.**
4. **Pembimbing** : **Ahmad Heryanto, S.Kom., M.T.**

Mengetahui, 4/10/23
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 19661203200641001

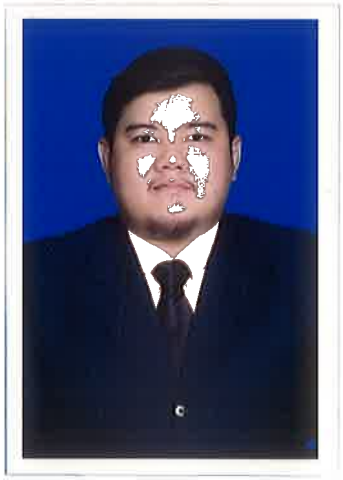
HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Ahmad Naufal Irfan
NIM	: 09011381722102
Program Studi	: Sistem Komputer
Judul	: Implementasi Fitur Seleksi Pada Malware Dengan Deep Neural Network

Hasil pengecekan *Software iThentivate/Turnitin* : 10%

Menyatakan Bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan dan plagiat. Apabila ditemukkan hasil penjiplakan atau plagiat dalam laporan ini tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, 03 Agustus 2023

Ahmad Naufal Irfan
09011381722102

MOTTO DAN PERSEMBAHAN

MOTTO:

JANGAN TERLALU LAMA LARUT DALAM KESEDIHAN PADA SEBUAH MASALAH, KARNA ADA BANYAK ORANG YANG MENUNGGU KITA UNTUK BANGKIT DAN BERKREATIVITAS KEMBALI

"Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya. Dia mendapat (pahala) dari (kebajikan) yang dikerjakannya dan dia mendapat (siksa) dari (kejahatan) yang diperbuatnya." (QS. Al-Baqarah 286)

KU PERSEMBAHKAN UNTUK:

- ORANG TUA SAYA YANG 3T (TERCINTA, TERSAYANG DAN TERKEREN) DAN KELUARGA SAYA YANG SELALU MENDUKUNG DAN JUGA MEMBERIKAN SEMANAGAT KEPADA SAYA.
- TEMAN-TEMAN SEPERJUANGAN SISTEM KOMPUTER UNIVERSITAS SRIWIJAYA YANG TIDAK AKAN TERLUPAKAN
- ALMAMATERKU UNIVERSITAS SRIWIJAYA

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan Proposal Tugas Akhir ini dengan judul "Implementasi Fitur Seleksi Pada *Malware Dengan Deep Neural Network*"

Dalam laporan ini penulis menjelaskan mengenai penerapan metode Teknik Seleksi Fitur dan penerapan algoritma *Deep Neural Network* untuk klasifikasi *malware*. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti tentang *malware* serta penerapan Seleksi Fitur dan klasifikasi *malware*.

Pada penyusunan proposal tugas akhir ini, tidak terlepas dari bantuan, bimbingan serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan kemudahan, kesehatan, serta kesempatan dalam pelaksanaan pembuatan Tugas Akhir ini.
2. Ibu, Ayah serta Adik- adikku dan seluruh keluarga tercinta yang telah memberikan dukungan dan nasehat-nasehat serta motivasi selama ini. Terima kasih atas dukungan baik berupa moral, material, maupun spiritual.
3. Bapak Jaidan Jauhari, S.Pd., M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakutas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T selaku Pembimbing Tugas Akhir Penulis. Terima kasih karena telah meluangkan waktunya untuk membimbing penulis, dalam menyelesaikan tugas akhir ini serta telah memberikan bimbingan dan nasehat selama perkuliahan.
6. Seluruh Dosen dan Staff Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.
7. Teman-teman yang selalu memberikan support, Tata, Nawawi, Hafidz, Marle, Hadi, Diyon Fidya, Atsna, Wirandy, Aqila dan lain-lainnya.
8. Teman-teman dari Komunitas White Tiger dan Empire IDP.
9. Teman-teman seperjuangan angkatan 2017 dan anak-anak SK17 indralaya dan Palembang khususnya yang selalu membersamai selama perkuliahan ini.

10. Serta semua pihak yang telah membantu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas akhir ini. Terima kasih banyak semuanya.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan Tugas Akhir ini, baik dari materi maupun teknik penyajiannya, mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu, penulis mengharapkan adanya kritik dan saran yang membangun agar dapat memperbaiki kekurangan-kekungan tersebut kedepannya nanti.

Akhir kata dengan segala keterbatasan, penulis berharap semoga penulisan Tugas Akhir ini dapat menjadi tambahan wawasan dan ilmu pengetahuan bagi mahasiswa yang memerlukan khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Palembang, 03 Agustus 2023

Penulis

IMPLEMENTASI FITUR SELEKSI PADA MALWARE DENGAN DEEP NEURAL NETWORK

Ahmad Naufal Irfan (09011381722102)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : ahmadnaufal1201@gmail.com

ABSTRAK

Malware adalah perangkat lunak berbahaya yang mengacu pada program yang secara sengaja mengeksploitasi kerentanan dalam sistem komputasi untuk tujuan yang berbahaya, Deep Neural Network adalah sebuah Artificial Neural Network dengan beberapa lapisan antara lapisan input dan output, Deep Neural Network sudah menjadi alternatif pembelajaran Machine Learning karena kemajuan yang signifikan dalam algoritma pelatihan Deep Neural Network dapat menemukan manipulasi matematis yang benar untuk mengubah input menjadi output, apakah itu hubungan linear atau hubungan non-linear. Jaringan bergerak melalui lapisan- lapisan yang menghitung probabilitas setiap keluaran. Seleksi fitur digunakan untuk mengurangi dimensi informasi dan fitur-fitur yang tidak relevan ataupun juga untuk mempertinggi efektifitas dan efisiensi kapabilitas dari algoritma klasifikasi .

Ransomeware adalah perangkat lunak berbahaya yang berupaya mengenkripsi file dan menahannya untuk tebusan. Pengguna harus membayar peretas untuk mendapatkan kembali akses ke file seperti gambar, video atau dokumen penting. Ransomware ini juga terdapat beberapa jenis malware yaitu Charger, Jisut, Koler, LockerPin, WannaLocker, PornDroid dan lain lain Dengan dilakukannya seleksi fitur terhadap hasil dari visualisasi data dapat mengurangi atribut yang tidak penting atau tidak relevan dalam data. Fitur seleksi univariate dipilih berdasarkan nilai korelasi yang tinggi dan baik. Dapat dilihat juga dalam setiap percobaan klasifikasi bahwa dengan menggunakan algoritma Deep neural network dengan pendekatan F1 Score dan tingkat akurasi yang tinggi

Kata Kunci *: Malware, Ransomware, Lockerpin, Deep Neural Network,* Seleksi Fitur

IMPLEMENTATION OF SELECTION FEATURE ON MALWARE WITH DEEP NEURAL NETWORK

Ahmad Naufal Irfan (09011381722102)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : ahmadnaufal1201@gmail.com

ABSTRACT

Malware is malicious software that refers to programs that deliberately exploit vulnerabilities in computing systems for malicious purposes, Deep Neural Network is an Artificial Neural Network with several layers between the input and output layers, Deep Neural Network has become an alternative to Machine Learning because of advances significant in the Deep Neural Network training algorithm can find the correct mathematical manipulations to convert inputs into outputs, whether it is a linear relationship or a non-linear relationship. The network moves through layers calculating the probability of each output. Feature selection is used to reduce information dimensions and irrelevant features or also to increase the effectiveness and efficiency capabilities of the classification algorithm.

Ransomeware is malicious software that attempts to encrypt files and holds them for ransom. Users have to pay hackers to regain access to files such as images, videos or important documents. This ransomware also has several types of malware, namely Charger, Jisut, Koler, LockerPin, WannaLocker, PornDroid and others. By selecting features, the results of data visualization can reduce attributes that are not important or irrelevant in the data. Univariate selection features are selected based on high and good correlation values. It can also be seen in each classification experiment that by using the Deep neural network algorithm with the F1 Score approach and a high degree of accuracy

Keyword : Malware, Ransomware, Lockerpin, Deep Neural Network, feature selection

DAFTAR ISI

HALAMAN

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Keamanan informasi merupakan suatu hal penting dalam era digital yang mengintegrasikan semua aspek ke dalam internet. Beberapa aspek yang harus dijaga dalam sebuah informasi yaitu Confidentiality, Integrity, Avaibility, Authentication, Authorization dan Non Repudation untuk memastikan bahwa informasi tersebut tidak terserang oleh pelaku kejahatan internet [1] Suatu informasi dapat dipastikan aman sangatlah sulit dikarenakan banyaknya penjahat internet yang berusaha untuk menyerang suatu system [2]. Analisa dinamis dari sebuah trafik di dalam internet diperlukan untuk mengetahui ancaman serangan malware dengan memerhatikan perilakunya di dalam jaringan internet[3]. Data trafik internet yang berjumlah banyak membuat proses analisa dinamis secara manual sulit untuk dilakukan, sehingga perlu adanya sebuah algoritma Machine Learning yang dapat memeriksa banyak trafik sekaligus.

Malware adalah perangkat lunak berbahaya yang mengacu pada program yangsecara sengaja mengeksploitasi kerentanan dalam sistem komputasi untuk tujuan yangberbahaya [4]. Dengan komputer dan Internet yang sudah menjadi bagian penting dalam kehidupan sehari-hari, malware merupakan ancaman serius bagi keamanan setiap pengguna komputer. Malware terus memfasilitasi serangan cyber, dimana sebagai penyerang, malware tetap menjadi salah satu alat utama kampanye mereka. Oleh karena itu, Untuk melawan penjahat cyber, penting bagi para pembela untuk memahami perilaku malware, seperti pola penyebaran atau rekrutmen keanggotaan, ukuran botnet, dan distribusi bot [5].

Berbagai kategori pendekatan deteksi telah diusulkan, termasuk *Signature Based*, yang membutuhkan aturan buatan tangan sendiri untuk bendapatkan data yang relevan agar bisa melakukan deteksi, dan *Machine Learning*, yang secara otomatis memberikan alasan tentang data *Malware* dan

Benignware agar sesuai dengan parameter model deteksi [6]. Sampai saat ini, komputer industri keamanan lebih memilih menggunakan metode *Signature Based* karena dilihat dari tingkat *Low False Positive Rates* yang dapat dicapai oleh metode tersebut. Namun, dalam beberapa tahun terakhir, *Machine Learning* berhasil mencapai deteksi tingkat tinggi pada tingkat *Low False Positive Rates* tanpa beban generasi tangan manusia yang diperlukan dengan metode manual.

Seleksi Fitur merupakan suatu proses untuk mengurangi dimensi atribut. Pengurangan dimensi tersebut dilakukan untuk mendapatkan atribut-atribut yang relevan dan tidak berlebihan sehingga dapat mempercepat proses klasifikasi dan dapat meningkatkan akurasi dari algoritme klasifikasi[7]. Pada penelitian [8], mengusulkan sebuah pendekatan berbasis pembelajaran mesin yang efektif untuk *Android Malware* Deteksi menggunakan algoritma genetika evolusioner untuk pemilihan fitur diskriminatif. Hasil eksperimen memvalidasi itu Algoritma genetik memberikan bantuan subset fitur yang paling optimal pengurangan dimensi fitur menjadi kurang dari setengah aslinya set fitur. Akurasi klasifikasi lebih dari 94% adalah pemilihan fitur postingan yang dipertahankan untuk berbasis pembelajaran mesin pengklasifikasi, saat mengerjakan dimensi fitur yang jauh berkurang, dengan demikian, berdampak positif pada kompleksitas komputasi pengklasifikasi belajar.

Saat ini, dengan peningkatan jumlah malware yang dihasilkan setiap hari, kebutuhan untuk metode yang lebih otomatis dan cerdas untuk belajar, beradaptasi, dan menangkap malware sangat penting, sejumlah solusi mutakhir ditawarkan para perusahaan keamanan untuk mencegah serangan malware berbahaya. Yang terbaru adalah kapabilitas *Machine Learning* untuk menangkal *Malware* secara real-time. *Machine Learning* sendiri adalah sebuah cabang aplikasi dari kecerdasan buatan yang fokus pada pengembangan sebuah sistem yang mampu belajar "sendiri" tanpa harus berulang kali di program oleh manusia. Salah satu arsitektur kerja dari *Machine Learning* adalah *Artificial Neural Network*, yang merupakan sistem komputasi yang diilhami oleh jaringan saraf biologis yang memiliki struktur seperti otak hewan, sedangkan *Deep Neural Network* memiliki struktur yang lebih rumit.

Deep Neural Network adalah sebuah *Artificial Neural Network* dengan

beberapalapisan antara lapisan input dan output, *Deep Neural Network* sudah menjadi alternatif pembelajaran *Machine Learning* karena kemajuan yang signifikan dalam algoritma pelatihan [9]. *Deep Neural Network* dapat menemukan manipulasi matematis yang benar untuk mengubah input menjadi output, apakah itu hubungan linear atau hubungannon-linear. Jaringan bergerak melalui lapisan- lapisan yang menghitung probabilitas setiap keluaran.

1.2. Rumusan Masalah

1. Bagaimana Menerapkan Proses Deep neural Network dalam Sistem identefikasi Malware ?
2. Bagaimana Mendaptkan hasil accuracy yang tinggi dalam sistem pendeteksian Malware berbasis DNN ?

1.3. Tujuan

Berdasarkan uraian diatas, maka peneliti akan memiliki tujuan yang dapat dicapaidari tugas akhir ini adalah sebagai berikut :

1. Menerapkan metode *Deep Neural Network* dalam sistem Deteksi Malware.
2. Sistem Deteksi Malware Berbasis Metode *Deep Neural Network* mendapatkan nilai Accuracy yang tinggi.

1.4. Manfaat

Adapun manfaat dari penelitian tugas akhir yang dilakukan, antara lain:

1. Dapat memperoleh tingkat akurasi dari proses fitur seleksi dalam klasifikasi

   malware .
2. Dapat mempelajari proses fitur seleksi dalam klasifikasi *malware*.

1.5. Batasan Masalah

Dari rumusan masalah dan latar belakang penelitian, maka berikut ini batasan masalah pada tugas akhir, antara lain :

1. Data yang digunakan dalam penelitian ini merupakan data *Malware*

Ransomware baru yang disebut CICAndMal2022[9].

2. Mengklasifikasikan menggunakan fitur seleksi *Univariate* dengan algoritma *Deep Nueral Network.*.

1.6. Metodologi Penelitian

Berikut adalah tahapan penelitian yang dilakukan untuk mencapai tujuan penelitian tugas akhir ini:

1. Tahap Pertama (Studi Pustaka/ Literatur)

   Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevanuntuk dijadikan sebagai penelitian, dengan mambaca artikel atau makalah penelitian yang berhubungan langsung dengan tugas akhir.
2. Tahap Kedua (Prosesing pengubahan data PCAP ke csv menggunakan CICFLOWMETER) Tahap ini membahas mengenai proses untuk mempersiapkan data yang akan digunakan.
3. Tahap Ketiga (Pengujian)

   Tahap ini merupakan tahap lanjutan dari proses tahap kedua yang telah dilakukan. Dengan melakukan pengujian berdasarkan fitur seleksi dan tidak memakai fitur seleksi dengan algoritma *Deep Neural Network.*.
4. Tahap Keempat (Analisa)

   Data yang diperoleh dari proses pengujian, kemudian dianalisis, sehingga didapatkan hasil data yang objektif dimana data diperoleh dari hasil pengujian.
5. Tahap kelima (Kesimpulan dan Saran)

   Pada tahap ini adalah membuat kesimpulan dari permasalahan, studi pustaka, metodologi, dan analisa hasil pengujian serta membuat beberapa saran yang dapat dijadikan penelitian selanjutnya.

1.7. Sistematika Penulisan

Pada penelitian tugas akhir ini peneliti akan menggunakan sistematikapenulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini akan menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, asumsi,metodelogi penelitian serta sistematika penulisan.

BAB II. LANDASAN TEORI

Bab ini akan membahas berbagai konsep dasar dan teori-teori yang berkaitan dengantopik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernahdilakukan sebelumnya termasuk sintesisnya.

BAB III. METODOLOGI

Bab ini akan menjelaskan tentang langkah-langkah (metodologi) perancangansoftware yang akan dibahas serta merancang aplikasi yang akan dibangun.

BAB IV. HASIL DAN ANALISA

Bab ini akan membahas mengenai hasil dari pengujian yang telah dilakukan

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan TugasAkhir.

DAFTAR PUSTAKA

[1] J Pujoseno, “Implementasi Deep Learning menggunakan Convolutional NeuralNetwork untuk Klasifikasi Alat Tulis" *ieexplore*, vol. 4, no. 3, pp. 1–13, 2018, [

[2] B latupono, “Implementasi Deep Learning Menggunakan Convolution Neural Network untuk Klasidikasi Gambar,” *Bitkom Res.*, vol. 63, no. 2, pp. 1–3, 2018,

[3] A. Tedyyana and S. Supria, “Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway,” *INOVTEK Polbeng - Seri Inform.*, vol.3, no. 1, p. 34, 2018, doi: 10.35314/isi.v3i1.340.

[4] S. K. David Snyder, Daniel Garcia-Romero, Gregory Sell, Daniel Povey, “X-Vectors:Robust DNN Embeddings for Speaker Recognition,” *ieeexplore*, 2018. https://ieeexplore.ieee.org/abstract/document/8461375

[5] F. Mahmud Kalash, Mrigank Rochan, Noman Muhammad, Neil DB Bruce, YangWang, “Klasifikasi Malware dengan Deep Convolutional Neural Networks,” *ieexplore*, 2018. https://ieeexplore.ieee.org/abstract/document/8328749

[6] C. P. M. Yeo, Y. Koo, Y. Yoon, T. Hwang, J. Ryu, J. Song, “Flow-based malwaredetection using convolutional neural network,” *ieeexplore*, 2018. https://ieeexplore.ieee.org/abstract/document/8343255 (accessed Jun. 02, 2023).

[7] R. B. and J. M. Anam Fatima, Ritesh Maurya, Malay Kishore Dutta, “Deteksi MalwareAndroid Menggunakan Algoritma Genetika Berbasis Seleksi Fitur yang Dioptimalkan dan Pembelajaran Mesin,” *ieeexplore*, 2019. https://ieeexplore.ieee.org/abstract/document/8769039 (accessed May 30, 2023).

[8] S. Z. M. S. Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, “Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-randomsubspace selection,” *sciencedirect*, 2019.

https://www.sciencedirect.com/science/article/abs/pii/S0167739X18321101

[9] K. Ivanedra and M. Mustikasari, "Implementasi Metode Recurrent Neural Network Pada Text the Implementation of Text Summarization With Abstractive," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 4, 2019, doi: 10.25126/jtiik.201961067.

[10] P. A. Nugroho, I. Fenriana, and R. Arijanto, "Implementasi Deep Learning Menggunakan Convolutional Neural Network (Cnn) Pada Ekspresi Manusia," *Algor*,vol. 2, no. 1, pp. 12–21, 2020.

[11] Zhou, Yang, and Wang, "Deep Learning untuk Deteksi Wajah yang Berhijab Menggunakan Algoritma Convolutional Neural Network (CNN) dengan Tensorflow," *file:///C:/Users/VERA/Downloads/ASKEP_AGREGAT_ANAK_and_REMAJA_PRINT. docx*, vol. 21, no. 1, pp. 1–9, 2020.

[12] M. A. P. Luis Francisco Martin Liras, Adolfo Rodriguez de Soto, "Feature analysis fordata-driven APT-related malware discrimination," *sciencedirect*, 2021. https://www.sciencedirect.com/science/article/abs/pii/S0167404821000262?via%3Dih ub (accessed May 30, 2023).

[13] D. Efriyani and F. Panjaitan, "Klasifikasi Malware Dengan Menggunakan RecurrentNeural Network," *J. Ilm. Matrik*, vol. 23, no. 3, pp. 310–316, 2021, doi: 10.33557/jurnalmatrik.v23i3.1592.

[14] A. K. Anson Pinhero, Anupama M L, Vinod P, CA Visaggio c, Aneesh N, Abhijith S,"Deteksi malware dilakukan dengan visualisasi dan deep neural network," *sciencedirect*, 2021. https://www.sciencedirect.com/science/article/abs/pii/S0167404821000717

[15] S. S. Lad and A. C. Adamuthe, "Malware classification with improved convolutionalneural network model," *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 6, pp. 30–43, 2020, doi: 10.5815/ijcnis.2020.06.03.

[16] A. T. David Bau, Jun-Yan Zhu, Hendrik Strobelt, "Understanding the role of individual units in a deep neural network," *pnas*, 2020. https://www.pnas.org/doi/abs/10.1073/pnas.1907375117 (accessed Jun. 02, 2023).

[17] R. Yunanto, A. P. Purfini, and A. Prabuwisesa, "Survei Literatur: Deteksi Berita PalsuMenggunakan Pendekatan Deep Learning," *J. Manaj. Inform.*, vol. 11, no. 2, pp. 118–130, 2021, doi: 10.34010/jamika.v11i2.5362.

[18] H. A. Pratiwi, M. Cahyanti, and M. Lamsani, "Implementasi Deep Learning Flower Scanner Menggunakan Metode Convolutional Neural Network," *Sebatik*, vol. 25, no.1, pp. 124–130, 2021, doi: 10.46984/sebatik.v25i1.1297.

[19] A. Ramdan, N. Widyasono, and H. Mubarok, “Prediksi Jaringan TOR dan VPN menggunakan Algoritma K-Nearest Neighbour pada Trafik Darknet,” *J. Sist. Cerdas*,vol. 05, no. 01, pp. 21–35, 2022.

[20] Dedi Natawijaya, “ANALISA ANCAMAN SERANGAN MALWARE PADA TRAFIK DARKNET MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBOR,” *Eprints repository software*, 2022. http://repositori.unsil.ac.id/4696/

[21] I. Shhadat, B. Bataineh, A. Hayajneh, and Z. A. Al-Sharif, “The Use of MachineLearning Techniques to Advance the Detection and Classification of Unknown Malware,” *Procedia Comput. Sci.*, vol. 170, no. 2019, pp. 917–922, 2020, doi: 10.1016/j.procs.2020.03.110.

[22] A. Kartono, A. Sularsa, and S. J. I. Ismail, “Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf,” vol. 5, no. 1, pp. 146–151, 2019, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/ view/8563/8431

[23] A. H. Lashkari, A. F. A. Kadir, L. Taheri, and A. A. Ghorbani, “Toward Developing a Systematic Approach to Generate Benchmark Android Malware Datasets and Classification,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2018-Octob, no. Cic,pp. 1–7, 2018, doi: 10.1109/CCST.2018.8585560.

[24] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun, and S. Ahmed, “Ransomware: A framework for security challenges in internet of things,” *2020 2nd Int. Conf. Comput.Inf. Sci. ICCIS 2020*, 2020, doi: 10.1109/ICCIS49240.2020.9257660.

[25] A. Harris and E. Rosanda, “Optimalisasi Seleksi Fitur Untuk Deteksi Serangan Pada IoT Menggunakan Classifier Subset Evaluator,” vol. 9, no. 4, pp. 885–893, 2022, doi:10.30865/jurikom.v9i4.4618.

[26] R. Sistem, M. D. Anasanti, K. Hilyati, and A. Novtariany, “Exploring feature selectiontechniques on Classification Algorithms for Predicting Type 2

Diabetes at Early Stage," vol. 5, no. 158, pp. 832–839, 2022.

[27] E. Ravi and M. U. Kumar, "A COMPARATIVE STUDY ON MACHINE LEARNING AND DEEP LEARNING METHODS FOR MALWARE DETECTION," vol. 100, no. 20, 2022.

[28] B. A. L. I. S. Al-rimy and M. A. Maarof, "A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction," vol. 8, 2020.

[29] "BOE-A-2011-16466.pdf."

[30] D. Ariyoga, R. Kurniawan, and A. Arifin, "Perbandingan Metode Seleksi Fitur Filter,"2022.

[31] J. M. Vidal, M. A. Sotelo Monge, and L. J. García Villalba, "Detecting workload- based and instantiation-based economic denial of sustainability on 5G environments,"*ACM Int. Conf. Proceeding Ser.*, no. August, 2018, doi: 10.1145/3230833.3233247.

[32] D. R. Sari, D. Teknik, I. Universitas, and I. Kalimantan, "Aplikasi Penerapan MetodeNeural Network Bahan Bakar Industri," vol. 16, no. 1, pp. 47–60, 2015.

[33] A. B. Mutiara and R. Refianti, *Buku Saku: PENGANTAR DEEP NEURAL NETWORKUNTUK SISTEM CERDAS Fetal Heartbeat Detector View project Similarity Analysisof Taekwondo Movement Using Data Motion View project*, no. September. 2018. [Online]. Available: https://www.researchgate.net/publication/327550451

[34] "TIPE JALAN MENGGUNAKAN ALGORITMA DEEP NEURAL NETWORK (DNN) SKRIPSI Oleh : FAIQ NUKHA," 2019.

[35] V. Amrizal and Q. Aini, *Naskah Kecerdasan Buatan_2*. 2013.

[36] R. M. Kosanke, "**済無**No Title No Title No Title," 2019.

[37] A. Raup, W. Ridwan, Y. Khoeriyah, S. Supiana, and Q. Y. Zaqiah, "Deep Learning dan Penerapannya dalam Pembelajaran," *JIIP - J. Ilm. Ilmu*

Pendidik., vol. 5, no. 9, pp.3258–3267, 2022, doi: 10.54371/jiip.v5i9.805.

[38] X. Zhou, J. Pang, and G. Liang, "Image classification for malware detection usingextremely randomized trees," *Proc. Int. Conf. Anti-Counterfeiting, Secur. Identification, ASID*, vol. 2017-Octob, no. 61472447, pp. 54–59, 2018, doi: 10.1109/ICASID.2017.8285743.

[39] R. Arief, "Klasifikasi Audio Ucapan Emosional Menggunakan Model LSTM," *Konf.Nas. Ilmu Komput.*, pp. 524–529, 2021.