DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA PROTOCOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *DEEP NEURAL NETWORK* (DNN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

Mohammad At'thawri Abel Fahd

09011381924141

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA PROTOCOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN *METODE DEEP NEURAL NETWORK* (DNN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Program Studi Sistem Komputer
Jenjang S1

Oleh:

Mohammad At'thawri Abel Fahd
09011381924141

Palembang, 27 Mei 2024

Mengetahui,
Ketua Jurusan Sistem Komputer

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

Pembimbing Tugas Akhir

Prof. Deris Stiawan, M.T., Ph.D
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jum'at

Tanggal : 17 Mei 2024

Tim Penguji

1. Ketua : Huda Ubaya, M.T.
2. Sekretaris : Nurul Afifah, S.Kom., M.Kom.
3. Penguji : Dr. Ahmad Zarkasi, M.T.
4. Pembimbing : Prof. Deris Stiawan, M.T., Ph.D.

Mengetahui, 27/5/24

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

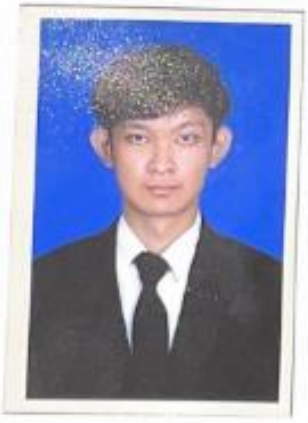
Nama : Mohammad At'thawri Abel Fahd

NIM : 09011381924141

Judul : Deteksi serangan *Denial of Service* (DoS) pada protocol jaringan IEC 61850 *Supervisory Control and Data Acquisition* (SCADA) dengan menggunakan metode *Deep Neural Network* (DNN)

Hasil Pengecekan Plagiat/Turnitin: 4%

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 adanya paksaan dari pihak manapun.



Palembang, Mei 2024

Mohammad At'thawri Abel Fahd

NIM. 09011381924141

KATA PENGANTAR

Segala puji dan syukur penulis ucapkan kepada Allah SWT, karena berkat rahmat dan karunia-Nyalah penulis dapat menyelesaikan tugas akhir ini dengan judul "Deteksi Serangan *Denial of Service* (DOS) pada Protocol Jaringan IEC 61850 *Supervisory Control and Data Acquisition* (SCADA) dengan menggunakan Metode *Deep Neural Network* (DNN)". Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW. beserta keluarga, Sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Pada kesempatan ini, penulis juga mengucapkan terima kasih kepada seluruh pihak yang telah membantu, membimbing, dan terus mendukung penulis dalam menyelesaikan tugas akhir ini diantaranya:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusul tugas akhir ini.
2. Kedua orang tua penulis yang selalu memberikan doa tebaik serta dukungan secara moril dan materil.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Sekretaris Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Iman Saladin B. Azhar, S.Kom., M.MSI., selaku Dosen Pembimbing Akademik.
7. Prof. Deris Stiawan, S.Kom., M.T., Ph.D., IPU., ASEAN-Eng. selaku Pembimbing tugas akhir.
8. Mbak Sari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal administrasi selama perkuliahan.
9. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmunya serta pengalamannya kepada penulis.

10. Teman-teman sebimbingan, Zaman, Dendi dan rezky yang banyak mendengarkan keluh kesah penulis dan menemani proses pengerjaan skripsi.
11. BACOD Mobile dan PDAK, teman-teman yang selalu ada di masa suka dan duka.
12. Winnie, Sandra, Gem, Pontana, Farid, Fadhiel, Syahir, Zhofran dan seluruh sahabat penulis yang selalu memberi dukungan yang tidak bisa penulis sebutkan satu persatu
13. Teman-teman sekelas SK19 Bukit Universitas Sriwijaya, Terimakasih untuk setiap kebersamaan dan bantuannya selama mengerjakan tugas akhir dan perkuliahan.
14. Kakak-kakak tingkat yang satu riset dengan terima kasih telah membantu penulis menyelesaikan tugas akhir ini.
15. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'anya dalam penyelesaian tugas akhir.

Kesempurnaan hanya milik Allah dan Rasul-nya, kesalahan, dan kekhilafan pasti selalu ada menghampiri setiap manusia terutama diri penulis pribadi. Maka dari itu jikalau dalam penulisan tugas akhir ini masih terdapat banyak kekurangan dan kesalahan. Penulis meminta kritik dan saran yang membangun dengan harapan agar dapat perbaiki di masa yang akan datang, dan semoga tulisan ini dapat bermanfaat bagi semuanya.

Palembang, Mei 2024
Penulis,

Mohammad At'thawri Abel Fahd
NIM. 09011381924141

DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA PROTOCOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *DEEP NEURAL NETWORK* (DNN)

MOHAMMAD AT'THAWRI ABEL FAHD (09011381924141)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : abelfahd@gmail.com

ABSTRAK

Deteksi serangan DoS penting untuk dilakukan karena pada jaringan SCADA yang dipakai pada perusahaan besar sehingga membuatnya rentan untuk diserang. Pada penelitian ini, digunakan metode *deep neural network* (DNN) untuk mendeteksi serangan DoS dalam dataset. Dataset yang digunakan pada penelitian ini merupakan *IEC61850SecurityDataset in 2019* yang berisi data protocol GOOSE pada jaringan SCADA yang sudah terkontaminasi DoS . Dataset diseimbangkan menggunakan teknik *oversampling*. Model tersebut menunjukkan hasil yang kurang memuaskan pada perbandingan data 70:30 dan mendapatkan hasil yang memuaskan pada perbandingan data 80:20, dengan akurasi 96,75%, *precision* 100%, *recall* 93,46 dan *f1 score* 96,62%. Hasil ini dapat menunjukkan bahwa model yang dipakai memiliki kinerja konsisten dan dapat diandalkan dalam tugas deteksi.

Kata Kunci : *Supervisory Control and Data Acquisition*, Deteksi Serangan, *Denial of Service*, *Deep Neural Network*

DENIAL OF SERVICE (DOS) ATTACK DETECTION ON IEC 61850 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK PROTOCOL USING DEEP NEURAL NETWORK (DNN) METHOD

MOHAMMAD AT'THAWRI ABEL FAHD (09011381924141)

Computer Engineering Department, Computer Science Faculty

Sriwijaya University

Email : abelfahd@gmail.com

ABSTRACT

DoS attack detection is important because SCADA networks are used in large companies, making them vulnerable to attack. In this research, the deep neural network (DNN) method is used to detect DoS attacks in the dataset. The dataset used in this study is the IEC61850SecurityDataset in 2019 which contains GOOSE protocol data on SCADA networks that have been contaminated with DoS. The dataset is balanced using the oversampling technique. The model shows unsatisfactory results at a data ratio of 70:30 and gets satisfactory results at a data ratio of 80:20, with an accuracy of 96.75%, precision 100%, recall 93.46 and f1 score 96.62%. These results can show that the model has consistent and reliable performance in the detection task..

Keywords : *Supervisory Control and Data Acquisition, Attack Detection, Denial of Service, Deep Neural Network*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Supervisory control and data acquisition (SCADA) protocol IEC 61850 merupakan sistem komunikasi yang diciptakan dengan tujuan menjadi spesifikasi universal bagi perancangan dan operasi jaringan listrik cerdas. Meskipun berfokus pada aspek komunikasi, standar ini memiliki cakupan yang lebih luas. Dengan kata lain, standar ini merinci model fungsi pengamanan dan kontrol listrik, bahasa konfigurasi perangkat, model data proses fisik, dan bahkan persyaratan kompatibilitas elektromagnetik dan lingkungan. Koleksi standar ini dirancang untuk mengatasi dua kebutuhan khusus dalam domain listrik. IEC 61850 bertujuan untuk menyediakan rangkaian protokol universal (terdiri dari 3 protokol) untuk komunikasi sistem tenaga serta kerangka pemodelan fungsi kontrol dan pengamanan yang terdistribusi [1].

Pada masa sebelumnya, komunikasi di dalam sub-station biasanya berlangsung secara langsung, mulai dari perangkat perlindungan menuju peralatan utama di kawasan saklar. Namun, dengan diperkenalkannya IEC 61850, bentuk komunikasi saat ini disediakan melalui sebuah jaringan yang menghubungkan beragam perangkat bersama-sama. Fenomena ini membuka potensi bagi pihak yang tidak diinginkan untuk memperoleh akses ke peralatan utama melalui pemindaian terhadap titik lemah pada satu atau lebih perangkat di dalam sistem sekunder sub-station, seperti *Intelligent Electronic Device* (IED). Di samping itu, jalur komunikasi saat ini meluas hingga mencakup peralatan utama yang menghubungkannya ke pusat pengiriman melalui jaringan, yang bisa dimanfaatkan dalam situasi serangan siber [2].

Karya-karya mutakhir dalam dunia teknologi telah mengidentifikasi beberapa keterbatasan dari IEC 61850. Sebagai contoh, struktur komunikasi berbasis IEC 61850 yang tidak aman dapat memberikan celah bagi para penyerang untuk memperoleh akses, menjalin komunikasi, dan tetap berada dalam jaringan secara konsisten. Untuk mengatasi keterbatasan ini serta memberikan tujuan keamanan siber bahkan melalui protokol komunikasi lainnya, standar IEC

62351 dikembangkan. Secara umum, Bagian 6 dari IEC 62351 adalah standar keamanan untuk protokol IEC 61850 (yaitu, spesifikasi GOOSE, *Sampled Value* (SV), dan *Manufacturing Message Specification* (MMS)). Namun, disebabkan oleh persyaratan laten *end-to-end* dari protokol GOOSE dan keterbatasan kemampuan komputasi pada *Intelligent Electronic Devices* (IEDs) dalam jaringan listrik pintar, seringkali tidak memungkinkan untuk menerapkan langkah-langkah keamanan yang dibutuhkan. Sebagai contoh, dalam sebuah SAS, standar komunikasi IEC 61850 Edisi 2 mengharuskan persyaratan waktu akhir-ke-akhir dari publikasi dan langganan pesan GOOSE berada dalam batas 4 ms dengan mempertimbangkan sistem tenaga frekuensi 60 Hz untuk perintah trip, yang tidak dapat dijamin ketika enkripsi berkelas atas IED yang ada diterapkan. Oleh karena itu, beberapa vendor yang patuh pada IEC 61850 belum menerapkan enkripsi pada IED mereka karena tambahan algoritma enkripsi mungkin sudah melebihi ambang batas maksimum laten IED akhir-ke-akhir. Akibatnya, banyak implementasi protokol GOOSE tetap rentan terhadap serangan dari penyerang cerdas dari dalam dan luar jaringan [3].

Hingga saat ini, belum ada solusi yang dapat dimplementasikan secara *global* untuk mencegah serangan DoS secara keseluruhan, karena serangan DoS memiliki banyak mekanisme dan teknik yang berbeda dan para *hacker* terus memperbarui teknik serangan yang sudah ada, bahkan membuat metode baru sendiri untuk melancarkan serangan. Saat ini, ada beberapa pendekatan yang dapat digunakan untuk mencegah serangan DoS. Salah satu cara melindungi diri dari serangan DoS yang bisa diterapkan dari *server* adalah dengan mengadopsi protokol yang mengelola penggunaan *server*. Protokol ini bertujuan untuk mengurangi kemungkinan orang mengekploitasi sumber daya yang tersedia pada *server* [4]. Namun, deteksi serangan DoS adalah keuntungan yang signifikan karena dapat membantu menangani masalah keamanan. Deteksi serangan DoS sangatlah penting dalam IEC 61850 karena membantu menjaga keamanan dan integritas sistem serta memastikan operasi yang efesien dan berkualitas. Dengan deteksi serangan DoS, sistem dapat mengidentifikasi beberapa frame yang telah di tapping seperti serangan DoS, DDoS, dan MITM.

Pada riset ini [5] membahas tentang deteksi serangan DoS menggunakan metode *deep neural network* (DNN) pada *dataset* SCADA IEC 61850. Melalui analisis dan perbandingan kinerja dari masing-masing dari keenam belas metode tersebut, tidak dapat ditemukan suatu keunggulan yang jelas dan konsisten. Metode yang berbasis DNN nampaknya memiliki kinerja yang lebih baik ketika diterapkan pada kumpulan data yang mengandung anomali kontekstual.

Karena ulasan diatas, penulis akan merekomendasikan untuk dilakukannya penelitian yang berjudul " Deteksi Serangan *Denial of Service* (DoS) pada protocol jaringan IEC 61850 *supervisory control and data acquisition* (SCADA) dengan menggunakan metode *Deep Neural Network* (DNN)".

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat disimpulkan rumusan masalah dalam penelitian ini antara lain sebagai berikut.

1. Bagaimana cara membedakan data normal dengan data serangan pada data IEC 61850?
2. Bagaimana cara menyesuaikan *dataset* yang dapat diimplementasikan untuk penyeimbangan data dengan tujuan memperoleh pembelajaran mesin yang efektif?
3. Bagaimana *machine learning* dapat mendeteksi serangan *Denial of Service* (DoS) pada IEC 61850 yang mungkin merupakan tindakan penyerangan sistem keamanan yang tidak sah, seperti serangan *hacker?*
4. Bagaimana mendeteksi serangan DoS pada data IEC 61850?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini antara lain:

1. *Dataset* merupakan data sekunder yang berasal dari *IEC 61850SecurityDataset in 2019*.
2. Penelitian ini menggunakan algoritma *deep neural network* (DNN) untuk deteksi serangan.

1.4 Tujuan

Berikut ini merupakan tujuan penelitian yang ingin dicapai berdasarkan perumusan masalah yang didapat, yaitu sebagai berikut.

1. Membedakan data normal dengan data serangan pada data IEC 61850.
2. Menyesuaikan *dataset* yang dapat diimplementasikan untuk penyeimbangan data dengan tujuan memperoleh pembelajaran mesin yang efektif.
3. Mendeteksi serangan *Denial of Service* (DoS) pada IEC 61850 yang mungkin merupakan tindakan penyerangan sistem keamanan yang tidak sah, seperti serangan *hacker*.

1.5 Manfaat

Adapun manfaat yang ingin dicapai dari penelitian ini yaitu sebagai berikut.

1. Dapat membedakan data normal dengan data serangan pada data IEC 61850.
2. Dengan menggunakan metode DNN dapat mendeteksi data normal dan data serangan pada jaringan IEC 61850.
3. Dapat mengatasi ketidakseimbangan pada *dataset* IEC 61850.

1.6 Metodologi Penelitian

Adapun penerapan metodologi penelitian yang digunakan pada penelitian yang berjudul "Deteksi Serangan *Denial of Service* (DOS) pada protocol jaringan IEC 61850 *supervisory control and data Acquisition* (SCADA) menggunakan metode *deep neural network* (DNN)" yaitu sebagai berikut.

1. Studi Pustaka dan Literatur

   Metode ini memungkinkan penulis untuk melakukan proses eksplorasi dan menggabungkan refrensi dari berbagai sumber, seperti jurnal, internet dan buku yang berhubungan dengan riset tugas akhir yang dilakukan.

2. Metode Konsultasi

   Metode ini memungkinkan penulis untuk berkonsultasi secara *real-time* atau secara *online* dengan narasumber yang memiliki ilmu dan pengertahuan yang luas tentang masalah yang dibahas pada riset ini.

3. Metode Pengolahan Data

Metode ini memungkinkan penulis untuk mengekstrak fitur dari data *pcap* digunakan dalam penelitian menjadi format *CSV*, dan kemudian dilakukanlah pemilihan fitur sesuai dengan pola serangan yang diidentifikasi.

4. Metode Pengerjaan Model dan Pengujian Data

Metode ini digunakan oleh penulis untuk membuat rancangan dari model *dataset* yang sudah diolah pada tahao sebelumnya dengan menggunakan *deep learning* untuk mencapai akurasi yang diharapkan.

5. Metode Analisa dan Kesimpulan

Pada tahap ini penulis melakukan analisis, membuat kesimpulan, dan membuat rekomendasi untuk penelitian ke depannya.

1.7 Sistematika Penulisan

Adapun sistematika pada penulisan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

BAB I menjelaskan latar belakang, tujuan, keuntungan, perumusan masalah, batasan masalah, metodologi penelitian,dan prosedur penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

BAB II mengandung literature review tentang penelitian sebelumnya dan teori yang relevan untuk mendukung penelitian ini. Teori–teori tersebut termasuk tersebut termasuk *supervisory control and data acquisition* (SCADA), *Denial of Service* (DoS), protocol IEC 61850, *deep learning* dan *deep neural network* (DNN).

BAB III METODOLOGI PENELITIAN

BAB III memberikan penjelasan tentang proses penelitian, kerangka kerja, serta perancangan dari model *deep neural network* (DNN) yang digunakan pada peneliian untuk mendeteksi serangan *Denial of Service* (DoS).

BAB IV HASIL DAN ANALISA

BAB IV akan membahas temuan penelitian dan menganalisis deteksi serangan *Denial of Service* (DoS) pada Protocol Jaringan IEC 61850 *Supervisory*

Control and Data Acquisition (SCADA) dengan menggunakan *Metode Deep Neural Network* (DNN) yang telah dilakukan.

BAB V KESIMPULAN DAN SARAN

BAB V berisi hasil penelitian dan rekomendasi untuk penelitian lanjutan.

DAFTAR PUSTAKA

[1] G. Elbez, K. Nahrstedt, and V. Hagenmeyer, "Early Detection of GOOSE Denial of Service (DoS) Attacks in IEC 61850 Substations," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 367–373. doi: 10.1109/SmartGridComm52983.2022.9961042.

[2] P. P. Biswas, H. Chuan Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation," 2019.

[3] S. Mocanu and J.-M. Thiriet, "Real-Time Performance and Security of IEC 61850 Process Bus Communications," *J. Cyber Secur. Mobil.*, vol. 2021, no. 2, pp. 1–42, 2021, doi: 10.13052/jcsm2245.

[4] S. Geges and W. Wibisono, "Geges, Wibisono-Pengembangan Pencegahan Serangan Distributed Denial Of Service (DDoS) Pada Sumber Daya Jarin-gan Dengan Integrasi Network Behavior Analysis dan Client Puzzle PENGEMBANGAN PENCEGAHAN SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA SUMBER DAYA JARINGAN DENGAN INTEGRASI NETWORK BEHAVIOR ANALYSIS DAN CLIENT PUZZLE."

[5] Z. Munawar and N. I. Putri, "KEAMANAN IOT DENGAN DEEP LEARNING DAN TEKNOLOGI BIG DATA," 2020.

[6] J. Audibert, P. Michiardi, F. Guyard, S. Marti, and M. A. Zuluaga, "Do Deep Neural Networks Contribute to Multivariate Time Series Anomaly Detection?," Apr. 2022, doi: 10.1016/j.patcog.2022.108945.

[7] R. Ryandhi, "PENERAPAN METODE ARTIFICIAL NEURAL NETWORK (ANN) UNTUK PERAMALAN INFLASI DI INDONESIA APPLICATION OF ARTIFICIAL NEURAL NETWORK (ANN) FOR INFLATION FORECASTING IN INDONESIA."

[8] J. Wira and G. Putra, "Pengenalan Konsep Pembelajaran Mesin dan Deep

Learning Edisi 1.4 (17 Agustus 2020)."

[9] N. I. Putri, Z. Munawar, and M. Kom, "DEEP LEARNING DAN TEKNOLOGI BIG DATA UNTUK KEAMANAN IOT."

[10] E. Rasywir, R. Sinaga, and Y. Pratama, "JURNAL MEDIA INFORMATIKA BUDIDARMA Evaluasi Pembangunan Sistem Pakar Penyakit Tanaman Sawit dengan Metode Deep Neural Network (DNN)," vol. 4, pp. 1206–1215, 2020, doi: 10.30865/mib.v4i4.2518.

[11] Sarp Nalcin, "StandardScaler vs. MinMaxScaler vs. RobustScaler: Which one to use for your next ML project?," https://medium.com/@onersarpnalcin/standardscaler-vs-minmaxscaler-vs-robustscaler-which-one-to-use-for-your-next-ml-project-ae5b44f571b9 .

[12] R. Mohammed, J. Rawashdeh, and M. Abdullah, "Machine Learning with Oversampling and Undersampling Techniques: Overview Study and Experimental Results," in *2020 11th International Conference on Information and Communication Systems, ICICS 2020*, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 243–248. doi: 10.1109/ICICS49469.2020.239556.

[13] T. Wongvorachan, S. He, and O. Bulut, "A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining," *Inf.*, vol. 14, no. 1, Jan. 2023, doi: 10.3390/info14010054.

[14] 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.

[15] J. Xu, Y. Zhang, and D. Miao, "Three-way confusion matrix for classification: A measure driven view," *Inf. Sci. (Ny).*, vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[16] R. Susmaga, "Confusion Matrix Visualization," *Intell. Inf. Process. Web Min.*, pp. 107–116, 2004, doi: 10.1007/978-3-540-39985-8_12.

[17] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, pp. 1–13, 2020, doi: 10.1186/s12864-019-6413-7.

[18] W. I. Rahayu, C. Prianto, and E. A. Novia, "Perbandingan Algoritma K-Means Dan Naïve Bayes Untuk Memprediksi Prioritas Pembayaran Tagihan Rumah Sakit Berdasarkan Tingkat Kepentingan Pada Pt. Pertamina (Persero)," *J. Tek. Inform.*,

vol. 13, no. 2, pp. 1–8, 2021, [Online]. Available: https://ejurnal.poltekpos.ac.id/index.php/informatika/article/view/1383

[19] Z. Meng, H. Huo, Z. Pan, L. Cao, J. Li, and F. Fan, “A gear fault diagnosis method based on improved accommodative random weighting algorithm and BB-1D-TP,” *Meas. J. Int. Meas. Confed.*, vol. 195, no. April, p. 111169, 2022, doi: 10.1016/j.measurement.2022.111169.

[20] H. Zhang, Z. Dong, M. Sun, H. Gu, and Z. Wang, “TP-CNN: A Detection Method for atrial fibrillation based on transposed projection signals with compressed sensed ECG,” *Comput. Methods Programs Biomed.*, vol. 210, p. 106358, 2021, doi: 10.1016/j.cmpb.2021.106358.

[21] M. Conciatori, A. Valletta, and A. Segalini, “Improving the quality evaluation process of machine learning algorithms applied to landslide time series analysis,” *Comput. Geosci.*, vol. 184, no. January, p. 105531, 2024, doi: 10.1016/j.cageo.2024.105531.