Volume 6 Nomor 2, Oktober 2023
e-ISSN : 2621-234X

Optimasi Metode Supervised Learning Dengan Menggunakan Particle Swarm Optimization Untuk Deteksi Malware

***Mayadi[1], Ismaniah[2], Tyastuti Sri Lestari[3], Wowon Priatna[4]**

Address : Universitas Bhayangkara Jakarta Raya/Fakultas Ilmu Komputer, Informatika, Indonesia[1,3,4],
Universitas Bhayangkara Jakarta Raya /Fakultas Teknik, Industri, Indonesia[2]

Email : mayadi@dsn.ubharajaya.ac.id[1], ismaniah@ubharajaya.ac.id[2], tyas@ubharajaya.ac.id[3],
wowon.priatna@dsn.ubharajaya.ac.id[4]

Abstrak

Tujuan dari penelitian ini adalah untuk deteksi malware untuk memberi solusi dalam Permasalahan muncul ketika user mengakses internet dan download file yang telah di susupi oleh malware. Salah satu solusi populer saat ini adalah menggunakan teknik pembelajaran mesin untuk melatih model malware dalam jumlah besar dengan mempertimbangkan fitur khusus yang memungkinkan prediksi apakah perangkat lunak tertentu adalah malware atau tidak berbahaya menggunakan algoritma pembelajaran mesin. Dataset yang digunakan adalah dataset deteksi malware dari Kaggle yang kemudian akan diklasifikasikan mengggunakan algorima ensemble classifier yang termasuk algoritma kategori supervised learning. Tingkatkan klasifikasi dengan pengoptimalan fitur menggunakan Particle Swarm Optimization (PSO). Penelitian ini menghasilkan nilai akurasi yang dihasilkan oleh algoritma Ensemble sebesar 92%, AUC 0.94%. selanjutnya klasifikasi dilakukan optimasi dengan PSO dihasilkan nilai akurasi naik sebesar 7.32% menjadi 100% akurasinya sedangkan AUC meningkat 0.059 menjadi AUC sebesar 1. Dari hasil penelitian yang dihasilkan maka seleksi fitur direkomendasikan sebelum dibangun model klasifikasi untuk deteksi malware.

Kata Kunci – Deteksi Malware, Particle Swarm Optimization, Supervised Learning

Abstract

The purpose of this research is for malware detection to solve problems that arise when users access the internet and download files that have been infiltrated by malware. One of the popular solutions today is to use machine learning techniques to train many malware models by considering special features that allow prediction of whether particular software is malware or harmless using machine learning algorithms. The dataset used is a malware detection dataset from Kaggle, which will then be classified using the ensemble classifier algorithm which belongs to the supervised learning category algorithm. Improve classification with feature optimization using Particle Swarm Optimization (PSO). This study resulted in an accuracy value generated by the Ensemble algorithm of 92%, AUC 0.94%. Then, the classification was optimized with PSO, resulting in an accuracy value increased by 7.32% to 100% accuracy while AUC increased by 0.059 to AUC of 1. From the results of the research produced, feature selection is recommended before building a classification model for malware detection.

Keywords *– Malware Detection,* Particle Swarm Optimization, Supervised Learning

1. Latar Belakang

Dengan pesatnya perkembangan Internet, malware menjadi salah satu ancaman dunia maya utama saat ini. Selama dekade terakhir, telah terjadi peningkatan 87% dalam infeksi malware dan program yang mungkin tidak diinginkan. Kontribusi signifikan datang dari file yang diunduh dari internet [1]. Perangkat lunak apa pun yang melakukan tindakan jahat, termasuk pencurian informasi, spionase, dll. Dapat disebut sebagai malware. Malware didefinisikan sebagai perangkat lunak

pengganggu yang menembus atau menghancurkan sistem tanpa izin pengguna[2]. Malware adalah konsep umum yang mengancam semua jenis perangkat[3].

Perancang malware terus menerus membuat malware baru dan menyebarkannya untuk menyerang target mereka. Meskipun teknik anti-malware tradisional banyak membantu dalam melindungi pengguna, teknik tersebut tetap tidak efektif dalam mendeteksi malware zero-day. Malware dapat membahayakan komputer korban dengan berbagai cara, termasuk memanipulasi data komputer, mengenkripsi data sensitif, atau bahkan memantau aktivitas korban tanpa persetujuan pemilik komputer. Risiko komputer yang menyimpan sebagian besar data penting kita terinfeksi oleh malware telah meningkat secara eksponensial[1]. Penyebab infeksi ini terjadi karena file yang diunduh dari dunia internet yang luas. Hanya perlu beberapa detik agar sistem kami disusupi. Permasalahan muncul ketika user mengakses internet dan download file yang telah di susupi oleh malware. Salah satu solusi populer saat ini adalah menggunakan teknik pembelajaran mesin untuk melatih model malware dalam jumlah besar dengan mempertimbangkan fitur khusus yang memungkinkan prediksi apakah perangkat lunak tertentu adalah malware atau tidak berbahaya menggunakan algoritma pembelajaran mesin[4]. Dalam optimasi fitur dapat digunakan algoritma *Particle Swarm Optimization* untuk optomasi akurasi klasifikasi terbaik[5].

Beberapa penelitian untuk klasifikasi deteksi malware adalah Penelitian Abdul aziz Habtor tahun 2021 deteksi malware menggunakan machine learning focus aplikasi jahat dan tidak jahat[3], deteksi malware menggunakan Menggunakan Native API System Calls dan diklasifikasi dengan machine learning[6], deteksi malware pada android menggunakan file string dalam deteksi[7], Analisis statis Deteksi Malware Android menggunakan supervised Learning[8].

Model klasifikasi akan menghasilkan nilai akurasi yang tinggi jika tidak terdapat distrbusi kelas yang tidak seimbang[9] yang dapat menyebabkan bias dalam aplikasi serta membani machine learning untuk membuat model klasifikasi. Salah satu Teknik untuk mengurangi kelas tidak seimbang digunakan Teknik data sampling yang dapat membagi kelas mayoritas menjadi kelas yang seimbang[10]. Teknik data sampling berhasil meningkatkan akurasi yang dihaslkan Ensemble Classifier[11], Teknik data sampling dapat mengatisipasi data kelas yang tidak seimbang[12]

Selain data sampling untuk meningkatkan nilai akurasi dari klasifikasi adalah metode pemilihan fitur dengan memilih subset fitur yang dipilih dari jumlah dataset[13], seleksi fitur adalah proses dimana Sebagian ruang fitur dipilih sesuai relevansinya dengan mempertimbangkan keluaran dari klasifikasi [14]. PSO merupakan algoritma Optimasi fitur dapat meningkatkan nilai akurasi yang dihasilkan PSO telah digunakan untuk optimasi peningkatan akurasi untuk Random forest, decision tree, naïve bayes dan KKN untuk klasifikasi dataset diabetes[15]. PSO dapat dikombinasikan dengan Teknik data sampling untuk meningkatkan akurasi dari algoritma an ensemble Classifier dalam klasifikasi[16]. Penelitian ini focus dan memberikan kotribusi keterbaruan diantaranya: membuat model klasifikasi kepuasaan layanan public menggunakan an ensemble classifier, menguji pengaruh pemilihan fitur terhadapat klasifikasi ensemble classifier, menguji pengaruh feature selection terhadap algoritma an ensemble classifier dan yang terakhir adalah kombinasi Teknik data sampling dan pemilihan fitur terhadap kinerja algoritma Ensemble classifier

Dari latar belakang permasalahan dan studi literatur pada penelitian terdahulu, maka tujuan penelitian ini adalah untuk deteksi malware menggunakan algoritma supervised learning yaitu Random Forest (RF), XGBOOST, catboost dan lightgbm, yang sebelumnya akan dilakukan *selection feature* untuk meningkatkan nilai akurasi, sehingga model yang dihasilkan dapat direkomendasikan untuk deteksi malware.

2. Metode

2.1 Dataset

Dataset untuk deteksi malware ini menggunakan data skunder bersumber dari Kaggle tediiri dari 35 variable dan jumlah 100000 record[17].

2.2 Metode Penelitian

Penelitian ini menggunakan 4 (empat) algoritma ensemble classifier diantaranya Random Forest (RF), XGBOOST, catboost dan lightgbm untuk klasifikasi kepuasaan layanan publik. Untuk mengantisipasi keterseimbangan kelas digunakan Teknik data samping menggunakan algoritma RUS. PSO digunakan sebagai algoritma untuk seleksi fitur sebagai optimasi algoritma klasifikasi. Adapun pemodelan yang akan dilakukan dalam penelitian ini:

a. Membuat model klasifikasi deteksi malware menggunakan ensemble classifier
b. Menguji pengaruh pemilihan fitur terhadapat klasifikasi ensemble classifier
c. Melakukan perbandingan hasil yang didapatkan hasil akurasi klasifikasi menggunakan optimasi dan sebelum menggunakan optimasi PSO.

2.3 Klasifikasi dengan Random Forest

Random Forest (RF) adalah algoritma yang menggunakan metode pemisahan biner rekursif untuk mencapai node akhir dalam struktur pohon berdasarkan pada pohon klasifikasi dan regresi[18]. Tiga yang wajib diketahu pada

algoritma random forest, pertama bootstrap sampling dalam membuat pohon prediksi, pada setiap pohon keputusan malakukan prediski secara random, prediksi dihasilkan melalui sebuah kombinasi pada masing-masing pohon keputusan secara majority vote dalam mengklasifikasikannya[19]. Adapun dalam Pembangunan algoritma RF terdiri dari 3 langkah yaitu: (1) Sampling himpunan bagian pelatihan k, (2) Pembuatan setiap model pohon keputusan, dan (3) Pengumpulan k pohon ke dalam model RF. Penggunaan algoritma RF untuk klasifikasi dapat diterapkan pada data imbalance dalam jumlah besar dengan memberikan hasil performa yang baik dan waktu eksekusi yang cepat[19][20].

2.4 Klasifikasi dengan XGBoost

Extreme Gradient Boosting (XGBoost) merupakan salah satu machine learning yang digunakan untuk prediksi dan klasifikasi yang memiliki struktur decision tree[21]. XGBoost merupakan salah satu metode boosting yang terdiri dari beberapa decision tree yang mana pohon sebelumnya dan pohon berikutnya akan saling betergantungan[22]. Pada saat melakukan klasifikasi, XGBoost akan melakukan update bobot pada masing-masing pohon yang dibangun sehingga diperoleh pohon klasifikasi yang kuat[23]. Persamaan (1) adalah mengitung XGBoost.

$$\bar{Y}\hat{\imath} = \sum_{k}^{K} f_k(x_i), f_k \epsilon F \quad (1)$$

2.5 Klasifikasi dengan Catboost

CatBoost adalah algoritma pembelajaran mesing yang masih tergabung dalam keluarga Gradient Boosted Decision Trees (GBDT) yang berada dalam lingkupan ensemble learning[24]. CatBoost adalah suatu algoritma yang dibuka secara umum untuk terus dikembangkan dalam lingkup dua kombinasi: Ordered Target Statistics dan Ordered Boosting, gabungan keduanya disebut dengan catboost[25].

2.6 Klasifikasi dengan LightGBM

Klasifikasi LightGBM tujuan nya adalah mencari model additive yang meniminalkan fungsi loss[26]. Persamaan algortima untuk meningkatkan regresi treesdapat digeneralkan pada persamaan 3, dimana model akhir dari model penambahan bertahap sederhana dari nilai b[27].

$$F(x) = \sum_{b=1}^{B} f^b(x) \quad (2)$$

2.7 Seleksi Fitur dengan Particle Swarm Optimization (PSO)

Tahap seleksi fitur dimaksudkan untuk menghilangkan fitur-fitur yang berlebihan dan tidak relevan didalam himpunan data[28] dan kunci sebagai analisis dari data sample yang berdimensi tinggi[29]. Seleksi fitur yang digunakan dalam penelitian ini adalah PSO dalam tahapan learning yang bertujuan untuk optimasi dari setiap data yang dihasilkan [30]. Tahapan dari metode PSO terdapat dalam penelitian[31].

2.8 Evaluasi Hasil Kinerja Klasifikasi

Evaluasi kinerja Klasifikasi. Berdasarkan nilai accuracy yang melatih seberapa sering model dihasilkan benar yang digambarkan menggunakan confusion matrix[32]. Evaluasi klasifikasi juga diukur kinerjanya menggunakan recall dan precision. Untuk menghitung nilai accuracy terdapat pada persamaan (1), precision persamaan (2), recall persamaan (3). Selain menggunakan confusion matrix baik buruk hasil prediksi suatu model klasifikasi juga dapat menggunakan Receiver Operating Characteristic (ROC)[32][33] dan Area Under the Curve (AUC)[34].

Accuracy = (TP+TN)/(TP+TN+FP+FN) (3)
Precision = (TP)/(TP+FP) (4)
Recall = (TP) / (TP+FN) (5)

Dimana TP= True Positive, TN=True Negative, FP=False Positive and FN = False Negative.

3. Hasil

Untuk membuat model klasifikasi algoritma ensemble classifier, optimasi fitur dan menangani kelas tidak seimbang maka digunakan tool pemograman python yang menyediakan library machine learning[35].

3.1 Hasil Klasifikasi menggunakan Algoritma esemble classifier

Hasil klasifikasi kepuasaan tingkat layanan pengguna menggunakan python dengan diproses oleh algoritma ensemble classifier dengan membagi data training 70% dan data testing sebesar 30%. Model klasifikasi di uji menggunakan confusion matrix untuk mendapatkan nilai akurasi, presisi dan recall. Hasil uji ditunjukan pada tabel 1.

Tabel 1. Cluster Data Penjualan

Algoritma	Accuracy	Recall	Precision	AUC
Random Forest	92.68%	1.00	0.89	0.941
XGBOOST	92.68%	1.00	0.89	0.941
Chatboost	92.68%	1.00	089	0.941
LightGBM	92.68%	1.00	089	0.941

Hasil klasifikasi yang dihasilkan masing-masing algoritma ensemble learning seperti yang ditunjukan pada tabel 1 dari nilai Accuracy, recall, precision dan AUC menunjukan nilai yang sama.

3.2 Hasil Klasifikasi menggunakan Algoritma ensemble classifier dengan dilakukan optimasi PSO

Untuk meningkatkan akurasi dilakukan juga seleksi fitur menggunakan algoritma PSO dengan partikel berjumlah 50 dimensi 35 serta nilai position >=0.5 sehingga menghasilkan fitur setelah diseleksi menjadi 8 fitur dari awalnya 35 fitur. Berikut hasil dari optimasi PSO dilanjutkan dengan membuat model Klasifikasi. Hasil modeling yang selanjutnya dilakukan uji klasifikasi ditunjukan pada tabel V.

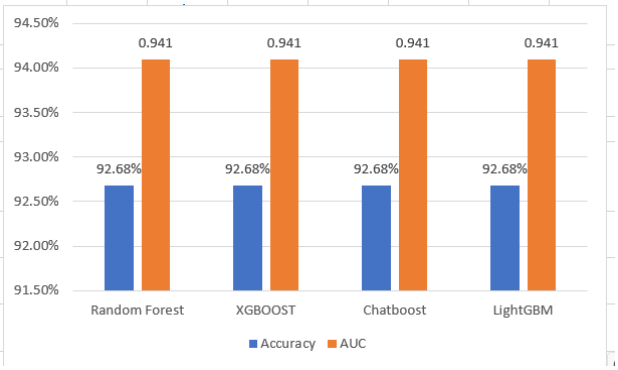
Tabel 2. Hasil Klasifikasi Kombinasi Dengan Seleksi Fitur

Algoritma	Accuracy	Recall	Precision	AUC
Random Forest + PSO	100%	1.00	0.89	1.00
XGBOOST+PSO	100%	1.00	0.89	1.00
Chatboost+PSO	100%	1.00	089	1.00
LightGBM+PSO	100%	1.00	089	1.00

Hasil klasifikasi yang ditunjukan pada tabel V menunjukan akurasi dan nilai AUC setelah dilakukan seleksi fitur nilai naik menjadi 100 dan 1.

3.3 Analisa Hasil Perbandingan Kinerja Klasifikasi

Tabel 1 dibuatkan Grafik yang ditunjukan dari gambar 1 adalah hasil kinerja klasifikasi yang dilakukan sebelum menggunakan optimasi dengan seleksi fitur. Dari grafik dapat dilihat semua algoritma ensemble classifier mendapatkan akurasi 92.68% dan nilai Auc 0.941 sehingga semua algoritma ini direkomendasikan untuk mendeteksi malware.



Gambar 1. Grafik Hasil Klasifikasi Sebelum Dilakukan Optimasi Fitur

Berdasarkan tabel 2 menunjukan peningkatan dalam nilai akurasi dan AUC dari setiap algoritma meningkat 7.32% dan nilai Auc meningkat sebesar 0.059. berikut tabel 3 adalah peningkatan nilai akurasi dan AUC setelah dioptimasi dengan PSO.

Dari hasil tabel 3 menunjukan bahwa setelah dilakukan optimasi klasifikasi menggunakan PSO tingkat akurasi mejadi meningkat untuk semua Algoritma ensemble classifier, sehingga untuk meningkatkan klasifikasi yang direkomendasikan untuk menggunakan optimasi pemilihan fitur sebelum membuat model klasifikasi.

Tabel 3. Hasil Perbandingan Klasifikasi

Algoritma	Akurasi Tanpa PSO	Akurasi+PSO	Kenaikan Akurasi	AUC Tanpa PSO	AUC+PSO
RF	92.68%	100%	7.32%	0.941	1
XGBooost	92.68%	100%	7.32%	0.941	1
Chatboost	92.68%	100%	7.32%	0.941	1
LightGBM	92.68%	100%	7.32%	0.941	1

4. Kesimpulan

Sebelum dilakukan optimasi Algoritma menunjukan algoritma masing-masing algoritma *ensemble* classifier mendapkan akurasi sebesar 92.68%. Setelah ditambahkan optimasi menggunakan PSO nilai akurasi 4 algoritma ensemble Classifier masing-masing naik 7.32%, sehingga nilai akurasi masing-masing Algoritma ensembke classifier mendapatkan akursi 100%. Dari hasil klasifikasi menunjukan model klasifikasi masing-masing algoritma ensemble classifier baik dilakukan optimasi dan tanpa digunakan optimasi mendapatkan nilai diatas 90%, sehingga 4 algoritma ensemble ini dapat digunakan untuk deteksi malware yang ditunjukan dari hasil uji klasifikasi dapat mengenali file terindentifikasi malware dan file tidak terindentifikasi malaware.

Saran untuk penelitian selanjutnya dalam deteksi malware sebaiknya menggunakan Teknik sampling terlebih dahulu sebelum dilakukan seleki fitur dan model klasifikasi yang telah dibuat untuk di uji dengan dataset yang berbeda.

References

[1] A. Kamboj, P. Kumar, A. K. Bairwa, and S. Joshi, "Detection of malware in downloaded files using various machine learning models," *Egypt. Informatics J.*, vol. 24, no. 1, pp. 81–94, 2022, doi: 10.1016/j.eij.2022.12.002.

[2] E. Raff and C. K. Nicholas, "Machine Learning for Malware Detection," *Mach. Learn. Malware Detect.*, 2024, doi: 10.1142/13017.

[3] S. A. Habtor and A. H. H. Dahah, "Machine-Learning Classifiers for Malware Detection Using Data Features," *J. ICT Res. Appl.*, vol. 15, no. 3, pp. 265–290, 2021, doi: 10.5614/ITBJ.ICT.RES.APPL.2021.15.3.5.

[4] A. Amer and N. A. Aziz, "Malware Detection through Machine Learning Techniques," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 5, pp. 2408–2413, 2019.

[5] T. Arifin and A. Herliana, "Optimasi Metode Klasifikasi dengan Menggunakan Particle Swarm Optimization untuk Identifikasi Penyakit Diabetes Retinopathy," vol. 4, no. 2, pp. 77–81, 2018.

[6] C. W. Kim, "NtMalDetect: A Machine Learning Approach to Malware Detection Using Native API System Calls," pp. 1–8, 2018, [Online]. Available: http://arxiv.org/abs/1802.05412.

[7] 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.

[8] R. B. Hadiprakoso, W. R. Aditya, and F. N. Pramitha, "Analisis Statis Deteksi Malware Android Menggunakan Algoritma Supervised Machine Learning," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 1, pp. 1–5, 2022, doi: 10.14421/csecurity.2022.5.1.3116.

[9] Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.

[10] B. Liu and G. Tsoumakas, "Dealing with class imbalance in classifier chains via random undersampling," *Knowledge-Based Syst.*, vol. 192, p. 105292, 2020, doi: 10.1016/j.knosys.2019.105292.

[11] Y. E. Kurniawati and Y. D. Prabowo, "Model optimisation of class imbalanced learning using ensemble classifier on over-sampling data," *IAES Int. J. Artif. Intell.*, vol. 11, no. 1, pp. 276–283, 2022, doi: 10.11591/ijai.v11.i1.pp276-283.

[12] L. Liu, X. Wu, S. Li, Y. Li, S. Tan, and Y. Bai, "Solving the class imbalance problem using ensemble algorithm: application of screening for aortic dissection," *BMC Med. Inform. Decis. Mak.*, vol. 22, no. 1, pp. 1–16, 2022, doi: 10.1186/s12911-022-01821-w.

[13] E. Purnamasari, D. Palupi Rini, and Sukemi, "Seleksi Fitur menggunakan Algoritma Particle Swarm Optimization pada Klasifikasi Kelulusan Mahasiswa dengan Metode Naive Bayes," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 469–475, 2020.

[14] S. A. Alsenan, I. M. Al-Turaiki, and A. M. Hafez, "Feature extraction methods in quantitative structure-activity relationship modeling: A comparative study," *IEEE Access*, vol. 8, pp. 78737–78752, 2020, doi: 10.1109/ACCESS.2020.2990375.

[15] A. Fauzi and A. H. Yunial, "Optimasi Algoritma Klasifikasi Naive Bayes, Decision Tree, K – Nearest Neighbor, dan Random Forest menggunakan Algoritma Particle Swarm Optimization pada Diabetes Dataset," *J. Edukasi dan Penelit. Inform.*, vol. 8, no. 3, p. 470, 2022, doi: 10.26418/jp.v8i3.56656.

[16] D. Zheng, C. Qin, and P. Liu, "Adaptive Particle Swarm Optimization Algorithm Ensemble Model Applied to Classification of Unbalanced Data," *Sci. Program.*, vol. 2021, no. 1, 2021, doi: 10.1155/2021/7589756.

[17] N. Saravana, "Malware Detection," *https://www.kaggle.com/*, 2017. https://www.kaggle.com/datasets/nsaravana/malware-detection.

[18] Z. Jin, J. Shang, Q. Zhu, C. Ling, W. Xie, and B. Qiang, "RFRSF: Employee Turnover Prediction Based on Random Forests and Survival Analysis," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12343 LNCS, pp. 503–515, 2020, doi: 10.1007/978-3-030-62008-0_35.

[19] W. Yustanti and N. Rochmawati, "Analisis Algoritma Klasifikasi untuk Memprediksi Karakteristik Mahasiswa pada Pembelajaran Daring," *J. Edukasi dan Penelit. Inform.*, vol. 8, no. 1, pp. 57–61, 2022.

[20] Yoga Religia, Agung Nugroho, and Wahyu Hadikristanto, "Klasifikasi Analisis Perbandingan Algoritma Optimasi pada Random Forest untuk Klasifikasi Data Bank Marketing," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 187–192, 2021, doi: 10.29207/resti.v5i1.2813.

[21] M. R. Givari, M. R. Sulaeman, and Y. Umaidah, "Perbandingan Algoritma SVM, Random Forest Dan XGBoost Untuk Penentuan Persetujuan Pengajuan Kredit," *Nuansa Inform.*, vol. 16, no. 1, pp. 141–149, 2022, doi: 10.25134/nuansa.v16i1.5406.

[22] H. H. Sinaga and S. Agustian, "Pebandingan Metode Decision Tree dan XGBoost untuk Klasifikasi Sentimen Vaksin Covid-19 di Twitter," *J. Nas. Teknol. dan Sist. Inf.*, vol. 8, no. 3, pp. 107–114, 2022, doi: 10.25077/teknosi.v8i3.2022.107-114.

[23] Z. Salam Patrous, "Evaluating XGBoost for User Classification by using Behavioral Features Extracted from Smartphone Sensors," p. 67, 2018, [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1240595&dswid=-6444.

[24] A. N. A. Aldania, A. M. Soleh, and K. A. Notodiputro, "A Comparative Study of CatBoost and Double Random Forest for Multi-class Classification," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 1, pp. 129–137, 2023, doi: 10.29207/resti.v7i1.4766.

[25] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "Catboost: Unbiased boosting with categorical features," *Adv. Neural Inf. Process. Syst.*, vol. 2018-Decem, no. Section 4, pp. 6638–6648, 2018.

[26] S. Touzani, J. Granderson, and S. Fernandes, "Gradient boosting machine for modeling the energy consumption of commercial buildings," *Energy Build.*, vol. 158, no. January 2018, pp. 1533–1543, 2018, doi: 10.1016/j.enbuild.2017.11.039.

[27] I. Wardhana, Musi Ariawijaya, Vandri Ahmad Isnaini, and Rahmi Putri Wirman, "Gradient Boosting Machine, Random Forest dan Light GBM untuk Klasifikasi Kacang Kering," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 1, pp. 92–99, 2022, doi: 10.29207/resti.v6i1.3682.

[28] Y. Wanli Sitorus, P. Sukarno, S. Mandala, F. Informatika, and U. Telkom, "Analisis Deteksi Malware Android menggunakan metode Support Vector Machine & Random Forest," *e-Proceeding Eng.*, vol. 8, no. 6, p. 12500, 2021.

[29] L. Zhang, "A Feature Selection Algorithm Integrating Maximum Classification Information and Minimum Interaction Feature Dependency Information," *Hindawi Comput. Intell. Neurosci.*, vol. 2021, 2021.

[30] Y. Zhang, S. Wang, P. Phillips, and G. Ji, "Binary PSO with mutation operator for feature selection using decision tree applied to spam detection," *Knowledge-Based Syst.*, vol. 64, pp. 22–31, 2014, doi: 10.1016/j.knosys.2014.03.015.

[31] A. G. Gad, *Particle Swarm Optimization Algorithm and Its Applications: A Systematic Review*, vol. 29, no. 5. Springer Netherlands, 2022.

[32] R. C. Chen, C. Dewi, S. W. Huang, and R. E. Caraka, "Selecting critical features for data classification based on machine learning methods," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00327-4.

[33] T. R. Shultz and S. E. Fahlman, *Encyclopedia of Machine Learning and Data Mining*. 2017.

[34] P. Sedgwick, "How to read a receiver operating characteristic curve," *BMJ*, vol. 350, no. May, 2015, doi: 10.1136/bmj.h2464.

[35] M. R. S. Alfarizi, M. Z. Al-farish, M. Taufiqurrahman, G. Ardiansah, and M. Elgar, "Penggunaan Python Sebagai Bahasa Pemrograman untuk Machine Learning dan Deep Learning," *Karya Ilm. Mhs. Bertauhid (KARIMAH TAUHID)*, vol. 2, no. 1, pp. 1–6, 2023.

UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
Kampus I: Jl. Harsono RM No. 67, Ragunan, Pasar Minggu, Jakarta Selatan, 12550
Telepon: (021) 27808121 – 27808882
Kampus II: Jl. Raya Perjuangan, Marga Mulya, Bekasi Utara, Jawa Barat, 17142
Telepon: (021) 88955882, Fax.: (021) 88955871
Web: fasilkom.ubharajaya.ac.id, E-mail: fasilkom@ubharajaya.ac.id

SURAT TUGAS

Nomor: ST/1019/X/2023/FASILKOM-UBJ

Pertimbangan : Dalam rangka mewujudkan Tri Dharma Perguruan Tinggi untuk Dosen di Universitas Bhayangkara Jakarta Raya maka dihimbau untuk melakukan penelitian.

Dasar :
1. Kalender Akademik Universitas Bhayangkara Jakarta Raya Tahun Akademik 2023/2024;
2. Rencana Kerja dan Anggaran Pembelanjaan Universitas Bhayangkara Jakarta Raya Tahun 2023.

DITUGASKAN

Kepada : Personil yang namanya tercantum dalam Surat Tugas ini.

NO.	NAMA	NIDN	JABATAN	KETERANGAN
1.	Mayadi, S.Kom., M.Kom.	0408087802	Dosen Tetap Prodi Informatika	Sebagai Penulis Pertama
2.	Dr. Dra. Tyastuti Sri Lestari, M.M.	0327036701	Dosen Tetap Prodi Informatika	Sebagai Penulis Ketiga
3.	Wowon Priatna, S.T., M.T.I.	0429118007	Dosen Tetap Prodi Informatika	Sebagai Penulis Keempat

Untuk :
1. Membuat Artikel Ilmiah dengan judul **"Optimasi Metode *Supervised Learning* dengan menggunakan *Particle Swarm Optimization* untuk Deteksi *Malware*"** pada media Jurnal Teknologi dan Ilmu Komputer (JUTIKOMP) Universitas Prima Indonesia, Vol. 6, No. 2, Oktober 2023, Hal. 150-155, E-ISSN: 2621-234X.
2. Melaksanakan tugas ini dengan penuh tanggung jawab.

Jakarta, 16 Oktober 2023
DEKAN FAKULTAS ILMU KOMPUTER

Dr. Dra. Tyastuti Sri Lestari, M.M.
NIP. 1408206

Dikelola oleh : Fakultas Teknologi dan Ilmu komputer Universitas Prima Indonesia I E-ISSN : 2621-234X

Optimasi Metode Supervised Learning Dengan Menggunakan Particle Swarm Optimization Untuk Deteksi Malware

Mayadi -
Universitas Bhayangkara Jakarta Raya

Ismaniah -
Universitas Bhayangkara Jakarta Raya

Tyastuti Sri Lestari
Universitas Bhayangkara Jakarta Raya

Wowon Priatna
Universitas Bhayangkara Jakarta Raya

DOI: https://doi.org/10.34012/jutikomp.v6i2.4281