E-ISSN 3032-601X & P-ISSN 3032-7105

Vol. 1, No. 3c, Juli 2024

MISTER

Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research

Jurnal Penelitian Multidisiplin dalam Ilmu Pengetahuan, Teknologi dan Pendidikan

UNIVERSITAS SERAMBI MEKKAH

KOTA BANDA ACEH

mister@serambimekkah.ac.id

Journal of Multidisciplinary Inquiry in Science Technology and Educational Research

Journal of MISTER

Vol. 1, No. 3c, Juli 2024

Pages: 1687-1695

Perbandingan Algoritma Klasifikasi untuk Deteksi Intrusi pada Jaringan Komputer (Literature Review)

Yuce Yuliani

Sistem Informasi, Fakultas Ilmu Komputer, Universitas Gunadarma, Depok, Jawa barat, Indonesia

Article in Journal of MISTER

Available at	:	https://jurnal-serambimekkah.org/index.php/mister/index
DOI	:	https://doi.org/10.32672/mister.v1i3c.2074

How to Cite this Article

APA	:	Yuliani, Y. (2024). Perbandingan Algoritma Klasifikasi untuk Deteksi Intrusi pada Jaringan Komputer (Literature Review). *MISTER: Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research*, *1*(3c), 1687 – 1695. https://doi.org/10.32672/mister.v1i3c.2074
Others Visit	:	https://jurnal-serambimekkah.org/index.php/mister/index

ISSN 3032-7105 ISSN 3032-601X

Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research
UNIVERSITAS SERAMBI MEKKAH
https://jurnal-serambimekkah.org/index.php/mister

e-ISSN 3032-601X & p-ISSN 3032-7105
Vol. 1 No. 3c, Juli, 2024
Doi: 10.32672/mister.v1i3c.2074
Hal. 1687-1695

Perbandingan Algoritma Klasifikasi untuk Deteksi Intrusi pada Jaringan Komputer (Literature Review)

Yuce Yuliani
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Gunadarma, Depok, Jawa barat, Indonesia

*Email Korespodensi: yuce@staff.gunadarma.ac.id

Diterima: 23-07-2024 | Disetujui: 24-07-2024 | Diterbitkan: 25-07-2024

ABSTRACT

In the increasingly advanced digital era, computer network security is becoming more crucial. Intrusion Detection Systems (IDS) play a vital role in identifying and preventing cyber-attacks. This study conducts a literature review to compare various classification algorithms used in intrusion detection in computer networks, including Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Naive Bayes, and Neural Networks. The results show that Neural Networks and Random Forest have high accuracy but require significant computational resources. Conversely, Naive Bayes and Decision Tree offer better speed and computational efficiency. These conclusions provide guidance for researchers and practitioners in selecting the appropriate algorithm based on the specific needs of the application and the characteristics of the data used.

Keywords: *Intrusion Detection System (IDS); Network Security; Classification Algorithms*

ABSTRAK

Dalam era digital yang semakin maju, keamanan jaringan komputer menjadi semakin krusial. Sistem Deteksi Intrusi (IDS) berperan penting dalam mengidentifikasi dan mencegah serangan siber. Studi ini melakukan tinjauan literatur untuk membandingkan berbagai algoritma klasifikasi yang digunakan dalam deteksi intrusi pada jaringan komputer, termasuk Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Naive Bayes, dan Neural Networks. Hasil menunjukkan bahwa Neural Networks dan Random Forest memiliki akurasi tinggi tetapi memerlukan sumber daya komputasi yang besar. Sebaliknya, Naive Bayes dan Decision Tree menawarkan kecepatan dan efisiensi komputasi yang lebih baik. Kesimpulan ini memberikan panduan bagi peneliti dan praktisi dalam memilih algoritma yang sesuai berdasarkan kebutuhan spesifik aplikasi dan karakteristik data yang digunakan.

Katakunci: Sistem Deteksi Intrusi (IDS); Keamanan Jaringan; Algoritma Klasifikasi

e-ISSN3032-601X & p-ISSN3032-7105

PENDAHULUAN

Deteksi intrusi pada jaringan komputer adalah masalah penting dalam keamanan komputer yang telah menarik banyak perhatian peneliti dalam beberapa tahun terakhir (Setiawan et al., 2021). Serangan pada jaringan komputer dapat menimbulkan kerugian yang signifikan, baik dari segi finansial maupun reputasi. Oleh karena itu, diperlukan sistem yang dapat mendeteksi aktivitas mencurigakan dan memberikan peringatan kepada administrator jaringan (Wijaya & Pratama, 2020). Salah satu metode yang digunakan untuk mendeteksi intrusi adalah dengan menggunakan *Intrusion Detection System* (Anwar et al., 2019). IDS dapat dibagi menjadi dua kategori, yaitu *signature-based* dan *anomaly-based* (Bhuyan et al., 2018). Signature-based IDS mengidentifikasi serangan dengan membandingkan pola lalu lintas jaringan dengan database serangan yang telah diketahui. Sementara itu, anomaly-based IDS mendeteksi anomali dalam lalu lintas jaringan berdasarkan model normal yang telah dibentuk.

Kedua metode ini memiliki kelebihan dan kekurangan masing-masing. *Signature-based* IDS efektif dalam mendeteksi serangan yang telah diketahui sebelumnya, namun tidak dapat mendeteksi serangan baru (Constantinides et al., 2019). Di sisi lain, *anomaly-based* IDS dapat mendeteksi serangan baru, tetapi memiliki tingkat false positive yang lebih tinggi. Penelitian terbaru telah menerapkan algoritma machine learning untuk meningkatkan performa IDS. Algoritma klasifikasi seperti *Naive Bayes* dan *deep learning* telah digunakan untuk mengklasifikasikan aktivitas jaringan menjadi normal atau anomali (Shashank & Balachandra, 2018).

Penelitian ini bertujuan untuk membandingkan performa beberapa algoritma klasifikasi dalam mendeteksi intrusi pada jaringan komputer. Algoritma yang akan digunakan adalah Naive Bayes, Decision Tree, Random Forest, dan Support Vector Machine. Data yang digunakan adalah NSL-KDD, yang merupakan penyempurnaan dari dataset KDD-Cup 99 yang sering digunakan dalam penelitian IDS (Solanki et al., 2020). Hasil penelitian menunjukkan bahwa algoritma Random Forest memiliki akurasi tertinggi dalam mendeteksi intrusi, diikuti oleh Support Vector Machine, Decision Tree, dan Naive Bayes (Adhi Tama et al., 2021). Algoritma Random Forest mampu mengidentifikasi serangan dengan tingkat true positive yang tinggi dan false positive yang rendah. Selain itu, algoritma ini juga robust terhadap fitur yang tidak relevan (Bhatia et al., 2020).

Studi ini bertujuan untuk meninjau dan membandingkan kinerja berbagai algoritma klasifikasi yang digunakan dalam deteksi intrusi pada jaringan komputer. Dengan menganalisis kelebihan, kekurangan, serta efektivitas masing-masing algoritma, diharapkan dapat memberikan wawasan yang lebih dalam untuk pemilihan algoritma yang paling sesuai dalam konteks tertentu. Penipuan atau serangan pada sistem komputer dan jaringan merupakan ancaman yang semakin meningkat seiring dengan pertumbuhan penggunaan internet. Oleh karena itu, kebutuhan akan sistem keamanan jaringan yang efektif dan efisien semakin penting. Deteksi Intrusi adalah salah satu komponen penting dalam mempertahankan keamanan jaringan (Singh & Khare, 2022). Metode deteksi intrusi berbasis mesin pembelajaran telah banyak diterapkan untuk mengidentifikasi aktivitas jaringan yang mencurigakan atau anomali.

Penelitian ini akan mengulas literatur yang ada untuk menilai kinerja berbagai algoritma tersebut dalam konteks deteksi intrusi pada jaringan komputer. Perbandingan ini akan mencakup aspek akurasi, kecepatan, kompleksitas, dan kemampuan untuk menangani berbagai jenis serangan. Hasil dari studi ini diharapkan dapat memberikan panduan bagi peneliti dan praktisi dalam memilih algoritma yang paling sesuai untuk kebutuhan spesifik mereka.

e-ISSN3032-601X & p-ISSN3032-7105

METODE PENELITIAN

Metode penelitian dengan menggunakan literature review melibatkan langkah-langkah sistematis untuk mengidentifikasi, menilai, dan menyintesis hasil penelitian yang telah dipublikasikan sebelumnya. Tujuannya adalah untuk mengumpulkan informasi dari berbagai sumber yang relevan untuk menjawab pertanyaan penelitian atau mencapai tujuan penelitian tertentu. Berikut adalah langkah-langkah dalam melakukan literature review untuk studi perbandingan algoritma klasifikasi untuk deteksi intrusi pada jaringan komputer.

HASIL

Berdasarkan review literatur yang telah dilakukan, berikut adalah hasil dari perbandingan beberapa algoritma klasifikasi yang digunakan untuk deteksi intrusi pada jaringan komputer:

Decision Tree

Decision Tree umumnya menunjukkan akurasi yang baik dalam mendeteksi serangan intrusi, terutama untuk dataset yang tidak terlalu besar. Algoritma Decision Tree merupakan salah satu algoritma Supervised Learning yang sering digunakan dalam klasifikasi dan regresi. Decision tree dapat digunakan untuk menyelesaikan tugas pengenalan pola dengan cara yang dapat diinterpretasikan (Siswoyo, 2020). Namun, algoritma ini memiliki kelemahan yaitu sensitif terhadap perubahan data pelatihan dan cenderung memiliki variansi yang tinggi (Zhang & Suganthan, 2015).

Untuk mengatasi kelemahan tersebut, telah dikembangkan beberapa metode ensemble seperti Random Forest dan Rotation Forest yang dapat meningkatkan akurasi klasifikasi. Penggunaan algoritma Decision Tree juga telah diterapkan untuk mengkategorikan berita berbahasa Indonesia dengan menggunakan feature selection berdasarkan Information Gain (Purwananto et al., 2004). Evaluasi akurasi algoritma klasifikasi dapat dilakukan dengan menghitung metrik seperti precision, accuracy, dan AUC. *Decision Tree* yang dibangun dapat menghasilkan aturan-aturan klasifikasi yang dapat digunakan untuk memprediksi kategori teks baru .

Secara umum, algoritma *Decision Tree* dan varian-variannya telah banyak diaplikasikan dalam berbagai bidang, termasuk dalam analisis data dan klasifikasi teks, dengan menunj[![ukkan hasil yang cukup baik.

Random Forest

Random Forest adalah algoritma pembelajaran mesin yang memadukan banyak pohon keputusan untuk menghasilkan prediksi yang lebih akurat (Raharjo et al., 2022). Metode ini memanfaatkan konsep ensemble learning, di mana banyak model individu digabungkan untuk meningkatkan performa (Chaudhari et al., 2022). Berbeda dengan Decision Tree yang hanya membangun satu pohon keputusan, *Random Forest* membangun banyak pohon keputusan yang saling independen dan menggabungkan hasil prediksi mereka melalui pemungutan suara.

Sifat *Random Forest* yang membangun banyak pohon keputusan membuatnya kurang sensitif terhadap perubahan data pelatihan dibandingkan *Decision Tree*. Dengan begitu, Random Forest dapat mengatasi masalah overfitting yang sering terjadi pada Decision Tree. Selain itu, proses pemodelan Random Forest dapat dioptimalkan melalui pemilihan parameter yang tepat, seperti jumlah pohon

keputusan dan kedalaman pohon, untuk mening-katkan akurasi prediksi (Rokach, 2016).

Dalam banyak kasus, *Random Forest* terbukti memiliki kinerja yang lebih baik dibandingkan Decision Tree, terutama dalam memprediksi variabel numerik. Metode ini telah diterapkan dalam berbagai bidang, seperti prediksi produksi daya pembangkit listrik tenaga surya dan prediksi rasio keuangan perbankan. Jadi, Random Forest cenderung memiliki akurasi yang lebih tinggi dibandingkan Decision Tree karena menggunakan konsep ensemble learning untuk memadukan banyak pohon keputusan. Meskipun demikian, Decision Tree tetap memiliki kelebihan dalam hal interpretabilitas yang lebih baik dibandingkan *Random Forest.*

Support Vector Machine (SVM)

Support Vector Machine adalah salah satu algoritma machine learning yang paling populer dan banyak digunakan dalam berbagai bidang seperti klasifikasi, regresi, deteksi anomali,dan lainnya (Kibriya et al., 2023). SVM dapat menyelesaikan masalah klasifikasi dengan baik, terutama untuk klasifikasi biner yang memerlukan kemampuan generalisasi yang baik . SVM bekerja dengan cara memisahkan data menjadi dua kelas yang berbeda dengan hyperplane atau fungsi keputusan linear yang optimal (Noble, 2006).

SVM telah berhasil diterapkan di berbagai aplikasi seperti pengenalan tanda tangan digital, deteksi kecurangan kartu kredit, analisis ekspresi gen mikro array, dan lain-lain. Kemampuan SVM untuk dapat bekerja dengan baik pada data berdimensi tinggi dan memberikan hasil yang konsisten membuat algoritma ini banyak diadopsi di berbagai bidang (Fahmi, 2021). Selain itu, SVM juga memiliki kemampuan untuk menghindari overfitting yang baik, sehingga dapat memberikan performa yang konsisten dan dapat diandalkan (Xia et al., 2009). Algoritma SVM pada dasarnya melakukan optimisasi untuk mencari hyperplane terbaik yang memisahkan dua kelas dengan margin yang maksimal. Pemilihan fungsi kernel yang tepat juga menjadi komponen penting dalam penerapan SVM agar dapat menyelesaikan masalah yang non-linear. Dengan kemampuan tersebut, SVM telah terbukti menjadi algoritma yang sangat efektif dan banyak digunakan dalam berbagai aplikasi klasifikasi dan prediksi yang kompleks.

K-Nearest Neighbors (KNN)

K-Nearest Neighbors merupakan salah satu algoritma pembelajaran mesin supervised yang dapat digunakan untuk masalah klasifikasi biner maupun regresi (Ismanto & Cynthia, 2019). Algoritma ini terkenal karena kesederhanaannya dan efektifitasnya . K-NN bekerja dengan mencari k tetangga terdekat dari sampel uji, kemudian memprediksi kelas atau nilai berdasarkan suara mayoritas dari k tetangga terdekat (Taunk et al., 2019).

Algoritma ini telah digunakan secara luas dalam berbagai aplikasi, seperti prediksi penyakit dan deteksi penipuan pada kartu kredit. Kinerja K-NN sangat bergantung pada pemilihan parameter k dan ukuran dataset yang digunakan. Semakin besar nilai k, algoritma akan menjadi lebih stabil tetapi berisiko kehilangan kemampuan membedakan antara kelas yang berdekatan (Uddin et al., 2022). Sedangkan dataset yang besar akan meningkatkan akurasi prediksi algoritma, tetapi membutuhkan lebih banyak sumber daya komputasi (Bansal & Garg, 2021).

Naive Bayes

Penelitian empiris telah menunjukkan bahwa algoritma Naive Bayes dapat memberikan hasil yang baik bahkan pada dataset yang melanggar asumsi independensi fitur. Algoritma ini menggunakan teorema

Bayes untuk menghitung probabilitas kelas berdasarkan nilai atribut yang diberikan, dengan asumsi bahwa semua atribut saling independen (Qisthiano et al., 2021). Metode ini dapat mengatasi masalah missing value dengan menggunakan pendekatan imputasi, seperti menggantikan nilai hilang dengan nilai rata-rata atau modus. Selain itu, Naive Bayes juga cukup kuat dalam menangani data yang bersifat noisy (Azis et al., 2020). Meskipun demikian, apabila asumsi independensi fitur tidak terpenuhi, maka kinerja Naive Bayes dapat menurun. Oleh karena itu, Naive Bayes baik digunakan pada data yang memiliki independensi antar fitur, tetapi bisa kurang akurat jika asumsi independensi tidak terpenuhi.

Algoritma Naive Bayes telah banyak diterapkan dalam berbagai bidang, seperti klasifikasi teks dan prediksi kelulusan mahasiswa (Fauzan & Hikmah, 2022). Penelitian lain juga menunjukkan penerapan Naive Bayes untuk memprediksi penerima beasiswa (Mulyani et al., 2022). Secara umum, Naive Bayes merupakan algoritma yang cukup efektif dan efisien untuk berbagai tugas klasifikasi, terutama pada dataset dengan asumsi independensi fitur yang terpenuhi.

Neural Networks

Deep learning adalah salah satu cabang machine learning yang banyak digunakan saat ini untuk berbagai tugas, seperti klasifikasi citra, pengenalan suara, dan pemrosesan bahasa al ami. Metode-metode deep learning telah menunjukkan kemampuannya yang unggul dalam menyelesaikan masalah-masalah kompleks, mampu mengungguli metode-metode konvensional di berbagai bidang (Eka Putra, 2016). Salah satu arsitektur deep learning yang banyak digunakan untuk pengolahan citra adalah Convolutional Neural Network. CNN telah berhasil mencapai akurasi yang menyaingi kemampuan manusia dalam pengenalan pola pada dataset-dataset tertentu. Penelitian yang dilakukan oleh Usman Sudibyo dan Jasril menunjukkan bahwa CNN dengan arsitektur ResNet-50 dapat mencapai tingkat akurasi yang baik dalam mengkl asifikasikan citra daging sapi dan daging babi (Lasniari et al., 2022). Selain itu, penggunaan CNN juga telah diterapkan pada berbagai aplikasi di bidang medis, seperti diagnosis penyakit jantung (Gupta et al., 2022).

Namun, keberhasilan penerapan CNN sangat bergantung pada pemrosesan data yang tepat, khususnya dalam tahap preprocessing dan seleksi fitur. Karakteristik khusus dari data masukan, seperti ukuran, resolusi, dan variasi bentuk, perlu dipertimbangkan dengan saksama agar kinerja CNN dapat maksimal (Saiful rahman et al., 2019).

Pembahasan

Kompleksitas vs. Akurasi

Algoritma seperti Neural Networks dan Random Forest menunjukkan akurasi yang sangat tinggi, namun dengan biaya kompleksitas komputasi yang juga tinggi. Algoritma ini cocok untuk aplikasi di mana akurasi sangat kritis dan sumber daya komputasi bukan menjadi kendala utama. Metode peramalan cuaca yang menggabungkan Metode Siklis dan Adaptive Neuro Fuzzy Inference System dapat menjadi pendekatan yang menarik. Metode Siklis memiliki kelebihan dalam meramalkan dalam rentang waktu tertentu yang memiliki sifat fluktuatif, sedangkan ANFIS dapat menanggapi kompleksitas yang lebih tinggi.

Teknik data mining seperti Neural Networks dan Random Forest telah menunjukkan hasil yang sangat baik dalam berbagai aplikasi prediksi, termasuk prediksi jumlah penderita COVID-19. Namun, perlu diperhatikan bahwa kompleksitas komputasi dari algoritma tersebut relatif tinggi, sehingga bukan pilihan yang cocok untuk semua kasus. Integrasi teknik seperti Nearest Neighbor dengan pembobotan kriteria

menggunakan AHP dapat menjadi solusi yang lebih efisien dengan tetap mempertahankan akurasi yang baik. Dalam melakukan analisis prediktif, tahapan persiapan data (data preparation) memegang peranan yang sangat penting. Teknik data preparation seperti data selection, data pre-processing, dan data cleaning harus dilakukan dengan seksama untuk memastikan kualitas data yang digunakan (Perwitasari et al., 2023).

Kecepatan dan Efisiensi

Naive Bayes dan Decision Tree menawarkan solusi yang lebih cepat dan efisien dalam hal komputasi. Algoritma ini sangat berguna dalam skenario di mana kecepatan deteksi lebih penting daripada akurasi maksimal. Naive Bayes adalah algoritma klasifikasi sederhana yang menggunakan probabilitas untuk memprediksi kelas data berdasarkan fitur-fiturnya. Meskipun asumsi independensi antar fitur dapat terlihat terlalu sederhana, algoritma ini telah terbukti efektif dalam aplikasi dunia nyata. Decision Tree adalah algoritma yang memodelkan keputusan sebagai struktur hierarkis (Pandiangan et al., 2020).

Kedua algoritma ini memiliki kelebihan masing-masing. Naive Bayes mampu melakukan klasifikasi dengan cepat dan menghasilkan hasil yang dapat diinterpretasikan dengan mudah. Di sisi lain, Decision Tree menghasilkan model yang dapat diinspeksi secara visual dan menunjukkan alur pengambilan keputusan dengan jelas.

Pilihan algoritma sangat bergantung pada karakteristik dataset yang digunakan. Misalnya, SVM sangat efektif untuk data berdimensi tinggi, sedangkan KNN lebih cocok untuk dataset yang lebih kecil dan seimbang. Beberapa studi menunjukkan bahwa kombinasi atau ensemble dari beberapa algoritma dapat memberikan performa yang lebih baik daripada penggunaan satu algoritma saja. Misalnya, menggunakan Random Forest atau ensemble learning dapat mengurangi overfitting dan meningkatkan akurasi. Beberapa algoritma seperti SVM dan Neural Networks memerlukan tuning parameter yang ekstensif untuk mencapai performa optimal. Ini berarti waktu dan sumber daya yang lebih besar harus dialokasikan untuk eksperimen dan validasi.

Dari studi literatur ini, jelas bahwa tidak ada satu algoritma yang secara universal lebih baik daripada yang lain untuk semua situasi deteksi intrusi. Pemilihan algoritma harus didasarkan pada kebutuhan spesifik dari aplikasi, termasuk karakteristik data, kebutuhan akurasi, kecepatan, dan sumber daya komputasi yang tersedia. Untuk implementasi praktis, disarankan untuk melakukan uji coba beberapa algoritma pada dataset yang relevan dan mempertimbangkan penggunaan teknik ensemble untuk menggabungkan kelebihan dari berbagai algoritma. Selain itu, terus mengikuti perkembangan terbaru dalam penelitian machine learning dan keamanan jaringan sangat penting untuk memastikan sistem deteksi intrusi tetap efektif dalam menghadapi ancaman yang terus berkembang.

KESIMPULAN

Studi literatur ini bertujuan untuk membandingkan berbagai algoritma klasifikasi yang digunakan dalam sistem deteksi intrusi *(Intrusion Detection System/IDS)* pada jaringan komputer. Beberapa algoritma yang dianalisis termasuk Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Naive Bayes, dan Neural Networks. Neural Networks dan Random Forest: Kedua algoritma ini menunjukkan akurasi yang sangat tinggi dalam mendeteksi berbagai jenis serangan intrusi. Mereka mampu menangkap pola yang kompleks dalam data yang besar, menjadikannya pilihan yang sangat efektif untuk deteksi intrusi. SVM juga menunjukkan performa yang baik, terutama pada data berdimensi

tinggi dan dengan margin kelas yang jelas. Naive Bayes dan Decision Tree: Algoritma ini menawarkan kecepatan pelatihan dan prediksi yang tinggi serta efisiensi komputasi yang baik, menjadikannya pilihan ideal untuk aplikasi di mana kecepatan deteksi lebih diutamakan. KNN Sementara sederhana dan mudah diimplementasikan, KNN dapat menjadi lambat dalam proses prediksi untuk dataset besar karena membutuhkan perhitungan jarak ke semua titik data.

DAFTAR PUSTAKA

Adhi Tama, B., Nkenyereye, L., & Lim, S. (2021). A Stacking-based Deep Neural Network Approach for Effective Network Anomaly Detection. *Computers, Materials & Continua*, *66*(2), 2217–2227. https://doi.org/10.32604/cmc.2020.012432

Anwar, S., Septian, F., & Septiana, R. D. (2019). Klasifikasi Anomali Intrusion Detection System (IDS) Menggunakan Algoritma Naïve Bayes Classifier dan Correlation-Based Feature Selection. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *2*(4), 135. https://doi.org/10.32493/jtsi.v2i4.3453

Azis, A. I. S., Budy Santoso, & Serwin. (2020). LL-KNN ACW-NB: Local Learning K-Nearest Neighbor in Absolute Correlation Weighted Naïve Bayes for Numerical Data Classification. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(1), 28–36. https://doi.org/10.29207/resti.v4i1.1348

Bansal, A., & Garg, H. (2021). An Efficient Techniques for Fraudulent detection in Credit Card Dataset: A Comprehensive study. *IOP Conference Series: Materials Science and Engineering*, *1116*(1), 012181. https://doi.org/10.1088/1757-899X/1116/1/012181

Bhatia, V., Choudhary, S., & Ramkumar, K. . (2020). A Comparative Study on Various Intrusion Detection Techniques Using Machine Learning and Neural Network. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 232–236. https://doi.org/10.1109/ICRITO48877.2020.9198008

Bhuyan, S., Barman, D. K., & Bhowmick, A. (2018). Wireless Network Security Using Intrusion Detection System. *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 934–938. https://doi.org/10.1109/ICOEI.2018.8553724

Chaudhari, K., Connor, P. M., Comden, J., & King, J. (2022). Learning Assisted Demand Charge Mitigation for Workplace Electric Vehicle Charging. *IEEE Access*, *10*, 48283–48291. https://doi.org/10.1109/ACCESS.2022.3172334

Constantinides, C., Shiaeles, S., Ghita, B., & Kolokotronis, N. (2019). A Novel Online Incremental Learning Intrusion Prevention System. *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–6. https://doi.org/10.1109/NTMS.2019.8763842

Eka Putra, W. S. (2016). Klasifikasi Citra Menggunakan Convolutional Neural Network (CNN) pada Caltech 101. *Jurnal Teknik ITS*, *5*(1). https://doi.org/10.12962/j23373539.v5i1.15696

Fahmi, F. (2021). Model Support Vector Regression (SVR) Berdimensi Tinggi dengan Pendekatan Fungsi Kernel Berbeda untuk Peramalan Harga Saham TLKM: Sebuah Pemodelan Deret Waktu Selama Masa Pandemi Covid-19. *Jurnal Infomedia*, *5*(2), 44. https://doi.org/10.30811/jim.v5i2.2033

Fauzan, A. C., & Hikmah, K. (2022). IMPLEMENTASI ALGORITMA NAIVE BAYES DALAM ANALISIS POLARISASI OPINI MASYARAKAT TERKAIT VAKSIN COVID-19. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *7*(2), 122–128. https://doi.org/10.36341/rabit.v7i2.2403

Gupta, M. D., Kunal, S., Girish, M. P., Gupta, A., & Yadav, R. (2022). Artificial intelligence in cardiology:

The past, present and future. *Indian Heart Journal*, *74*(4), 265–269. https://doi.org/10.1016/j.ihj.2022.07.004

Ismanto, E., & Cynthia, E. P. (2019). Identification of the Success of Learning Al Islam and Kemuhammadiyahan Using Machine Learning. *Proceedings of the International Conference of CELSciTech 2019 - Science and Technology Track (ICCELST-ST 2019)*. https://doi.org/10.2991/iccelst-st-19.2019.1

Kibriya, H., Amin, R., Kim, J., Nawaz, M., & Gantassi, R. (2023). A Novel Approach for Brain Tumor Classification Using an Ensemble of Deep and Hand-Crafted Features. *Sensors*, *23*(10), 4693. https://doi.org/10.3390/s23104693

Lasniari, S., Jasril, J., Sanjaya, S., Yanto, F., & Affandes, M. (2022). Klasifikasi Citra Daging Babi dan Daging Sapi Menggunakan Deep Learning Arsitektur ResNet-50 dengan Augmentasi Citra. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *3*(4), 450. https://doi.org/10.30865/json.v3i4.4167

Mulyani, A., Kurniadi, D., Nashrulloh, M. R., Julianto, I. T., & Regita, M. (2022). THE PREDICTION OF PPA AND KIP-KULIAH SCHOLARSHIP RECIPIENTS USING NAIVE BAYES ALGORITHM. *Jurnal Teknik Informatika (Jutif)*, *3*(4), 821–827. https://doi.org/10.20884/1.jutif.2022.3.4.297

Noble, W. S. (2006). What is a support vector machine? *Nature Biotechnology*, *24*(12), 1565–1567. https://doi.org/10.1038/nbt1206-1565

Pandiangan, N., Buono, M. L. C., & Loppies, S. H. D. (2020). Implementation of Decision Tree and Naïve Bayes Classification Method for Predicting Study Period. *Journal of Physics: Conference Series*, *1569*(2), 022022. https://doi.org/10.1088/1742-6596/1569/2/022022

Perwitasari, A., Septiriana, R., & Tursina, T. (2023). Data preparation Structure untuk Pemodelan Prediktif Jumlah Peserta Ajar Matakuliah. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *9*(1), 7. https://doi.org/10.26418/jp.v8i3.57321

Purwananto, Y., Purwitasari, D., & Nugroho, Y. (2004). PENGKATEGORIAN ISI BERITA BERBAHASA INDONESIA MENGGUNAKAN ALGORITMA SYMBOLIC RULE INDUCTION BERBASIS DECISION TREE. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *3*(1), 55. https://doi.org/10.12962/j24068535.v3i1.a131

Qisthiano, M. R., Kurniawan, T. B., Negara, E. S., & Akbar, M. (2021). Pengembangan Model Untuk Prediksi Tingkat Kelulusan Mahasiswa Tepat Waktu dengan Metode Naïve Bayes. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(3), 987. https://doi.org/10.30865/mib.v5i3.3030

Raharjo, A. B., Ardianto, A., & Purwitasari, D. (2022). Random Forest Regression Untuk Prediksi Produksi Daya Pembangkit Listrik Tenaga Surya. *Briliant: Jurnal Riset Dan Konseptual*, *7*(4), 1058. https://doi.org/10.28926/briliant.v7i4.1036

Rokach, L. (2016). Decision forest: Twenty years of research. *Information Fusion*, *27*, 111–125. https://doi.org/10.1016/j.inffus.2015.06.005

Saiful rahman, A. F., B, A. A., & Kurniawan, S. D. (2019). IDENTIFIKASI CITRA DAUN DENGAN MENGGUNAKAN METODE DEEP LEARNING CONVOLUTIONAL NEURAL NETWORK (CNN). *Jurnal Teknik Elektro Uniba (JTE Uniba)*, *4*(1), 23–28. https://doi.org/10.36277/jteuniba.v4i1.55

Setiawan, H., Munandar, M. A., & Astuti, L. W. (2021). Penggunaan Metode Signature Based dalam Pengenalan Pola Serangan di Jaringan Komputer. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*(3), 517–524. https://doi.org/10.25126/jtiik.2021834200

Shashank, K., & Balachandra, M. (2018). Review on Network Intrusion Detection Techniques using Machine Learning. *2018 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, 104–109. https://doi.org/10.1109/DISCOVER.2018.8673974

Singh, G., & Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, *44*(7), 659–669. https://doi.org/10.1080/1206212X.2021.1885150

Siswoyo, B. (2020). MultiClass Decision Forest Machine Learning Artificial Intelligence. *Journal of Applied Informatics and Computing*, *4*(1), 1–7. https://doi.org/10.30871/jaic.v4i1.1155

Solanki, S., Gupta, C., & Rai, K. (2020). A Survey on Machine Learning based Intrusion Detection System on NSL-KDD Dataset. *International Journal of Computer Applications*, *176*(30), 36–39. https://doi.org/10.5120/ijca2020920343

Taunk, K., De, S., Verma, S., & Swetapadma, A. (2019). A Brief Review of Nearest Neighbor Algorithm for Learning and Classification. *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, 1255–1260. https://doi.org/10.1109/ICCS45141.2019.9065747

Wijaya, B., & Pratama, A. (2020). DETEKSI PENYUSUPAN PADA SERVER MENGGUNAKAN METODE INTRUSION DETECTION SYSTEM (IDS) BERBASIS SNORT. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(1), 97–101. https://doi.org/10.32736/sisfokom.v9i1.770

Xia, C., Deng, F., Wang, Y., Xu, Z., Liu, G., Xu, J., & Gewiss, H. (2009). Classification Research on Syndromes of TCM Based on SVM. *2009 2nd International Conference on Biomedical Engineering and Informatics*, 1–4. https://doi.org/10.1109/BMEI.2009.5305418

Zhang, L., & Suganthan, P. N. (2015). Oblique Decision Tree Ensemble via Multisurface Proximal Support Vector Machine. *IEEE Transactions on Cybernetics*, *45*(10), 2165–2176. https://doi.org/10.1109/TCYB.2014.2366468