Jurnal Sistem Informasi dan Teknik Informatika
Vol. 1, No. 1, February 2023, pp. 28~33
E-ISSN: 0000-0000, P-ISSN: 0000-0000, DOI: -

Preliminary Study for Cyber Intrusion Detection Using Machine Learning Approach

Amirah, Fitrah Karimah
PT. Lentera Ilmu Publisher, Prabumulih, Indonesia

Article Info

Article history:

Received Nov 10th, 2022
Revised Jan 20th, 2023
Accepted Feb 10th, 2023

Corresponding Author:

Amirah
PT. Lentera Ilmu Publisher,
Prabumulih, Indonesia
Email:
white99pasific@gmail.com

Abstrak

Artikel ini membahas pentingnya keamanan sistem informasi di era teknologi saat ini dan bagaimana ancaman serangan cyber yang semakin kompleks menuntut pendekatan yang lebih canggih dalam deteksi dan pencegahannya. Studi awal ini mengeksplorasi potensi penerapan Machine Learning dalam deteksi intrusi cyber sebagai langkah awal untuk mengembangkan sistem deteksi yang adaptif dan responsif terhadap ancaman yang terus berkembang. Melalui metodologi yang melibatkan pengumpulan data representatif tentang serangan cyber, persiapan data, dan pemilihan model Machine Learning, artikel ini menjelaskan tahapan awal untuk memahami dan menguji potensi teknologi ini dalam konteks keamanan cyber. Meskipun mencakup contoh dataset, langkah-langkah persiapan data, dan pemilihan beberapa algoritma Machine Learning, studi ini hanya sampai pada tahap pemilihan model, sementara proses pelatihan model dan evaluasi performa menjadi fokus pekerjaan selanjutnya. Kesimpulan dari studi awal ini menekankan pentingnya pemilihan algoritma yang sesuai dengan fitur-fitur tertentu untuk deteksi intrusi yang efektif terhadap ancaman cyber yang semakin berkembang.

Kata Kunci: Keamanan sistem informasi, Serangan cyber, Machine Learning

Abstract

This article discusses the importance of information system security in the current technological era and how the increasingly complex threat of cyber attacks demands a more sophisticated approach to detection and prevention. This initial study explores the potential of applying Machine Learning in cyber intrusion detection as a first step to developing detection systems that are adaptive and responsive to evolving threats. Through a methodology involving the collection of representative data on cyber attacks, data preparation, and Machine Learning model selection, this article describes the initial stages for understanding and testing the potential of this technology in the context of cyber security. Although it includes an example dataset, data preparation steps, and the selection of several Machine Learning algorithms, this study only gets to the model selection stage, while the model training process and performance evaluation are the focus of future work. The conclusions of this initial study emphasize the importance of selecting appropriate algorithms with specific features for effective intrusion detection against growing cyber threats.

Keywords: *Information system security, Cyber attacks, Machine Learning*

1. PENDAHULUAN

Pada era di mana teknologi telah merasuki setiap aspek kehidupan kita, keamanan sistem informasi menjadi suatu keharusan yang semakin mendesak. Ancaman serangan cyber semakin berkembang dan menuntut pendekatan yang lebih canggih untuk mendeteksi dan mencegahnya. Dalam menjawab tantangan

ini, pendekatan berbasis Machine Learning menjadi terobosan yang menjanjikan dalam mengidentifikasi pola-pola aneh atau serangan dalam lalu lintas data [1], [2], [3], [4]. Studi awal ini mengambil peran penting dalam mengeksplorasi potensi penerapan Machine Learning dalam deteksi intrusi cyber, dengan tujuan utama merintis jalan bagi pengembangan sistem deteksi yang lebih adaptif dan responsif terhadap ancaman-ancaman yang semakin kompleks.

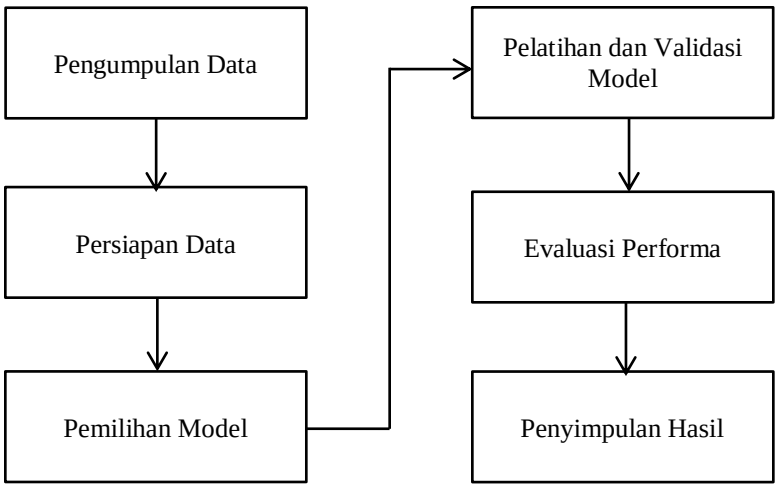
Keamanan sistem informasi menjadi fokus yang semakin krusial seiring dengan interkoneksi yang meluas dalam dunia digital. Serangan cyber, mulai dari yang sederhana hingga yang sangat kompleks, telah menjadi ancaman serius bagi individu, perusahaan, bahkan infrastruktur Negara [5], [6], [7]. Dalam konteks ini, pendekatan tradisional dalam deteksi intrusi, seperti penandatanganan pola serangan, seringkali kurang mampu menangkap serangan yang baru dan tidak teridentifikasi sebelumnya. Inilah di mana Machine Learning dapat menjadi kunci dalam menghadapi tantangan ini dengan memberikan sistem kemampuan untuk belajar dan beradaptasi terhadap pola-pola serangan yang berkembang.

Penelitian ini bertujuan untuk memberikan landasan awal yang kokoh dalam memahami serta menguji potensi Machine Learning dalam konteks deteksi intrusi cyber. Fokusnya adalah pada penggunaan algoritma Machine Learning untuk mengidentifikasi pola-pola mencurigakan dalam data lalu lintas jaringan yang dapat mengindikasikan adanya serangan cyber. Dengan melakukan analisis mendalam terhadap berbagai metode Machine Learning, diharapkan akan terungkap potensi serta batasan dalam menggunakan pendekatan ini dalam menghadapi ancaman-ancaman keamanan yang semakin canggih.

Melalui penggabungan teknologi Machine Learning dengan kebutuhan mendesak akan keamanan cyber, study ini berharap dapat memberikan kontribusi penting dalam pengembangan sistem deteksi intrusi yang adaptif dan efektif. Dengan memahami dan menggali potensi teknologi ini pada tahap awal, diharapkan akan tercipta landasan yang kuat bagi pengembangan solusi keamanan yang lebih canggih dan responsif dalam menghadapi dinamika ancaman cyber yang terus berkembang.

2. METODE

Metodologi penelitian yang dapat diterapkan untuk studi awal mengenai deteksi intrusi cyber dengan pendekatan Machine Learning melibatkan serangkaian langkah yang sistematis dan cermat. Berikut adalah beberapa tahapan metodologi yang dapat digunakan (Gambar 1):



Gambar 1. Desain Penelitian

2.1. Pengumpulan Data

Tahap pertama adalah mengumpulkan dataset yang representatif tentang serangan cyber. Data ini dapat terdiri dari berbagai jenis serangan seperti DoS, malware, phishing, dan serangan lainnya. Sumber data dapat berasal dari repositori publik yang menyediakan dataset serangan cyber atau dari simulasi serangan yang direkam secara internal.

2.2. Persiapan Data

Data yang dikumpulkan perlu disiapkan sebelum dapat digunakan untuk pelatihan dan pengujian model Machine Learning. Langkah ini melibatkan pembersihan data untuk menghilangkan noise,

pengkodean fitur-fitur yang relevan, dan pembagian data menjadi subset untuk pelatihan, validasi, dan pengujian model.

2.3. Pemilihan Model Machine Learning

Tahap selanjutnya adalah memilih model atau algoritma Machine Learning yang sesuai untuk deteksi intrusi cyber. Ini dapat mencakup penggunaan Decision Trees, Support Vector Machines, Neural Networks, atau ensemble learning seperti Random Forests. Setiap model akan dievaluasi untuk melihat performanya dalam mendeteksi serangan berdasarkan dataset yang ada.

2.4. Pelatihan dan Validasi Model

Model Machine Learning yang dipilih akan dilatih menggunakan data yang telah dipersiapkan sebelumnya. Proses pelatihan ini akan melibatkan penyesuaian parameter-parameter model untuk meningkatkan akurasi dan kinerja deteksi intrusi. Selanjutnya, model akan divalidasi menggunakan subset data yang terpisah untuk memastikan bahwa model tidak mengalami overfitting dan dapat melakukan generalisasi dengan baik.

2.5. Evaluasi Performa

Performa model akan dievaluasi menggunakan metrik-metrik seperti akurasi, presisi, recall, dan F1-score [8]. Analisis ini akan memberikan pemahaman tentang seberapa baik model-machine learning yang diimplementasikan dapat mendeteksi dan mengklasifikasikan serangan cyber dengan benar.

2.6. Penyimpulan Hasil

Hasil dari evaluasi performa akan dianalisis secara mendalam untuk mengevaluasi kekuatan dan kelemahan dari pendekatan Machine Learning yang diadopsi dalam deteksi intrusi. Penyimpulan ini akan menginformasikan tentang kemungkinan pengembangan dan peningkatan yang diperlukan dalam model untuk mencapai tingkat keakuratan dan responsivitas yang lebih baik.

Dalam artikel ini penulis hanya membahas sampai pada tahap ketiga yaitu pemilihan model machine learning, untuk tahap pelatihan model dan seterusnya akan menjadi pekerjaan selanjutnya dimasa mendatang.

3. HASIL DAN PEMBAHASAN

Tahap pertama setelah memiliki pengetahuan melalui studi literatur adalah proses pengumpulan data, kemudian persiapan data dan pemilihan model machine learning.

3.1. Pengumpulan Data

Dataset dalam konteks Machine Learning adalah kumpulan data yang terstruktur dan terorganisir yang digunakan untuk melatih, menguji, dan mengembangkan model atau algoritma Machine Learning. Dataset terdiri dari contoh-contoh yang direpresentasikan dalam bentuk fitur atau atribut, yang diberikan dengan label atau tanpa label tergantung pada jenis pembelajaran yang dilakukan: supervised learning (dengan label) atau unsupervised learning (tanpa label).

1. Fitur/Atribut: Ini adalah variabel atau informasi yang digunakan oleh model untuk membuat prediksi atau menemukan pola. Contohnya, dalam dataset untuk prediksi harga rumah, fitur mungkin mencakup luas tanah, jumlah kamar tidur, lokasi, dll.
2. Label: Dalam supervised learning, label adalah hasil yang ingin diprediksi oleh model. Misalnya, dalam masalah klasifikasi spam email, label akan menunjukkan apakah email tersebut adalah spam atau bukan (spam = 1, bukan spam = 0).
3. Observasi/Sampel: Setiap baris dalam dataset mewakili satu contoh data atau observasi. Misalnya, jika dataset mewakili informasi tentang pelanggan, setiap baris dapat mewakili satu pelanggan.

Dataset dibagi menjadi set pelatihan (training set) untuk melatih model, set validasi (validation set) untuk mengevaluasi kinerja selama pelatihan, dan set pengujian (test set) untuk menguji kinerja model yang telah dilatih [9]. Dataset yang baik dan representatif sangat penting untuk mendapatkan model Machine Learning yang efektif dan akurat. Dataset dapat berasal dari berbagai sumber, termasuk data yang terkumpul dari sensor-sensor, rekaman transaksi, informasi dari database, atau hasil dari pengambilan sampel dalam penelitian atau eksperimen tertentu. Preprocessing data, seperti membersihkan data yang tidak lengkap atau tidak valid, normalisasi, dan ekstraksi fitur, seringkali dilakukan sebelum dataset digunakan untuk melatih model Machine Learning. Contoh dataset yang dapat digunakan untuk studi awal deteksi intrusi cyber dengan pendekatan Machine Learning (Tabel 1):

Tabel 1. Contoh Dataset

Durasi (detik)	Protocol Type	Service	Flag	Byte In	Byte Out	Outcome
0.2	TCP	http	SF	215	450	Normal
0.5	UDP	domain	S0	0	0	Intrusion
2.0	TCP	ftp	REJ	0	0	Intrusion
1.6	UDP	private	RSTO	234	123	Normal
0.8	TCP	ssh	SF	153	231	Normal
3.2	TCP	smtp	RSTO	0	0	Intrusion
2.1	UDP	domain	S0	0	0	Intrusion
1.9	TCP	http	SF	124	432	Normal
0.4	UDP	private	S0	0	0	Intrusion
2.5	TCP	ftp	REJ	0	0	Intrusion

Dataset ini terdiri dari beberapa kolom yang mewakili atribut-atribut atau fitur-fitur tertentu dan label "Outcome" yang menunjukkan apakah kejadian tersebut dianggap sebagai serangan (Intrusion) atau tidak (Normal). Berikut adalah penjelasan untuk setiap kolom dalam tabel:

1. Durasi (detik): Atribut ini menunjukkan durasi dari kegiatan atau aktivitas tertentu dalam detik. Contohnya, nilai 0.2 detik pada baris pertama menunjukkan kegiatan tersebut berlangsung selama 0.2 detik.
2. Protocol Type: Ini adalah jenis protokol yang digunakan dalam aktivitas jaringan. Contohnya, TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol) adalah jenis protokol yang umum digunakan dalam komunikasi jaringan.
3. Service: Kolom ini menunjukkan layanan atau service yang digunakan dalam aktivitas jaringan. Misalnya, http (Hypertext Transfer Protocol) digunakan untuk akses web, ftp (File Transfer Protocol) untuk transfer file, ssh (Secure Shell) untuk akses jarak jauh yang aman, dll.
4. Flag: Flag dalam konteks jaringan mengacu pada status atau tanda dari koneksi tersebut. Contohnya, SF (Established Connection), S0 (Connection Attempt), dan REJ (Connection Rejected) adalah beberapa contoh status koneksi yang dapat terlihat dalam aktivitas jaringan.
5. Byte In: Ini adalah jumlah byte yang masuk selama koneksi atau aktivitas tertentu. Nilai 215 pada baris pertama menunjukkan bahwa ada 215 byte yang masuk dalam aktivitas tersebut.
6. Byte Out: Kolom ini mencatat jumlah byte yang keluar selama koneksi atau aktivitas jaringan berlangsung. Misalnya, nilai 450 pada baris pertama menunjukkan bahwa ada 450 byte yang keluar selama aktivitas tersebut.
7. Outcome: Label "Outcome" menunjukkan hasil atau klasifikasi dari aktivitas jaringan tersebut. Jika tertulis "Normal", itu berarti aktivitas tersebut dianggap sebagai aktivitas yang normal. Namun, jika tertulis "Intrusion", itu menandakan bahwa aktivitas tersebut dianggap sebagai serangan atau intrusion pada sistem.

Tabel ini menggambarkan beberapa contoh aktivitas atau transaksi jaringan dengan atribut-atribut tertentu yang merepresentasikan karakteristik dari aktivitas tersebut. Dataset semacam ini dapat digunakan untuk melatih model Machine Learning untuk mengklasifikasikan aktivitas jaringan apakah termasuk sebagai serangan atau tidak, berdasarkan fitur-fitur yang tercatat dalam tabel.

3.2. Persiapan Data

Tahap persiapan data dalam konteks Machine Learning adalah salah satu langkah kunci sebelum menggunakan dataset untuk melatih atau menguji model. Ini melibatkan sejumlah langkah untuk mempersiapkan data agar dapat digunakan secara efektif dalam proses pembelajaran. Berikut penjelasan tahapan persiapan data untuk dataset yang Anda berikan:

1. Penanganan Nilai Tidak Valid: Periksa dataset untuk nilai yang tidak valid atau tidak masuk akal. Dalam dataset ini, terdapat beberapa nilai yang patut diperhatikan, misalnya pada kolom "Byte In" dan "Byte Out" yang memiliki nilai 0. Hal ini bisa mengindikasikan koneksi yang tidak berhasil atau tidak memiliki transmisi data. Langkah ini penting untuk mengetahui apakah data yang tidak valid perlu dihapus atau diolah lebih lanjut.
2. Encoding Fitur Kategorikal: Beberapa kolom seperti "Protocol Type", "Service", dan "Flag" merupakan fitur kategorikal yang perlu diubah ke dalam bentuk numerik agar dapat diproses oleh algoritma Machine Learning. Hal ini dapat dilakukan dengan teknik seperti one-hot encoding, di mana setiap nilai kategori diganti menjadi kolom biner terpisah untuk setiap nilai unik dalam kolom tersebut.

3. Normalisasi atau Standarisasi: Beberapa algoritma Machine Learning dapat memberikan performa yang lebih baik jika data dinormalisasi atau distandarisasi. Ini berarti menyesuaikan skala atau rentang nilai dari setiap fitur agar tidak ada satu fitur pun yang mendominasi proses pembelajaran.
4. Pembagian Dataset: Dataset perlu dibagi menjadi set pelatihan (training set) dan set pengujian (test set). Set pelatihan digunakan untuk melatih model, sedangkan set pengujian digunakan untuk menguji kinerja model yang sudah dilatih. Dalam hal ini, pembagian dataset perlu dilakukan dengan proporsi yang tepat untuk memastikan evaluasi yang akurat terhadap model.
5. Penanganan Ketidakseimbangan Kelas: Jika terdapat ketidakseimbangan antara jumlah sampel dari kelas "Intrusion" dan "Normal" dalam label "Outcome", langkah penanganan kelas minoritas seperti oversampling, undersampling, atau menggunakan teknik pembobotan dapat dipertimbangkan untuk menghindari bias dalam pembelajaran model.

Tahapan persiapan data ini penting dalam memastikan bahwa dataset siap digunakan untuk melatih atau menguji model Machine Learning. Hal ini membantu dalam meningkatkan kualitas pembelajaran model serta memastikan hasil yang akurat dan dapat diandalkan saat digunakan untuk tugas-tugas analisis atau prediksi.

3.3. Pemilihan Model Machine Learning

berikut contoh 5 algoritma Machine Learning beserta fitur-fitur yang dapat diterapkan dalam penelitian deteksi intrusi cyber (Tabel 2):

Tabel 2. Pilihan Algoritma Machine Learning

No	Algoritma	Fitur-fitur yang Digunakan	Penjelasan
1	Decision Trees [10]	Durasi (detik), Protocol Type, Service, Flag, Byte In, Byte Out	Algoritma ini membuat keputusan berdasarkan aturan-aturan yang terbentuk dari fitur-fitur, membagi data ke dalam set keputusan berdasarkan nilai-nilai fitur.
2	Support Vector Machines [11], [12]	Durasi (detik), Protocol Type, Service, Flag, Byte In, Byte Out	SVM mencari hyperplane terbaik yang dapat memisahkan dua kelas dengan margin terbesar di antara kelas tersebut dalam ruang fitur.
3	Random Forests [13]	Durasi (detik), Protocol Type, Service, Flag, Byte In, Byte Out	Algoritma ini menggunakan beberapa pohon keputusan untuk melakukan klasifikasi. Setiap pohon memberikan hasil dan hasil mayoritas dipilih sebagai output.
4	Neural Networks [14]	Durasi (detik), Protocol Type, Service, Flag, Byte In, Byte Out	Jaringan saraf tiruan menggunakan lapisan-lapisan neuron yang saling terhubung untuk melakukan pemetaan dari input ke output.
5	k-Nearest Neighbors [15]	Durasi (detik), Protocol Type, Service, Flag, Byte In, Byte Out	Model ini menggunakan jarak terdekat dari titik-titik data tetangga untuk melakukan prediksi pada titik data baru berdasarkan mayoritas kelas di antara tetangganya.

Fitur-fitur yang dijelaskan dalam tabel ini mencakup atribut-atribut seperti durasi aktivitas, jenis protokol, layanan yang diakses, status flag koneksi, serta jumlah byte masuk dan keluar dalam aktivitas jaringan. Setiap algoritma memiliki cara yang berbeda dalam memanfaatkan fitur-fitur ini untuk melakukan prediksi terhadap aktivitas jaringan apakah termasuk sebagai serangan atau tidak. Pemilihan algoritma yang sesuai sangat tergantung pada karakteristik dataset dan kebutuhan spesifik dari penelitian deteksi intrusi cyber.

4. KESIMPULAN

Penulis melihat bahwa keamanan sistem informasi merupakan hal yang sangat penting dalam era teknologi saat ini. Ancaman serangan cyber semakin meningkat dan mengharuskan pendekatan yang lebih

canggih untuk mendeteksi dan mencegahnya. Di sinilah pendekatan berbasis Machine Learning menjadi relevan, karena mampu mengidentifikasi pola serangan atau anomali dalam lalu lintas data. Studi awal ini bertujuan untuk mengeksplorasi potensi penerapan Machine Learning dalam deteksi intrusi cyber sebagai upaya merintis jalan bagi pengembangan sistem deteksi yang adaptif dan responsif terhadap ancaman yang semakin kompleks. Terkait metodologi, penelitian ini melibatkan beberapa tahap sistematis, dimulai dari pengumpulan data tentang serangan cyber yang dapat berasal dari berbagai sumber, persiapan data untuk membersihkan, mengkodekan, dan mempersiapkan dataset, serta pemilihan model Machine Learning yang sesuai untuk deteksi intrusi. Pemilihan model mencakup beberapa algoritma yang dapat digunakan, seperti Decision Trees, Support Vector Machines, Random Forests, Neural Networks, dan k-Nearest Neighbors, yang masing-masing menggunakan fitur-fitur tertentu untuk melakukan prediksi terhadap aktivitas jaringan.

Dalam prosesnya, studi ini telah memperkenalkan contoh dataset yang mencakup atribut-atribut yang merepresentasikan aktivitas jaringan, seperti durasi, jenis protokol, layanan, status flag koneksi, byte masuk dan keluar, serta label yang menunjukkan apakah aktivitas tersebut dianggap sebagai serangan atau tidak. Selain itu, langkah-langkah persiapan data juga dijelaskan, termasuk penanganan nilai tidak valid, encoding fitur kategorikal, normalisasi data, pembagian dataset, dan penanganan ketidakseimbangan kelas. Namun, studi ini hanya mencakup tahap awal, yaitu pemilihan model Machine Learning, sementara proses pelatihan model dan evaluasi performa belum disertakan. Kesimpulan dari tahap awal ini menyoroti pentingnya pemilihan algoritma yang sesuai dengan fitur-fitur tertentu dan kebutuhan spesifik penelitian untuk memastikan deteksi intrusi yang efektif dalam menghadapi ancaman cyber yang terus berkembang.

DAFTAR PUSTAKA

[1] A. Sanmorino, "A study for DDOS attack classification method," *J. Phys.: Conf. Ser.*, vol. 1175, p. 012025, Mar. 2019, doi: 10.1088/1742-6596/1175/1/012025.

[2] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," *Procedia Computer Science*, vol. 218, pp. 2420–2429, 2023, doi: 10.1016/j.procs.2023.01.217.

[3] H. C. Altunay and Z. Albayrak, "A hybrid CNN + LSTM based intrusion detection system for industrial IoT networks," *Eng. Sci. Technol. an Int. J.*, vol. 38, p. 101322, 2023, doi: 10.1016/j.jestch.2022.101322.

[4] F. Ullah, S. Ullah, G. Srivastava, and J. C.-W. Lin, "IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic," *Digit. Commun. Networks*, 2023, doi: 10.1016/j.dcan.2023.03.008.

[5] M. P. Karpowicz, "Adaptive tuning of network traffic policing mechanisms for DDoS attack mitigation systems," *Eur. J. Control*, vol. 61, pp. 101–118, 2021, doi: 10.1016/j.ejcon.2021.07.001.

[6] J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, and S. Kandeepan, "A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks," *Eng. Sci. Technol. an Int. J.*, vol. 31, p. 101065, 2022, doi: 10.1016/j.jestch.2021.09.011.

[7] A. Iranmanesh and H. Reza Naji, "A protocol for cluster confirmations of SDN controllers against DDoS attacks," *Comput. Electr. Eng.*, vol. 93, no. June, p. 107265, 2021, doi: 10.1016/j.compeleceng.2021.107265.

[8] P. Fränti and R. Mariescu-Istodor, "Soft precision and recall," *Pattern Recognit. Lett.*, vol. 167, pp. 115–121, 2023, doi: 10.1016/j.patrec.2023.02.005.

[9] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Computer Science*, vol. 167, pp. 1561–1573, 2020, doi: 10.1016/j.procs.2020.03.367.

[10] Y. Li, E. Herrera-Viedma, G. Kou, and J. A. Morente-Molinera, "Z-number-valued rule-based decision trees," *Inf. Sci. (Ny).*, vol. 643, no. May, p. 119252, 2023, doi: 10.1016/j.ins.2023.119252.

[11] I. Zoppis, G. Mauri, and R. Dondi, Kernel methods: Support vector machines, vol. 1–3. *Elsevier Ltd.*, 2018. doi: 10.1016/B978-0-12-809633-8.20342-7.

[12] A. Gatera, M. Kuradusenge, G. Bajpai, C. Mikeka, and S. Shrivastava, "Comparison of random forest and support vector machine regression models for forecasting road accidents," *Sci. African*, vol. 21, p. e01739, 2023, doi: 10.1016/j.sciaf.2023.e01739.

[13] G. Stavropoulos, R. van Voorstenbosch, F.-J. van Schooten, and A. Smolinska, Random Forest and Ensemble Methods, *2nd ed. Elsevier Inc.*, 2020. doi: 10.1016/b978-0-12-409547-2.14589-5.

[14] S. Belattar, O. Abdoun, and E. K. Haimoudi, "Performance analysis of the application of convolutional neural networks architectures in the agricultural diagnosis," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 1, pp. 156–162, 2022, doi: 10.11591/ijeecs.v27.i1.pp156-162.

[15] Z. Sun, J. Wang, and M. Q. H. Meng, "Multi-Tree Guided Efficient Robot Motion Planning," *Procedia Comput. Sci.*, vol. 209, pp. 40–49, 2022, doi: 10.1016/j.procs.2022.10.096.