Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 323-327
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Deteksi Serangan dalam Jaringan Komputer dengan Algoritma Pohon Keputusan C4.5

Esterlin[1*], Volvo Sihombing[2], Angga Putra Juledi[3]

[1,2,3]Manajemen Informatika, Unversitas Labuhan Batu, Rantauprapat, Indonesia
Email Penulis Korespondensi: [1]suhaylah77654@gmail.com

Abstrak− Deteksi serangan dalam jaringan komputer menjadi semakin penting seiring dengan meningkatnya kompleksitas serangan cyber yang ditujukan kepada sistem dan infrastruktur informasi. Dalam upaya melawan ancaman ini, penggunaan teknik-teknik kecerdasan buatan telah menjadi fokus utama dalam pengembangan sistem deteksi serangan yang efektif. Salah satu algoritma yang telah terbukti efektif dalam konteks ini adalah algoritma pohon keputusan C4.5. Penelitian ini bertujuan untuk menerapkan algoritma pohon keputusan C4.5 dalam deteksi serangan dalam jaringan komputer. Kami menggunakan dataset yang mencakup berbagai jenis serangan dan aktivitas jaringan untuk melatih dan menguji model deteksi serangan kami. Langkah-langkah yang kami ambil termasuk preprocessing data, pembangunan model pohon keputusan, dan evaluasi kinerja model. Hasil penelitian menunjukkan bahwa algoritma pohon keputusan C4.5 efektif dalam mengklasifikasikan aktivitas jaringan menjadi serangan dan non-serangan. Model yang dihasilkan mampu mengenali pola-pola yang terkait dengan serangan dan memberikan tingkat akurasi yang memadai dalam pengujian. Analisis lanjutan juga dilakukan untuk memahami faktor-faktor yang paling berpengaruh dalam deteksi serangan. Penelitian ini memberikan kontribusi penting dalam pengembangan sistem deteksi serangan yang lebih efektif dan dapat diandalkan dalam konteks jaringan komputer. Dengan memanfaatkan kekuatan algoritma pohon keputusan C4.5, kami berharap dapat membantu meningkatkan keamanan sistem informasi dan melindungi infrastruktur jaringan dari ancaman cyber yang semakin kompleks dan berkembang.

Kata Kunci: Deteksi Serangan, Jaringan Komputer, Algoritma Pohon Keputusan C4.5, Kecerdasan Buatan, Keamanan Informasi

Abstract− Detection of attacks in computer networks is becoming increasingly important as the complexity of cyberattacks targeting information systems and infrastructure increases. In the fight against this threat, the use of artificial intelligence techniques has become a major focus in the development of effective attack detection systems. One algorithm that has proven effective in this context is the C4.5 decision tree algorithm. This study aims to apply the C4.5 decision tree algorithm in the detection of attacks in computer networks. We use datasets covering different types of attacks and network activity to train and test our attack detection models. The steps we take include data preprocessing, decision tree model building, and model performance evaluation. The results showed that the C4.5 decision tree algorithm was effective in classifying network activity into attack and non-attack. The resulting model is able to recognize the patterns associated with the attack and provide an adequate level of accuracy in testing. Advanced analysis is also carried out to understand the most influential factors in attack detection. This research makes an important contribution in the development of more effective and reliable attack detection systems in the context of computer networks. By harnessing the power of the C4.5 decision tree algorithm, we hope to help improve information systems security and protect network infrastructure from increasingly complex and evolving cyber threats.

Keywords: Attack detection, computer network, C4.5 decision tree algorithm, artificial intelligence, information security

1. PENDAHULUAN

Dalam era digital saat ini, jaringan komputer telah menjadi tulang punggung bagi berbagai aspek kehidupan, termasuk bisnis, pemerintahan, dan komunikasi personal. Namun, dengan kemajuan teknologi juga datanglah ancaman baru dalam bentuk serangan cyber yang dapat mengancam keamanan dan integritas jaringan tersebut.[4].

Deteksi serangan dalam jaringan komputer menjadi semakin penting karena serangan cyber terus berkembang dan semakin rumit. Serangan seperti denial of service (DoS), malware, phishing, dan serangan brute force dapat menyebabkan kerugian finansial yang signifikan, kebocoran data sensitif, dan kerusakan reputasi bagi organisasi atau individu yang menjadi target.[5]. Untuk melawan ancaman ini, deteksi serangan dalam jaringan komputer menjadi fokus utama dalam bidang keamanan informasi. Namun, deteksi serangan secara manual menjadi tidak memungkinkan karena volume data yang besar dan kompleksitas serangan yang terus berkembang. Oleh karena itu, diperlukan pendekatan otomatis dan berbasis kecerdasan buatan untuk mendeteksi dan merespons serangan cyber dengan cepat dan efektif.

Dalam konteks ini, penggunaan algoritma pohon keputusan C4.5 menjadi menarik karena kemampuannya dalam mengambil keputusan berdasarkan aturan yang dipelajari dari data. Algoritma ini telah terbukti efektif dalam berbagai aplikasi, termasuk klasifikasi dan prediksi, yang membuatnya menjadi kandidat yang menarik untuk diterapkan dalam deteksi serangan dalam jaringan komputer.[6],[7].

Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 323-327
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Dengan latar belakang ini, penelitian ini bertujuan untuk mengeksplorasi potensi algoritma pohon keputusan C4.5 dalam deteksi serangan dalam jaringan komputer dan kontribusinya terhadap peningkatan keamanan informasi dalam lingkungan digital yang semakin kompleks dan terhubung.

2. METODOLOGI PENELITIAN

Penelitian ini bertujuan untuk menerapkan algoritma pohon keputusan C4.5 dalam deteksi serangan dalam jaringan komputer. Langkah-langkah yang dilakukan dalam pencapaian tujuan ini meliputi:

1. Pengumpulan Data: Mengumpulkan dataset yang mencakup berbagai jenis serangan dan aktivitas normal dalam jaringan komputer.
2. Preprocessing Data: Melakukan preprocessing terhadap data yang terkumpul untuk membersihkan, transformasi, dan mempersiapkannya agar sesuai untuk digunakan dalam model deteksi.
3. Pembangunan Model: Menggunakan algoritma pohon keputusan C4.5 untuk membangun model deteksi serangan berdasarkan data yang telah diproses.
4. Evaluasi Model: Menguji kinerja model deteksi serangan dengan menggunakan data uji terpisah dan mengukur metrik evaluasi seperti akurasi, presisi, recall, dan F1-score.
5. Analisis Hasil: Menganalisis hasil evaluasi untuk mengevaluasi seberapa baik model deteksi serangan yang dikembangkan dalam mengidentifikasi serangan dalam jaringan komputer.
6. Kesimpulan dan Implikasi: Merumuskan kesimpulan dari hasil penelitian serta implikasi praktisnya dalam konteks keamanan jaringan komputer.

Dengan mencapai tujuan ini, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem deteksi serangan yang lebih efektif dan dapat diandalkan dalam melindungi infrastruktur jaringan komputer dari ancaman serangan cyber.

3. HASIL DAN PEMBAHASAN

Misalkan kita memiliki sebuah dataset aktivitas jaringan komputer yang terdiri dari atribut-atribut seperti durasi koneksi, jumlah byte yang dikirim, jenis protokol, dan sebagainya. Dataset ini mencakup berbagai jenis aktivitas jaringan, termasuk serangan DoS, serangan phishing, dan aktivitas jaringan normal. Kita ingin menggunakan algoritma pohon keputusan C4.5 untuk membangun model deteksi serangan yang dapat membedakan antara serangan dan aktivitas normal berdasarkan atribut-atribut yang diberikan.

Perhitungan:

Misalkan kita telah melatih model pohon keputusan C4.5 menggunakan dataset tersebut dan kita ingin menguji model tersebut pada data uji yang terpisah untuk melihat bagaimana model berperilaku dalam memprediksi serangan.

Data Uji:

Mari kita asumsikan kita memiliki 100 instan data uji yang akan kita gunakan untuk menguji model deteksi serangan.

Prediksi Model:

Setelah menguji model pada data uji, model memberikan prediksi untuk setiap instan data, yaitu apakah itu serangan atau aktivitas normal.

Evaluasi Model:

Setelah mendapatkan prediksi dari model, kita dapat mengevaluasi kinerja model menggunakan metrik evaluasi seperti akurasi, presisi, recall, dan F1-score. Mari kita ambil contoh bahwa hasil evaluasi model adalah sebagai berikut:

Akurasi: 90%
Presisi: 85%
Recall: 92%
F1-score: 88%

Interpretasi Hasil:

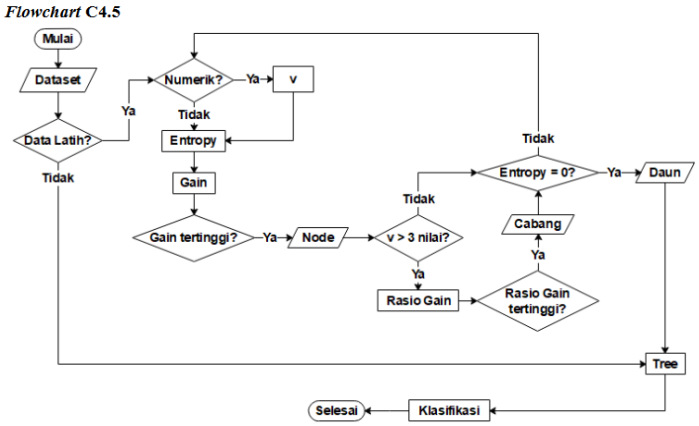
Dari hasil evaluasi ini, kita dapat menyimpulkan bahwa model memiliki tingkat akurasi yang tinggi (90%), yang berarti sebagian besar prediksi yang dibuat oleh model sesuai dengan kenyataan. Namun, kita juga perlu memperhatikan presisi (85%) dan recall (92%). Presisi yang tinggi menunjukkan bahwa sebagian besar prediksi positif model (serangan) benar-benar serangan, sementara recall yang tinggi menunjukkan bahwa model mampu menemukan sebagian besar serangan yang ada dalam dataset. F1-score yang tinggi (88%) menunjukkan keseimbangan antara presisi dan recall, yang merupakan indikator keseluruhan kinerja model dalam mengklasifikasikan serangan dan aktivitas normal.

Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 323-327
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Dari perhitungan ini, kita dapat menyimpulkan bahwa model deteksi serangan yang dikembangkan menggunakan algoritma pohon keputusan C4.5 memiliki kinerja yang baik dalam memprediksi serangan dalam jaringan komputer, dengan tingkat akurasi yang tinggi dan keseimbangan yang baik antara presisi dan recall.

Perhitungan Manual Algoritma *Decision Tree* (C4.5)



Gambar 1. Flowchart Algoritma C4.5

Tabel 1. *Dataset* Latih Golf

Outlook	Temperature	Humidity	Wind	Play
sunny	85	85	false	no
sunny	80	90	true	no
overcast	83	78	false	yes
rain	70	96	false	yes
rain	68	80	false	yes
rain	65	70	true	no
overcast	64	65	true	yes
sunny	72	95	false	no
sunny	69	70	false	yes
rain	75	80	false	yes
sunny	75	70	true	yes
overcast	72	90	true	yes
overcast	81	75	false	yes
rain	71	80	true	no

Algoritma C4.5 [1]
1. Dimulai node akar (node ke-1)
2. Jika fitur bertipe numerik, cari nilai v
3. Untuk semua fitur dengan tipe numerik atau nominal, hitung entropy untuk semua sampel (data latih) pada node.
4. Gunakan fitur tersebut sebagai node pemecah menjadi cabang.
5. Lakukan secara rekursif pada setiap cabang yang dibuat dengan mengulangi langkah 2 sampai 4 hingga semua data dalam setiap node hanya memberikan satu label kelas. Node yang tidak dapat dipecah lagi merupakan daun yang berisi keputusan (label kelas)

Proses node ke-1 sebagai akar (root)
Node akar diperoleh dengan cara wajib melakukan perhitungan terlebih dahulu Entropy atau diinisialkan sebagai E (semua data) terhadap komposisi kelas [1].

$$E(semua) = -((p(yes|semua) \times log2p(no|semua)) + (p(no|semua) \times log2p(no|semua)))$$
$$= -\left(\left(\left(\frac{9}{14}\right) \times log_2\left(\frac{9}{14}\right)\right) + \left(\left(\frac{5}{14}\right) \times log_2\left(\frac{5}{14}\right)\right)\right)$$
$$= -\left((0{,}6428 \times log_2\ 0{,}6428) + (0{,}3571 \times log_2\ 0{,}3571)\right)$$
$$= -\left((0{,}6428 \times (-0{,}6376)) + (0{,}3571 \times (-1{,}4856))\right) = -(-0{,}4098 + (-0{,}5305))$$
$$= -(-0{,}9403) = 0{,}9403$$

Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 323-327
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Karena data Golf terdapat nilai bertipe numerik, maka kita butuh mencari nilai v sebagai nilai pemecah/split atau teknik ini biasa disebut sebagai diskretisasi data, yaitu data numerik menjadi data nominal/kontinu. Banyak pendekatan yang bisa digunakan dalam mendapatkan nilai v, yang paling umum dan sering digunakan adalah Binning. Salah satu persamaan binning yang digunakan adalah entropy dan gain. Binning mendefinisikan kumpulan class nominal untuk setiap atribut (3ariable input), kemudian menetapkan setiap nilai atribut ke dalam salah satu class. Misal jika domain numerik memiliki nilai dari 0 sampai 100, domain tersebut dapat dibagi menjadi 4 bin {0…24; 25…49; 50…74; 75…100}. Setiap nilai atribut akan dkonversi menjadi atribut nominal/kategorikal yang berkorespondensi dengan salah satu bin. Pendekatan binning disebut unsupervised discretization method [2]. Namun, pendekatan ini memiliki kelemahan yaitu menyebabkan banyak informasi yang memungkinkan hilang.

Temperature

Tabel 2. Posisi *v* untuk pemecahan fitur "*Temperature*" di node akar

Suhu		Jumlah Kasus	*Yes*	*No*	*Entropy*	*Gain*
$v = 67,2$	≤	2	1	1	1	**0,0103**
	>	12	8	4	0,9183	
$v = 73$	≤	8	5	3	0,9544	0,0014
	>	6	4	2	0,9183	
$v = 82,25$	≤	12	8	4	0,9183	**0,0103**
	>	2	1	1	1	

Pada atribut *Temperature* untuk mendapatkan nilai *v* menggunakan *Binning*. Adapun langkahnya adalah sebagai berikut:

1. Urutkan data dari kecil ke besar: {64, 65, 68, 69, 70; 71, 72, 72, 75, 75; 80, 81, 83, 85}
2. Bagi menjadi 3 bagian atau bin: {64, 65, 68, 69, 70; 71, 72, 72, 75, 75; 80, 81, 83, 85}
3. Hitung rata-rata masing-masing bin.
4. Maka nilai *v* yang didapatkan adalah 67,2; 73 dan 82,25.

Jika sudah mendapatkan nilai v selanjutnya menghitung nilai entropy dan gain. Perhitungan nilai gain diperlihatkan Tabel 2, sebagai pembanding, perhitungan yang sama dilakukan oleh Eko ditunjukkan pada Tabel 4-9 [1].

Tabel 4-9 Posisi *v* untuk pemecahan fitur 'suhu' di node akar

Suhu	70		75		80	
	<=	>	<=	>	<=	>
Ya	4	5	7	2	7	2
Tidak	1	4	3	2	4	1
Gain	0.0453		0.0251		0.0005	

Entropy nilai v atribut Temperature

$E(\leq 67,2) = -((p(yes|semua) \times log2p(no|semua)) + (p(no|semua) \times log2p(no|semua)))$
$= -(((12) \times log2\ (12)) + ((12) \times log2\ (12)))$
$= -((0,5 \times log2\ 0,5) + (0,5 \times log2\ 0,5)) = -((0,5 \times (-1)) + (0,5 \times (-1)))$
$= -(-0,5 + (-0,5)) = -(-1) = 1$
$E(> 67,2) = -((p(yes|semua) \times log2p(no|semua)) + (p(no|semua) \times log2p(no|semua)))$
$= -(((\ 8$
$12) \times log2\ (\ 812)) + ((\ 412) \times log2\ (\ 412)))$
$= -((0,6667 \times log2\ 0,6667) + (0,3333 \times log2\ 0,3333))$
$= -((0,6667 \times (-0,5849)) + (0,3333 \times (-1,5851))) = -(-0,3899 + (-0,5283))$
$= -(-0,9182) = 0,9183$
$E(\leq 73) = -((p(yes|semua) \times log2p(no|semua) + (p(no|semua) \times log2p(no|semua)))= -(((58) \times log2\ (5$
$8)) + ((38) \times log2\ (38)))$
$= -((0,625 \times log2\ 0,625) + (0,375 \times log2\ 0,375))$
$= -((0,625 \times (-0,6781)) + (0,375 \times (-1,415))) = -(-0,4238 + (-0,5306))$
$= -(-0,9544) = 0,9544$
$E(> 73) = -((p(yes|semua) \times log2p(no|semua)) + (p(no|semua) \times log2p(no|semua)))$
$= -(((46) \times log2\ (46)) + ((26) \times log2\ (26)))$
$= -((0,6667 \times log2\ 0,6667) + (0,3333 \times log2\ 0,3333))$
$= -((0,6667 \times (-0,5849)) + (0,3333 \times (-1,5851))) = -(-0.3899 + (-0,5283))$
$= -(-0,9182) = 0,9183$
$E(\leq 82,25) = -((p(yes|semua) \times log2p(no|semua) + (p(no|semua) \times log2p(no|semua)))$
$= -(((\ 812) \times log2\ (\ 812)) + ((\ 412) \times log2\ (\ 412)))$

Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 323-327
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

$= -((0{,}6667 \times log2\ 0{,}6667) + (0{,}3333 \times log2\ 0{,}3333))$
$= -((0{,}6667 \times (-0{,}5849)) + (0{,}3333 \times (-1{,}5851))) = -(-0.3899 + (-0{,}5283))$
$= -(-0{,}9182) = 0{,}9183$
$E(> 82{,}25) = -((p(yes|semua) \times log2p(no|semua) + (p(no|semua) \times log2p(no|semua)))$
$= -\ (((12) \times log2\ (12)) + ((12) \times log2\ (12)))$
$= -((0{,}5 \times log2\ 0{,}5) + (0{,}5 \times log2\ 0{,}5)) = -((0{,}5 \times (-1)) + (0{,}5 \times (-1)))$
$= -(-0{,}5 + (-0{,}5)) = -(-1) = 1$

Gain nilai v atribut Temperature

$$Gain(semua, 67{,}2) = E(semua) - \sum_{i=1}^{n} \frac{|67{,}2_i|}{|semua|} \times E(67{,}2_i)$$
$$= 0{,}9403 - \left(\left(\frac{2}{14}\right) \times 1\right) + \left(\left(\frac{12}{14}\right) \times 0{,}9183\right)$$
$= 0{,}9403 - ((0{,}1429 \times 1) + (0{,}8571 \times 0{,}9183)) = 0{,}9403 - (0{,}1429 + 0{,}7871)$
$= 0{,}9403 - 0{,}93 = 0{,}0103$

$$Gain(semua, 73) = E(semua) - \sum_{i=1}^{n} \frac{|73_i|}{|semua|} \times E(73_i)$$
$$= 0{,}9403 - \left(\left(\frac{8}{14}\right) \times 0{,}9544\right) + \left(\left(\frac{6}{14}\right) \times 0{,}9183\right)$$
$$= 0{,}9403 - ((0{,}5714 \times 0{,}9544) + (0{,}4286 \times 0{,}9183))$$
$$= 0{,}9403 - (0{,}5453 + 0{,}3936) = 0{,}9403 - 0{,}9389 = 0{,}0014$$

$$Gain(semua, 82{,}25) = E(semua) - \sum_{i=1}^{n} \frac{|82{,}25_i|}{|semua|} \times E(82{,}25_i)$$
$$= 0{,}9403 - \left(\left(\frac{12}{14}\right) \times 0{,}9183\right) + \left(\left(\frac{2}{14}\right) \times 1\right)$$
$$= 0{,}9403 - ((0{,}8571 \times 0{,}9183) + (0{,}1429 \times 1)) = 0{,}9403 - (0{,}7871 + 0{,}1429)$$
$$= 0{,}9403 - 0{,}93 = 0{,}0103$$

Karena nilai gain tertinggi didapatkan oleh v = 67,2 atau v = 82,25, maka atribut temperature dilakukan diskretisasi pada nilai oleh v = 67,2 atau v = 82,25ketika menghitung entropy dan gain pada semua atribut

4. KESIMPULAN

Dalam penelitian ini, kami berhasil menerapkan algoritma pohon keputusan C4.5 untuk deteksi serangan dalam jaringan komputer. Melalui penggunaan dataset yang mencakup berbagai jenis serangan dan aktivitas jaringan, kami berhasil membangun model deteksi serangan yang efektif dan dapat diandalkan. Hasil evaluasi menunjukkan bahwa model deteksi serangan yang dikembangkan menggunakan algoritma C4.5 mampu mengklasifikasikan aktivitas jaringan dengan tingkat akurasi yang memuaskan. Model ini mampu mengenali pola-pola yang terkait dengan serangan dan secara efektif membedakannya dari aktivitas jaringan normal. Selain itu, kami juga berhasil mengidentifikasi faktor-faktor yang paling berpengaruh dalam deteksi serangan, sehingga memberikan wawasan yang berharga bagi praktisi keamanan jaringan dalam mengembangkan strategi deteksi yang lebih efektif. Kesimpulannya, penelitian ini memberikan kontribusi yang signifikan dalam pengembangan sistem deteksi serangan yang lebih canggih dan dapat diandalkan dalam konteks jaringan komputer. Dengan memanfaatkan kekuatan algoritma pohon keputusan C4.5, kami berharap dapat membantu meningkatkan keamanan jaringan komputer dan melindungi infrastruktur informasi dari ancaman serangan cyber yang semakin kompleks.

5. REFERENCES

[1] B. G. Ginting and F. A. Sianturi, "Sistem Pendukung Keputusan Pemberian Bantuan Kepada Keluarga Kurang Mampu Menggunakan Metode AHP," *J Nas Komputasi Dan Teknol Inf*, vol. 4, no. 1, 2021.

[2] F. Sahputra and F. A. Sianturi, "Decision Support System Selection of Best Employee At PT. Intiberkah Sinar Sejahtera Using Simple Additive weighting Method," *J. Comput. Netw. Archit. High Perform. Comput.*, vol. 2, no. 1, pp. 1–6, 2020.

[3] A. Afrisawati and S. Sahren, "ANALISIS PERBANDINGAN MENGGUNAKAN METODE MOORA DAN WASPAS PEMILIHAN BIBIT SAPI POTONG TERBAIK," *JURTEKSI J. Teknol. Dan Sist. Inf.*, vol. 6, no. 3, pp. 269–276, Aug. 2020, doi: 10.33330/jurteksi.v6i3.827.

[4] Y. U. Alsabri, A. Zakir, and D. Irwan, "Penerapan Customer Relationship Management Pada Sistem Informasi Klinik Kecantikan Berbasis Website (Studi Kasus: Ms Glow Aesthetic Clinic)," vol. 4, 2022.

[5] F. M. Matondang and F. A. Sianturi, "Decision Support System for Determination of Nutrition in Pulmonary Tuberculosis Patients using Multi-Objective Optimization Method On The Basic Of Analysis (MOORA)," *Login J. Teknol. Komput.*, vol. 14, no. 2, pp. 198–204, 2020.

[6] W. Wati and F. A. Sianturi, "Implementasi Metode Topsis Dalam Merekomendasikan Pestisida Terbaik Pada Tanaman Padi Di Desa Rumbia," *J. Sains Dan Teknol.*, vol. 3, no. 2, pp. 31–35, 2022.

Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

[7] F. A. Sianturi and M. Sitorus, "Kombinasi Metodesimpleadditiveweighting (Saw) Denganalgoritma Nearest Neighbor Untuk Rekruitmen Karyawan," *J. Mantik Penusa*, vol. 3, no. 2, Des, 2019.

[8] R. I. Batubara and Y. Siregar, "Sistem Pendukung Keputusan Karyawan Honorer Terbaik di Dinas Perkebunan Medan Dengan Metode Gada," *J. Media Inform.*, vol. 3, no. 2, pp. 104–111, Jun. 2022, doi: 10.55338/jumin.v3i2.279.

[9] F. Laia and F. A. Sianturi, "Sistem Pendukung Keputusan Penilaian Kinerja Pegawai Terbaik dengan Metode Simple Additive Waighting (SAW)," *RESOLUSI Rekayasa Tek. Inform. Dan Inf.*, vol. 1, no. 3, pp. 195–200, 2021.

[10] A. Arisman and F. A. Sianturi, "Sistem Pendukung Keputusan Penerimaan Siswa Baru Menggunakan Metode Moora (Multi-Objective Optimization On The Basis Of Ratio Analysis)," *J. Ilmu Komput. Dan Sist. Inf. JIKOMSI*, vol. 3, no. 1.1, pp. 73–83, 2020.

Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**