Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/index
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893

Penerapan Metode SAW Pada Sistem Pendukung Keputusan Penentuan Perangkat Lunak Anti Virus

DOI: http://dx.doi.org/10.35889/jutisi.v14i3.2920

Muhammad Alif Arramzy[1], Pratiwi[2*], Winny Purbaratry[3]
Teknologi Informasi, IKPIA Perbanas, Jakarta, Indonesia
muhammad.alif@perbanas.id, pratiwi@perbanas.id, winny.purbaratri@perbanas.id
**Email Corresponding Author*: pratiwi@perbanas.id

Abstract

The increasing dependence of society on computers and the internet highlights the urgency of protecting data and privacy from cyber threats. Antivirus software is one of the common solutions; however, the abundance of options, each with its own advantages and disadvantages, often makes it difficult for users to select the most suitable one. This study aims to assist users in choosing the best free antivirus through a systematic approach using a decision support system. The method applied is Simple Additive Weighting (SAW) with five evaluation criteria: scanning speed, detection capability, rating, resource optimization, and available features. Five antivirus software were tested as alternatives, namely Windows Security, Avira, Avast, Bitdefender, and Kaspersky. The testing and calculation results indicate that Windows Security ranked the highest with a vector value of 0.257, due to its high detection rate, fast scanning performance, good rating, and sufficient features. Therefore, the SAW method proves effective in providing objective and systematic recommendations for selecting the best antivirus software.

Keywords: *Decision support system; Simple additive weighting; Antivirus*

Abstrak

Meningkatnya ketergantungan masyarakat terhadap sistem komputer dan internet menimbulkan urgensi akan perlindungan data dan privasi dari ancaman siber. Salah satu solusi yang umum digunakan adalah perangkat lunak antivirus, namun banyaknya pilihan dengan kelebihan dan kekurangan masing-masing seringkali menimbulkan kebingungan dalam menentukan pilihan yang tepat. Penelitian ini bertujuan untuk membantu pengguna dalam memilih antivirus gratis terbaik dengan pendekatan sistematis melalui sistem pendukung keputusan. Metode yang digunakan adalah *Simple Additive Weighting* (SAW) dengan lima kriteria penilaian, yaitu kecepatan pemindaian, kemampuan deteksi, rating, optimasi sumber daya, dan jumlah fitur. Lima perangkat lunak antivirus diuji sebagai alternatif, yakni Windows Security, Avira, Avast, Bitdefender, dan Kaspersky. Hasil pengujian dan perhitungan menunjukkan bahwa Windows Security memperoleh peringkat tertinggi dengan nilai vektor 0,257 karena memiliki kecepatan dan tingkat deteksi yang tinggi, rating yang baik, serta fitur yang cukup banyak. Dengan demikian, metode SAW terbukti efektif dalam memberikan rekomendasi obyektif dan sistematis untuk pemilihan perangkat lunak antivirus terbaik.

Kata kunci: *Sistem pendukung keputusan; Simple additive weighting; Antivirus*

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah memberikan kemudahan yang signifikan dalam aktivitas sehari-hari, baik dalam hal pekerjaan, pendidikan, maupun hiburan. Namun, di balik kemudahan tersebut, muncul ancaman serius berupa serangan siber yang dapat merugikan pengguna secara finansial, merusak sistem, hingga mencuri data pribadi. Di sinilah keamanan komputer, keamanan jaringan, keamanan siber, keamanan teknologi informasi merupakan hal yang penting bagi semua pengguna internet [1]. Keamanan komputer dan jaringan menjadi isu yang semakin penting, terutama di era digital saat ini, di mana hampir semua aktivitas manusia terkoneksi dengan internet. Beberapa cara sudah dapat digunakan untuk

memitigasi, bahkan mengamankan sistem komputer dari penyerang-penyerang yang tidak bertanggung jawab ini [2]. Oleh karena itu, perlindungan melalui perangkat lunak antivirus merupakan kebutuhan mendasar untuk menjaga integritas, kerahasiaan, dan ketersediaan data serta sistem.

Saat ini tersedia beragam perangkat lunak antivirus, baik yang berbayar maupun gratis, dengan menawarkan fitur dan keunggulan masing-masing. Standar jaringan atau *Network Standard* seperti *Bluetooth*, *Wi-Fi*, Perangkat AI atau *Artificial Intelligence* seperti *Machine Learning*, *Smartpone*, dan banyak lagi yang bernama "*Smart*" di *Internet of Things* terus berkembang dan perlindungan untuk itu juga harus terus di tingkatkan [3]. Aksesibilitas yang tinggi juga berarti kemudahan untuk terkena serangan yang tinggi juga. Kompleksitas yang tinggi pada Keamanan Siber merupakan tantangan yang signifikan, oleh karena itu ada baiknya jika semua penggunanya lebih mengetahui dan memahami bahaya-bahaya di dunia siber [4]. Kondisi ini justru menimbulkan masalah baru, yaitu kesulitan pengguna dalam menentukan pilihan antivirus yang sesuai dengan kebutuhan mereka. Masalah ini dapat diukur dari aspek teknis, seperti kecepatan pemindaian, kemampuan mendeteksi ancaman, efisiensi penggunaan sumber daya, kualitas berdasarkan rating independen, serta jumlah fitur yang tersedia. Banyaknya alternatif dengan variabel kinerja yang beragam membuat proses pemilihan antivirus seringkali bersifat subyektif, tidak efisien, dan berpotensi menimbulkan keputusan yang kurang optimal bagi pengguna.

Untuk mengatasi permasalahan tersebut, diperlukan sebuah pendekatan sistematis melalui *Decision Support System* (DSS) yang mampu membantu pengguna dalam melakukan pemilihan antivirus secara obyektif. Salah satu metode yang relevan adalah *Simple Additive Weighting* (SAW), yang dikenal efektif dalam pengambilan keputusan multi-kriteria karena kemampuannya menjumlahkan nilai bobot dari setiap variabel penilaian. Namun, seperti halnya semua metode yang ada, tentu memiliki kelebihan dan kekurangan masing-masing, serta pro dan kontra yang tidak dapat dihindari [5]. Oleh karena itu, akan jauh lebih baik apabila pilihan yang diberikan kepada pengguna dikurasi atau disediakan pedoman yang jelas agar dapat menyesuaikan dengan kebutuhan dan kemampuan pribadi pengguna [6]. Dalam konteks ini, metode SAW memberikan landasan rasional karena mampu mengolah variabel-variabel terukur secara konsisten, sehingga hasil rekomendasi lebih obyektif, adil, dan dapat dijadikan dasar dalam pengambilan keputusan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menerapkan metode SAW pada sistem pendukung keputusan dalam menentukan perangkat lunak antivirus gratis terbaik di antara Windows Security, Avira, Avast, Bitdefender, dan Kaspersky. Penelitian ini diharapkan dapat memberikan manfaat praktis bagi pengguna komputer, yaitu berupa pedoman obyektif dalam memilih antivirus sesuai kebutuhan, sekaligus manfaat akademis berupa kontribusi pada pengembangan model DSS berbasis metode SAW di bidang keamanan komputer. Selain itu, hasil penelitian dapat menjadi referensi awal untuk penelitian lanjutan yang mengkaji variabel dan alternatif antivirus secara lebih luas dan mendalam.

2. Tinjauan Pustaka

Metode *Simple Additive Weighting* (SAW) sebagai salah satu pendekatan dalam *Multi-Criteria Decision Making* (MCDM) telah banyak digunakan dalam penelitian terkait pemilihan perangkat lunak dan evaluasi performa sistem. Dalam konteks pengembangan algoritma cerdas, Ridho et al. (2022) memanfaatkan metode *neural network* untuk prediksi harga rumah, dengan mengolah parameter seperti luas tanah, jumlah kamar, dan lokasi [7]. Walaupun tidak menggunakan SAW, penelitian ini menunjukkan bagaimana metode komputasional dapat dioptimalkan untuk menghasilkan keputusan yang lebih akurat berdasarkan multiatribut. Prinsip serupa dapat diadopsi dalam pemilihan perangkat lunak, termasuk antivirus, dengan memanfaatkan pendekatan sistematis berbasis bobot kriteria.

Kajian terkait keamanan perangkat lunak dilakukan oleh Matin (2023) yang mengaplikasikan *GridSearchCV* pada *Random Forest* untuk deteksi malware [8]. Penelitian ini menekankan pentingnya optimasi parameter dalam meningkatkan performa algoritma deteksi. Sementara itu, Belea (2023) mengkaji metode deteksi malware berbasis analisis statis, dinamis, dan hibrida [9]. Kedua penelitian ini memberikan landasan bahwa pemilihan perangkat lunak antivirus harus mempertimbangkan performa teknis secara multidimensi, mulai dari tingkat deteksi, ketahanan terhadap serangan baru, hingga efisiensi penggunaan sumber daya.

Selain penelitian teknis, pengembangan sistem pendukung keputusan berbasis MCDM telah diterapkan dalam berbagai bidang. Studi mengenai penerapan metode TOPSIS dalam pemilihan *smartphone Android* menunjukkan bagaimana metode berbasis perbandingan bobot dapat membantu pengguna menentukan perangkat yang sesuai dengan preferensi [10]. Penelitian ini memberikan indikasi bahwa SAW, dengan struktur perhitungan yang lebih sederhana, berpotensi memberikan hasil serupa namun dengan transparansi yang lebih tinggi.

Pada domain aplikasi geografis, Nuraeni et al. (2022) menerapkan sistem informasi geografis (SIG) untuk pemetaan lahan garapan dengan mempertimbangkan kriteria spasial dan produktivitas [11]. Studi ini relevan karena menunjukkan bagaimana keputusan berbasis perangkat lunak dapat dipandu oleh model matematis dengan parameter yang terukur. Demikian pula, Octiva et al. (2024) menyoroti tantangan dan peluang dalam implementasi teknologi informasi pada UMKM [12]. Penelitian ini memperlihatkan pentingnya pemilihan perangkat lunak yang adaptif terhadap kebutuhan organisasi dengan keterbatasan sumber daya, yang juga menjadi isu penting dalam pemilihan antivirus di lingkungan pengguna dengan kapabilitas perangkat yang beragam.

Dimensi sosial juga turut berkontribusi dalam kajian pemanfaatan perangkat lunak. Jaya dan Setiawan (2020) menyoroti strategi pelestarian cagar budaya berbasis keputusan pengunjung [13], sedangkan Asmara dan Purbokusumo (2022) membahas instrumen kebijakan penataan ruang untuk manajemen sumber daya pertanian [14]. Walaupun berbeda domain, kedua studi ini menekankan bahwa pemilihan alternatif terbaik membutuhkan integrasi aspek teknis dan preferensi pengguna, yang sejalan dengan prinsip pengambilan keputusan pada pemilihan perangkat lunak antivirus.

Dalam ranah pendidikan, Mardiana et al. (2024) meninjau gaya belajar siswa auditorial dalam menyelesaikan soal bentuk aljabar [15], sementara Yaum et al. (2022) mengembangkan aplikasi asistif berbasis *speech-to-text* untuk mahasiswa disabilitas rungu [16]. Kedua penelitian ini menunjukkan relevansi pemanfaatan perangkat lunak dalam meningkatkan efektivitas belajar, dengan pendekatan pemilihan aplikasi berbasis kebutuhan khusus. Hal ini mendukung gagasan bahwa pemilihan antivirus juga harus berlandaskan kebutuhan spesifik pengguna, baik dari sisi keamanan, performa, maupun kemudahan penggunaan.

Dari perspektif rekayasa perangkat lunak, Nassif et al. (2023) memperkenalkan pendekatan *learning to rank* untuk prediksi cacat perangkat lunak [17]. Studi ini menekankan pentingnya penentuan prioritas pada berbagai alternatif solusi yang tersedia, yang konsepnya serupa dengan perankingan dalam metode SAW. Selanjutnya, Liu et al. (2019) melalui sistem *MultiScan* memperlihatkan parameter kunci yang harus diperhatikan dalam pemilihan perangkat lunak antivirus, seperti kecepatan pemindaian, tingkat deteksi, dan efisiensi sumber daya [18]. Lebih lanjut, Ashik et al. (2021) menegaskan efektivitas *machine learning* dan *deep learning* dalam mendeteksi malware dengan menganalisis artefak yang berbeda [19].

Berbagai penelitian terdahulu telah berupaya menyelesaikan masalah pemilihan perangkat lunak maupun deteksi malware dengan pendekatan beragam, mulai dari *machine learning*, *decision making methods*, hingga integrasi SIG dan sistem asistif. Namun demikian, belum ditemukan penelitian yang secara eksplisit menerapkan metode SAW untuk pemilihan perangkat lunak antivirus dengan mengintegrasikan parameter teknis yang komprehensif. Penelitian ini mengisi celah tersebut dengan menghadirkan model sistem pendukung keputusan berbasis SAW yang memproses kriteria teknis antivirus—seperti tingkat deteksi, *false positive rate*, kecepatan pemindaian, efisiensi sumber daya, dan kelengkapan fitur. Dengan pendekatan ini, penelitian memberikan kontribusi akademis berupa pengembangan metodologi MCDM pada domain keamanan perangkat lunak, sekaligus manfaat praktis berupa sistem rekomendasi antivirus yang lebih obyektif, adaptif, dan sesuai dengan kebutuhan pengguna.

3. Metodologi

3.1 Algoritma SAW

Algoritma Simple Additive Weighting (SAW) digunakan dalam penelitian ini untuk menentukan alternatif antivirus terbaik berdasarkan sejumlah kriteria. SAW dipilih karena kesederhanaannya dalam melakukan perhitungan berbasis *multi-criteria decision making* (MCDM) serta kemampuannya menghasilkan keputusan yang obyektif dan sistematis.
Formula matematis SAW adalah sebagai berikut:

1. Normalisasi Bobot
   $w'_j \frac{w_j}{\sum_{k=1}^{n} w_k}$ .....(1)
2. Normalisasi Matriks Keputusan
   $$r_{ij} = \begin{cases} \frac{x_{ij}}{max_i x_{ij}}, & jika\ Kj\ adalah\ kriteria\ benefit \\ \frac{max_i x_{ij}}{x_{ij}}, & jika\ Kj\ adalah\ kriteria\ cost \end{cases}$$ ..... (2)
3. Perhitungan Skor Terbobot (S)
   $S_i = \sum_{j=1}^{n} (w'_j . r_{ij})$ .....(3)
4. Normalisasi Akhir (V)
   $V_i \frac{S_i}{\sum_{k=1}^{m} S_k}$ .....(4)

Alternatif dengan nilai V_i tertinggi ditetapkan sebagai peringkat pertama atau pilihan terbaik.

3.2 Data dan Variabel

Objek kajian dalam penelitian ini adalah lima perangkat lunak antivirus gratis, yaitu: Windows Security (A1), Avira (A2), Avast (A3), Bitdefender (A4), dan Kaspersky (A5). Parameter input yang diproses merupakan kriteria penilaian antivirus dengan bobot tertentu, yaitu:

K1: Kecepatan Pemindaian (benefit, bobot 45)
K2: Kemampuan Deteksi (benefit, bobot 15)
K3: Rating (benefit, bobot 5)
K4: Optimasi Sumber Daya (cost, bobot 5)
K5: Fitur Tersedia (benefit, bobot 30)

Nilai kriteria diperoleh melalui uji coba pemindaian, pengujian deteksi dengan virus uji, observasi pemakaian sumber daya, serta analisis rating dan fitur. Skala penilaian menggunakan rentang 1–5. Parameter output adalah nilai preferensi akhir Vi yang menunjukkan peringkat tiap alternatif antivirus.
Jumlah sampel data dalam penelitian ini adalah lima alternatif antivirus yang dinilai berdasarkan lima kriteria sebagaimana disebutkan di atas.

3.3 Teknik Validasi Performa Algoritma SAW

Validasi kinerja algoritma SAW dilakukan dengan cara:

1) Pemeriksaan Konsistensi Perhitungan
   - Memastikan bahwa langkah normalisasi bobot, normalisasi matriks keputusan, hingga perhitungan vektor S dan V sesuai dengan formula matematis.
   - Hasil setiap langkah dicatat dalam bentuk tabel (normalisasi, skor, vektor) untuk memastikan transparansi.
2) Uji Sensitivitas
   - Melakukan perubahan bobot pada salah satu atau beberapa kriteria untuk melihat apakah hasil peringkat berubah signifikan.
   - Hal ini menguji ketahanan algoritma terhadap variasi bobot.
3) Validasi Obyektivitas
   - Membandingkan hasil akhir peringkat dengan fakta kinerja empiris (misalnya ulasan independen atau hasil pengujian laboratorium antivirus).
   - Jika hasil ranking SAW sejalan dengan hasil pengujian eksternal, maka algoritma dianggap valid.

Dengan teknik ini, penelitian dapat menunjukkan sejauh mana algoritma SAW dapat diandalkan dalam memberikan rekomendasi obyektif pada kasus pemilihan perangkat lunak antivirus.

4. Hasil dan Pembahasan

Dari hasil pemindaian dan pengujian awal, didapatkan bobot dari kriteria yang ditentukan sebagai berikut:

Tabel 1. Kriteria, Atribut, dan Bobot yang Ditentukan

Nomor	Kode Kriteria	Kriteria	Atribut	Bobot
1	K1	Kecepatan	Benefit	45
2	K2	Deteksi	Benefit	15
3	K3	Rating	Benefit	5
4	K4	Optimasi	Cost	5
5	K5	Fitur	Benefit	30

Penilaian dari kriteria yang ditentukan adalah sebagai berikut.

Tabel 2. Variabel, dan Nilai Bobot yang Ditentukan

K1	Nilai	K2	Nilai	K3	Nilai	K4	Nilai	K5	Nilai
#5	1	0	1	<6	1	#1	1	<5	1
#4	2	1	2	9	2	#2	2	8	2
#3	3	2	3	12	3	#3	3	10	3
#2	4	3	4	15	4	#4	4	12	4
#1	5	4	5	≥18	5	#5	5	≥15	5

Untuk K1 berdasarkan peringkat di mana paling cepat akan mendapatkan nilai paling tinggi juga, K2 berdasarkan berapa kali antivirus berhasil mendeteksi *malware* berupa virus, K3 berdasarkan penilaian oleh AV-TEST, K4 berdasarkan peringkat yang paling efisien mendapatkan nilai paling sedikit, dan K5 berdasarkan berapa jumlah fitur gratis yang disediakan.

Tabel 3. Alternatif yang Dipilih, dan Kodenya

No	Kode Alternatif	Alternatif
1	A1	Windows Security
2	A2	Avira
3	A3	Avast
4	A4	Bitdefender
5	A5	Kaspersky

4.1 Kriteria Kecepatan

Kecepatan dalam melakukan pemindaian adalah salah satu faktor yang penting untuk sebuah perangkat lunak antivirus. Saat terjadi serangan, kecepatan sangat berpengaruh dalam mencegah aktor jahat dari melakukan perusakan. Perangkat lunak antivirus yang tidak cepat, akan tidak mampu mengejar pergerakan aktor jahat yang semakin lincah, dan cepat dalam menjalankan penyerangannya. Oleh karena itu, penilaian terbaik akan diberikan kepada alternatif yang memiliki kecepatan memindai dengan berkas per detik paling banyak. Berdasarkan tabel di atas, berikut hasil penilaian pada kriteria kecepatan:

Tabel 4.Tabel Hasil Total '*Full scan'* Kriteria Tingkat Kecepatan

Rata-rata berkas per detik pemindaian Full scan					
Alternatif	**Uji coba 1**	**Uji coba 2**	**Uji coba 3**	**Uji coba 4**	**Total**
Windows Security	1.149	1.558	1.295	1.451	5.453
Avira	1.073	1.051	1,023	1.086	4.233
Avast	638	760	739	736	2.873
Bitdefender	1.299	693	1.318	1.345	4.655
Kaspersky	886	737	849	881	3.353

Rata-rata dihitung dengan menjumlahkan Uji coba 1, 2, 3, 4, menjadi 'Total', dan membagi hasilnya dengan 4. Contohnya, (250 + 250 + 250 + 250) ÷ 4 = 250 rata-rata berkas per detik. Berikut hasil perhitungan rata-rata:

Tabel 5. Tabel Hasil Penilaian Kriteria Tingkat Kecepatan

Peringkat	Kode	Alternatif	Rata-rata	Nilai
1	A1	Windows Security	1,363	5
2	A4	Bitdefender	1,163	4
3	A2	Avira	1,058	3
4	A5	Kaspersky	838	2
5	A3	Avast	718	1

4.2 Kriteria Kemampuan mendeteksi dan mencegah

Kemampuan untuk mendeteksi *malware* seperti virus adalah krusial untuk perangkat lunak antivirus. Untuk uji coba ini, peneliti akan menggunakan *Test Virus* yang tidak berbahaya. Test Virus ini sengaja dibuat oleh *European Institute for Computer Antivirus Research* (EICAR) atau Institut Eropa untuk Penelitian Antivirus Komputer untuk melakukan penelitian antivirus dengan aman, tanpa risiko terkena infeksi virus yang aktif, dan berbahaya. Untuk Test Virus ini dapat diunduh dari IKARUS *Security Software*, sebuah perusahaan berasal dari Austria. IKARUS sudah berpengalaman dalam keamanan siber sejak tahun 1986.

Berdasarkan hasil penelitian di atas, semua perangkat lunak antivirus berhasil mendeteksi, dan/atau mencegah tes virus yang di unduh empat dari empat kali percobaan. Ini berarti, semua alternatif mendapatkan nilai sebesar lima poin.

Tabel 6. Tabel Hasil Penilaian Kriteria Deteksi

Kode Alternatif	Alternatif	Total deteksi	Nilai
A1	Windows Security	4	5
A2	Avira	4	5
A3	Avast	4	5
A4	Bitdefender	4	5
A5	Kaspersky	4	5

4.3 *Kriteria Penilaian atau rating*

Menggunakan penilaian yang dikeluarkan oleh lembaga independen AV-TEST. AV-TEST memberikan Windows Security, 6 poin dalam Perlindungan, 6 poin dalam Performa, dan 5,5 poin dalam kegunaan. Dengan total poin berupa 17,5 poin.AV-TEST memberikan Avira, 6 poin dalam perlindungan, 5,5 poin dalam performa, dan 6 poin dalam kegunaan. Dengan total poin berupa 17,5 poin. AV-TEST memberikan Avast, 6 poin dalam perlindungan, 6 poin dalam performa, dan 6 poin dalam kegunaan. Dengan total poin berupa 18 poin. AV-TEST memberikan Bitdefender, 6 poin dalam perlindungan, 6 poin dalam performa, dan 6 poin dalam kegunaan. Dengan total poin berupa 18 poin. AV-TEST memberikan Kaspersky, 6 poin dalam perlindungan, 6 poin dalam performa, dan 6 poin dalam kegunaan. Dengan total poin berupa 18 poin.

Tabel 7.Tabel Hasil Penilaian Poin Kriteria Rating

Alternatif	Perlindungan	Performa	Kegunaan	Total
Kaspersky	6	6	6	18
Bitdefender	6	6	6	18
Avast	6	6	6	18
Windows Security	6	6	5,5	17,5
Avira	6	5,5	6	17,5

Tabel 8.Tabel Hasil Penilaian Akhir Kriteria Rating

Kode Alternatif	Alternatif	Nilai
A5	Kaspersky	5
A4	Bitdefender	5
A3	Avast	5
A1	Windows Security	4
A2	Avira	4

4.4 Kriteria Optimasi

Diukur berdasarkan aktivitas utilitas CPU, Berbeda dengan kriteria yang lain yang memiliki nilai positif, pada kriteria 'Optimasi' nilai bersifat negatif di mana makin rendah nilainya, makin bagus hasilnya. Berdasarkan hasil penelitian di atas, nilai negatif akan diberikan ke perangkat lunak yang menggunakan sumber daya komputer secara intensif.

Penilaian akan dilakukan sesuai dengan persentase utilitas CPU, dari empat utilitas CPU berdasarkan 4 kali uji coba, akan di jumlahkan hasilnya, lalu akan dibagi 4 untuk menemukan rata-ratanya. Contoh: Perangkat lunak 'A' menggunakan utilitas CPU 30% pada uji coba #1, 30% CPU uji coba #2, 30% CPU uji coba #3, dan 30% CPU uji coba #4, maka dijumlahkan 30% + 30% + 30% + 30% menjadi 120% dan dibagi jumlah uji coba (empat) maka rata-rata menjadi 30%.

Tabel 9.Tabel Hasil Penilaian Kriteria Optimasi

Alternatif	Uji coba #1	Uji coba #2	Uji coba #3	Uji coba #4	Total
Windows Security	100%	100%	100%	54%	354%
Avira	49%	100%	100%	48%	297%
Avast	31%	23%	18%	27%	99%
Bitdefender	68%	100%	22%	41%	231%
Kaspersky	57%	69%	67%	42%	235%

Tabel 10.Tabel Hasil Penilaian Akhir Kriteria Optimasi

Peringkat	Kode	Alternatif	Rata-rata	Nilai
1	A1	Windows Security	88,5%	5
2	A2	Avira	74,25%	4
3	A5	Kaspersky	58,75%	3
4	A4	Bitdefender	57,75%	2
5	A3	Avast	24,75%	1

4.5 Kriteria Fitur-fitur yang ditawarkan

Penilaian kriteria 'Fitur' dilakukan dengan membandingkan jumlah fitur gratis antara perangkat-perangkat lunak antivirus yang dievaluasi. Perangkat lunak antivirus dengan fitur gratis lebih dari atau sama dengan 15 akan mendapatkan poin 5, dan yang lebih sedikit dari 5 fitur akan mendapatkan poin terendah yaitu 1.

Tabel 11.Tabel Hasil Penilaian Akhir Kriteria Fitur

Peringkat	Kode	Alternatif	Fitur gratis	Nilai
1	A2	Avira	18	5
2	A3	Avast	15	5
3	A1	Windows Security	14	4
4	A5	Kaspersky	9	2
5	A4	Bitdefender	4	1

4.6 *Penilaian*

Berdasarkan data dan penilaian kriteria sebelumnya, didapatkan perhitungan penilaian akhir bobot kriteria. Tabel 12 mendatakan alternatif-alternatif dengan nilainya pada kriteria masing- masing.

Tabel 12. Tabel Data Bobot Kriteria, dan Penilaiannya

Kode Alternatif	Kecepatan (K1) (+)	Deteksi (K2) (+)	Rating (K3) (+)	Optimasi (K4) (-)	Fitur (K5) (+)
A1	5	5	4	5	4
A2	3	5	4	4	5
A3	1	5	5	1	5
A4	4	5	5	2	1
A5	2	5	5	3	2
Bobot	45	15	5	5	30

Setelah itu, dilakukan normalisasi nilai, dan bobot. Hasilnya dapat dilihat pada Tabel 13 di bawah. Dapat dilihat bahwa pada kriteria kecepatan, alternatif A1 memiliki nilai tertinggi, sementara pada kriteria deteksi, semua alternatif memiliki nilai yang tinggi. Untuk kriteria *rating*, alternatif A3, A4, dan A5 memiliki nilai tertinggi, dengan alternatif A1, dan A2 memiliki nilai yang lebih rendah. Pada kriteria optimasi, alternatif A3 memiliki nilai tertinggi, namun perlu diingat Kembali, kriteria 4 bersifat negatif atau *cost* di mana nilai yang lebih rendah adalah nilai yang lebih baik.

Tabel 13. Tabel Normalisasi Nilai, dan Bobot

Kode Alternatif	Kecepatan (K1) (+)	Deteksi (K2) (+)	Rating (K3) (+)	Optimasi (K4) (-)	Fitur (K5) (+)
A1	1.000	1.000	0.800	0.200	0.800
A2	0.600	1.000	0.800	0.250	1.000
A3	0.200	1.000	1.000	1.000	1.000
A4	0.800	1.000	1.000	0.500	0.200
A5	0.400	1.000	1.000	0.333	0.400
Bobot	0.450	0.150	0.050	0.050	0.300

Pada perhitungan Vektor S atau penjumlahan bobot, alternatif A1 yaitu perangkat lunak antivirus ‘Windows Security’ mendapatkan nilai tertinggi pada angka 0.890. Meskipun nilai kriteria optimasi yang bersifat negatif paling tertinggi, alternatif A3 dibantu dengan tingginya juga nilai kriteria K2, K3, dan K4. Alternatif A3 adalah satu-satunya alternatif yang memiliki nilai sempurna pada tiga kriteria positif atau *benefit*.

Tabel 14. Tabel Perhitungan Vektor S

Kode Alternatif	Kecepatan (K1) (+)	Deteksi (K2) (+)	Rating (K3) (+)	Optimasi (K4) (-)	Fitur (K5) (+)	Vektor S
A1	1.000	1.000	0.800	0.200	0.800	0.890
A2	0.600	1.000	0.800	0.250	1.000	0.773
A3	0.200	1.000	1.000	1.000	1.000	0.640
A4	0.800	1.000	1.000	0.500	0.200	0.645
A5	0.400	1.000	1.000	0.333	0.400	0.517
Bobot	0.450	0.150	0.050	0.050	0.300	
					Total	3.465

Dari perhitungan Vektor S atau penjumlahan bobot, perhitungan Vektor V atau nilai akhir dapat dilakukan. Dapat di lihat pada Tabel 15 di bawah ini, alternatif dengan nilai Vektor V tertinggi atau terbaik adalah alternatif ‘Windows Security’ dengan kode alternatif A1.

Tabel 15. Tabel Perhitungan Vektor V

Kode Alternatif	Alternatif	Vektor S	Vektor V
A1	Windows Security	0.890	0.257
A2	Avira	0.773	0.223
A3	Avast	0.640	0.185
A4	Bitdefender	0.645	0.186
A5	Kaspersky	0.517	0.149
Total		3.833	1

Pada Tabel 16 ini, yang di mana merupakan tabel terakhir, dapat dilihat hasil Vektor V, yang dimana alternatif perangkat lunak antivirus 'Windows Security dengan kode alternatif A1 menempati peringkat tertinggi dengan nilai Vektor V sebesar 0.257.

Tabel 16. Tabel Pemeringkatan Akhir

Kode Alternatif	Alternatif	Vektor V	Peringkat
A1	Windows Security	0.257	1
A2	Avira	0.223	2
A4	Bitdefender	0.186	3
A3	Avast	0.185	4
A5	Kaspersky	0.149	5

4.7 Validasi Performa Algoritma

Validasi algoritma Simple Additive Weighting (SAW) dalam penelitian ini bertujuan untuk menilai reliabilitas dan akurasi metode dalam menghasilkan rekomendasi pemilihan perangkat lunak antivirus. Validasi dilakukan melalui tiga pendekatan, yaitu pemeriksaan konsistensi perhitungan, analisis sensitivitas bobot kriteria, serta konfirmasi obyektivitas terhadap data empiris.

1) Pemeriksaan Konsistensi Perhitungan

Tahap pertama validasi dilakukan dengan menelusuri setiap langkah komputasi SAW, mulai dari normalisasi bobot, normalisasi matriks keputusan, hingga kalkulasi skor preferensi. Hasil perhitungan menunjukkan bahwa Windows Security (A1) memperoleh nilai skor tertinggi (S = 0,890; V = 0,257), diikuti Avira (A2) dengan skor 0,773 (V = 0,223), serta Bitdefender (A4), Avast (A3), dan Kaspersky (A5) pada peringkat berikutnya. Konsistensi nilai yang diperoleh dari tahapan normalisasi hingga vektor preferensi akhir menunjukkan bahwa algoritma SAW berjalan sesuai formulasi matematis yang digunakan. Hal ini sejalan dengan temuan [5] bahwa SAW menghasilkan keputusan yang stabil pada kasus pemilihan dengan kriteria terukur.

2) Analisis Sensitivitas Bobot Kriteria

Validasi selanjutnya dilakukan dengan uji sensitivitas, yaitu menganalisis perubahan hasil pemeringkatan akibat variasi bobot kriteria. Hasil pengujian menunjukkan bahwa perubahan bobot pada kriteria tertentu, misalnya peningkatan bobot fitur (K5), dapat menggeser posisi Avira (A2) lebih dekat ke peringkat teratas. Sebaliknya, peningkatan bobot kecepatan pemindaian (K1) tetap mempertahankan Windows Security (A1) sebagai alternatif terbaik. Hal ini menegaskan bahwa meskipun SAW sensitif terhadap perubahan bobot, hasil pemeringkatan utama tetap robust. Analisis sensitivitas ini penting karena mencerminkan bagaimana perubahan preferensi pengguna atau stakeholder dapat memengaruhi hasil keputusan, sesuai dengan rekomendasi penelitian terdahulu [6].

3) Konfirmasi Obyektivitas terhadap Data Empiris

Langkah terakhir validasi dilakukan dengan membandingkan hasil pemeringkatan SAW terhadap kinerja empiris antivirus berdasarkan uji fungsional, review pengguna, serta publikasi independen. Windows Security unggul pada aspek deteksi dan integrasi sistem, sedangkan Avira dan Avast lebih menonjol pada fitur tambahan. Kesesuaian antara hasil perhitungan SAW dan performa nyata antivirus di lapangan menunjukkan bahwa algoritma ini mampu

merepresentasikan kondisi empiris secara obyektif. Dengan demikian, hasil pemeringkatan yang diperoleh tidak hanya valid secara matematis tetapi juga relevan secara praktis.

4.8 Pembahasan

Permasalahan utama yang diidentifikasi dalam penelitian ini adalah kesulitan pengguna dalam menentukan perangkat lunak antivirus gratis yang paling sesuai di tengah banyaknya pilihan dengan kinerja dan fitur yang heterogen. Kondisi tersebut berimplikasi pada potensi pengambilan keputusan yang bersifat subjektif, tidak sistematis, dan berisiko tidak optimal. Temuan penelitian ini menunjukkan bahwa penerapan algoritma Simple Additive Weighting (SAW) mampu mereduksi persoalan tersebut melalui suatu mekanisme pengambilan keputusan multi-kriteria yang obyektif, transparan, dan terukur.

Melalui integrasi lima kriteria yang dianggap paling relevan—kecepatan pemindaian, kemampuan deteksi, rating, optimasi sumber daya, dan fitur—algoritma SAW menghasilkan pemeringkatan yang konsisten dan dapat diaudit. Hasil akhir memperlihatkan bahwa Windows Security memperoleh nilai preferensi tertinggi (V=0,257V=0,257V=0,257), diikuti oleh Avira (V=0,223V=0,223V=0,223), sedangkan Bitdefender, Avast, dan Kaspersky menempati peringkat berikutnya. Dengan demikian, SAW berhasil menyelesaikan masalah yang telah diidentifikasi pada bagian pendahuluan, yaitu kebutuhan akan kerangka obyektif yang memandu pengguna dalam menentukan prioritas pilihan.

Lebih jauh, sifat fleksibilitas SAW memungkinkan penyesuaian bobot kriteria sesuai preferensi pengguna. Misalnya, peningkatan bobot pada fitur (K5) dapat menggeser posisi Avira ke peringkat yang lebih tinggi, sementara penekanan pada kecepatan pemindaian (K1) mempertahankan dominasi Windows Security. Hal ini menunjukkan bahwa algoritma SAW tidak hanya efektif dalam memberikan solusi bagi kasus spesifik, tetapi juga menyediakan suatu kerangka pengambilan keputusan yang dapat digunakan kembali pada kondisi atau kebutuhan yang berbeda.

Penelitian ini memberikan penguatan empiris terhadap beberapa literatur [20] yang telah menunjukkan efektivitas SAW dalam konteks pengambilan keputusan multi-kriteria. Berbagai studi terdahulu mengonfirmasi bahwa SAW unggul dalam menghasilkan hasil yang konsisten, sederhana, dan transparan pada kasus seleksi dengan parameter kuantitatif. Hasil penelitian ini mendukung bukti tersebut dengan menunjukkan bahwa SAW tetap efektif ketika diterapkan pada domain keamanan komputer, khususnya pemilihan perangkat lunak antivirus. Dengan demikian, penelitian ini tidak hanya mereplikasi, tetapi juga memperluas ruang lingkup penerapan SAW.

Temuan penelitian ini juga dapat diposisikan secara komparatif dengan penelitian terdahulu yang menggunakan metode lain, seperti *Analytical Hierarchy Process* (AHP) [21] atau *Fuzzy Multi-Criteria Decision Making* [22]. Studi-studi tersebut menunjukkan bahwa metode-metode tersebut dapat menghasilkan rekomendasi yang berbeda akibat perbedaan struktur bobot, preferensi, atau jenis kriteria yang digunakan. Penelitian ini menunjukkan bahwa SAW menawarkan baseline yang stabil dan dapat direplikasi, di mana perubahan bobot dapat menghasilkan variasi peringkat yang logis dan dapat dijelaskan melalui analisis sensitivitas. Dengan demikian, kontribusi penelitian ini terletak pada penegasan peran SAW sebagai metode dasar yang dapat dipadukan atau dibandingkan dengan metode lain untuk memperkaya kualitas pengambilan keputusan.

Temuan penelitian ini juga berkontribusi pada upaya pengintegrasian bukti ilmiah terkait penggunaan SAW dalam proses penentuan prioritas. Pertama, penelitian ini menambahkan dimensi baru dengan memasukkan kriteria eksternal yang tervalidasi, seperti rating dari lembaga independen, sehingga meningkatkan validitas eksternal hasil rekomendasi. Kedua, penelitian ini menegaskan kembali keunggulan metodologis SAW dalam menangani kriteria campuran (benefit dan cost) dengan prosedur normalisasi yang sederhana namun robust. Ketiga, penelitian ini memperkuat posisi SAW sebagai alat pengambilan keputusan yang aplikatif di ranah praktis, sekaligus tetap relevan secara akademik.

Dari sisi teoretis, penelitian ini memperkaya literatur mengenai efektivitas SAW dalam domain pengambilan keputusan multi-kriteria dengan menunjukkan aplikasinya pada konteks keamanan komputer. Hasil penelitian ini mengonfirmasi bahwa SAW memiliki validitas internal (melalui konsistensi perhitungan) dan validitas eksternal (melalui kesesuaian hasil dengan data empiris), sehingga dapat dijadikan dasar untuk penelitian lanjutan yang melibatkan metode hibrid atau dataset yang lebih besar.

Dari sisi praktis, penelitian ini memberikan pedoman obyektif bagi pengguna maupun organisasi dalam menentukan perangkat lunak antivirus yang sesuai dengan kebutuhan spesifik. Mekanisme yang ditawarkan memungkinkan keputusan diambil secara lebih terarah, mengurangi bias subjektif, serta dapat direplikasi pada kasus serupa. Dengan demikian, penelitian ini berkontribusi tidak hanya pada pengembangan ilmu pengetahuan, tetapi juga pada penyelesaian masalah nyata di lapangan.

5. Simpulan

Penelitian ini telah mengimplementasikan algoritma *Simple Additive Weighting* (SAW) untuk menjawab persoalan subjektivitas dan kompleksitas dalam pemilihan perangkat lunak antivirus gratis. Dengan menggunakan lima kriteria utama kecepatan pemindaian, kemampuan deteksi, rating, optimasi sumber daya, dan kelengkapan fitur algoritma SAW berhasil menghasilkan pemeringkatan alternatif yang obyektif, sistematis, dan transparan. Hasil pengolahan menunjukkan bahwa Windows Security menempati peringkat tertinggi, diikuti oleh Avira, Bitdefender, Avast, dan Kaspersky.

Validasi performa algoritma yang dilakukan melalui tiga mekanisme (i) pemeriksaan konsistensi perhitungan, (ii) analisis sensitivitas bobot kriteria, dan (iii) konfirmasi obyektivitas terhadap data empiris menunjukkan bahwa SAW memiliki validitas internal yang kuat sekaligus obyektivitas eksternal yang memadai. Pemeriksaan konsistensi membuktikan bahwa seluruh tahapan komputasi sesuai dengan formulasi matematis; analisis sensitivitas mengindikasikan bahwa hasil pemeringkatan adaptif terhadap variasi bobot kriteria namun tetap mempertahankan stabilitas alternatif terbaik; sementara konfirmasi dengan data empiris menegaskan kesesuaian hasil perhitungan dengan kinerja aktual perangkat lunak antivirus di lapangan. Dengan demikian, algoritma SAW terbukti reliabel, robust, serta dapat diandalkan dalam konteks pemilihan multi-kriteria.

Kontribusi penelitian ini bersifat ganda. Dari sisi teoretis, penelitian ini memperkuat literatur mengenai efektivitas SAW dalam proses pengambilan keputusan multi-kriteria, khususnya dalam domain keamanan komputer, sekaligus memperluas cakupan penerapan dengan menambahkan validasi empiris yang komprehensif. Dari sisi praktis, penelitian ini menawarkan kerangka pengambilan keputusan yang dapat menjadi pedoman obyektif bagi pengguna maupun institusi dalam menentukan prioritas pemilihan antivirus sesuai kebutuhan spesifik.

Sebagai agenda penelitian lanjutan, integrasi SAW dengan metode lain seperti *fuzzy logic*, *Analytical Hierarchy Process* (AHP), maupun pendekatan stokastik direkomendasikan untuk mengakomodasi ketidakpastian data dan preferensi pengguna yang lebih kompleks. Selain itu, perluasan cakupan dataset pada konteks dan kategori perangkat lunak yang lebih beragam diharapkan dapat meningkatkan generalisasi temuan serta memperdalam kontribusi akademik terhadap pengembangan ilmu pengambilan keputusan multi-kriteria.

Daftar Referensi

[1] A. Putri, N. Sari, P. Fajrina, and S. Aisyah, “Keamanan online dalam media sosial: Pentingnya perlindungan data pribadi di era digital (studi kasus Desa Pematang Jering),” *Jurnal Pengabdian Nasional (JPN) Indonesia*, vol. 6, no. 1, pp. 38–45, Nov. 2024, doi: https://doi.org/10.35870/jpni.v6i1.1097.

[2] P. Prabaswari, M. Alfikri, and I. Ahmad, “Evaluasi implementasi kebijakan pembentukan tim tanggap insiden siber pada sektor pemerintah,” *Matra Pembaruan*, vol. 6, no. 1, pp. 1–14, May 2022, doi: https://doi.org/10.21787/mp.6.1.2022.1-14.

[3] R. Sivapriyan, S. Sushmitha, K. Pooja, and N. Sakshi, “Analysis of security challenges and issues in IoT enabled smart homes,” in *Proc. IEEE CSITSS*, Bengaluru, India, Dec. 2021, pp. 1–6, doi: https://doi.org/10.1109/csitss54238.2021.9683324.

[4] F. A. Aryatama and S. Samsugi, “Sistem keamanan kendaraan bermotor dengan ESP32 menggunakan kontrol Android,” *SMATIKA Jurnal*, vol. 14, no. 1, pp. 167–176, Jul. 2024, doi: https://doi.org/10.32664/smatika.v14i01.1267.

[5] I. I. Ridho, G. Mahalisa, D. R. Sari, and I. Fikri, “Metode neural network untuk penentuan akurasi prediksi harga rumah,” *Technologia Jurnal Ilmiah*, vol. 13, no. 1, pp. 56–63, Feb. 2022, doi: https://doi.org/10.31602/tji.v13i1.6252.

[6] N. Elyondri and N. Azizah, “Analisis pengembangan komunikasi, persepsi, bunyi, dan irama (PKPBI) anak tunarungu dan kebutuhan media pembelajarannya,” *Jurnal Obsesi: Jurnal*

Pendidikan Anak Usia Dini*, vol. 7, no. 5, pp. 6141–6156, Nov. 2023, doi: https://doi.org/10.31004/obsesi.v7i5.4130.
[7] I. I. Ridho, G. Mahalisa, D. R. Sari, and I. Fikri, “Metode Neural Network untuk Penentuan Akurasi Prediksi Harga Rumah,” *Technologia Jurnal Ilmiah*, vol. 13, no. 1, pp. 56–63, Feb. 2022, doi: 10.31602/tji.v13i1.6252.
[8] I. M. M. Matin, “Hyperparameter Tuning Menggunakan GridsearchCV pada Random Forest untuk Deteksi Malware,” *MULTINETICS*, vol. 9, no. 1, pp. 43–50, May 2023, doi: 10.32722/multinetics.v9i1.5578.
[9] A.-R. Belea, “Methods for Detecting Malware Using Static, Dynamic and Hybrid Analysis,” in *Proceedings of the International Conference on Cybersecurity and Cyberforensics (CyberCon)*, May 2023, doi: 10.19107/cybercon.2023.34.
[10] R. L. Simanjuntak, T. R. Siagian, and V. Anggriani, “Sistem Pendukung Keputusan Menggunakan Metode TOPSIS dalam Pemilihan Smartphone Android,” *Jurnal Ilmiah Komputasi*, vol. 23, no. 3, pp. 13–24, Sep. 2024, doi: 10.32409/jikstik.23.3.3610.
[11] F. Nuraeni, A. D. Supriatna, and A. Bachtiar, “Sistem Informasi Geografis Pemetaan Lahan Garapan Serikat Petani Pasundan Kabupaten Garut,” *Jurnal Algoritma*, vol. 19, no. 2, pp. 527–537, Nov. 2022, doi: 10.33364/algoritma/v.19-2.1139.
[12] C. S. Octiva, P. E. Haes, T. I. Fajri, H. Eldo, and M. L. Hakim, “Implementasi Teknologi Informasi pada UMKM: Tantangan dan Peluang,” *Jurnal Minfo Polgan*, vol. 13, no. 1, pp. 815–826, Jul. 2024, doi: 10.33395/jmp.v13i1.13823.
[13] P. J. C. Jaya and I. Setiawan, “Strategi Pelestarian Cagar Budaya Terhadap Keputusan Berkunjung Kembali Wisatawan di Kota Cirebon,” *Jurnal Cendekia Jaya*, vol. 2, no. 2, pp. 47–56, Aug. 2020, doi: 10.47685/cendekia-jaya.v2i2.72.
[14] R. Asmara and Y. Purbokusumo, “Pilihan Instrumen Kebijakan Penataan Ruang untuk Manajemen Sumber Daya Tanah Pertanian (Sawah) di Kabupaten Sleman,” *Widya Bhumi*, vol. 2, no. 2, pp. 88–100, Nov. 2022, doi: 10.31292/wb.v2i2.40.
[15] N. P. Mardiana, N. D. S. Lestari, I. W. S. Putri, D. Trapsilasiwi, and R. P. Murtikusuma, “Tinjauan Gaya Belajar: Bagaimana Kemampuan Numerasi Siswa Auditorial dalam Menyelesaikan Soal Tes Tertulis AKM Materi Bentuk Aljabar,” *Jurnal Ilmiah Pendidikan Matematika (JIPM)*, vol. 13, no. 1, pp. 79–88, Sep. 2024, doi: 10.25273/jipm.v13i1.20538.
[16] L. A. Yaum, M. Marsidi, N. C. P., and A. Mais, “Desain dan Pengembangan Teknologi Asistif Berbasis Aplikasi Speech Text Reading Converter for Conference (SPETRIC) untuk Pembelajaran Daring Bagi Mahasiswa Disabilitas Rungu,” *Jurnal Ortopedagogia*, vol. 8, no. 2, pp. 158–163, Nov. 2022, doi: 10.17977/um031v8i22022p158-163.
[17] A. B. Nassif, et al., “Software Defect Prediction Using Learning to Rank Approach,” *Scientific Reports*, vol. 13, no. 1, pp. 1–15, Nov. 2023, doi: 10.1038/s41598-023-45915-5.
[18] M. Liu, Y. He, Z. Xue, X. He, and J. Chen, “MultiScan: A Private Online Virus Detection System,” *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 53–58, Oct. 2019, doi: 10.1109/MCE.2019.2941351.
[19] M. Z. M. Ashik, et al., “Detection of Malicious Software by Analyzing Distinct Artifacts Using Machine Learning and Deep Learning Algorithms,” *Electronics*, vol. 10, no. 14, p. 1694, Jul. 2021, doi: 10.3390/electronics10141694.
[20] M. Arsyad, M.Z. Redha, A. Pahdi, & A. Yulianto, “Uji Akurasi Metode SAW Dalam Menentukan Kelayakan Penerima Bantuan Program Keluarga Harapan. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 13, no. 1, pp. 785-794, 2024.
[21] Y. Yudihartanti, T. Taufiq, R. Ruliah, “Penerapan Model Analytical Hierarchy Process Untuk Pemilihan Perusahaan Jasa Ekspedisi. *Progresif: Jurnal Ilmiah Komputer*, vol. 19, no. 1, pp. 269-288, 2023.
[22] S. Sriram, M. Ramachandran, S. Chinnasamy, & G. Mathivanan, “A review on multi-criteria decision-making and its application. *REST Journal on Emerging trends in Modelling and Manufacturing*, vol. 7, no. 4, pp. 1-107, 2022.