INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

Analisis Tingkat Risiko Virus Komputer Menggunakan Metode Simple Additive Weighting SAW

Ade Kurnia Ramzani[1)] Muhammad Irsan[2)] Fathi Ahyar[3)]

Fakultas Sains dan Teknologi, Universitas Labuhanbatu

e-mail: bangkurnia7@gmail.com, ahmadirsan9000@gmail.com, fathiahyar54@gmail.com

Corresponding Author : bangkurnia7@gmail.com

ABSTRACT

The rapid advancement of information technology has led to increased computer and network usage across various activities; however, it has also heightened the risk of cyberattacks, particularly those involving computer viruses or malware. Since each type of malware possesses distinct characteristics and varying levels of danger, a method is required to objectively assess the risk level of each virus. This study aims to analyze computer virus risk levels using the Simple Additive Weighting (SAW) method. The alternatives evaluated in this study include Trojans, Worms, Spyware, Ransomware, and Adware. The criteria employed encompass the rate of spread, system damage, data theft capability, detection difficulty, and impact on system performance. The SAW method was applied through a process involving criteria weighting, decision matrix normalization, preference value calculation, and alternative ranking. The results indicate that Ransomware achieved the highest preference value (0.96), thereby ranking first as the virus with the highest risk level. This was followed by Trojans (0.81), Worms (0.74), Spyware (0.71), and Adware (0.48). These findings demonstrate that the SAW method facilitates a systematic and objective analysis of computer virus risk levels, serving as a basis for prioritizing responses to malware threats.

Keywords: Computer Virus, Malware, Decision Support System, Simple Additive Weighting, Cybersecurity.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan manusia. Pemanfaatan teknologi digital tidak hanya digunakan dalam sektor pendidikan dan bisnis, tetapi juga telah menjadi bagian penting dalam aktivitas pemerintahan, kesehatan, serta layanan publik. Meningkatnya ketergantungan terhadap sistem digital menyebabkan keamanan informasi menjadi salah satu aspek yang perlu mendapatkan perhatian khusus. Di sisi lain, perkembangan teknologi tersebut juga diikuti oleh meningkatnya ancaman siber yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data pada suatu sistem informasi[1], [2].

Ancaman siber dapat muncul dalam berbagai bentuk, mulai dari pencurian data, peretasan jaringan, hingga penyebaran perangkat lunak berbahaya atau malware. Malware merupakan salah satu ancaman yang paling sering digunakan oleh pelaku kejahatan siber untuk memperoleh keuntungan maupun merusak sistem milik korban. Kehadiran malware tidak hanya menimbulkan kerugian

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

finansial, tetapi juga dapat menyebabkan gangguan operasional, kehilangan data penting, serta menurunkan tingkat kepercayaan pengguna terhadap sistem yang digunakan[3], [4].

Malware atau *malicious software* adalah program yang dirancang untuk melakukan aktivitas berbahaya tanpa sepengetahuan pengguna. Malware memiliki berbagai jenis seperti trojan, worm, spyware, ransomware, adware, dan keylogger. Setiap jenis malware memiliki karakteristik, metode penyebaran, serta dampak yang berbeda-beda terhadap sistem komputer. Perbedaan karakteristik tersebut menyebabkan tingkat risiko yang ditimbulkan oleh masing-masing malware tidak dapat disamakan sehingga diperlukan suatu mekanisme untuk melakukan penilaian risiko secara objektif dan terukur[5].

Seiring berkembangnya teknologi keamanan, pelaku serangan siber juga terus mengembangkan teknik yang lebih kompleks untuk menghindari deteksi sistem keamanan konvensional. Beberapa malware modern mampu beroperasi secara tersembunyi di dalam sistem, mengumpulkan informasi sensitif pengguna, serta berkomunikasi dengan server penyerang tanpa diketahui oleh korban. Kondisi ini menunjukkan bahwa ancaman malware tidak lagi sekadar mengganggu kinerja perangkat, tetapi juga dapat menjadi sarana pencurian informasi dan pelanggaran privasi dalam skala yang lebih luas[6].

Upaya pencegahan dan penanganan malware memerlukan pemahaman yang baik mengenai tingkat bahaya dari setiap jenis ancaman. Penentuan prioritas penanganan menjadi penting karena sumber daya keamanan yang dimiliki oleh individu maupun organisasi sering kali terbatas. Oleh sebab itu, diperlukan suatu pendekatan yang mampu membantu proses pengambilan keputusan dalam menentukan jenis malware yang memiliki tingkat risiko paling tinggi sehingga dapat diprioritaskan untuk ditangani terlebih dahulu. Pendekatan tersebut harus mampu mempertimbangkan berbagai faktor yang memengaruhi tingkat risiko suatu malware[7][8].

Salah satu teknologi yang dapat digunakan untuk membantu proses pengambilan keputusan adalah Sistem Pendukung Keputusan (SPK). Sistem Pendukung Keputusan merupakan sistem berbasis komputer yang dirancang untuk membantu pengguna dalam memilih alternatif terbaik berdasarkan sejumlah kriteria tertentu. SPK mampu mengurangi subjektivitas dalam proses pengambilan keputusan serta memberikan hasil yang lebih sistematis dan terukur dibandingkan dengan penilaian secara manual[9][10].

Dalam implementasinya, Sistem Pendukung Keputusan memiliki berbagai metode yang dapat digunakan untuk menyelesaikan permasalahan pengambilan keputusan multikriteria. Salah satu metode yang paling banyak digunakan adalah metode Simple Additive Weighting (SAW). Metode SAW dikenal memiliki konsep yang sederhana,

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

mudah dipahami, dan mampu menghasilkan perangkingan alternatif berdasarkan nilai preferensi yang diperoleh dari proses pembobotan dan normalisasi data. Selain itu, metode ini memiliki tingkat akurasi yang baik dalam membantu menentukan alternatif terbaik berdasarkan sejumlah kriteria yang telah ditentukan[11][12].

Metode SAW telah banyak diterapkan pada berbagai bidang, seperti pemilihan siswa terbaik, penerima beasiswa, penentuan karyawan terbaik, hingga rekomendasi produk berdasarkan kebutuhan pengguna. Keberhasilan metode tersebut dalam menyelesaikan berbagai permasalahan pengambilan keputusan menunjukkan bahwa SAW dapat digunakan untuk melakukan analisis terhadap objek yang memiliki banyak atribut penilaian. Oleh karena itu, metode SAW dinilai sesuai untuk diterapkan dalam proses analisis tingkat risiko virus komputer yang melibatkan beberapa kriteria penilaian risiko[13][14].

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis tingkat risiko beberapa jenis virus komputer menggunakan metode Simple Additive Weighting (SAW). Analisis dilakukan dengan mempertimbangkan sejumlah kriteria yang berkaitan dengan karakteristik malware, seperti tingkat penyebaran, kemampuan merusak sistem, potensi pencurian data, tingkat kesulitan deteksi, dan dampaknya terhadap kinerja perangkat. Hasil penelitian diharapkan dapat memberikan informasi mengenai tingkat risiko masing-masing virus komputer serta membantu pengguna maupun organisasi dalam menentukan prioritas penanganan ancaman siber secara lebih efektif dan terukur.

.

2. METODE PE NELITIAN

2.1 *Tahapan Penelitian*

Penelitian ini dilakukan melalui beberapa tahapan, yaitu identifikasi masalah, studi literatur, penentuan alternatif dan kriteria penilaian, pemberian bobot kriteria, penyusunan matriks keputusan, proses normalisasi, perhitungan nilai preferensi menggunakan metode *Simple Additive Weighting* (SAW), serta perangkingan alternatif untuk menentukan tingkat risiko virus komputer. Tahapan tersebut disusun secara sistematis agar proses pengambilan keputusan dapat dilakukan secara objektif berdasarkan kriteria yang telah ditetapkan. Metode SAW dipilih karena mampu menyelesaikan permasalahan pengambilan keputusan multikriteria melalui proses pembobotan, normalisasi, dan perhitungan nilai preferensi sehingga menghasilkan alternatif terbaik berdasarkan nilai akhir yang diperoleh[15][16].

Gambar 1. Tahapan Metode Penelitian

2.2 *Sistem Pengambilan Keputusan*

Sistem Pendukung Keputusan (SPK) merupakan sistem berbasis komputer yang dirancang untuk membantu proses pengambilan keputusan dengan mengolah data dan informasi menjadi suatu rekomendasi yang dapat digunakan sebagai dasar dalam menentukan alternatif terbaik. SPK berfungsi untuk meningkatkan efektivitas dan objektivitas pengambilan keputusan, terutama pada permasalahan yang melibatkan banyak kriteria dan alternatif. Dalam penelitian ini, SPK digunakan untuk membantu proses analisis tingkat risiko virus komputer berdasarkan beberapa kriteria penilaian yang telah ditentukan, sehingga dapat diperoleh hasil perangkingan risiko secara sistematis dan terukur menggunakan metode *Simple Additive Weighting*[17].

2.2 *Simple Additive Weighting*

Simple Additive Weighting merupakan salah satu metode dalam Sistem Pendukung Keputusan yang digunakan untuk menyelesaikan permasalahan Multi Attribute Decision Making (MADM). Metode SAW dikenal sebagai metode penjumlahan terbobot karena bekerja dengan menjumlahkan seluruh nilai alternatif yang telah dikalikan dengan bobot masing-masing kriteria. Metode ini dipilih karena memiliki proses perhitungan yang sederhana, mudah dipahami, serta mampu menghasilkan proses perangkingan alternatif secara objektif berdasarkan nilai dan bobot kriteria yang digunakan[18].

Tahapan pertama dalam metode SAW adalah melakukan proses normalisasi matriks keputusan agar seluruh nilai alternatif dapat diperbandingkan pada skala yang sama. Rumus normalisasi untuk atribut benefit dan cost ditunjukkan sebagai berikut:

Untuk atribut benefit:

$$r_{ij} = \frac{x_{ij}}{\max x_{ij}}$$

Untuk atribut cost :

$$r_{ij} = \frac{\min x_{ij}}{x_{ij}}$$

Keterangan:

r_{ij} = nilai hasil normalisasi
x_{ij} = nilai alternatif pada setiap kriteria
$\max x_{ij}$ = nilai terbesar kriteria pada setiap benefit
$\min x_{ij}$ = nilai terkecil pada kriteria cost

Setelah proses normalisasi selesai dilakukan, tahap berikutnya adalah menghitung nilai preferensi setiap alternatif menggunakan rumus penjumlahan terbobot berikut:

$$V_i = \sum_{j=1}^{n} w_j r_{ij}$$

Keterangan:

V_i = nilai preferensi alternatif

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

w_j = bobot setiap kriteria
r_{ij} = nilai hasil normalisasi
n = jumlah kriteria

3. HASIL DAN PEMBAHASAN

3.1 *Analisis Masalah*

Virus komputer atau malware merupakan salah satu ancaman keamanan siber yang terus berkembang dan dapat menimbulkan berbagai dampak negatif terhadap sistem komputer maupun jaringan. Setiap jenis malware memiliki karakteristik, metode penyebaran, serta tingkat bahaya yang berbeda-beda, sehingga proses penanganannya memerlukan prioritas yang tepat. Namun, dalam praktiknya masih banyak pengguna yang mengalami kesulitan dalam menentukan malware yang memiliki tingkat risiko paling tinggi karena penilaian sering dilakukan secara subjektif tanpa mempertimbangkan berbagai faktor risiko secara menyeluruh. Oleh karena itu, diperlukan suatu metode yang mampu membantu proses analisis risiko secara objektif berdasarkan beberapa kriteria yang relevan, seperti tingkat penyebaran, kerusakan sistem, kemampuan pencurian data, tingkat kesulitan deteksi, dan dampaknya terhadap performa perangkat. Melalui penerapan Sistem Pendukung Keputusan menggunakan metode *Simple Additive Weighting* (SAW), proses penilaian risiko malware dapat dilakukan secara sistematis sehingga menghasilkan informasi yang dapat digunakan sebagai dasar dalam menentukan prioritas penanganan ancaman keamanan siber.

3.2 *Penerapan Metode SAW*

Penerapan metode *Simple Additive Weighting* (SAW) pada penelitian ini dilakukan untuk menentukan tingkat risiko virus komputer berdasarkan beberapa kriteria yang telah ditetapkan. Metode SAW digunakan dengan cara memberikan bobot pada setiap kriteria penilaian, kemudian melakukan proses normalisasi dan perangkingan terhadap seluruh alternatif virus komputer. Kriteria yang digunakan dalam penelitian ini terdiri dari tingkat penyebaran, kerusakan sistem, kemampuan pencurian data, tingkat kesulitan deteksi, dan dampak terhadap performa sistem. Penentuan bobot dilakukan berdasarkan tingkat kepentingan masing-masing kriteria dalam menentukan risiko suatu virus sehingga hasil analisis yang diperoleh dapat digunakan sebagai dasar dalam menentukan prioritas penanganan ancaman malware.

Kode	Kriteria	Jenis Atribut	Bobot
C1	Tingkat Penyebaran	Benefit	25%
C2	Kerusakan Sistem	Benefit	25%
C3	Kemampuan Pencurian Data	Benefit	20%
C4	Tingkat Kesulitan Deteksi	Benefit	15%
C5	Dampak terhadap	Benefit	15%

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

Kode	Kriteria	Jenis Atribut	Bobot
	Performa Sistem		

Tabel 3.2. Bobot Tiap Kriteria

Setelah menentukan kriteria dan bobot penilaian, selanjutnya ditentukan alternatif virus komputer yang akan dianalisis, yaitu:

A1 = Trojan

A2 = Worm

A3 = Spyware

A4 = Ransomware

A5 = Adware

Alternatif	C1	C2	C3	C4	C5
A1	4	4	5	4	3
A2	5	4	2	3	4
A3	3	3	5	5	2
A4	5	5	4	5	5
A5	3	2	2	2	3

Tabel 3.1. Nilai Alternatif terhadap Kriteria

Perhitungan dilakukan sesuai dengan tahapan metode *Simple Additive Weighting* (SAW), yaitu:

Atribut Benefit

$r_{ij} = x_{ij} / \max(x_{ij})$

Atribut Cost

$r_{ij} = \min(x_{ij}) / x_{ij}$

Keterangan:

r_{ij} = nilai normalisasi

x_{ij} = nilai alternatif pada setiap kriteria

$\max(x_{ij})$ = nilai maksimum pada suatu kriteria

$\min(x_{ij})$ = nilai minimum pada suatu kriteria

Karena semua kriteria yang kita gunakan pada penelitian virus komputer adalah Benefit (semakin tinggi nilainya semakin berbahaya), maka perhitungannya menggunakan rumus :

$$\mathbf{r_{ij} = x_{ij} / \max(x_{ij})}$$

Perhitungan dilakukan sesuai dengan tahapan metode Simple Additive Weighting (SAW), yaitu:

Kriteria C1 (Tingkat Penyebaran)

A1 untuk Trojan :

r11 = 4/5 = 0,80

A2 untuk Worm :

r21 = 5/5 = 1,00

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

A3 untuk Spyware :

r31 = 3/5 = 0,60

A4 untuk Ransomware :

r41 = 5/5 = 1,00

A5 untuk Adware :

r51 = 3/5 = 0,60

Kriteria C2 (Kerusakan Sistem)

A1 untuk Trojan :

r12 = 4/5 = 0,80

A2 untuk Worm :

r22 = 4/5 = 0,80

A3 untuk Spyware :

r32 = 3/5 = 0,60

A4 untuk Ransomware :

r42 = 5/5 = 1,00

A5 untuk Adware :

r52 = 2/5 = 0,40

Kriteria C3 (Kemampuan Pencurian Data)

A1 untuk Trojan :

r13 = 5/5 = 1,00

A2 untuk Worm :

r23 = 2/5 = 0,40

A3 untuk Spyware :

r33 = 5/5 = 1,00

A4 untuk Ransomware :

r43 = 4/5 = 0,80

A5 untuk Adware :

r53 = 2/5 = 0,40

Kriteria C4 (Tingkat Kesulitan Deteksi)

A1 untuk Trojan :

r14 = 4/5 = 0,80

A2 untuk Worm :

r24 = 3/5 = 0,60

A3 untuk Spyware :

r34 = 5/5 = 1,00

A4 untuk Ransomware :

r44 = 5/5 = 1,00

A5 untuk Adware :

r54 = 2/5 = 0,40

Kriteria C5 (Dampak terhadap Performa Sistem)

A1 untuk Trojan :

r15 = 3/5 = 0,60

A2 untuk Worm :

r25 = 4/5 = 0,80

A3 untuk Spyware :

r35 = 2/5 = 0,40

A4 untuk Ransomware :

r45 = 5/5 = 1,00

A5 untuk Adware :

r55 = 3/5 = 0,60

Setelah seluruh proses normalisasi selesai, diperoleh matriks normalisasi sebagai berikut:

Alternatif	**1**	**2**	**3**	**4**	**5**
A1 (Trojan)	,80	,80	,00	,80	,60
A2 (Worm)	,00	,80	,40	,60	,80
A3 (Spyware)	,60	,60	,00	,00	,40
A4 (Ransomware)	,00	,00	,80	,00	,00
A5 (Adware)	,60	,40	,40	,40	,60

3.3 *Perhitungan Nilai Preferensi*

Setelah proses normalisasi matriks keputusan selesai dilakukan, tahap berikutnya adalah menghitung nilai preferensi setiap alternatif virus komputer menggunakan metode Simple Additive Weighting (SAW). Perhitungan nilai preferensi dilakukan dengan mengalikan setiap nilai hasil normalisasi dengan bobot masing-masing kriteria kemudian menjumlahkan seluruh hasil perkalian tersebut. Alternatif dengan nilai preferensi tertinggi menunjukkan virus yang memiliki tingkat risiko paling tinggi.

Diketahui bobot setiap kriteria sebagai berikut:

C1 = 25% = 0,25

C2 = 25% = 0,25

C3 = 20% = 0,20

C4 = 15% = 0,15

C5 = 15% = 0,15

Perhitungan nilai preferensi:

A1 untuk Trojan

V1 = (0,25 × 0,80) + (0,25 × 0,80) + (0,20 × 1,00) + (0,15 × 0,80) + (0,15 × 0,60)

V1 = 0,20 + 0,20 + 0,20 + 0,12 + 0,09

V1 = **0,81**

A2 untuk Worm

V2 = (0,25 × 1,00) + (0,25 × 0,80) + (0,20 × 0,40) + (0,15 × 0,60) + (0,15 × 0,80)

V2 = 0,25 + 0,20 + 0,08 + 0,09 + 0,12

V2 = **0,74**

A3 untuk Spyware

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

V3 = (0,25 × 0,60) + (0,25 × 0,60) + (0,20 × 1,00) + (0,15 × 1,00) + (0,15 × 0,40)

V3 = 0,15 + 0,15 + 0,20 + 0,15 + 0,06

V3 = **0,71**

A4 untuk Ransomware

V4 = (0,25 × 1,00) + (0,25 × 1,00) + (0,20 × 0,80) + (0,15 × 1,00) + (0,15 × 1,00)

V4 = 0,25 + 0,25 + 0,16 + 0,15 + 0,15

V4 = **0,96**

A5 untuk Adware

V5 = (0,25 × 0,60) + (0,25 × 0,40) + (0,20 × 0,40) + (0,15 × 0,40) + (0,15 × 0,60)

V5 = 0,15 + 0,10 + 0,08 + 0,06 + 0,09

V5 = **0,48**

Berdasarkan hasil perhitungan nilai preferensi menggunakan metode *Simple Additive Weighting* (SAW), diperoleh hasil perangkingan tingkat risiko virus komputer berdasarkan nilai preferensi tertinggi hingga terendah. Hasil perangkingan tersebut dapat dilihat pada Tabel 4.

No	Alternatif	Nilai Preferensi	Perankingan
	A1 (Trojan)	0,81	2
	A2 (Worm)	0,74	3
	A3 (Spyware)	0,71	4
	A4 (Ransomware)	0,96	1
	A5 (Adware)	0,48	5

Tabel 4. Hasil Perangkingan Tingkat Risiko Virus Komputer

Berdasarkan Tabel 4 dapat diketahui bahwa alternatif A4 yaitu Ransomware memperoleh nilai preferensi tertinggi sebesar 0,96. Hasil tersebut menunjukkan bahwa Ransomware merupakan jenis malware yang memiliki tingkat risiko paling tinggi dibandingkan alternatif lainnya berdasarkan kriteria tingkat penyebaran, kerusakan sistem, kemampuan pencurian data, tingkat kesulitan deteksi, dan dampak terhadap performa sistem. Sementara itu, alternatif A5 yaitu Adware memperoleh nilai preferensi terendah sebesar 0,48, sehingga memiliki tingkat risiko yang relatif lebih rendah dibandingkan jenis malware lainnya. Dengan demikian, hasil perangkingan menggunakan metode SAW dapat digunakan sebagai dasar dalam menentukan prioritas penanganan ancaman malware pada sistem komputer.

4. PEMBAHASAN

Berdasarkan hasil perhitungan menggunakan metode *Simple Additive Weighting* (SAW), diperoleh nilai preferensi yang berbeda untuk setiap alternatif virus komputer. Perbedaan nilai tersebut dipengaruhi oleh skor masing-masing alternatif pada setiap kriteria yang digunakan, yaitu tingkat penyebaran, kerusakan sistem, kemampuan pencurian data, tingkat kesulitan deteksi, dan dampak terhadap performa sistem. Metode SAW mampu mengolah seluruh kriteria tersebut

melalui proses normalisasi dan pembobotan sehingga menghasilkan nilai akhir yang dapat digunakan sebagai dasar dalam menentukan tingkat risiko setiap virus komputer secara objektif dan terukur.

Hasil perangkingan menunjukkan bahwa **Ransomware (A4)** memperoleh nilai preferensi tertinggi sebesar **0,96**, sehingga menempati peringkat pertama sebagai virus dengan tingkat risiko paling tinggi. Tingginya nilai tersebut disebabkan karena Ransomware memiliki skor yang tinggi pada hampir seluruh kriteria penilaian, terutama pada aspek kerusakan sistem, tingkat penyebaran, dan dampaknya terhadap performa perangkat. Selain itu, ransomware juga dikenal sebagai malware yang mampu mengenkripsi data korban sehingga pengguna kehilangan akses terhadap data penting dan sering kali harus membayar sejumlah uang tebusan untuk mendapatkan kembali akses tersebut. Kondisi ini menjadikan ransomware sebagai salah satu ancaman siber yang paling berbahaya bagi pengguna individu maupun organisasi.

Sementara itu, **Adware (A5)** memperoleh nilai preferensi terendah sebesar **0,48**, sehingga memiliki tingkat risiko yang lebih rendah dibandingkan alternatif lainnya. Meskipun demikian, adware tetap berpotensi mengganggu kenyamanan pengguna melalui munculnya iklan yang tidak diinginkan serta dapat memengaruhi kinerja perangkat. Secara keseluruhan, hasil penelitian menunjukkan bahwa metode SAW dapat digunakan untuk membantu proses analisis tingkat risiko virus komputer dengan mempertimbangkan berbagai kriteria secara bersamaan. Hasil perangkingan yang diperoleh diharapkan dapat menjadi acuan dalam menentukan prioritas penanganan malware sehingga upaya mitigasi ancaman keamanan siber dapat dilakukan secara lebih efektif dan efisien.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, metode *Simple Additive Weighting* (SAW) dapat diterapkan untuk menganalisis tingkat risiko virus komputer berdasarkan beberapa kriteria penilaian, yaitu tingkat penyebaran, kerusakan sistem, kemampuan pencurian data, tingkat kesulitan deteksi, dan dampak terhadap performa sistem. Melalui proses pembobotan, normalisasi, dan perhitungan nilai preferensi, metode SAW mampu menghasilkan perangkingan tingkat risiko virus komputer secara sistematis dan objektif.

Hasil perhitungan menunjukkan bahwa **Ransomware (A4)** memperoleh nilai preferensi tertinggi sebesar **0,96**, sehingga menempati peringkat pertama sebagai virus dengan tingkat risiko paling tinggi. Selanjutnya diikuti oleh **Trojan (A1)** dengan nilai preferensi **0,81**, **Worm (A2)** sebesar **0,74**, **Spyware (A3)** sebesar **0,71**, dan **Adware (A5)** sebesar **0,48**. Hasil tersebut menunjukkan bahwa ransomware merupakan ancaman yang perlu mendapatkan prioritas penanganan karena memiliki dampak yang paling besar berdasarkan kriteria yang digunakan dalam penelitian.

Dengan demikian, penerapan metode SAW terbukti dapat membantu proses pengambilan

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

keputusan dalam menentukan prioritas penanganan virus komputer berdasarkan tingkat risikonya. Hasil penelitian ini diharapkan dapat menjadi referensi bagi pengguna maupun organisasi dalam memahami tingkat bahaya berbagai jenis malware sehingga langkah pencegahan dan penanganan dapat dilakukan secara lebih efektif. Untuk penelitian selanjutnya, jumlah alternatif dan kriteria penilaian dapat diperluas agar menghasilkan analisis yang lebih komprehensif dan sesuai dengan perkembangan ancaman keamanan siber yang terus berubah.

ACUAN REFERENSI

[1] B. L. Handoko, A. Swat, L. Lindawati, and M. Mustapha,"Application of Computer Assisted Audit[1] Pertamina, *Keamanan Siber Perusahaan*. 2020. [Online]. Available at: https://www.pertamina.com/id/keamanan-siber-perusahaan%0Ahttps://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/458

[2] J. I. Sosial, "AL-BAHST", vol 2, no 1, bll 8–16, 2024.

[3] F. Prasepta en S. Surbakti, "Edukasi Keamanan Siber Berdigital dengan Aman Pendahuluan Dalam era digital saat ini , keamanan siber menjadi aspek penting yang harus diperhatikan oleh setiap individu maupun Lembaga (Abdullah & Ikasari , 2023). Tingginya tingkat adopsi teknologi digit", vol 5636, no 4, bll 868–878, 2024.

[4] E. Keamanan, J. W. Dan, D. Agustina, M. R. Aulia, en N. Afriandi, "Pengenalan Ancaman Dan Pencegahan Serangan Siber Melalui", vol 1, bll 643–649, 2025.

[5] Y. D. P. Rahayu en N. Trianto, "Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1", *Info Kripto*, no 1, 2021.

[6] R. Setiawan en R. Surya Kusuma, "Analisis Forensik Jaringan terhadap Infeksi Malware MetaStealer: Penerapan Metode SWGDE", *J. Cyber Heal. Comput.*, vol 3, no 1, bll 6–14, 2025, doi: 10.64163/jochac.v3i1.48.

[7] Z. Fuada, "Penerapan Keamanan Jaringan Menggunakan Sistem Snort Dan Honeypot Sebagai Pendeteksi Dan Pencegah Malware Skripsi", bll 1–55, 2023.

[8] K. Ulvi, G. Rasikha, R. Aulia, S. Rika, en M. Hidayani, "Kajian Ancaman Malware dan Upaya Pencegahan melalui Penguatan Keamanan Sistem Komputer", *JIKUM J. Ilmu Komput.*, vol 2, no 1, bll 108–110, 2026, doi: 10.62671/jikum.v2i1.155.

[9] M. Setya en D. Utomo, "PENERAPAN METODE SAW (SIMPLE ADDITIVE WEIGHT) PADA SISTEM PENDUKUNG KEPUTUSAN UNTUK PEMBERIAN BEASISWA PADA SMA NEGERI 1 CEPU JAWA TENGAH".

[10] H. T. Sihotang en M. S. Siboro, "APLIKASI SISTEM PENDUKUNG KEPUTUSAN PENENTUAN SISWA

INFORMATIKA
Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 14 No.2 /Mei/2026
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

BERMASALAH MENGGUNAKAN METODE SAW PADA SEKOLAH SMP SWASTA MULIA PRATAMA MEDAN", 2016.

[11] A. Setiadi, Y. Yunita, en A. R. Ningsih, "Penerapan Metode Simple Additive Weighting(SAW) Untuk Pemilihan Siswa Terbaik", *J. Sisfokom (Sistem Inf. dan Komputer)*, vol 7, no 2, bll 104–109, 2018, doi: 10.32736/sisfokom.v7i2.572.

[12] S. Melati en G. Triyono, "PEMODELAN SISTEM PENDUKUNG KEPUTUSAN PENENTUAN SISWA TERBAIK MENGGUNAKAN METODE SIMPLE ADDICTIVE WEIGHTING (SAW)".

[13] A. Wanto en H. Damanik, "Analisis Penerapan Sistem Pendukung Keputusan Terhadap Seleksi Penerima Beasiswa BBM (Bantuan Belajar Mahasiswa) Pada Perguruan Tinggi Menggunakan Metode Simple Additive Weighting (SAW) (Studi Kasus : AMIK Tunas Bangsa Pematangsiantar)", 2015.

[14] F. F. 4) 1) Ikmah 1) , Almas Adlil Wafi 2) , Ely Purnawati 3), "SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN KARYAWAN TERBAIK Sistem Informasi Universitas Amikom Yogyakarta Abstraksi Keywords : Pendahuluan Metode Penelitian", vol 6, no 1, bll 33–38, 2023.

[15] A. Wanto en H. Damanik, "… Keputusan Terhadap Seleksi Penerima Beasiswa BBM (Bantuan Belajar Mahasiswa) Pada Perguruan Tinggi Menggunakan Metode Simple Additive Weighting …", *Pros. Semin. Nas. Rekayasa II*, no November, bll 323–333, 2015, [Online]. Available at: https://osf.io/bvjm9/download

[16] M. S. S. Hengki Tamando Sihotang, "Swasta Mulia Pratama Medan", *JIPN (Journal Informatics Pelita Nusantara)*, vol 1, no 1, bll 1–6, 2016, [Online]. Available at: http://e-jurnal.pelitanusantara.ac.id/index.php/JIPN/article/view/148/69

[17] M. S. . Utomo, "Penerapan Metode Saw (Simple Additive Weight) Pada Sistem Pendukung Keputusan Untuk Pemberian Beasiswa Pada Sma Negeri 1 Cepu Jawa Tengah", *Fak. Ilmu Komput. Univ. Dian Nuswantoro, Semarang*, bll 1–12, 2015.

[18] M. Simaremare, A. Putera, en U. Siahaan, "Decision Support System in Selecting The Appropriate Laptop Using Simple Additive Weighting", bll 215–222, 2016.