BAB II
TINJAUAN PUSTAKA

2.1 Penelitian yang Relevan

Penelitian ini mengkaji beberapa studi terdahulu yang relevan sebagai dasar perbandingan dan penguatan terhadap penelitian yang sedang dilakukan. Kajian tersebut difokuskan pada kesesuaian topik, metodologi yang digunakan, serta temuan utama dari penelitian sebelumnya agar dapat memperjelas posisi dan kontribusi penelitian ini.

Penelitian pertama yang dilakukan oleh (Kodrat, 2024), berjudul *"A hybrid AHP-TOPSIS for risk analysis in maritime cybersecurity based on 3D models"*, mengusulkan pendekatan analisis risiko keamanan siber melalui integrasi metode *Analytical Hierarchy Process* (AHP) *dan Technique for Order of Preference by Similarity to Ideal Solution* (TOPSIS). Penelitian ini berfokus pada penilaian risiko dalam konteks sistem keamanan maritim, dengan mengidentifikasi tiga dimensi risiko utama, yaitu *Threat*, *Vulnerability*, dan *Consequence*, yang diperoleh melalui studi literatur serta *expert judgment*. Setelah struktur hierarki kriteria disusun untuk proses pembobotan menggunakan AHP, metode TOPSIS diterapkan guna melakukan pemeringkatan tingkat risiko dan menampilkan hasilnya dalam bentuk matriks risiko tiga dimensi. Hasil penelitian menunjukkan bahwa aspek prosedur perusahaan memiliki tingkat risiko tertinggi (0,368), sedangkan kesiapan sistem kapal memperoleh nilai risiko paling rendah (0,048). Temuan ini menegaskan bahwa kombinasi AHP–TOPSIS mampu memberikan evaluasi risiko yang sistematis dan terukur pada lingkungan keamanan yang kompleks. Relevansi penelitian tersebut terhadap penelitian ini terletak pada penggunaan TOPSIS sebagai metode pemeringkatan risiko serta penekanan pada variabel *Vulnerability* sebagai faktor penting dalam pengambilan keputusan terkait keamanan.

Penelitian kedua yang dilakukan oleh Almotiri (2024), berjudul *"Improving Network Resilience Against DDoS Attacks: A Fuzzy TOPSIS Strategy"* mengusulkan pendekatan evaluasi ketahanan jaringan terhadap serangan DDoS menggunakan metode Fuzzy TOPSIS.

Penelitian ini memanfaatkan data hasil audit keamanan jaringan yang mencakup atribut teknis seperti kemampuan deteksi intrusi, kemampuan pencegahan, strategi respons, dan toleransi terhadap intrusi. Untuk menangani ketidakpastian dalam penilaian setiap atribut, penelitian ini menerapkan logika fuzzy sebelum dilakukan pemeringkatan menggunakan TOPSIS. Hasil penelitian menunjukkan bahwa jaringan N6 menjadi jaringan paling tangguh, disusul oleh N1 dan N5, serta membuktikan bahwa Fuzzy TOPSIS efektif dalam memberikan evaluasi kuantitatif terhadap ketahanan jaringan dalam kondisi data yang tidak pasti. Relevansi penelitian ini terhadap skripsi yang saya lakukan terletak pada penerapan metode TOPSIS dalam domain keamanan siber. Meskipun fokusnya pada ketahanan jaringan terhadap DDoS, pendekatan multi-kriteria yang digunakan memberikan dasar metodologis yang sejalan dengan penelitian ini dalam menentukan prioritas kerentanan secara terukur berdasarkan atribut keamanan yang berbeda.

Penelitian ketiga yang dilakukan oleh Walkowski *et al.* (2021), berjudul *"Automatic CVSS-Based Vulnerability Prioritization and Response with Context Information and Machine Learning"* berfokus pada otomasi proses prioritisasi kerentanan berbasis CVSS v3.x dengan mempertimbangkan konteks operasional sistem ICT. Data kerentanan diperoleh melalui pemindai jaringan dan diolah untuk menghitung *Environmental Score* yang menyesuaikan dampak kerentanan terhadap lingkungan sistem yang spesifik. Selanjutnya, algoritma *machine learning* digunakan untuk menentukan prioritas perbaikan kerentanan secara otomatis. Hasil penelitian menunjukkan bahwa penggunaan *Environmental Score* dapat mengurangi estimasi jam kerja perbaikan hingga 8% serta menurunkan risiko dibandingkan hanya mengandalkan *Base Score*. Penelitian ini sangat relevan dengan penelitian saya karena menyoroti keterbatasan *CVSS Base Score* dan pentingnya mempertimbangkan konteks operasional dalam prioritisasi kerentanan. Selain itu, variabel keamanan seperti *Confidentiality, Integrity, dan Availability* (CIA) yang menjadi dasar CVSS turut memperkuat pemilihan kriteria dalam penelitian ini.

Penelitian keempat yang dilakukan oleh Mohd Shabbir (2025), berjudul *"Evaluating the Impact of Security Risks Through Fuzzy AHP–TOPSIS Method"* mengevaluasi faktor-faktor risiko keamanan informasi menggunakan pendekatan hibrida Fuzzy AHP dan Fuzzy TOPSIS. Penulis mengidentifikasi beberapa parameter risiko utama dalam keamanan perangkat lunak, yaitu *Confidentiality, Integrity, Availability* (CIA), *Authentication*, dan *Authorization*. Fuzzy AHP digunakan untuk menentukan bobot kriteria dalam kondisi penilaian yang tidak pasti, sedangkan Fuzzy TOPSIS diterapkan untuk meranking prioritas risiko keamanan. Hasil penelitian menunjukkan bahwa *Authorization* merupakan kriteria paling kritis, disusul oleh *Integrity* dan *Authentication*. Penelitian ini menegaskan efektivitas metode TOPSIS dalam memberikan pemeringkatan prioritas risiko secara terukur. Relevansi penelitian ini terhadap skripsi saya terletak pada penggunaan atribut keamanan standar, khususnya CIA Triad, yang juga menjadi komponen penting dalam data CVSS Kaspersky. Dengan demikian, penelitian ini memperkuat landasan teoritis dalam pemilihan kriteria kerentanan pada penelitian ini.

Penelitian kelima yang dilakukan oleh Zulfa *et al.* (2025), berjudul *"Penerapan Metode TOPSIS dalam Sistem Informasi Pengaduan Keresahan dan Kejahatan Lingkungan Berbasis Web"* mengembangkan sebuah sistem informasi berbasis web yang mengintegrasikan algoritma TOPSIS untuk menentukan prioritas penanganan laporan masyarakat. Penelitian ini menggunakan beberapa kriteria utama, yaitu urgensi, dampak, frekuensi, dan responsibilitas, yang diolah secara otomatis oleh sistem menggunakan *framework* Laravel dan basis data MySQL. Algoritma TOPSIS diterapkan untuk menghitung skor preferensi (Vi) guna menghasilkan perankingan prioritas penanganan laporan. Hasil pengujian menggunakan metode Black Box menunjukkan bahwa sistem berhasil menjalankan proses perhitungan TOPSIS dengan valid dan membantu admin dalam proses pengambilan keputusan. Relevansi penelitian ini terhadap skripsi terletak pada aspek implementasi teknis, khususnya sebagai referensi apabila metode TOPSIS hendak diintegrasikan ke dalam sistem berbasis web untuk pemrosesan data Kaspersky secara otomatis.

Penelitian keenam oleh Kostelić (2025), berjudul *"TOPSIS-based Framework for Evaluating Employee Cybersecurity Risk"* mengusulkan kerangka evaluasi risiko keamanan siber karyawan dengan memanfaatkan pembobotan AHP dan pemeringkatan menggunakan TOPSIS. Penelitian ini menggunakan lima kriteria risiko utama, yaitu *risky behavior, knowledge, compliance, attitudes, dan training,* yang dikembangkan dengan menggunakan data simulasi yang disesuaikan dari instrumen HAIS-Q dan BCISQ. Pembobotan dilakukan melalui metode perbandingan berpasangan *(Saaty scale),* kemudian matriks keputusan dinormalisasi dan dianalisis menggunakan TOPSIS untuk menghitung *relative closeness* (C*) terhadap solusi ideal. Hasil penelitian menunjukkan bahwa kerangka tersebut mampu membedakan tingkat risiko karyawan secara sistematis, dengan *risky behavior* sebagai kriteria terpenting. Meskipun penelitian ini masih menggunakan data simulasi, relevansinya terhadap skripsi ini terletak pada penerapan TOPSIS dalam konteks keamanan siber dan penggunaan pembobotan berbasis AHP, meskipun objek penelitian dan sumber datanya berbeda dari dataset kerentanan nyata yang digunakan dalam penelitian ini.

Penelitian ketujuh yang dilakukan oleh Khan *et al.* (2024), berjudul *"Enhanced Mechanism to Prioritize the Cloud Data Privacy Model Using AHP–TOPSIS"* mengembangkan mekanisme pemrioritasan model privasi data cloud dengan mengintegrasikan metode AHP untuk pembobotan kriteria dan TOPSIS untuk pemeringkatan model privasi. Data diperoleh dari perusahaan penyedia layanan cloud, dengan mempertimbangkan kriteria seperti biaya implementasi, efektivitas, dan risiko privasi. Hasil penelitian menunjukkan bahwa metode AHP–TOPSIS mampu menghasilkan urutan prioritas model privasi yang efektif dalam manajemen keamanan cloud. Walaupun penelitian ini relevan secara metodologis karena menggunakan pendekatan MCDM yang sama, fokus utamanya adalah pada privasi data cloud, bukan pada penanganan kerentanan perangkat lunak. Perbedaan tersebut menegaskan bahwa penelitian ini memiliki konteks yang lebih teknis pada aspek privasi, sedangkan skripsi ini lebih menitikberatkan pada manajemen kerentanan dan patching berdasarkan data operasional Kaspersky.

Penelitian kedelapan oleh Alnajim *et al.* (2026), yang berjudul *"Cyber Security Challenges for Software Vendors Through a Fuzzy-TOPSIS Approach"* membahas penentuan prioritas tantangan keamanan siber yang dihadapi vendor perangkat lunak. Penelitian ini diawali dengan *Systematic Literature Review* untuk mengidentifikasi 13 tantangan keamanan utama, yang selanjutnya divalidasi oleh 35 pakar industri. Evaluasi dilakukan menggunakan pendekatan Fuzzy TOPSIS guna menangani ketidakpastian penilaian pakar dan memberikan bobot serta pemeringkatan terhadap tantangan tersebut. Hasil penelitian menunjukkan bahwa *"Cyber Security Issues"* menduduki peringkat pertama dengan nilai kedekatan 0.768, diikuti oleh *"Lack of Proper Awareness"* Penelitian ini memberikan bukti kuat bahwa metode TOPSIS dan variannya efektif untuk memprioritaskan isu-isu keamanan yang kompleks dan ambigu. Relevansinya terhadap skripsi ini sangat tinggi karena mendukung pemilihan metode TOPSIS untuk proses prioritasi berbasis keamanan, meskipun objek yang diprioritaskan berbeda.

Penelitian kesembilan oleh Alshahrani *et al.* (2022), berjudul *"Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS"* menganalisis faktor risiko TI dari berbagai organisasi dengan melibatkan pakar keamanan dan manajer risiko. Penilaian faktor risiko dilakukan menggunakan Fuzzy Logic untuk mengatasi ketidakpastian dalam penilaian subjektif para ahli, dan hasilnya diperingkat menggunakan Fuzzy TOPSIS. Penelitian ini menunjukkan bahwa pendekatan Fuzzy TOPSIS mampu mengidentifikasi faktor risiko signifikan secara lebih akurat, seperti kegagalan keamanan data dan ketidakstabilan jaringan. Penelitian ini relevan karena menggunakan metode Fuzzy TOPSIS dalam konteks manajemen risiko TI, namun berbeda dari skripsi ini yang berfokus pada pengolahan dataset kerentanan perangkat lunak secara langsung dari sistem keamanan Kaspersky.

Penelitian kesepuluh yang dilakukan oleh Pratiwi Sumantri *et al.* (2021), berjudul *"Implementation of TOPSIS in Recommendations for New Position in Companies"* menerapkan metode TOPSIS untuk menentukan rekomendasi promosi jabatan pegawai berdasarkan beberapa kriteria seperti pengalaman kerja, penilaian kinerja, tingkat pendidikan, dan kemampuan komunikasi. Penilaian linguistik dikonversi ke nilai numerik,

kemudian melalui langkah normalisasi, pembobotan, dan perhitungan nilai preferensi TOPSIS, penelitian ini menghasilkan kandidat terbaik dengan nilai 0.748. Walaupun berada di luar domain keamanan siber, penelitian ini relevan secara metodologis karena menunjukkan efektivitas TOPSIS dalam menghasilkan pemeringkatan objektif berdasarkan banyak kriteria, sebagaimana digunakan dalam penelitian ini untuk memprioritaskan kerentanan berdasarkan kriteria keamanan yang terukur.

2.1.1 Matriks Penelitian

Tabel 2. 1 Matriks Penelitian

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
1	Putra *et al.* (2023)	*A Hybrid AHP–TOPSIS for Risk Analysis in Maritime Cybersecurity Based on 3D Models*	Studi literatur & *expert judgment*	Analisis risiko keamanan siber maritim	AHP + TOPSIS	Penelitian ini relevan karena menunjukkan penggunaan TOPSIS dalam pemeringkatan risiko keamanan dan mengintegrasikan variabel *Vulnerability*. Konsep analisis multikriteria ini menjadi landasan metodologis bagi

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
						penelitian ini dalam menyusun prioritas kerentanan berdasarkan data Kaspersky.
2	Almotiri (2024)	*Improving Network Resilience Against DDoS Attacks: A Fuzzy TOPSIS Strategy*	Data audit serangan DDoS	Mitigasi serangan jaringan	Fuzzy TOPSIS	Relevan secara metodologis karena menerapkan varian TOPSIS dalam konteks keamanan siber. Meskipun objeknya ketahanan jaringan terhadap DDoS, pendekatan perankingan multi-kriteria mendukung penggunaan TOPSIS dalam penelitian ini

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
						untuk menentukan prioritas kerentanan perangkat lunak.
3	Balsam *et al.* (2025)	*Automatic CVSS-Based Vulnerability Prioritization and Response with Context Information and Machine Learning*	Database CVSS hasil pemindaian ICT	Prioritisasi kerentanan berbasis CVSS	ML + CVSS Environmental Score	Penelitian ini relevan karena fokus pada prioritas kerentanan dan penggunaan CVSS sebagai indikator risiko. Hal ini memperkuat pemilihan kriteria *Severity* dalam penelitian ini serta menegaskan pentingnya konteks operasional dalam

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
						pemeringkatan kerentanan.
4	Shabbir *et al.* (2025)	*Evaluating the Impact of Security Risks through Fuzzy AHP–TOPSIS Method*	Identifikasi faktor risiko CIA & Authorization	Evaluasi dampak risiko keamanan	Fuzzy AHP + Fuzzy TOPSIS	Relevan karena menggunakan TOPSIS dalam konteks keamanan informasi dan menekankan pentingnya atribut CIA, yang juga merupakan dasar dalam CVSS. Penelitian ini mendukung justifikasi pemilihan kriteria dalam penelitian ini.
5	Zulfa *et al.* (2025)	Penerapan Metode TOPSIS dalam Sistem	Data laporan masyarakat	Prioritas penanganan laporan	TOPSIS (*Web System*)	Relevan dari sisi implementasi teknis, memberikan contoh

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
		Informasi Pengaduan Berbasis Web				bagaimana algoritma TOPSIS diintegrasikan ke dalam sistem aplikasi. Hal ini dapat menjadi referensi apabila penelitian ini dikembangkan menjadi dashboard prioritas kerentanan berbasis data Kaspersky.
6	Kostelić (2025)	*TOPSIS-Based Framework for Evaluating Employee Cybersecurity Risk*	Data simulasi berbasis HAIS-Q dan BCISQ	Evaluasi risiko keamanan siber berbasis faktor manusia	AHP weighting + TOPSIS	Relevan karena menggunakan pembobotan AHP dan TOPSIS dalam domain keamanan siber. Perbedaannya pada objek

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
						(risiko karyawan), namun metode yang digunakan mendukung penggunaan TOPSIS untuk penentuan prioritas kerentanan pada penelitian ini.
7	Khan (2024)	*Enhanced Mechanism to Prioritize the Cloud Data Privacy Model Using AHP–TOPSIS*	Data model privasi cloud	Prioritas model privasi data	AHP + TOPSIS	Relevan secara metodologis karena menunjukkan efektivitas AHP–TOPSIS untuk pemeringkatan, namun berbeda konteks. Penelitian ini menguatkan penggunaan metode MCDM pada skripsi ini,

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
						meskipun penelitian ini menilai kerentanan perangkat lunak dan variabel operasional seperti *Device Count dan Update Availability.*
8	Alnajim *et al.* (2026)	*Cyber Security Challenges for Software Vendors Through a Fuzzy-TOPSIS Approach*	SLR + kuesioner pakar	Prioritas tantangan keamanan vendor perangkat lunak	Fuzzy TOPSIS	Sangat relevan karena menggunakan TOPSIS untuk memprioritaskan isu keamanan kompleks. Penelitian ini mendukung pemilihan metode TOPSIS dalam skripsi ini dan menunjukkan

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
						bahwa TOPSIS efektif untuk prioritas berbasis risiko di domain keamanan siber.
9	Rafique *et al.* (2021)	*Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS*	Survei pakar TI	Manajemen risiko TI	Fuzzy TOPSIS	Relevan karena menggunakan metode TOPSIS dalam evaluasi risiko TI. Meskipun tidak fokus pada kerentanan perangkat lunak, penelitian ini memperkuat dasar teoritis penggunaan TOPSIS sebagai alat untuk pengambilan keputusan multikriteria dalam penelitian ini.

No	Nama Penulis (Tahun)	Judul Penelitian	Sumber Data	Klasifikasi Masalah	Arsitektur / Metode	Keterkaitan Penelitian
10	Pratiwi Sumantri *et al.* (2021)	*Implementation of TOPSIS in Recommendations for New Position in Companies*	Data kinerja pegawai	Sistem pendukung keputusan promosi	TOPSIS	Relevan secara metodologis karena membuktikan bahwa TOPSIS mampu menghasilkan pemeringkatan objektif berdasarkan banyak kriteria. Hal ini sejalan dengan penelitian ini yang menggunakan TOPSIS untuk meranking kerentanan berdasarkan kriteria keamanan yang terukur.

Berdasarkan matriks penelitian di atas, terlihat bahwa metode TOPSIS dan berbagai pengembangannya (AHP–TOPSIS, Fuzzy TOPSIS, hingga kombinasi dengan Machine Learning) telah banyak digunakan dalam pengambilan keputusan multikriteria, khususnya pada domain keamanan siber dan manajemen risiko. Beberapa penelitian berfokus pada evaluasi risiko keamanan secara umum, mitigasi serangan jaringan, pemeringkatan faktor risiko TI, hingga prioritas model privasi data cloud.

Namun demikian, terdapat beberapa celah penelitian yang dapat diidentifikasi:

1. Sebagian besar penelitian berfokus pada evaluasi risiko secara makro, bukan pada prioritisasi kerentanan perangkat lunak secara spesifik berdasarkan data operasional nyata.
2. Penggunaan variabel kontekstual operasional masih terbatas, terutama kombinasi variabel seperti *Severity Score*, *Device Count*, *Age in Days*, dan *Update Availability* dalam satu model prioritisasi.
3. Belum banyak penelitian yang menggunakan dataset aktual dari sistem keamanan perusahaan, seperti hasil pemindaian kerentanan dari *Kaspersky Security Center* dalam konteks manajemen *patch* di lingkungan organisasi nyata.

Berdasarkan kondisi tersebut, penelitian ini menempati posisi yang berbeda dibandingkan studi sebelumnya. Penelitian ini secara khusus menerapkan metode TOPSIS untuk memprioritaskan kerentanan perangkat lunak dengan memanfaatkan data operasional nyata dari PT PLN Nusa Daya. Selain itu, penelitian ini mengintegrasikan variabel teknis dan kontekstual secara bersamaan guna menghasilkan prioritas yang lebih representatif terhadap kondisi aktual organisasi. Dengan pendekatan tersebut, penelitian ini diharapkan dapat memberikan kontribusi praktis dalam membantu proses pengambilan keputusan terkait manajemen kerentanan dan penentuan prioritas penanganan secara lebih sistematis, objektif, dan berbasis data nyata.

2.2 Landasan Teori

Landasan teori mengulas bermacam teori yang dipakai dalam penelitian ini. Teori-teori tersebut dikumpulkan dan diambil dari berbagai buku, jurnal, serta artikel yang dapat dipercaya yang membahas, mendukung, dan menjadi acuan bagi penelitian ini.

2.2.1 Kerentanan (*Vulnerability*)

Kerentanan (*vulnerability*) merujuk pada kelemahan pada sistem, aplikasi, jaringan, atau konfigurasi yang dapat dimanfaatkan oleh pihak tidak berwenang dan berpotensi mengganggu kerahasiaan, integritas, serta ketersediaan informasi (*confidentiality, integrity, and availability* / CIA). Kerentanan tidak semata-mata bersumber dari aspek teknis perangkat lunak, tetapi juga dapat muncul akibat kesalahan konfigurasi, praktik operasional yang kurang aman, serta pengelolaan aset digital yang belum optimal (Chimezie *et al.,* 2024). Kondisi ini diperkuat oleh *Buku Kajian Ketahanan Siber: Manajemen Kerentanan*, yang menyatakan bahwa meningkatnya intensitas serangan siber di Indonesia mencerminkan masih banyaknya celah keamanan pada aplikasi dan sistem informasi yang belum dikelola secara memadai (Nurhidayat *et al.,* 2024).

Perkembangan teknologi informasi yang semakin pesat mendorong aktivitas pemindaian keamanan menghasilkan temuan kerentanan dalam jumlah besar, sementara kapasitas sumber daya mitigasi organisasi relatif terbatas. Situasi tersebut menuntut adanya mekanisme prioritisasi yang sistematis agar kerentanan dengan tingkat risiko tertinggi dapat ditangani secara tepat dan efisien (Fitriani, 2024). Pandangan ini sejalan dengan pedoman yang menekankan bahwa manajemen kerentanan harus dilakukan secara berkelanjutan serta melibatkan berbagai pemangku kepentingan, sehingga proses mitigasi dapat disesuaikan dengan tingkat urgensi masing-masing kerentanan (Nurhidayat *et al.,* 2024). Selain itu, penilaian risiko tidak hanya bergantung pada tingkat keparahan, tetapi juga dipengaruhi oleh konteks operasional, tingkat keterpaparan aset, serta dinamika peluang eksploitasi yang terus berkembang (Huda *et al.,* 2024).

Dalam praktiknya, urgensi penanganan kerentanan umumnya ditentukan berdasarkan empat faktor utama, yaitu tingkat keparahan dampak (*severity*), ketersediaan pembaruan keamanan (*Update Availability*), usia kerentanan (*Age in Days*), dan jumlah perangkat terdampak (*Device Count*). Keempat faktor tersebut sejalan dengan pedoman dan diperkuat dengan menegaskan bahwa proses identifikasi dan analisis kerentanan perlu mempertimbangkan dampak potensial, peluang eksploitasi, serta cakupan aset yang terpengaruh (Nurhidayat *et al.,* 2024).

Berdasarkan landasan tersebut, penelitian ini menggunakan konsep kerentanan sebagai dasar penetapan kriteria dalam metode TOPSIS. Kriteria *severity, Update Availability, Age in Days,* dan *Device Count* dipilih karena merepresentasikan faktor risiko utama yang memengaruhi prioritas penanganan kerentanan pada lingkungan sistem PT PLN Nusa Daya. Penerapan TOPSIS diharapkan mampu menghasilkan pemeringkatan kerentanan yang objektif, terukur, dan relevan dengan kondisi operasional perusahaan.

2.2.2 Manajemen Kerentanan *(Vulnerability Management)*

Manajemen kerentanan merupakan proses sistematis yang mencakup identifikasi, analisis, penentuan prioritas, dan perbaikan kelemahan keamanan pada sistem informasi. Tujuan utama dari proses ini adalah memastikan bahwa celah keamanan yang berpotensi dieksploitasi dapat ditangani secara tepat sebelum menimbulkan dampak yang signifikan bagi organisasi. (Fronita M, 2023), menegaskan bahwa manajemen kerentanan tidak terbatas pada aktivitas pendeteksian semata, tetapi juga mencakup analisis risiko serta implementasi langkah mitigasi, seperti penerapan *patch* keamanan.

Azza *et al.* (2025), menjelaskan bahwa manajemen kerentanan merupakan bagian integral dari penguatan ketahanan siber. Proses ini meliputi identifikasi aset, pemantauan kerentanan, penilaian risiko, serta penetapan prioritas penanganan. Penilaian risiko dilakukan dengan mempertimbangkan tingkat dampak terhadap aset, peluang eksploitasi, dan konteks operasional sistem, sehingga tindakan mitigasi yang diambil dapat lebih efektif dan terarah.

Karena jumlah temuan kerentanan pada organisasi umumnya sangat besar, proses prioritisasi tidak dapat dilakukan secara acak. Haoxing & System (n.d.), menjelaskan bahwa pendekatan *risk-based vulnerability management* merupakan strategi yang paling efektif, karena mempertimbangkan faktor-faktor risiko seperti potensi dampak, kemungkinan eksploitasi, nilai aset, dan tingkat keterpaparan sistem. Hal ini sejalan dengan Azza *et al.* (2025), yang menekankan pentingnya pemetaan risiko sebagai dasar penentuan prioritas perbaikan, agar sumber daya mitigasi difokuskan pada kerentanan yang paling kritis.

Selain aspek prioritisasi Lyu *et al.* (2025), menegaskan bahwa *patch management* merupakan komponen penting dalam manajemen kerentanan, khususnya ketika pembaruan keamanan telah tersedia. Penundaan penerapan *patch* pada aset kritis dapat meningkatkan risiko eksploitasi. Oleh karena itu, proses manajemen kerentanan perlu mempertimbangkan faktor teknis dan operasional, seperti jadwal pemeliharaan, ketergantungan antar sistem, serta potensi gangguan terhadap layanan.

Dalam penelitian ini, proses prioritisasi kerentanan didasarkan pada empat kriteria utama, yaitu severity, *Age in Days*, *Update Availability*, dan *Device Count*. Keempat faktor tersebut memberikan gambaran yang lebih komprehensif terkait tingkat ancaman dan urgensi penanganan. Dengan menerapkan pendekatan berbasis risiko melalui metode TOPSIS, prioritas penanganan kerentanan dapat ditetapkan secara objektif dan sesuai kebutuhan keamanan PT PLN Nusa Daya.

2.2.3 Sistem Pendukung Keputusan (SPK)

Sistem Pendukung Keputusan (SPK) atau *Decision Support System* (DSS) merupakan sistem berbasis komputer yang dirancang untuk membantu pengambil keputusan dalam menangani permasalahan yang bersifat tidak terstruktur maupun semi-terstruktur. DSS tidak bertujuan menggantikan peran manusia, melainkan berfungsi sebagai alat bantu dengan menyediakan data yang terintegrasi, model analisis, serta antarmuka interaktif yang mendukung evaluasi alternatif secara sistematis dan terukur (Alahmadi & Jamjoom, 2022).

Dalam organisasi modern, DSS memiliki peran yang semakin penting karena mampu mengolah data historis maupun data *real-time* untuk menghasilkan rekomendasi yang lebih objektif dan akurat. Liu *et al.* (2021), menyatakan bahwa DSS berperan dalam mengurangi bias subjektif pada proses pengambilan keputusan, terutama pada kondisi yang melibatkan analisis multikriteria atau risiko yang kompleks. Dukungan komputasi dan model matematis pada DSS turut meningkatkan konsistensi keputusan serta membantu organisasi merespons perubahan lingkungan secara lebih cepat dan efisien.

Secara umum, DSS terdiri atas empat komponen utama, yaitu:

1. Basis Data/Basis Pengetahuan (*Database/Knowledge Base*)

   Berfungsi sebagai media penyimpanan data dan informasi yang dibutuhkan dalam proses analisis dan pengambilan keputusan.

2. Basis Model (*Model Base*)

   Menyediakan berbagai model matematis dan analitis, termasuk teknik statistik, optimisasi, serta metode pengambilan keputusan multikriteria yang digunakan untuk mengevaluasi alternatif keputusan.

3. Antarmuka Pengguna (*User Interface*)

   Berperan sebagai penghubung antara pengguna dan sistem, sehingga proses interaksi, evaluasi, dan interpretasi hasil dapat dilakukan secara intuitif dan fleksibel.

4. Pengguna (*User*)

   Merupakan pihak pengambil keputusan yang memanfaatkan keluaran sistem sebagai dasar dalam memilih alternatif keputusan secara rasional

Dalam konteks keamanan informasi, DSS telah banyak dimanfaatkan untuk mendukung proses evaluasi dan prioritisasi risiko. Liu *et al.* (2021), menunjukkan bahwa penerapan DSS memungkinkan integrasi berbagai faktor risiko, seperti tingkat keparahan, tingkat paparan, dan dampak, sehingga rekomendasi yang dihasilkan menjadi lebih objektif

dan konsisten dibandingkan dengan penilaian manual. Selain itu, Alahmadi & Jamjoom (2022), menegaskan bahwa DSS berbasis data mampu meningkatkan akurasi pengambilan keputusan pada domain dengan tingkat ketidakpastian yang tinggi, termasuk keamanan jaringan.

Pada penelitian ini, Sistem Pendukung Keputusan digunakan sebagai landasan konseptual dalam penerapan metode TOPSIS. Melalui pendekatan DSS, proses penentuan prioritas kerentanan dapat dilakukan secara lebih terstruktur, terukur, dan minim subjektivitas, sehingga mendukung penetapan penanganan kerentanan yang paling mendesak pada PT PLN Nusa Daya.

2.2.4 Pengambilan Keputusan Multi-Kriteria (MCDM)

Multi-Criteria Decision Making (MCDM) merupakan pendekatan pengambilan keputusan yang digunakan ketika suatu permasalahan harus dievaluasi berdasarkan lebih dari satu kriteria. Berbeda dengan metode pengambilan keputusan sederhana yang hanya mempertimbangkan satu faktor, MCDM memungkinkan penilaian alternatif dilakukan secara simultan dengan mempertimbangkan berbagai kriteria, baik yang bersifat kuantitatif maupun kualitatif. Azhar *et al.* (2021), menyatakan bahwa MCDM menyediakan kerangka kerja yang sistematis dan terukur untuk mendukung pengambilan keputusan yang lebih objektif, khususnya pada permasalahan dengan tingkat kompleksitas tinggi.

Seiring dengan berkembangnya sistem dan teknologi modern, MCDM banyak diterapkan pada bidang yang membutuhkan analisis prioritas secara komprehensif, seperti manajemen risiko, rekayasa sistem, pengelolaan sumber daya, hingga evaluasi keamanan informasi. Triantaphyllou (2021), menjelaskan bahwa MCDM sangat efektif digunakan ketika jumlah alternatif yang dinilai relatif banyak dan setiap alternatif memiliki karakteristik yang berbeda pada masing-masing kriteria. Pendekatan ini memungkinkan proses pengambilan keputusan tetap terukur meskipun data yang dianalisis bersifat kompleks dan

multidimensional. Secara umum, penerapan MCDM dilakukan melalui beberapa tahapan utama, yaitu:

1. Mendefinisikan permasalahan
2. Menetapkan tujuan dan batasan penelitian,
3. Mengidentifikasi alternatif Solusi
4. Menentukan kriteria penilaian
5. Memilih metode MCDM yang sesuai
6. Melakukan evaluasi alternatif menggunakan model matematis
7. Menetapkan solusi atau alternatif terbaik.

Beberapa metode yang umum digunakan dalam pendekatan MCDM antara lain *Analytic Hierarchy Process* (AHP), *Simple Additive Weighting* (SAW), *VlseKriterijumska Optimizacija I Kompromisno Resenje* (VIKOR), serta *Technique for Order of Preference by Similarity to Ideal Solution* (TOPSIS). Setiap metode memiliki karakteristik dan keunggulan masing-masing yang dapat disesuaikan dengan jenis data, jumlah kriteria, serta tujuan analisis yang ingin dicapai.

Dalam penelitian ini, MCDM digunakan sebagai dasar pemilihan metode TOPSIS. Pendekatan MCDM memungkinkan penggabungan berbagai kriteria penilaian kerentanan, yaitu *severity*, *Age in Days*, *Update Availability*, dan *Device Count*, ke dalam satu kerangka pengambilan keputusan yang terstruktur. Dengan mengacu pada tahapan MCDM sebagaimana dijelaskan oleh Rachman Jaya *et al.* (2021), proses pemeringkatan prioritas kerentanan dapat dilakukan secara objektif dan terukur, sehingga hasil yang diperoleh relevan dengan kebutuhan operasional PT PLN Nusa Daya.

2.2.5 Metode TOPSIS *(Technique for Order of Preference by Similarity to Ideal Solution)*

Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) merupakan salah satu metode *Multi-Criteria Decision Making* (MCDM) yang banyak digunakan untuk menyelesaikan permasalahan pemilihan dan pemeringkatan alternatif. Metode ini

diperkenalkan oleh Hwang & Yoon (2021), dengan prinsip dasar bahwa alternatif terbaik adalah alternatif yang memiliki jarak paling dekat dengan solusi ideal positif (*Positive Ideal Solution/PIS*) dan jarak paling jauh dari solusi ideal negatif (*Negative Ideal Solution/NIS*). Pendekatan berbasis kedekatan terhadap kondisi ideal ini menjadikan TOPSIS bersifat rasional, intuitif, dan relatif mudah diterapkan dalam berbagai konteks pengambilan keputusan (Kou, 2022).

Salah satu karakteristik utama TOPSIS adalah kemampuannya mempertahankan nilai asli data tanpa melakukan transformasi yang berlebihan. Dengan demikian, perbedaan karakteristik antar alternatif tetap dapat direpresentasikan secara proporsional. (Zavadskas *et al.,* 2020), menyatakan bahwa keunggulan TOPSIS terletak pada kemampuannya menghasilkan peringkat yang mencerminkan kondisi nyata dari setiap alternatif. Selain itu, TOPSIS memiliki efisiensi komputasi yang baik dan telah banyak diaplikasikan dalam berbagai bidang, seperti evaluasi kinerja, manajemen risiko, pemilihan teknologi, serta keamanan informasi (Mavi *et al.,* 2021).

Secara operasional, TOPSIS diawali dengan proses normalisasi data untuk menghilangkan perbedaan skala antar kriteria. Selanjutnya, setiap kriteria diberikan bobot sesuai tingkat kepentingannya, kemudian ditentukan solusi ideal positif dan negatif. Jarak masing-masing alternatif terhadap kedua solusi ideal tersebut dihitung untuk memperoleh nilai preferensi yang digunakan sebagai dasar pemeringkatan. S. R. Wicaksono (2023), menjelaskan bahwa mekanisme ini memungkinkan TOPSIS menghasilkan peringkat alternatif berdasarkan kedekatan relatif terhadap kondisi ideal yang diharapkan.

Langkah-langkah dalam metode TOPSIS mengacu pada S. R. Wicaksono (2023), yang meliputi:

1. Pembentukan Matriks Keputusan

$$X = \left[x_{ij}\right]_{m \times n} \tag{2.1}$$

2. Hitung *Normalized Decission Matrix* (Matriks Keputusan ternormalisasi)

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{2.2}$$

3. Hitung *Weight Normalized Decission Matrix* (Matriks Keputusan ternormalisasi dan terbobot).

$$v_{ij} = w_j r_{ij} \tag{2.3}$$

4. Rumus Menghitung Solusi Ideal Positif dan Negatif

$$A^+ = (\max v(1,j), \max v(2,j), \dots, \max v(n,j)) \tag{2.4}$$

$$A^- = (min\ v(1,j), min\ v(2,j), \dots, min\ v(n,j)) \tag{2.5}$$

5. Rumus hitung jarak ke solusi ideal positif

$$D_i^+ = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^+\right)^2} \tag{2.6}$$

6. Rumus hitung jarak ke solusi ideal negatif:

$$D_i^- = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^-\right)^2} \tag{2.7}$$

7. Menghitung Nilai Preferensi

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} \tag{2.8}$$

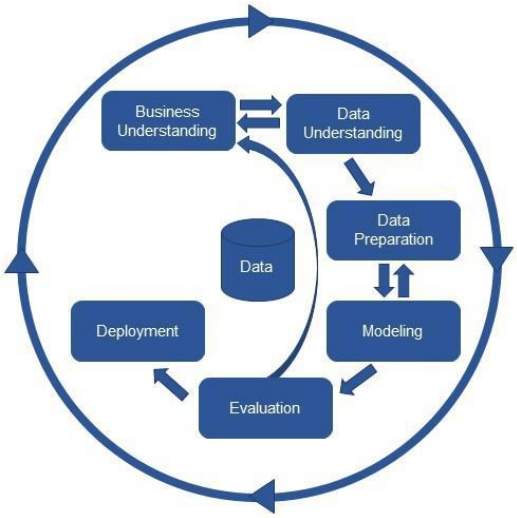
Namun, pada penelitian ini, penentuan bobot kriteria tidak dilakukan oleh penulis, melainkan ditetapkan langsung oleh pihak perusahaan berdasarkan kebijakan keamanan dan prioritas risiko internal yang berlaku. Pendekatan ini memastikan bahwa bobot yang digunakan selaras dengan kondisi operasional serta kebutuhan nyata organisasi. Atas dasar tersebut, metode TOPSIS diterapkan secara langsung tanpa dikombinasikan dengan metode lain seperti AHP, karena fokus penelitian ini adalah menghasilkan pemeringkatan kerentanan yang praktis, kontekstual, dan mudah diimplementasikan dalam lingkungan perusahaan.

Beberapa penelitian sebelumnya mengombinasikan TOPSIS dengan metode lain, seperti *Analytic Hierarchy Process* (AHP), untuk memperoleh bobot kriteria secara lebih objektif (Kahraman *et al.,* 2021). Namun, penelitian ini tidak menggunakan pendekatan hibrida tersebut. Namun, pada penelitian ini, penentuan bobot kriteria tidak dilakukan oleh peneliti, melainkan ditetapkan langsung oleh pihak perusahaan berdasarkan kebijakan keamanan dan prioritas risiko internal yang berlaku. Pendekatan ini memastikan bahwa bobot yang digunakan selaras dengan kondisi operasional serta kebutuhan nyata organisasi. Pendekatan ini bertujuan agar hasil pemeringkatan kerentanan yang dihasilkan lebih relevan terhadap kebutuhan operasional PT PLN Nusa Daya serta mencerminkan kondisi aktual di lapangan.

2.2.6 *CRISP-DM (Cross-Industry Standard Process for Data Mining)*

CRISP-DM (*Cross-Industry Standard Process for Data Mining*) merupakan standar proses yang dirancang sebagai pedoman umum dalam penyelesaian masalah berbasis data, baik pada konteks bisnis maupun penelitian, melalui tahapan data mining yang sistematis dan terstruktur (A. Karmila, 2024). Metodologi ini terdiri atas enam fase utama yang membentuk siklus hidup proyek data mining, yaitu *Business Understanding, Data Understanding, Data*

Preparation, Modeling, Evaluation, dan Deployment. Keenam fase tersebut bersifat berurutan namun tetap fleksibel untuk disesuaikan dengan kebutuhan proyek (Rifai *et al.,* 2019). Sebagai kerangka kerja yang komprehensif, CRISP-DM memfasilitasi integrasi berbagai keterampilan Teknologi Informasi (TI) guna mendukung tujuan bisnis sekaligus meningkatkan peluang keberhasilan pengolahan data (Siswipraptini *et al.,* 2023).



Gambar 2. 1 CRISP-DM (Rifai et al., 2019)

1. *Business Understanding*

Tahap *Business Understanding* berfokus pada pemahaman tujuan organisasi serta permasalahan yang akan diselesaikan melalui analisis data. Pada fase ini ditetapkan arah penelitian, ruang lingkup, dan batasan analisis agar solusi yang dikembangkan selaras dengan kebutuhan pengguna (S. Karmila *et al.,* 2024). Dalam penelitian ini, tahap ini digunakan untuk mengidentifikasi kebutuhan PT PLN Nusa Daya dalam menentukan prioritas penanganan kerentanan perangkat secara objektif dan terukur.

2. *Data Understanding*

Tahap *Data Understanding* dilakukan untuk memahami karakteristik data yang digunakan melalui proses pengumpulan, eksplorasi awal, serta pemeriksaan kualitas data. Kegiatan pada tahap ini meliputi identifikasi struktur data, pengecekan

kelengkapan, dan analisis deskriptif terhadap variabel yang relevan (Rifai *et al.,* 2019). Data yang dianalisis berasal dari hasil pemindaian Kaspersky, yang mencakup variabel *severity, Age in Days, Device Count,* dan *Update Availability*.

3. *Data Preparation*

Tahap *Data Preparation* bertujuan menghasilkan dataset akhir yang siap digunakan pada proses pemodelan (S. Karmila *et al.,* 2024). Pada tahap ini dilakukan pembersihan data untuk menangani *missing values* dan duplikasi, pemilihan atribut yang relevan, serta transformasi data agar sesuai dengan kebutuhan analisis. Tahap ini belum mencakup proses matematis TOPSIS seperti normalisasi dan pembobotan, karena proses tersebut dilakukan pada fase *Modeling*.

4. *Modeling*

Tahap *Modeling* merupakan fase penerapan metode analitik untuk membangun model yang sesuai dengan tujuan penelitian. Dalam penelitian ini digunakan metode TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*) untuk melakukan pemeringkatan kerentanan berdasarkan pendekatan multikriteria. Proses pemodelan meliputi pembentukan matriks keputusan, normalisasi data, pembobotan kriteria, penentuan solusi ideal positif dan negatif, perhitungan jarak, serta penentuan nilai preferensi dan peringkat akhir (Kou, 2022).

5. *Evaluation*

Tahap *Evaluation* dilakukan untuk menilai konsistensi dan rasionalitas hasil pemeringkatan yang diperoleh dari penerapan metode TOPSIS. Evaluasi difokuskan pada kesesuaian urutan prioritas kerentanan dengan tingkat keparahan serta dampak risiko yang terdapat dalam data operasional. Melalui tahap ini, dapat diketahui apakah hasil pemeringkatan yang dihasilkan metode TOPSIS dapat digunakan secara logis

dan praktis dalam mendukung proses penentuan prioritas penanganan kerentanan (Siswipraptini *et al.,* 2023)

6. *Deployment*

Tahap Deployment merupakan fase penyajian hasil analisis kepada pihak terkait agar dapat dimanfaatkan dalam proses pengambilan keputusan. Hasil penerapan metode TOPSIS disajikan dalam bentuk tabel pemeringkatan dan visualisasi data untuk memperjelas distribusi tingkat risiko serta nilai preferensi masing-masing kerentanan (Wirth & Hipp, 2021). Penyajian ini bertujuan memberikan rekomendasi prioritas penanganan kerentanan yang dapat dipertimbangkan oleh PT PLN Nusa Daya dalam pengelolaan keamanan sistem.

2.2.7 Kriteria Penilaian Kerentanan

Kriteria penilaian kerentanan digunakan untuk menilai tingkat risiko serta menentukan urgensi penanganan setiap celah keamanan. Nurhidayat *et al.* (2024), menegaskan bahwa penilaian kerentanan tidak hanya berfokus pada aspek teknis, tetapi juga harus mempertimbangkan konteks operasional aset, mengingat setiap kerentanan memiliki tingkat dampak dan peluang eksploitasi yang berbeda. Evaluasi yang dilakukan secara sistematis memungkinkan organisasi menetapkan prioritas mitigasi secara lebih efektif dan berbasis risiko. Berdasarkan data hasil pemindaian *Kaspersky Security Center*, penelitian ini menggunakan empat kriteria utama, yaitu *Severity Level, Update Availability, Age in Days,* dan *Device Count.*

1. *Severity Level/ Severity Score*

Severity Level merepresentasikan tingkat keparahan dampak yang ditimbulkan apabila suatu kerentanan berhasil dieksploitasi. Nilai ini umumnya diturunkan dari *Common Vulnerability Scoring System* (CVSS) yang mencerminkan dampak terhadap aspek kerahasiaan, integritas, dan ketersediaan sistem. Scarfone & Souppaya (2021), menyatakan bahwa tingkat keparahan merupakan parameter utama dalam proses prioritisasi karena secara langsung menggambarkan potensi kerusakan yang dapat terjadi. Oleh karena itu, dalam penelitian ini *Severity Level* diperlakukan sebagai kriteria *benefit*, di mana nilai yang lebih tinggi menunjukkan prioritas penanganan yang lebih mendesak.

2. *Updates Availability / Updates Score*

Update Availability menunjukkan ketersediaan pembaruan keamanan atau *patch* yang dapat digunakan untuk menutup suatu kerentanan. Shimizu & Hashimoto (2025), menyebutkan bahwa keberadaan *patch* merupakan salah satu mekanisme mitigasi risiko yang paling efektif, karena memungkinkan organisasi melakukan perbaikan secara cepat dan terukur. Dengan demikian, *Update Availability* diperlakukan sebagai kriteria *benefit*, di mana nilai yang lebih tinggi mengindikasikan kesiapan mitigasi yang lebih baik.

3. *Age in Days*

Age in Days menggambarkan durasi waktu sejak suatu kerentanan pertama kali diidentifikasi. Kerentanan yang dibiarkan dalam jangka waktu lama cenderung memiliki risiko eksploitasi yang lebih tinggi, seiring dengan semakin luasnya penyebaran informasi terkait celah tersebut (Krisper *et al.,* 2020). Berdasarkan pertimbangan tersebut, *Age in Days* diklasifikasikan sebagai kriteria *Cost*, sehingga nilai yang lebih rendah menunjukkan tingkat risiko yang lebih kecil.

4. *Device Count*

Device Count merepresentasikan jumlah perangkat yang terdampak oleh suatu kerentanan. Kou *et al.* (2022), menjelaskan bahwa semakin banyak perangkat yang terpengaruh, semakin besar *attack surface* yang terbentuk, sehingga potensi risiko juga meningkat. Oleh karena itu, dalam penelitian ini *Device Count* diperlakukan sebagai kriteria *benefit*, karena semakin besar jumlah perangkat terdampak, semakin tinggi urgensi penanganannya.

Dengan mempertimbangkan keempat kriteria tersebut, proses prioritisasi kerentanan dapat dilakukan secara lebih objektif dan terukur. Kriteria yang digunakan dinilai mampu merepresentasikan kondisi risiko yang relevan dalam praktik manajemen kerentanan dan selanjutnya menjadi dasar perhitungan metode TOPSIS untuk menentukan prioritas penanganan yang selaras dengan kebutuhan operasional PT PLN Nusa Daya.

2.2.8 Pembobotan Nilai

Pembobotan nilai merupakan tahapan penting dalam Sistem Pendukung Keputusan berbasis *Multi-Criteria Decision Making* (MCDM), termasuk metode TOPSIS, karena setiap kriteria memiliki tingkat pengaruh yang berbeda terhadap hasil keputusan. Perbedaan bobot kriteria secara langsung memengaruhi hasil pemeringkatan alternatif, sehingga penetapannya harus dilakukan secara terstruktur dan sesuai dengan karakteristik permasalahan. Dalam konteks analisis kerentanan keamanan sistem, pembobotan berfungsi untuk menunjukkan kontribusi relatif masing-masing faktor risiko dalam menentukan prioritas penanganan (Chen, 2020).

Secara umum, penentuan bobot kriteria dapat dilakukan melalui dua pendekatan, yaitu pendekatan subjektif dan pendekatan objektif. Pendekatan subjektif didasarkan pada penilaian ahli (*expert judgement*), pengalaman praktis, serta kebijakan organisasi dalam menetapkan prioritas risiko. Sementara itu, pendekatan objektif memanfaatkan metode matematis, seperti *Entropy Weight Method*, untuk menghasilkan bobot berdasarkan variasi atau karakteristik distribusi data. Namun demikian, beberapa studi menunjukkan bahwa

pendekatan subjektif lebih sesuai diterapkan pada bidang keamanan siber karena mampu mengakomodasi faktor operasional dan kebijakan internal yang sulit direpresentasikan hanya melalui perhitungan statistic (Mukhametzyanov, 2021).

Penelitian ini menerapkan pendekatan subjektif terarah, di mana penentuan bobot kriteria dilakukan oleh PT PLN Nusa Daya berdasarkan kebijakan keamanan siber yang berlaku. Proses pembobotan melibatkan tim ahli keamanan perusahaan yang memiliki pemahaman menyeluruh terhadap pola risiko, tingkat urgensi perbaikan, serta kondisi operasional perangkat. Dengan demikian, bobot yang digunakan bukan merupakan subjektivitas penulis, melainkan mencerminkan kebutuhan nyata dan prioritas strategis perusahaan. Pendekatan ini sejalan dengan pandangan bahwa pembobotan kriteria perlu mempertimbangkan konteks organisasi agar hasil prioritisasi risiko menjadi lebih relevan dan aplikatif (Mukhametzyanov, 2021).

Dalam metode TOPSIS, bobot kriteria digunakan sebagai faktor pengali pada matriks keputusan yang telah dinormalisasi, sehingga kriteria dengan bobot lebih besar akan memberikan pengaruh yang lebih dominan terhadap hasil pemeringkatan. Oleh karena itu, pembobotan harus memenuhi prinsip relevansi dan konsistensi, di mana total bobot bernilai satu agar perhitungan tetap proporsional (Wu *et al.,* 2023).

2.2.9 Kategorisasi Risiko

Kategorisasi risiko merupakan proses pengelompokan tingkat risiko untuk membantu organisasi menetapkan prioritas penanganan kerentanan secara efektif. Dalam manajemen keamanan informasi, risiko umumnya diklasifikasikan ke dalam tiga tingkat, yaitu *High Risk, Medium Risk*, dan *Low Risk*, guna memastikan fokus penanganan diarahkan pada ancaman yang paling signifikan Tingkat risiko ditentukan berdasarkan kombinasi kemungkinan eksploitasi (*likelihood*) dan besarnya dampak (*impact*) yang ditimbulkan apabila kerentanan dimanfaatkan (Security *et al.,* 2022).

1. *High Risk* merupakan kerentanan dengan dampak dan kemungkinan eksploitasi yang tinggi, sehingga berpotensi menyebabkan gangguan operasional,

kebocoran data, atau kompromi sistem. Kerentanan ini harus menjadi prioritas utama dan ditangani segera (*immediate remediation*).

2. *Medium Risk* adalah kerentanan dengan dampak atau peluang eksploitasi yang moderat. Meskipun tidak bersifat kritis secara langsung, kerentanan ini tetap memerlukan mitigasi yang dilakukan secara terjadwal setelah penanganan risiko tinggi (*scheduled remediation*).
3. *Low Risk* mencakup kerentanan dengan dampak minimal dan peluang eksploitasi yang rendah. Penanganannya umumnya dilakukan melalui pemeliharaan rutin, namun tetap perlu dipantau untuk mengantisipasi potensi peningkatan risiko di masa mendatang (Security *et al.,* 2022).

Dalam penelitian ini, klasifikasi risiko digunakan untuk mengelompokkan nilai preferensi hasil metode TOPSIS ke dalam tiga kategori risiko utama. Pengelompokan ini mendukung tahap *deployment* melalui visualisasi diagram pie untuk menunjukkan distribusi kerentanan, sehingga membantu PT PLN Nusa Daya memahami tingkat ancaman dan merencanakan mitigasi secara lebih terarah.

2.2.10 Visualisasi Data

Visualisasi data merupakan cara penyajian data dalam bentuk grafis untuk membantu pengguna memahami pola, hubungan, dan sebaran data secara lebih cepat dan akurat. Visualisasi berperan penting dalam menyampaikan informasi kuantitatif maupun kualitatif secara intuitif melalui grafik dan diagram sehingga mendukung pengambilan keputusan berbasis data (Romero-Organvídez & others, 2024).

Pemilihan jenis visualisasi harus disesuaikan dengan karakteristik data dan tujuan analisis. Qu (2024), menyatakan bahwa *pie chart* efektif untuk menunjukkan proporsi kategori, sedangkan *line chart* sesuai untuk menggambarkan tren dan variasi nilai. Visualisasi yang tepat mempermudah perbandingan data, identifikasi pola, serta interpretasi hasil analisis, termasuk bagi pengguna non-teknis.

1. *Pie Chart* untuk Distribusi Kategori Risiko

   Pie chart digunakan untuk menampilkan distribusi tingkat risiko kerentanan (*High, Medium, dan Low*) berdasarkan nilai preferensi TOPSIS. Grafik ini menunjukkan proporsi setiap kategori risiko secara jelas dan memudahkan identifikasi risiko yang paling dominan (Nugroho, 2025).

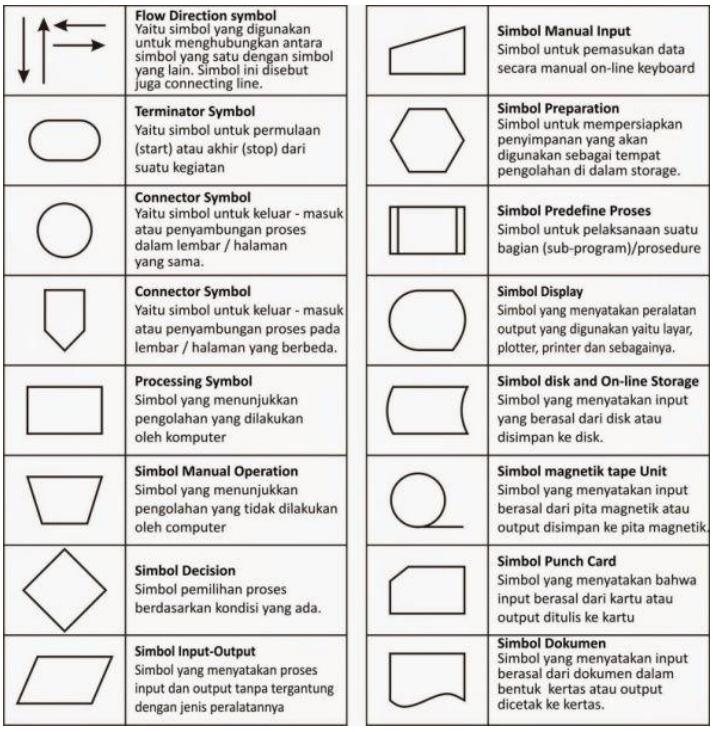
2. *Line Chart* untuk Persebaran Nilai TOPSIS

   Line chart digunakan untuk memvisualisasikan persebaran nilai preferensi kerentanan hasil metode TOPSIS. Visualisasi ini membantu menunjukkan perbedaan prioritas antar kerentanan serta variasi nilai yang menjadi dasar penentuan strategi penanganan (Qu, 2024).

Visualisasi data mendukung tahap *Deployment* dalam CRISP-DM dengan menyajikan hasil analisis secara ringkas dan mudah dipahami. Penggunaan *pie chart* dan *line chart* membantu PT PLN Nusa Daya dalam mengevaluasi risiko serta menentukan strategi mitigasi secara lebih efektif.

2.2.11 *Flowchart*

Flowchart atau diagram alir merupakan representasi visual yang menggambarkan algoritma atau tahapan sistematis dalam suatu sistem. Diagram ini digunakan oleh analis sistem untuk mendokumentasikan serta menyampaikan alur logis sistem kepada programmer agar mudah dipahami dan diimplementasikan (Rosaly & Prasetyo, 2021). *Flowchart* disusun menggunakan simbol-simbol standar yang merepresentasikan proses, keputusan, *input, output*, serta arah alur kerja, sehingga membentuk urutan proses yang jelas dan terstruktur.



Gambar 2. 2 Simbol Flowchart (Sutanti et al., 2020)

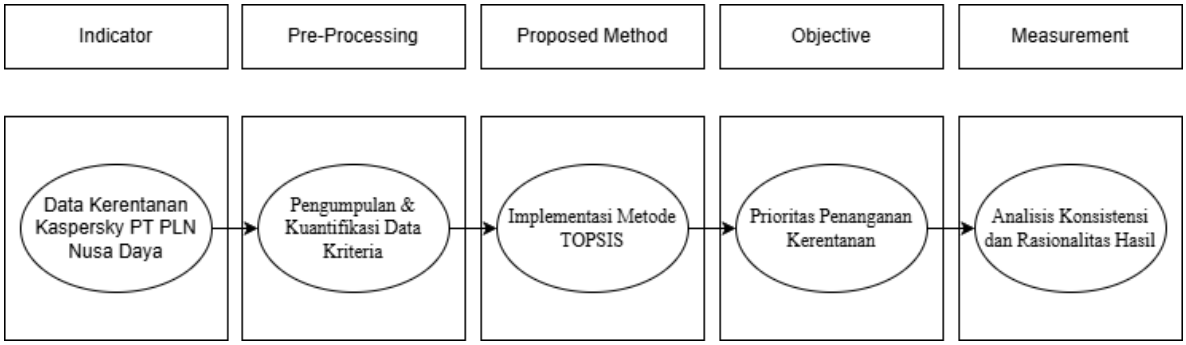
2.2.12 Python

Python merupakan bahasa pemrograman tingkat tinggi berorientasi objek yang bersifat lintas platform, bertipe data dinamis, dan memiliki sintaks yang mudah dibaca. Fleksibilitasnya memungkinkan pengolahan data skala besar, pengembangan algoritma termasuk *machine learning*, layanan web, hingga penerapan *data mining* secara efisien (Alfarizi *et al.,* 2023). Popularitas Python dalam *scientific computing* didukung oleh ekosistem pustaka yang kuat, mulai dari NumPy, Pandas, dan SciPy untuk komputasi numerik hingga TensorFlow, PyTorch, dan Scikit-Learn untuk pengembangan model pembelajaran mesin tingkat lanjut.

2.3 Kerangka Pemikiran

Kerangka pemikiran menggambarkan alur logis penelitian dari tahap input hingga keluaran akhir. Menurut Siswipraptini *et al.* (2023), kerangka pemikiran berfungsi untuk

menjelaskan tahapan penelitian secara sistematis, mulai dari pengumpulan data hingga penyusunan hasil, sehingga menjadi pedoman konseptual dalam pelaksanaan penelitian sesuai landasan teori yang digunakan.



Gambar 2. 3 Kerangka Pemikiran

1. *Indicator* (Indikator/Input Awal)

Penelitian ini diawali dengan pengumpulan data kerentanan yang bersumber dari sistem *Kaspersky Security Center* milik PT PLN Nusa Daya. Data tersebut menjadi landasan utama dalam proses analisis. Adapun atribut yang digunakan meliputi *Severity Level, Update Availability, Age in Days,* dan *Device Count.* Keempat atribut ini dipilih karena mewakili dimensi risiko yang penting, yaitu tingkat keparahan kerentanan, ketersediaan solusi atau pembaruan, lamanya kerentanan terdeteksi, serta jumlah perangkat yang terdampak. Dengan demikian, setiap kerentanan dapat dinilai secara lebih komprehensif, tidak hanya dari satu sudut pandang.

2. *Pre-Processing* (Pra-Pemrosesan)

Data yang telah dikumpulkan kemudian melalui tahap pra-pemrosesan untuk memastikan kualitas dan kelayakannya sebelum dianalisis lebih lanjut. Proses ini mencakup seleksi atribut yang relevan, pembersihan data dari duplikasi maupun inkonsistensi, serta transformasi data ke dalam format numerik agar dapat diolah menggunakan metode TOPSIS. Hasil dari tahap ini adalah matriks keputusan yang

tersusun secara sistematis, di mana setiap kerentanan diperlakukan sebagai alternatif dan setiap atribut risiko sebagai kriteria penilaian.

3. *Proposed Method* (Metode yang Diusulkan)

Tahap ini dilakukan dengan menerapkan metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS) sebagai pendekatan utama dalam proses pemeringkatan. Metode ini digunakan untuk menentukan prioritas kerentanan berdasarkan beberapa kriteria secara simultan. Proses perhitungan meliputi normalisasi matriks keputusan, pemberian bobot pada setiap kriteria, penentuan solusi ideal positif dan negatif, penghitungan jarak masing-masing alternatif terhadap solusi ideal, serta penentuan nilai preferensi akhir. Melalui tahapan ini diperoleh urutan prioritas kerentanan yang dapat dijadikan dasar dalam pengambilan keputusan.

4. *Objective* (Tujuan)

Penelitian ini bertujuan menghasilkan sistem prioritas penanganan kerentanan yang objektif dan terukur sesuai dengan kondisi operasional PT PLN Nusa Daya. Hasil pemeringkatan diharapkan mampu membantu tim keamanan dalam menentukan langkah penanganan secara lebih terarah, dengan mempertimbangkan kombinasi berbagai kriteria risiko, bukan hanya bertumpu pada satu indikator saja.

5. *Measurement* (Pengukuran/Validasi)

Tahap evaluasi dilakukan untuk menilai konsistensi serta rasionalitas hasil pemeringkatan yang dihasilkan oleh metode TOPSIS. Evaluasi difokuskan pada analisis distribusi nilai preferensi dan kesesuaiannya dengan tingkat keparahan serta dampak operasional yang tercermin dalam data. Melalui proses ini dapat dipastikan bahwa hasil prioritisasi yang diperoleh bersifat logis, relevan, dan layak digunakan sebagai dasar rekomendasi dalam pengelolaan kerentanan di lingkungan organisasi.