

Prioritas Risiko Keamanan Siber Berbasis Fuzzy Tsukamoto pada Assesmen Cybersecurity

Zain Jamal Husain¹, Arry Maulana Syarif²

^{1,2}Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang, Indonesia

¹11202416100@mhs.dinus.ac.id, ²arry.maulana@dsn.dinus.ac.id

Info Artikel

Riwayat Artikel:

Received 2026-03-10

Revised 2026-05-06

Accepted 2026-05-08

Corresponding Author:

Zain Jamal Husain

Email: 11202416100@mhs.dinus.ac.id



This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.

Abstract – Increasing cyber threats require organizations to adopt measurable mechanisms for cybersecurity risk prioritization. The Cyber Security Maturity (CSM) framework issued by Badan Siber dan Sandi Negara is widely used to assess cybersecurity capability; however, its results remain descriptive and lack computational support for prioritization. This study proposes a cybersecurity risk prioritization model using Fuzzy Logic Tsukamoto, with maturity values from five CSM aspects as input variables. A total of 100 simulated datasets were generated using a rule-based scenario approach to represent diverse maturity conditions. Trapezoidal and triangular membership functions were applied, and the fuzzy rule base consisted of 15 rules based on the weakest-link principle. Results show that 88% of the data include at least one aspect in a transition zone and are consistently processed by the model. The output produces a distribution of 46% low, 44% medium, and 10% high risk within a 0–100 range, providing a structured, measurable, and reproducible prioritization approach.

Keywords: Cybersecurity; Cybersecurity Assessment; Fuzzy Tsukamoto; Risk Prioritization

Abstrak – Peningkatan ancaman siber menuntut organisasi untuk memiliki mekanisme terukur dalam menentukan prioritas risiko keamanan siber. Kerangka Cyber Security Maturity (CSM) yang diterbitkan oleh Badan Siber dan Sandi Negara banyak digunakan untuk menilai kapabilitas keamanan siber organisasi, namun hasil asesmennya masih bersifat deskriptif dan belum menyediakan mekanisme komputasional untuk menentukan prioritas risiko. Penelitian ini mengembangkan model prioritas risiko keamanan siber menggunakan Fuzzy Logic Tsukamoto dengan memanfaatkan nilai maturity dari lima aspek CSM sebagai variabel input. Data penelitian terdiri dari 100 data simulasi yang dibangun melalui pendekatan rule-based scenario simulation untuk merepresentasikan berbagai kondisi kematangan keamanan siber. Fungsi keanggotaan menggunakan kurva trapezoidal dan triangular, sedangkan basis aturan fuzzy terdiri dari 15 aturan berdasarkan prinsip weakest link. Hasil penelitian menunjukkan bahwa 88% data simulasi memiliki minimal satu aspek pada zona transisi antar kategori linguistik dan berhasil dipetakan secara konsisten oleh model. Proses inferensi dan defuzzifikasi menghasilkan distribusi risiko sebesar 46% rendah, 44% sedang, dan 10% tinggi dalam rentang skor 0–100. Model yang diusulkan menghasilkan pendekatan yang terstruktur, numerik, terukur, dan dapat direplikasi dalam menentukan prioritas risiko keamanan siber.

Kata Kunci: Assesmen Keamanan Siber; Fuzzy Tsukamoto; Keamanan Siber; Prioritas Risiko

I. PENDAHULUAN

Pertumbuhan layanan digital pada institusi pendidikan dan sektor publik meningkatkan ketergantungan terhadap sistem informasi sekaligus memperbesar eksposur terhadap ancaman siber. Lanskap ancaman terus berkembang dengan teknik serangan yang semakin kompleks dan sulit diprediksi. Alani (2023) menunjukkan bahwa teknik obfuscation pada malware modern menyulitkan proses identifikasi [1], sedangkan Gibert et al (2020) menegaskan bahwa dinamika ancaman yang cepat mengurangi efektivitas pendekatan deteksi konvensional. Kondisi ini menuntut mekanisme klasifikasi risiko yang lebih adaptif dan berbasis analisis data [2], [3], [4].

Di Indonesia, Badan Siber dan Sandi Negara (BSSN) menginisiasi kerangka Cyber Security Maturity (CSM-BSSN) sebagai standar nasional untuk menilai tingkat kematangan keamanan siber [5]. Kerangka ini mencakup lima aspek utama, yaitu Tata Kelola, Identifikasi, Proteksi, Deteksi, dan Respons. Namun, hasil asesmen CSM-BSSN masih bersifat deskriptif dan belum menyediakan mekanisme komputasional untuk mengonversi nilai *maturity* menjadi klasifikasi prioritas risiko yang terukur dan konsisten. Penelitian ini juga mengacu pada prinsip manajemen risiko sebagaimana direkomendasikan dalam ISO/IEC 27005 dan NIST SP 800-30 [6].

Ketiadaan mekanisme komputasional klasifikasi prioritas berbasis maturity menimbulkan tantangan karena penentuan prioritas masih bergantung pada expert judgement yang berpotensi menghasilkan rekomendasi tidak konsisten [7], [8]. Di sisi lain, berbagai penelitian menunjukkan bahwa logika fuzzy efektif dalam menangani ketidakpastian dan mampu mengonversi parameter linguistik menjadi keluaran kuantitatif yang stabil [9], [10].

Apiecionek (2025) juga menunjukkan bahwa pendekatan fuzzy tetap relevan untuk mendukung keamanan pada lingkungan IoT yang dinamis dan kompleks [8]. Sejumlah studi juga menunjukkan penerapan logika fuzzy pada penilaian risiko di berbagai konteks [6], [7], [11].

Meskipun berbagai penelitian telah menerapkan logika fuzzy pada penilaian risiko keamanan informasi, belum ditemukan studi yang secara khusus mentransformasikan hasil asesmen maturity CSM-BSSN menjadi skor prioritas risiko numerik. Oleh karena itu, penelitian ini mengisi research gap tersebut melalui integrasi framework nasional CSM-BSSN dengan mekanisme inferensi Tsukamoto untuk menghasilkan klasifikasi prioritas risiko yang terukur dan konsisten. Untuk memperjelas research gap dan kebaruan penelitian, perbandingan studi terdahulu disajikan pada Tabel 1.

TABEL 1
PERBANDINGAN PENELITIAN TERDAHULU DAN KEBARUAN PENELITIAN

Penelitian	Fokus	Kontribusi
Kerimkhulle et al. (2023)	Risiko keamanan IIoT	Menunjukkan fuzzy efektif untuk penilaian risiko IIoT
Merola et al. (2024)	Penilaian risiko berbasis fuzzy	Mengembangkan kerangka risk assessment berbasis fuzzy
Apiecionek (2025)	Solusi keamanan IoT berbasis fuzzy	Menunjukkan relevansi fuzzy pada lingkungan IoT
Korystin et al. (2025)	Evaluasi keamanan dengan fuzzy sets	Menerapkan fuzzy sets untuk evaluasi keamanan
Penelitian yang diusulkan	Klasifikasi prioritas risiko keamanan siber	Mengonversi maturity menjadi skor risiko

Berdasarkan gap penelitian tersebut, studi ini mengusulkan model klasifikasi prioritas risiko berbasis metode Tsukamoto dengan memanfaatkan nilai maturity dari lima aspek CSM-BSSN sebagai variabel input. Model yang dikembangkan memformalkan hubungan nonlinier antara maturity dan risiko untuk menghasilkan skor numerik yang dapat digunakan sebagai dasar prioritas mitigasi dan pengambilan keputusan. Pendekatan ini menunjukkan relevansi logika fuzzy sebagai mekanisme klasifikasi risiko pada lingkungan keamanan informasi yang kompleks dan dinamis [12].

II. METODE

Tahapan penelitian mengikuti prinsip Design Science Research (DSR) sebagaimana dikemukakan oleh Hevner et al. (2004) [13], [14] dan dikembangkan lebih lanjut dalam metodologi penelitian sistem informasi oleh Peffers et al. [15]. Pendekatan ini dipilih karena berfokus pada pengembangan dan evaluasi artefak berupa model klasifikasi prioritas risiko keamanan siber berbasis metode Tsukamoto. Kerangka DSR memungkinkan proses perancangan dilakukan secara sistematis, memiliki landasan konseptual yang jelas, serta dapat diuji melalui tahap demonstrasi dan evaluasi artefak.

Tahapan penelitian meliputi identifikasi permasalahan dan perancangan model klasifikasi prioritas risiko berbasis model Tsukamoto, yang selanjutnya didemonstrasikan dan dievaluasi menggunakan data simulasi. Evaluasi model dilakukan melalui pengujian perilaku model untuk menilai konsistensi aturan, respons pada kondisi ekstrem, dan kecenderungan perubahan hasil klasifikasi terhadap variasi nilai maturity. Evaluasi difokuskan pada data simulasi, sedangkan validasi menggunakan data empiris atau expert judgement menjadi agenda penelitian lanjutan.

A. Data Penelitian

Data penelitian menggunakan data simulasi yang disusun untuk merepresentasikan berbagai skenario kondisi *maturity* keamanan siber pada lima aspek CSM-BSSN. Setiap skenario merepresentasikan satu organisasi hipotetik, sedangkan kode a–e menunjukkan nilai maturity pada masing-masing aspek. Sebanyak 100 data simulasi dihasilkan menggunakan pendekatan rule-based scenario simulation, dengan nilai pada rentang 0–5 yang ditentukan secara acak terbatas (constrained random) menggunakan distribusi uniform sesuai kategori linguistik rendah, sedang, dan tinggi. Dataset mencakup kondisi seimbang antar aspek, ketimpangan (weakest link), serta skenario transisi dan peningkatan bertahap.

Jumlah 100 skenario dipilih untuk memberikan variasi kombinasi input yang memadai dan representatif dalam evaluasi model. Jumlah tersebut dinilai cukup untuk menguji konsistensi perilaku model pada berbagai kondisi maturity, termasuk skenario seimbang, ketimpangan antar aspek, kondisi ekstrem, dan zona transisi, tanpa meningkatkan kompleksitas simulasi secara berlebihan. Data simulasi ini tidak merepresentasikan kondisi historis maupun institusi tertentu, melainkan digunakan untuk mengevaluasi perilaku, sensitivitas, dan konsistensi model.

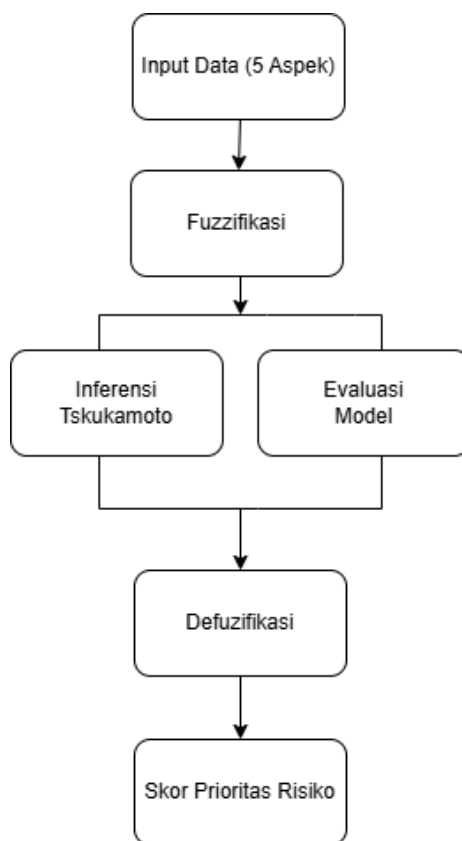
B. Identifikasi Masalah

Identifikasi masalah difokuskan pada pengolahan data asesmen CSM-BSSN sebagai masukan model. Data CSM menghasilkan nilai maturity pada lima aspek keamanan dalam skala 0–5 yang bersifat linguistik dan tidak linier. Nilai tersebut belum dapat digunakan secara langsung untuk menentukan klasifikasi prioritas risiko karena tidak merepresentasikan tingkat urgensi risiko secara numerik. Permasalahan utama pada tahap ini adalah bagaimana memetakan variasi nilai maturity antar aspek, baik yang seimbang maupun tidak seimbang ke dalam satu skor prioritas risiko yang konsisten. Oleh karena itu, diperlukan mekanisme komputasional yang mampu mengolah nilai maturity multi-aspek secara simultan dan menghasilkan keluaran risiko yang proporsional terhadap kondisi maturity organisasi.

C. Perencanaan Model Fuzzy Tsukamoto

Perancangan model dilakukan untuk memetakan nilai maturity CSM-BSSN ke dalam skor prioritas risiko secara komputasional. Metode inferensi Fuzzy Tsukamoto dipilih karena karakteristiknya memungkinkan pembentukan keluaran crisp melalui fungsi keanggotaan monoton, sehingga sesuai untuk kebutuhan prioritasasi risiko dalam bentuk skor numerik 0–100 [16], [17].

Dibandingkan metode Mamdani yang umumnya memerlukan proses defuzzifikasi global pada tahap akhir, Tsukamoto memberikan keluaran pada tingkat aturan sehingga interpretasi hasil menjadi lebih langsung dan terstruktur [17]. Sementara itu, dibandingkan metode AHP yang bergantung pada pembobotan pairwise judgement, pendekatan fuzzy lebih adaptif dalam merepresentasikan transisi maturity dan ketidakpastian antar level penilaian [18]. Dengan karakteristik tersebut, metode ini dinilai sesuai untuk klasifikasi prioritas risiko berbasis maturity pada kerangka CSM-BSSN. Alur proses inferensi fuzzy Tsukamoto ditunjukkan pada Gambar 1.



Gambar 1. Alur Proses Inferensi Fuzzy Tsukamoto

Tahapan perancangan meliputi penetapan variabel fuzzy, pembentukan fungsi keanggotaan linguistik, formalisasi aturan fuzzy (rule base), serta mekanisme defuzzifikasi berbasis rata-rata terbobot. Variabel input merepresentasikan nilai maturity pada lima aspek CSM, sedangkan variabel output berupa skor prioritas risiko. Secara umum, sebuah variabel fuzzy X direpresentasikan sebagai pasangan antara nilai input dan derajat keanggotaannya [17], [19]

$$X = \{(x, \mu_X(x)) \mid x \in \mathbb{R}, 0 \leq \mu_X(x) \leq 1\} \quad (1)$$

Setiap variabel memiliki himpunan linguistik $L = \{L_1, L_2, \dots, L_n\}$ yang merepresentasikan kategori rendah, sedang, dan tinggi. Untuk merepresentasikan transisi nilai maturity yang bersifat gradual dan tidak linier, fungsi keanggotaan dirancang menggunakan bentuk segitiga dan trapesium [17], [19].

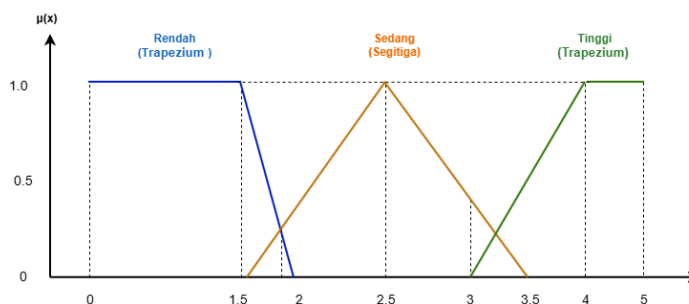
Fungsi keanggotaan segitiga dengan parameter (a, b, c) dirumuskan sebagai:

$$\mu_A(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a < x \leq b \\ \frac{c-x}{c-b}, & b < x < c \\ 0, & x \geq c \end{cases} \quad (2)$$

Sedangkan fungsi keanggotaan trapesium dengan parameter (a, b, c, d) dinyatakan sebagai:

$$\mu_A(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a < x \leq b \\ 1, & b < x \leq c \\ \frac{d-x}{d-c}, & c < x < d \\ 0, & x \geq d \end{cases} \quad (3)$$

Pada variabel input maturity dengan domain 0–5, himpunan fuzzy dibagi ke dalam tiga kategori linguistik, yaitu rendah, sedang, dan tinggi. Kategori rendah dimodelkan menggunakan fungsi keanggotaan trapesium dengan parameter $(0, 0, 1.5, 2.0)$, kategori sedang menggunakan fungsi segitiga dengan parameter $(1.5, 2.5, 3.5)$, sedangkan kategori tinggi menggunakan fungsi keanggotaan trapesium dengan parameter $(3.0, 4.0, 5.0, 5.0)$. Area overlap antar himpunan digunakan untuk merepresentasikan transisi gradual antar level maturity. Parameter fungsi keanggotaan ditetapkan secara proporsional pada domain 0–5 agar setiap kategori memiliki representasi yang seimbang dan transisi antar level maturity dapat dimodelkan secara halus. Representasi fungsi keanggotaan variabel input ditunjukkan pada Gambar 2.



Gambar 2. Fungsi Keanggotaan Variabel Input Maturity

D. Formalisasi Aturan Fuzzy (Rule base)

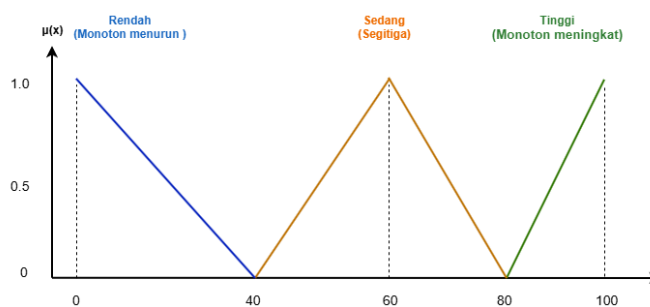
Rule base diformalisasi untuk merepresentasikan hubungan antara nilai maturity pada lima aspek CSM dan tingkat risiko yang dihasilkan. Formulasi aturan didasarkan pada prinsip weakest link pada CSM dan COBIT, yaitu bahwa tingkat risiko dipengaruhi oleh aspek maturity terendah atau kondisi ketidakseimbangan antar aspek. Setiap aturan dirumuskan dalam bentuk IF–THEN dengan menggunakan kombinasi operator logika fuzzy min (AND) dan max (OR). Operator min digunakan untuk merepresentasikan kondisi konjungtif antar aspek, sedangkan operator max digunakan untuk merepresentasikan kondisi disjungtif ketika satu aspek dengan maturity rendah dapat meningkatkan risiko secara signifikan [17], [20]. Melalui proses formalisasi ini, rule base direduksi menjadi 15 aturan fuzzy yang representatif untuk mencakup pola dominan risiko rendah, sedang, tinggi, kondisi weakest link, serta keseimbangan antar aspek tanpa kehilangan karakteristik utama asesmen CSM-BSSN.

E. Mekanisme Inferensi Tsukamoto

Mekanisme inferensi fuzzy Tsukamoto digunakan untuk menghitung skor prioritas risiko berdasarkan nilai maturity yang telah melalui proses fuzzifikasi. Pada metode Tsukamoto, setiap aturan fuzzy memiliki konsekuensi yang bersifat monoton terhadap domain output, sehingga menghasilkan nilai crisp pada tingkat aturan [16]. Nilai aktivasi setiap aturan (α) ditentukan berdasarkan derajat keanggotaan fuzzy pada variabel input menggunakan operator min untuk relasi konjungtif (AND) dan operator max untuk relasi disjungtif (OR), sesuai dengan struktur rule base yang telah diformalisasi. Nilai α -predikat merepresentasikan tingkat pemenuhan kondisi pada masing-masing aturan fuzzy. Untuk aturan global seperti semua aspek \geq medium, kondisi tersebut dimodelkan sebagai kombinasi OR antara himpunan medium dan high pada tiap aspek, kemudian digabungkan menggunakan operator AND antar aspek.

Sementara itu, aturan empat high dan satu medium dievaluasi pada seluruh kombinasi aspek yang memenuhi kondisi tersebut, lalu dipilih nilai aktivasi tertinggi sebagai representasi aturan.

Variabel output prioritas risiko didefinisikan pada domain 0–100 untuk merepresentasikan tingkat urgensi risiko dan dibagi ke dalam tiga kategori linguistik, yaitu rendah, sedang, dan tinggi. Model menerapkan hubungan berbanding terbalik antara tingkat maturity dan skor risiko, sehingga semakin tinggi maturity, semakin rendah nilai risiko yang dihasilkan. Kategori rendah berada pada interval 0–40 dengan kecenderungan monoton menurun, sedangkan kategori tinggi berada pada interval 80–100 dengan kecenderungan monoton meningkat. Kategori sedang direpresentasikan pada rentang 40–80 sebagai zona transisi klasifikasi hasil akhir. Representasi fungsi keanggotaan variabel output ditunjukkan pada Gambar 3.



Gambar 3. Fungsi Keanggotaan Variabel Output Prioritas Risiko

Nilai crisp dari setiap aturan dihitung melalui fungsi konsekuen berdasarkan nilai aktivasi aturan sesuai mekanisme inferensi Tsukamoto. Nilai risiko akhir diperoleh melalui proses agregasi seluruh keluaran parsial menggunakan metode rata-rata terbobot [21], yang dirumuskan sebagai berikut:

$$Z = \frac{\sum_{i=1}^n \alpha_i z_i}{\sum_{i=1}^n \alpha_i} \quad (4)$$

F. Demonstrasi Artefak dan Evaluasi Model

Data simulasi dihasilkan menggunakan pendekatan rule-based scenario simulation, di mana setiap skenario disusun secara sistematis berdasarkan prinsip pengukuran maturity sebagaimana digunakan dalam kerangka evaluasi keamanan siber [10], [22]. Nilai setiap aspek berada pada rentang 0–5 dan ditentukan secara acak terbatas (constrained random) sesuai kategori linguistik rendah, sedang, dan tinggi, sehingga tetap konsisten dengan logika penilaian maturity dan aturan fuzzy.

Proses demonstrasi mencakup fuzzifikasi nilai maturity, perhitungan aktivasi aturan (firing strength), penentuan nilai crisp pada tingkat aturan menggunakan metode Tsukamoto, serta agregasi seluruh keluaran untuk memperoleh skor prioritas risiko akhir [1], [2]. Output model berupa skor numerik pada rentang 0–100 yang diklasifikasikan ke dalam kategori risiko rendah, sedang, dan tinggi. Tahap ini bertujuan memastikan model bekerja sesuai rancangan dan menghasilkan keluaran yang proporsional terhadap variasi nilai maturity berdasarkan rule base yang ditetapkan [17].

Evaluasi artefak dilakukan melalui behavior-based evaluation dengan tiga teknik utama. Pertama, uji konsistensi aturan untuk memastikan keluaran model selaras dengan rule base, terutama pada kondisi ketimpangan nilai maturity antar aspek. Kedua, pengujian kasus ekstrem (edge case evaluation) untuk menilai Respons model pada kondisi terbaik, terburuk, dan skenario weakest link [17], guna memastikan bahwa hasil klasifikasi tetap sesuai dengan prinsip risiko keamanan siber [20], [21]. Ketiga, uji monotonisitas untuk mengamati perubahan skor risiko ketika nilai maturity meningkat secara bertahap, sehingga peningkatan maturity tidak menghasilkan kenaikan tingkat risiko. Hasil evaluasi digunakan untuk menilai kelayakan model sebagai mekanisme klasifikasi prioritas risiko keamanan siber berbasis nilai maturity.

III. HASIL DAN PEMBAHASAN

Implementasi model pada data simulasi menunjukkan bahwa nilai maturity pada lima aspek CSM-BSSN berpengaruh langsung terhadap skor prioritas risiko yang dihasilkan. Pemetaan ke kategori linguistik rendah, sedang, dan tinggi mampu merepresentasikan peningkatan kapabilitas keamanan siber secara nonlinier [16], [22].

Hasil simulasi juga menunjukkan bahwa ketidakseimbangan nilai maturity antar aspek dapat meningkatkan risiko meskipun aspek lain berada pada kondisi yang lebih baik, sehingga kondisi weakest link dapat teridentifikasi. Selain itu, perubahan kecil pada aspek yang berada di zona transisi tetap tercermin pada perubahan skor akhir. Temuan ini menunjukkan bahwa klasifikasi risiko tidak hanya ditentukan oleh nilai rata-rata maturity, tetapi juga oleh pola

ketimpangan antar aspek. Dengan demikian, pendekatan fuzzy mampu mengubah hasil asesmen maturity yang bersifat statis menjadi indikator prioritas risiko yang lebih operasional untuk pengambilan keputusan.

A. Fuzzifikasi Multi Input

Fuzzifikasi dilakukan untuk mengonversi nilai maturity crisp pada lima aspek CSM-BSSN ke dalam derajat keanggotaan fuzzy pada kategori linguistik rendah, sedang, dan tinggi [2], [17]. Proses ini diterapkan secara independen pada setiap aspek menggunakan fungsi keanggotaan yang telah ditetapkan pada tahap perancangan model. Tahap fuzzifikasi dilakukan terhadap seluruh data simulasi dengan nilai pada rentang 0–5 yang dihasilkan melalui pendekatan acak terbatas (constrained random) agar tetap konsisten dengan logika penilaian maturity dan aturan fuzzy.

Dari 100 data simulasi, sebanyak 88 skenario (88%) memiliki minimal satu aspek CSM-BSSN pada zona transisi antar kategori linguistik, yang ditandai oleh lebih dari satu derajat keanggotaan aktif secara bersamaan. Sebaliknya, 12 skenario (12%) menunjukkan dominasi satu kategori pada seluruh aspek, yang merepresentasikan kondisi relatif stabil atau ekstrem. Distribusi ini menunjukkan bahwa sebagian besar organisasi berada pada area transisi, sehingga pendekatan fuzzy relevan untuk menangkap sensitivitas perubahan maturity dan ketimpangan antar aspek [6], [7]. Tabel 2 memperlihatkan dua hasil fuzzifikasi.

TABEL 2
HASIL FUZZIFIKASI PADA DUA SKENARIO SIMULASI

Skenario	Aspek	Nilai Maturity	μ Rendah	μ Sedang	μ Tinggi
S-1a	Tata Kelola	1,8	0,40	0,30	0,00
S-1b	Identifikasi	2,6	0,00	0,90	0,00
S-1c	Proteksi	3,1	0,00	0,40	0,10
S-1d	Deteksi	3,9	0,00	0,00	0,90
S-1e	Respons	1,9	0,20	0,40	0,00
S-2a	Tata Kelola	4,6	0,00	0,00	1,00
S-2b	Identifikasi	3,7	0,00	0,00	0,70
S-2c	Proteksi	4,8	0,00	0,00	1,00
S-2d	Deteksi	2,2	0,00	0,70	0,00
S-2e	Respons	3,3	0,00	0,20	0,30

Hasil fuzzifikasi menunjukkan bahwa nilai maturity pada batas kategori menghasilkan derajat keanggotaan parsial pada lebih dari satu himpunan linguistik, sedangkan nilai yang berada jauh dalam suatu kategori menunjukkan dominasi derajat keanggotaan. Pola ini mencerminkan hubungan nonlinier antara maturity dan risiko serta mendukung prinsip weakest link. Derajat keanggotaan tersebut selanjutnya digunakan sebagai input pada tahap inferensi metode Tsukamoto untuk menentukan aktivasi aturan (firing strength) dan skor prioritas risiko [1], [2].

B. Inferensi Tsukamoto

Metode Tsukamoto diterapkan untuk menghitung skor prioritas risiko berdasarkan derajat keanggotaan hasil fuzzifikasi pada lima aspek CSM-BSSN [7]. Hasil inferensi menunjukkan bahwa aturan dengan konsekuen risiko tinggi cenderung aktif ketika satu atau lebih aspek berada pada kondisi maturity rendah atau terjadi ketidakseimbangan antar aspek, meskipun aspek lain berada pada kategori sedang atau tinggi. Pola ini menegaskan prinsip weakest link, di mana kelemahan pada satu aspek dapat mendominasi tingkat risiko keseluruhan [17].

Sebaliknya, ketika sebagian besar aspek memiliki derajat keanggotaan dominan pada kategori tinggi, aturan dengan konsekuen risiko rendah menjadi lebih aktif sehingga skor risiko akhir mengalami penurunan. Kondisi ini menunjukkan bahwa model tidak hanya mempertimbangkan nilai maturity rata-rata, tetapi juga sensitif terhadap distribusi maturity antar aspek.

Nilai crisp hasil inferensi pada setiap aturan selanjutnya diagregasi untuk memperoleh skor prioritas risiko akhir. Skor yang dihasilkan mampu membedakan berbagai skenario simulasi dengan pola maturity yang berdekatan, sehingga menunjukkan Respons model yang gradual dan konsisten. Rule base yang digunakan dalam proses inferensi disajikan pada Tabel 3.

TABEL 3
 ATURAN FUZZY TSUKAMOTO BERBASIS COBIT – CSM-BSSN

No	Aturan Fuzzy (IF-THEN)	Output
R1	IF Proteksi Low OR Deteksi Low THEN Risk	High
R2	IF Tata Kelola Low OR Identifikasi Low THEN Risk	High
R3	IF Respons Low THEN Risk	High
R4	IF Proteksi Low AND Deteksi Medium THEN Risk	High
R5	IF Identifikasi Low AND Respons Medium THEN Risk	High
R6	IF Proteksi Medium AND Deteksi Medium THEN Risk	Medium
R7	IF Tata Kelola Medium AND Identifikasi Medium THEN Risk	Medium
R8	IF Proteksi Medium AND Respons Medium THEN Risk	Medium
R9	IF Tata Kelola High AND Deteksi Medium THEN Risk	Medium
R10	IF Identifikasi High AND Respons Medium THEN Risk	Medium
R11	IF Proteksi High AND Deteksi High THEN Risk	Low
R12	IF Semua Aspek \geq Medium THEN Risk	Low
R13	IF Semua Aspek High THEN Risk	Low
R14	IF Tata Kelola High AND Identifikasi High AND Respons High THEN Risk	Low
R15	IF Empat Aspek High AND Satu Medium THEN Risk	Low

C. Defuzzifikasi Tsukamoto

Skor prioritas risiko akhir diperoleh melalui agregasi nilai crisp (z_i) dari setiap aturan aktif dengan mempertimbangkan derajat aktivasi aturan (firing strength, α_i) menggunakan rata-rata berbobot sesuai mekanisme Tsukamoto [1], [2]. Ilustrasi parsial rule aktif pada dua skenario simulasi yang digunakan sebelumnya disajikan pada Tabel 4.

TABEL 4
 ILUSTRASI PARSIAL RULE AKTIF PADA SKENARIO S-1 DAN S-2

Skenario	Rule Aktif	α_i (Firing Strength)	z_i (Crisp Rule)
S-1a	R2, R7, R12	0.4; 0.3; 0.3	88; 52; 28
S-1b	R7, R12	0.3; 0.3	52; 28
S-1c	R8, R11	0.4; 0.1	56; 36
S-1d	R11, R12	0.1; 0.3	36; 28
S-1e	R3, R12	0.2; 0.3	84; 28
S-2a	R14, R12	0.3; 0.3	28; 28
S-2b	R14	0.3	28
S-2c	R12	0.3	28
S-2d	R9	0.7	68
S-2e	R10, R12	0.2; 0.3	48; 28

Nilai z_i merepresentasikan keluaran crisp dari setiap aturan fuzzy yang aktif sebagai komponen agregasi dalam satu skenario simulasi, sedangkan α_i menunjukkan kontribusi masing-masing aturan terhadap skor risiko akhir. Sebagai ilustrasi, agregasi rule aktif pada skenario S-1 menghasilkan skor akhir sebesar 59,29 yang berada pada kategori sedang. Pendekatan yang sama diterapkan pada seluruh skenario untuk memperoleh skor akhir masing-masing. Ringkasan hasil inferensi multi-input pada beberapa skenario representatif disajikan pada Tabel 5.

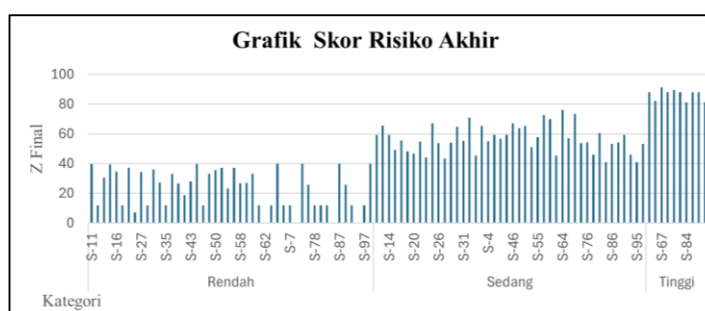
TABEL 5
 HASIL INFERENSI MULTI-INPUT DAN SKOR KLASIFIKASI RISIKO AKHIR PADA SEPULUH SKENARIO

Skenario	Rule Aktif	α_i (Firing Strength)	z_i (Crisp Rule)	Z Final	Kategori
S-11	R3, R10, R11, R12	0.4;0.3;0.7;0.3	88;52;12;28	39,76	Rendah
S-16	R8, R10, R11, R12, R13, R14	0.2;0.1;0.3;0.3;0.1;0.1	48;44;28;28;36;36	34,55	Rendah
S-27	R9, R10, R11, R12	0.2;0.1;0.3;0.3	48;44;28;28	34,22	Rendah
S-1	R2, R3, R7, R8, R11, R12	0.4;0.2;0.3;0.4;0.1;0.3	88;84;52;56;36;28	59,29	Sedang
S-2	R9, R10, R12, R14	0.7;0.2;0.3;0.3	68;48;28;28	48,27	Sedang
S-14	R1, R6, R7, R8, R9, R10, R12	0.4;0.3;0.2;0.7;0.3;0.1;0.3	88;52;48;68;52;44;28	59,3	Sedang
S-20	R6, R7, R8, R9, R12	0.4;0.4;0.4;0.1;0.4	56;56;56;44;24	46,59	Sedang
S-67	R1, R2, R3, R4, R5, R6, R8	0.7;1;0.4;0.7;0.3;0.1;0.1	94;100;88;94;86;44;44	91,33	Tinggi
S-84	R1, R2, R3, R5, R6, R7, R8, R12	0.4;0.7;0.7;0.1;0.3;0.1;0.1;0.1	88;94;94;82;52;44;44;36	81,2	Tinggi
S-100	R1, R2, R3, R4, R5, R6, R8	0.4;1;0.7;0.4;0.1;0.3;0.1	88;100;94;88;82;52;44	88,13	Tinggi

Hasil defuzzifikasi menunjukkan bahwa skor risiko bervariasi antar skenario, termasuk pada skenario dengan nilai maturity yang relatif berdekatan. Variasi ini menunjukkan bahwa model responsif terhadap distribusi nilai maturity antar aspek dan tidak hanya dipengaruhi oleh nilai rata-rata secara keseluruhan.

Skenario dengan ketidakseimbangan nilai maturity, terutama ketika satu atau lebih aspek berada pada kategori rendah atau zona transisi, cenderung menghasilkan skor risiko lebih tinggi karena dominasi aturan dengan konsekuensi risiko tinggi. Sebaliknya, distribusi nilai yang lebih merata pada kategori sedang hingga tinggi menghasilkan aktivasi aturan risiko rendah yang lebih dominan.

Hal ini menunjukkan bahwa meskipun beberapa aspek memiliki risiko tinggi, keberadaan aspek dengan nilai lebih rendah tetap memengaruhi kondisi risiko secara keseluruhan. Pola tersebut menegaskan bahwa metode Tsukamoto mampu merepresentasikan hubungan nonlinier antara maturity dan risiko serta mendukung prinsip weakest link, di mana kelemahan pada satu aspek dapat memberikan pengaruh signifikan terhadap hasil klasifikasi. Distribusi skor risiko akhir pada seluruh data simulasi ditunjukkan pada Gambar 4.



Gambar 4. Hasil Skor Risiko Akhir pada 100 Skenario Simulasi

Dari 100 skenario simulasi, diperoleh 46 skenario kategori rendah, 44 kategori sedang, dan 10 kategori tinggi. Dominasi kategori sedang menunjukkan bahwa sebagian besar kombinasi maturity berada pada kondisi transisi, sedangkan kategori rendah dan tinggi menegaskan kemampuan model dalam mengenali kondisi ekstrem secara proporsional.

D. Pembahasan

Hasil fuzzifikasi, inferensi, dan defuzzifikasi pada seluruh skenario simulasi menunjukkan bahwa model yang diusulkan mampu menghasilkan klasifikasi prioritas risiko keamanan siber secara konsisten pada rentang skor 0–100 yang terbagi ke dalam kategori rendah, sedang, dan tinggi [1], [2]. Sebaran skor risiko akhir pada Gambar 4

menunjukkan bahwa sistem tidak hanya memproses nilai maturity secara numerik, tetapi juga menangkap variasi distribusi maturity antar aspek CSM-BSSN dalam menentukan tingkat prioritas risiko.

Representasi fungsi keanggotaan menunjukkan bahwa area overlap antar himpunan fuzzy memungkinkan transisi maturity direpresentasikan secara gradual. Perubahan kecil pada nilai maturity tidak menghasilkan perubahan klasifikasi yang tajam, tetapi berubah proporsional sesuai derajat keanggotaan. Karakteristik ini menunjukkan sensitivitas pendekatan terhadap perubahan kondisi organisasi, terutama pada aspek yang berada di zona transisi.

Skenario dengan ketidakseimbangan nilai maturity, terutama ketika satu atau lebih aspek berada pada kategori rendah atau zona transisi, cenderung menghasilkan skor risiko lebih tinggi karena dominasi aturan berkonsekuensi risiko tinggi. Sebaliknya, distribusi maturity yang lebih merata pada kategori sedang hingga tinggi mendorong dominasi aturan risiko rendah sehingga skor akhir menurun. Temuan ini menegaskan bahwa tingkat risiko tidak semata-mata ditentukan oleh nilai rata-rata maturity, tetapi juga oleh aspek dengan tingkat maturity terendah sesuai prinsip weakest link pada kerangka CSM-BSSN [6], [21].

Temuan tersebut sejalan dengan pendekatan CSM-BSSN yang menekankan peningkatan aspek terlemah sebagai prioritas penguatan keamanan siber. Dengan demikian, hasil asesmen maturity yang semula bersifat deskriptif dapat ditransformasikan menjadi klasifikasi prioritas risiko yang lebih terukur. Secara konseptual, pendekatan Fuzzy Logic Tsukamoto efektif dalam merepresentasikan hubungan nonlinier antara maturity dan risiko keamanan siber serta menjaga sensitivitas terhadap perubahan kecil pada aspek kritis [16].

Penelitian ini tidak dirancang sebagai studi komparatif antar metode fuzzy maupun metode pengambilan keputusan lainnya. Fokus utama penelitian adalah pengembangan artefak berupa model klasifikasi prioritas risiko yang mentransformasikan hasil asesmen CSM-BSSN dari bentuk deskriptif menjadi skor numerik yang terstruktur. Oleh karena itu, evaluasi difokuskan pada perilaku model, meliputi konsistensi rule base, respons pada kondisi ekstrem, sensitivitas terhadap perubahan input, dan sifat monotonic output.

Hasil pengujian juga menunjukkan bahwa mekanisme inferensi Tsukamoto mampu menghasilkan skor risiko numerik secara langsung pada setiap aturan aktif, sehingga proses prioritasasi dapat dilakukan secara terstruktur. Karakteristik ini memudahkan interpretasi hasil pada berbagai kombinasi maturity dan mendukung implementasi sebagai alat bantu pengambilan keputusan dalam penentuan prioritas peningkatan keamanan siber pada organisasi.

IV. SIMPULAN

Penelitian ini mengembangkan model klasifikasi prioritas risiko keamanan siber berbasis Fuzzy Logic Tsukamoto dengan memanfaatkan nilai maturity pada lima aspek CSM-BSSN sebagai variabel input. Model mampu mengonversi hasil asesmen maturity yang bersifat linguistik menjadi skor risiko kontinu pada rentang 0–100 secara terstruktur dan terukur. Hasil menunjukkan bahwa distribusi maturity antar aspek berpengaruh signifikan terhadap skor risiko. Ketidakseimbangan pada satu aspek, terutama pada kategori rendah atau zona transisi, cenderung meningkatkan prioritas risiko. Temuan ini menegaskan prinsip weakest link, yaitu aspek terlemah dapat memengaruhi tingkat risiko secara keseluruhan. Kontribusi utama penelitian ini adalah penyediaan mekanisme komputasional yang mentransformasikan asesmen CSM-BSSN yang sebelumnya deskriptif menjadi prioritas risiko numerik yang terukur dan dapat direplikasi. Keterbatasan penelitian terletak pada penggunaan data simulasi dan belum dipertimbangkannya faktor risiko eksternal. Penelitian selanjutnya disarankan menggunakan data empiris, menambahkan variabel eksternal, serta menguji model pada konteks organisasi nyata.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Badan Siber dan Sandi Negara atas ketersediaan kerangka CSM-BSSN yang menjadi rujukan utama dalam penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pembimbing atas arahan dan masukan selama penyusunan penelitian.

DAFTAR PUSTAKA

- [1] Y. Tsukamoto, "An approach to fuzzy reasoning method," in *Advances in Fuzzy Set Theory and Applications*, M. Gupta, R. Ragade, and R. Yager, Eds. Amsterdam, Netherlands: North-Holland, 1979, pp. 137–149.
- [2] T. J. Ross, *Fuzzy Logic with Engineering Applications*, 3rd ed. Hoboken, NJ, USA: Wiley, 2010. doi: 10.1002/9781119994374.
- [3] C. Gilbert and M. Gilbert, "The impact of AI on cybersecurity defense mechanisms: Future trends and challenges," *Global Scientific Journal*, vol. 12, pp. 427–441, Sep. 2024. doi: 10.11216/gsj.2024.09.229721.
- [4] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic literature review on security risks and its practices in secure software development," *IEEE Access*, vol. 10, pp. 5456–5481, 2022. doi: 10.1109/ACCESS.2022.3140181.
- [5] M. M. Alani, A. Mashatan, and A. Miri, "XMal: A lightweight memory-based explainable obfuscated-malware detector," *Computers & Security*, vol. 133, p. 103409, Oct. 2023. doi: 10.1016/j.cose.2023.103409.
- [6] F. Merola, C. Bernardeschi, and G. Lami, "A risk assessment framework based on fuzzy logic for automotive systems," *Safety*, vol. 10, no. 2, p. 41, Apr. 2024. doi: 10.3390/safety10020041.
- [7] S. Kerimkhulle *et al.*, "Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things," *Symmetry*, vol. 15, no. 10, p. 1958, Oct. 2023. doi: 10.3390/sym15101958.

- [8] Ł. Apiecionek, "Fuzzy network solutions for IoT security," in *Proc. IEEE EUROCON 2025*, Jun. 2025, pp. 1–5. doi: 10.1109/EUROCON64445.2025.11073458.
- [9] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, "A comprehensive survey of recent Internet measurement techniques for cyber security," *Computers & Security*, vol. 128, p. 103123, May 2023. doi: 10.1016/j.cose.2023.103123.
- [10] Badan Siber dan Sandi Negara, "Tools cyber security maturity (CSM) v1.10," Jakarta, Indonesia, 2021.
- [11] O. Korchenko, O. Korystin, V. Shulha, S. Kazmirchuk, S. Demediuk, and S. Zybin, "Sustainable development of smart regions via cybersecurity of national infrastructure: A fuzzy risk assessment approach," *Sustainability*, vol. 17, no. 19, p. 8757, Sep. 2025. doi: 10.3390/su17198757.
- [12] A. Barlybayev and A. Turginbayeva, "Development and implementation of an advanced fuzzy expert system for the assessment of information security risks," *Journal of Computational and Cognitive Engineering*, vol. 4, no. 4, pp. 570–580, Apr. 2025. doi: 10.47852/bonviewJCCE52024683.
- [13] P. Radanliev *et al.*, "Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial Internet of Things and Industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, p. 13, Dec. 2020. doi: 10.1186/s42400-020-00052-8.
- [14] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, Mar. 2004.
- [15] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.
- [16] L. A. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning—III," *Information Sciences*, vol. 9, no. 1, pp. 43–80, Jan. 1975. doi: 10.1016/0020-0255(75)90017-1.
- [17] S. Napitupulu, E. B. Nababan, and P. Sihombing, "Comparative analysis of fuzzy inference Tsukamoto, Mamdani, and Sugeno in the horticulture export selling price," in *Proc. IEEE MECnIT 2020*, Jun. 2020, pp. 183–187. doi: 10.1109/MECnIT48290.2020.9166587.
- [18] H. Fakhrafar, *Quantifying Uncertainty in Risk Assessment Using Fuzzy Theory*. arXiv, 2020. doi: 10.48550/arXiv.2009.09334.
- [19] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965. doi: 10.1016/S0019-9958(65)90241-X.
- [20] B. Cassottana, M. M. Roomi, D. Mashima, and G. Sansavini, "Resilience analysis of cyber-physical systems: A review of models and methods," *Risk Analysis*, vol. 43, no. 11, pp. 2359–2379, Nov. 2023. doi: 10.1111/risa.14089.
- [21] J. W. Park and S. J. Lee, "A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence," *Annals of Nuclear Energy*, vol. 142, p. 107432, Jul. 2020. doi: 10.1016/j.anucene.2020.107432.
- [22] H. Irawan, A. H. Muhammad, and A. Nasiri, "Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS Controls v8," *INOVTEK Polbeng - Seri Informatika*, vol. 9, no. 1, Jun. 2024. doi: 10.35314/isi.v9i1.3973.