Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/BA08.20250343
Published: December 20, 2025

Prioritizing Distributed Denial of Service (DDoS) Attack Factors in Digital Twins Using AHP Weighted TOPSIS

S M Julfiker Zahid
Industrial Engineering and Management Department
Khulna University of Engineering and Technology
Khulna, Bangladesh
julfikerzahid2@gmail.com

Kazi Omar Faruk
Industrial Engineering and Management Department
Khulna University of Engineering and Technology
Khulna, Bangladesh
koffaruk007@gmail.com

Abstract

Digital Twins (DTs) are leading-edge technologies in Industry 4.0 that facilitate monitoring, real-time simulation, and optimization of physical systems. However, their significant integration with Cyber-Physical Systems (CPS) and Internet of Things (IoT) makes them vulnerable to crucial cyber-attacks. One of them is a Distributed Denial of Service (DDoS) attack, which causes a major risk to the integrity of data and operational continuity. This study methodically identifies and ranks the primary factors leading to DDoS attacks on Digital Twin systems. Implementing an integrated Multi-Criteria Decision-Making (MCDM) method, the Analytic Hierarchy Process (AHP) is employed to assign weights to evaluation criteria based on expert opinions, while the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is used to rank the identified causative factors. The findings indicate that the lack of distributed threat detection, vulnerable network protocols, and an extensive attack surface represent the most critical attack factors. A comprehensive sensitivity analysis validates the stability of these rankings, offering a justified prioritization to support the development of targeted and effective defense strategies for securing the implementations of DTs against alarming cyber-attacks.

Keywords
Digital Twins, Cyber-attacks, Distributed Denial of Service (DDoS), Cybersecurity.

1. Introduction
The incorporation of Digital Twins is currently revolutionizing industries through the facilitation of real-time simulation and operations. This integration introduces significant vulnerabilities in critical systems, especially to Distributed Denial of Service (DDoS) cyber-attacks. Such kinds of attacks can disrupt essential operations by saturating system resources, resulting in major financial and safety issues. This study is driven by the urgent need to enhance the security of digital twins. The main goal is to methodically identify and rank the essential factors that affect DDoS attacks. Developing this prioritized list is crucial for establishing focused and efficient countermeasures, ultimately improving the stability of digital twin systems.

1.1 Objectives

- Identifying several causes of Distributed Denial of Service (DDoS) cyber-attacks associated with digital twin systems
- Prioritizing identified causes using the AHP weighted TOPSIS method.
- Validating the robustness of the rankings through a comprehensive sensitivity analysis.

2. Literature Review

Digital Twins (DTs) are a revolutionary concept in the context of Industry 4.0, serving as a dynamic virtual representation of a system or physical object throughout its lifecycle, continuously updated using simulation models and real-time data synchronization (Tao et al., 2018). The conceptual foundation of digital twins is built upon three core components: the physical entity in real space, the virtual entity in virtual space, and the seamless data connectivity that integrates them, as addressed by Grieves and Vickers (2017). This framework has transitioned from a theoretical model to an important technology that facilitates operational optimization, smart manufacturing, and predictive maintenance. The practical application of digital twins relies heavily on the framework established by Internet of Things (IoT) and Cyber-Physical Systems (CPS), which offer the essential network of actuators, sensors, and embedded systems to gather and transfer data from the physical environment (Lee et al., 2019). This synergy establishes a closed-loop system in which the physical state notifies the virtual model and the virtual model optimizes or controls the physical entity. The applications have fairly extended from manufacturing to include healthcare, smart cities, and aerospace, showcasing their broad potential (Fuller et al., 2020). However, this advanced integration and two-way data exchange considerably broaden the potential for cyber-attacks. As Kaur et al. (2020) note, the reliability and accessibility of the data stream are of utmost importance. Any compromise may result in the physical system functioning according to a flawed virtual model, which could have potentially catastrophic consequences. The intricate nature of DT architectures is frequently characterized by cloud-edge orchestration and diverse data sources, which present numerous vulnerabilities within their foundational CPS and IoT components. These vulnerabilities include weak edge computing nodes, insecure communication protocols, and inadequate device authentication (Khan et al., 2021). Despite serving as the foundation of strength, this complex interconnection simultaneously positions Digital Twins as prime targets for advanced cyber-attacks. Therefore, a security-centric design approach is urgently required. Among the various cyber-attacks, Distributed Denial of Service (DDoS) attacks represent a notably serious and sudden threat to the operational integrity of Digital Twins. A DDoS attack seeks to affect a service's availability by consuming its resources with an array of malicious traffic originating from several distributed sources. Within the framework of a DT, this attack may target the communication channel connecting the physical and virtual entities, the endpoints of data ingestion, or the virtual model's computational resources itself (Sadeghi et al., 2020). The outcome of this scenario is a breakdown in essential real-time synchronization, resulting in a phenomenon referred to as digital model drift, whereby the virtual representation progressively deviates from the physical reality (Anton et al., 2021). For an industrial digital twin managing a production line, this could imply that the virtual model remains blind to an overheating component or other mechanical faults, thereby hindering predictive maintenance signals and resulting in unplanned downtime and equipment damage. The impact is particularly significant in infrastructure fields such as water treatment plants and smart grids, where a DDoS-associated control and loss of visibility might turn into threats to public safety (Cárdenas et al., 2019). Research by Al-Hawawreh et al. (2022) especially connects the proliferation of IoT botnets with the heightened large-scale DDoS attacks targeting industrial CPS, which constitute the foundation of several DT implementations. Although conventional IT security has established a variety of DDoS mitigation techniques, these are frequently inadequate to meet the low-latency and real-time demands of CPS and DTs (Mohan et al., 2023). Recent research has initiated keeping track of security challenges, particularly to DTs with DDoS, which is recognized as a major barrier to data availability (Liu et al., 2022). Furthermore, Yurekten and Demirci (2021) examined SDN-driven adaptive defense strategies emphasizing the importance of dynamic responses within these environments.

However, a major gap still exists in the present body of literature. Although a number of studies effectively recognize the presence of DDoS attacks and suggest generic mitigation strategies, there remains a deficiency of targeted research that systematically identifies and prioritizes the particular architectural and technical factors of a DT system that predominantly influence its vulnerability to DDoS attacks. Table 1 shows the significant causes of DDoS attacks on digital twin systems, which are considered as alternative starting from A1 to A12 numerically. Security efforts may be misdirected in the absence of a clear, quantitatively solid understanding of which vulnerabilities, be it in the data processing pipeline, cloud API gateway, or edge device connection protocol. This study aims to fill this gap by not only identifying these causative factors but also implementing AHP-weighted TOPSIS, a comprehensive Multi-

Criteria Decision-Making (MCDM) approach, to rank them according to their significance as well as verify the rankings through a sensitivity analysis. This provides a practical framework to secure the implementations of Digital Twins against one of the most threatening attacks (Table 1).

Table 1. Attack Factors of Distributed Denial of Service Attack on Digital Twin Systems

Alternative	Causes of DDoS Attacks	References
A1	Multiple compromised systems targeting a DT	Hussaini et al., 2022
A2	Exploitable network protocols and services	Hussaini et al., 2022
A3	Lack of filtering in DT networks	Otoom et al., 2025
A4	No throttling exhausts system resources	Suhail et al., 2023
A5	Vulnerable public-facing endpoints	Kararslan et al., 2021
A6	Absence of load balancing or traffic mitigation tools	Kararslan et al., 2021
A7	Lack of system resilience and redundancy	De Azambuja et al., 2024
A8	Poor incident response planning	De Azambuja et al., 2024
A9	No distributed threat detection	Abdullahi et al., 2024
A10	Resource exhaustion vulnerability	Abdullahi et al., 2024
A11	Weak security in IoT device connectivity	Anda et al., 2021
A12	Large attack surface in pipeline network systems	Anda et al., 2021

3. Methods

AHP Weighted TOPSIS is an integrated approach of Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). This method produces a more comprehensive and accurate final result by first using AHP to objectively identify the importance of each criterion, then using TOPSIS to assess and rank the available solutions based on those weights (Zeng et al., 2021). The method is explained step by step as follows:

Step 1: Determine AHP Weights

1.1: Construction of pairwise comparison matrix:

AHP involves pairwise comparison of criteria based on importance. Let the requirements be represented in a matrix A. The element a_{ij} represents the relative importance of criterion i over criterion j. Use the scale: 1 (equal), 3 (moderate), 5 (strong), 7 (very strong), 9 (extreme). Reciprocals for inverse comparisons.

1.2: Calculation of the weight vector from the pairwise matrix

- Normalize the matrix by columns (each element divided by the sum of its column).
- Average the rows to get the weight vector w.

1.3: Checking for the consistency validation:

- Calculate the consistency ratio (CR) to ensure the judgments are consistent.
- If CR < 0.1 (10%), judgments are consistent.

a. Compute A * w, where w is the weight vector: $Aw = \lambda_{max} w$

b. Compute the eigenvalue: $\lambda_{max} = \frac{1}{n}\sum \frac{(Aw)_i}{w_i}$

c. Compute Consistency Index (CI) = $(\lambda_{max}\text{-}n)/(n\text{-}1)$

d. CR = CI / RI, where RI is the random index.

Step 2: Construct the Decision Matrix

This matrix column is specified to an attribute, and each row to an alternative. The decision matrix $X = [x_{ij}]_{m\times n}$ is constructed as :

$$X=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{17} \\ x_{21} & x_{22} & \cdots & x_{27} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{m7} \end{bmatrix}$$

where x_{ij} denotes the score assigned to alternative i under criterion j.

Step 3: Normalize the decision matrix

Obtain the normalized decision matrix r_{ij}. This can be represented as:

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

Step 4: Weighted Normalized Matrix

$$v_{ij} = w_j \times r_{ij}$$

Each normalized value is multiplied by the corresponding AHP weight. The AHP method calculates the performance variables' weight corresponding to different performances. A matrix stores all judgments in this method.

Step 5: Determine Ideal & Negative-Ideal Solutions

The positive ideal solution A+ indicates the most preferable alternative, and the negative ideal solution A- indicates the least preferable alternative.

For a positive ideal solution,

$$A^+ = \{\mathrm{v1}^+, \mathrm{v2}^+, \ldots, \mathrm{vn}^+\}, \quad where\ v_j{}^+ = \{max_i(v_{ij}), min_i(v_{ij})\}$$

For a negative ideal solution,

$$A^- = \{\mathrm{v1}^-, \mathrm{v2}^-, \ldots, \mathrm{vn}^-\}, \qquad where\ v_j{}^- = \{min_i(v_{ij}), max_i(v_{ij})\}$$

Step 6: Determine the distance measures

The separation of each alternative from the ideal solutions given by the n-dimensional Euclidean distance from the following equations:

$$S_i^+ = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^+)^2}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^-)^2}$$

Step 7: Compute Closeness Coefficient

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-}$$

Step 8: Preference Order Ranking

The best choice is defined as the alternative corresponding to the top relative proximity. The CC_i for every case is termed the property index of multi-performance in this study. The DDoS cause with the highest CC_i value represents the most serious and harmful reason, since it is closest to the positive ideal solution and farthest from the negative one.

4. Ranking DDoS Key Factors

We have found 12 alternatives of DDoS attack factors on digital twin systems, which are mentioned in Table 1 of the literature review section. For the factor ranking, the main evaluation dimensions or criteria selected from the expert opinion of relevant fields are as follows:

C1: Severity of Impact
C2: Probability of Occurrence
C3: Difficulty of Detection
C4: Difficulty of Prevention
C5: Attack Propagation Speed
C6: Resource Exhaustion Level
C7: System Recovery Time

Experts compare each criterion pairwise on a Saaty scale (1–9):
1 = equal importance
3 = moderate importance
5 = strong importance
7 = very strong importance
9 = extreme importance

Step 1: Determine AHP Weights
The Analytic Hierarchy Process (AHP) determines the relative importance of the seven evaluation criteria using Saaty's 1–9 scale. Table 2 and Table 3 show the pairwise comparison matrix and the normalized matrix (N), respectively.

Table 2. Pairwise Comparison Matrix (Synthetic Expert Judgement)

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
C1	1.00	3.00	2.00	4.00	5.00	2.00	3.00
C2	0.33	1.00	0.50	2.00	3.00	0.33	0.50
C3	0.50	2.00	1.00	3.00	4.00	0.50	2.00
C4	0.25	0.50	0.33	1.00	2.00	0.25	0.33
C5	0.20	0.33	0.25	0.50	1.00	0.20	0.25
C6	0.50	3.00	2.00	4.00	5.00	1.00	3.00
C7	0.33	2.00	0.50	3.00	4.00	0.33	1.00

Column Sums: [3.11, 11.83, 6.58, 17.50, 24.00, 4.61, 10.08].

Table 3. Normalized Matrix (N)

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
C1	0.321	0.254	0.304	0.229	0.208	0.434	0.298
C2	0.107	0.085	0.076	0.114	0.125	0.072	0.050
C3	0.161	0.169	0.152	0.171	0.167	0.108	0.198
C4	0.080	0.042	0.050	0.057	0.083	0.054	0.033
C5	0.064	0.028	0.038	0.029	0.042	0.043	0.025
C6	0.161	0.254	0.304	0.229	0.208	0.217	0.298
C7	0.107	0.169	0.076	0.171	0.167	0.072	0.099

Average of rows gives the weight vector: Weights (W) = [0.293, 0.090, 0.161, 0.057, 0.038, 0.239, 0.122]
Consistency Check:
Weighted Sum Vector: WSV=A × W = [2.189, 0.656, 1.214, 0.414, 0.278, 1.829, 0.903]
Consistency Vector: WSV ÷ W = [7.471, 7.289, 7.540, 7.263, 7.316, 7.653, 7.402]
Eigenvalue: λmax = (7.471 + 7.289 + 7.540 + 7.263 + 7.316 + 7.653 + 7.402) ÷ 7 = 7.419
Consistency Index Calculation: CI = (λmax - n) ÷ (n - 1) = (7.419 - 7) ÷ 6 = 0.070
Consistency Ratio: RI (Random Index for n=7) = 1.32
CR = CI ÷ RI = 0.070 ÷ 1.32 = 0.053 < 0.10

Hence, the pairwise comparison matrix is consistent (CR = 0.053 < 0.10).

Step 2: Construct the Decision Matrix (Table 4 and Table 5)

Table 4. Decision Matrix

	C1	C2	C3	C4	C5	C6	C7
A1	7	6	5	6	5	7	6
A2	8	7	6	7	6	8	7
A3	6	5	7	5	4	6	5
A4	7	8	6	7	7	7	8
A5	5	6	4	6	5	5	6
A6	6	7	5	6	6	6	7
A7	7	6	6	7	5	7	6
A8	6	5	5	6	4	6	5
A9	8	7	7	8	7	8	7
A10	7	6	5	7	6	7	6
A11	6	7	6	6	5	6	7
A12	7	7	6	7	7	7	7

Step 3: Normalized decision matrix (R)

Table 5. Normalized Decision Matrix (R)

	C1	C2	C3	C4	C5	C6	C7
A1	0.264	0.247	0.232	0.247	0.235	0.264	0.247
A2	0.302	0.288	0.278	0.288	0.282	0.302	0.288
A3	0.226	0.206	0.325	0.206	0.188	0.226	0.206
A4	0.264	0.329	0.278	0.288	0.329	0.264	0.329
A5	0.189	0.247	0.186	0.247	0.235	0.189	0.247
A6	0.226	0.288	0.232	0.247	0.282	0.226	0.288
A7	0.264	0.247	0.278	0.288	0.235	0.264	0.247
A8	0.226	0.206	0.232	0.247	0.188	0.226	0.206
A9	0.302	0.288	0.325	0.329	0.329	0.302	0.288
A10	0.264	0.247	0.232	0.288	0.282	0.264	0.247
A11	0.226	0.288	0.278	0.247	0.235	0.226	0.288
A12	0.264	0.288	0.278	0.288	0.329	0.264	0.288

Step 4: Weighted Normalized Matrix
$V = \text{diag}(W) \times R$, where $W = [0.293, 0.090, 0.161, 0.057, 0.038, 0.239, 0.122]$. Table 6 shows the weighted normalized matrix.

Table 6. Weighted Normalized Matrix

	C1	C2	C3	C4	C5	C6	C7
A1	0.077	0.022	0.037	0.014	0.009	0.063	0.030
A2	0.088	0.026	0.045	0.016	0.011	0.072	0.035
A3	0.066	0.019	0.052	0.012	0.007	0.054	0.025
A4	0.077	0.030	0.045	0.016	0.013	0.063	0.040
A5	0.055	0.022	0.030	0.014	0.009	0.045	0.030
A6	0.066	0.026	0.037	0.014	0.011	0.054	0.035
A7	0.077	0.022	0.045	0.016	0.009	0.063	0.030
A8	0.066	0.019	0.037	0.014	0.007	0.054	0.025
A9	0.088	0.026	0.052	0.019	0.013	0.072	0.035

A10	0.077	0.022	0.037	0.016	0.011	0.063	0.030
A11	0.066	0.026	0.045	0.014	0.009	0.054	0.035
A12	0.077	0.026	0.045	0.016	0.013	0.063	0.035

Step 5: Determine Ideal & Negative-Ideal Solutions
Positive Ideal Solution (A^+): $A^+ = [\max(v_{1j}), \max(v_{2j}), ..., \max(v_{7j})]$
Negative Ideal Solution (A^-): $A^- = [\min(v_{1j}), \min(v_{2j}), ..., \min(v_{7j})]$
Table 7 shows the positive ideal solution and the negative ideal solution.

Table 7. Positive Ideal Solution and Negative Ideal Solution

Solution Type	C1	C2	C3	C4	C5	C6	C7
Positive Ideal (A^+)	0.088	0.030	0.052	0.019	0.013	0.072	0.040
Negative Ideal (A^-)	0.055	0.019	0.030	0.012	0.007	0.045	0.025

Step 6: Determine the distance measures.
Distance to Positive Ideal Solution (S^+):

$$S_i^+ = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^+)^2}$$

Distance to Negative Ideal Solution (S^-):

$$S_i^- = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^-)^2}$$

Table 8 shows the distance to the positive and negative ideal solution.

Table 8. Distance to Positive Ideal Solution and Negative Ideal Solution

Alternative	**S^+ (Positive Ideal)**	**S^- (Negative Ideal)**
A1	0.028	0.030
A2	0.010	0.047
A3	0.039	0.025
A4	0.017	0.037
A5	0.049	0.007
A6	0.029	0.021
A7	0.020	0.032
A8	0.040	0.015
A9	0.007	0.049
A10	0.023	0.030
A11	0.029	0.024
A12	0.015	0.042

Step 7: Compute Closeness Coefficient and Final Ranking

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-}$$

The computations of the closeness coefficient and final ranking are shown in the results and discussion section.

5. Sensitivity Analysis

This sensitivity analysis assesses the stability of the final DDoS cause rankings when AHP weights are adjusted slightly. This helps to verify the robustness of this model. Table 9 shows the baseline data.

Table 9. Baseline Data for Sensitivity Analysis

Criterion	Description	Weight
C1	Severity of Impact	0.293
C2	Probability of Occurrence	0.090
C3	Difficulty of Detection	0.161
C4	Difficulty of Prevention	0.057
C5	Attack Propagation Speed	0.038
C6	Resource Exhaustion Level	0.239
C7	System Recovery Time	0.122

Step 1: Define the Sensitivity Scenarios

We'll create 3 scenarios, each increasing one criterion weight by +10%, starting from criterion 1 to criterion 3, while proportionally reducing the others so that the total sum = 1. Mathematically,

$$w_k' = w_k \times (1 + 0.1)$$

$$w_j' = w_j \times \frac{1 - w_k'}{1 - w_k}, \forall j \neq k$$

Step 2: Recalculate TOPSIS for Each Scenario (Table 10- Table 15)

For each scenario, replace the old AHP weight vector W_0 with the new W_k' and compute:

a. New weighted normalized matrix $V' = R \times W'$

b. New ideal (A^+) and negative-ideal (A^-) solutions

c. New S^+ and S^-

d. New Closeness Coefficients (CC_i')

Scenario 1: Varying criterion1 by +10%,

Table 10. Adjusted AHP Weights

Criterion	Base Weight	+10% Adjustment	Normalized Weight
C1	0.293	0.293 × 1.1 = 0.3223	0.3223 / 1.029 = 0.313
C2	0.090	scaled	0.087
C3	0.161	scaled	0.156
C4	0.057	scaled	0.055
C5	0.038	scaled	0.037
C6	0.239	scaled	0.232
C7	0.122	scaled	0.119

Table 11. CC and Ranking

Alternative	CC
A9	0.895
A2	0.829
A4	0.694
A12	0.666
A7	0.616
A10	0.564
A1	0.555
A11	0.430
A3	0.422
A6	0.378
A8	0.298
A5	0.116

Scenario 2. Varying criterion 2 by +10%,

Table 12. Adjusted AHP Weights

Criterion	Weight
C1	0.290
C2	0.098
C3	0.160
C4	0.056
C5	0.038
C6	0.237
C7	0.121

Table 13. Closeness Coefficients and Ranking

Alternative	CC
A9	0.887
A2	0.821
A4	0.699
A12	0.666
A7	0.609
A10	0.554
A1	0.545
A11	0.440
A3	0.425
A6	0.384
A8	0.294
A5	0.123

Scenario 3: Varying criterion3 by +10%,

Table 14. Adjusted AHP Weights

Criterion	Weight
C1	0.288
C2	0.089
C3	0.174
C4	0.056
C5	0.037
C6	0.235
C7	0.120

Table 15. Closeness Coefficients and Ranking

Alternative	CC
A9	0.893
A2	0.816
A4	0.696
A12	0.666
A7	0.614
A10	0.548
A1	0.540
A3	0.445
A11	0.445
A6	0.380
A8	0.297
A5	0.118

The resultant top cause and rank stability for all three 3 scenarios are shown in the results and discussion section.

6. Results and Discussion:

Applying the AHP weighted TOPSIS methodology to the DDoS attack factors on digital twin systems, we obtained Table 16, which presents the closeness coefficient and final ranking for each alternative key factor of DDoS attack. Table 16 is constructed from the formula mentioned in step 7 of the method section.

Table 16. Closeness Coefficient and Final Ranking

Alternative	DDoS Causative Factors	Closeness Coefficient	Rank (C_i)
A9	No distributed threat detection	0.875	1
A2	Exploitable network protocols and services	0.825	2
A12	Large attack surface in pipeline network systems	0.737	3
A4	No throttling exhausts system resources	0.685	4
A7	Lack of system resilience and redundancy	0.615	5
A10	Resource exhaustion vulnerability	0.566	6
A1	Multiple compromised systems targeting a DT	0.517	7
A11	Weak security in IoT device connectivity	0.453	8
A6	Absence of load balancing or traffic mitigation tools	0.420	9
A3	Lack of filtering in DT networks	0.391	10
A8	Poor incident response planning	0.273	11
A5	Vulnerable public-facing endpoints	0.125	12

The integration of the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) in this work provides a useful framework for ranking the causes of Distributed Denial of Service (DDoS) attacks. These rankings are on the basis of various operational and technical criteria. The rankings represent that the lack of distributed threat detection (A9) is the most crucial factor contributing to DDoS vulnerability. This is succeeded by exploitable network protocols and services (A2) and the large attack surface in pipeline network systems (A12). As directed by this ranking, the key aspects influencing DDoS resilience across digital infrastructures are detection systems and proactive protection. The high weight assigned to Resource Exhaustion Level (C6 = 0.239) and Severity of Impact (C1 = 0.293) brings out the significance of system-level effects in expert evaluations. These findings are compatible with recent studies, which demonstrate that DDoS attacks basically use resource exhaustion techniques. These techniques lead to economic disruption and service unavailability rather than specifically compromising data. The comparatively lower weights for Difficulty of Prevention (C4=0.057) and Attack Propagation Speed (C5 = 0.038) show that, while they influence attack dynamics, they are considered less critical compared to the overall system durability and operational impact. The pattern of ranking indicates the dependencies among system protection protocols. Alternatives such as A4 (No throttling exhausts system resources) and A7 (Lack of system resilience and redundancy) hold the fourth and fifth places, respectively. This underlines how redundancy planning and resource management affect the prevention of attacks. These results assure that real-time monitoring and design of infrastructure play an important role in the resilience of distributed systems. The sensitivity analysis makes these results more reliable. Table 17 shows the resultant top cause and rank stability after the sensitivity analysis. The leading cause (A9) remained consistent across all three weight-variation scenarios. This stability indicates that the AHP-weighted TOPSIS model maintains robustness even when expert evaluations are marginally modified.

Table 17. Top Cause and Rank stability after Sensitivity Analysis

Scenario	Varied Criterion	Top Cause (Rank 1)	Rank Stability
S1	C1 (Severity)	A9	Stable
S2	C2 (Probability)	A9	Stable
S3	C3 (Detection Difficulty)	A9	Stable

The consistency ratio (CR = 0.053 < 0.1) of the AHP pairwise matrix confirms that the expert evaluations were devoid of substantial bias and logical coherence. Consequently, it can be stated that the produced rankings are reliable for making strategic decisions in cybersecurity. Reducing attack surfaces through proper network segmentation, reducing exploitable network protocols, and access control can further improve resilience. The model illustrates the contribution of each factor, providing decision-makers with a data-driven framework for resource allocation in cybersecurity planning. The proposed integrated solution exhibits scalability and applicability that extend beyond the evaluation of DDoS attacks. The AHP weighted TOPSIS framework serves as a tool for evaluating a range of cyber risks, including critical infrastructure security, vulnerability management, and intrusion detection by changing the options and criteria. This versatility spotlights its potential as a wide-ranging tool for MCDM in the domains of cybersecurity.

7. Conclusion

This research explored the identification and systematic prioritization of the primary factors contributing to Distributed Denial of Service (DDoS) attacks in Digital Twin (DT) systems by integrating the Analytic Hierarchy Process (AHP) with the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). Through the development and implementation of a combined model, we dealt with the fundamental problem of the absence of a robust, quantitative approach for guiding resource allocation among various potential attack factors. We have also validated our results by three weight-variation scenarios through sensitivity analysis. Future research may cover real-time monitoring and probabilistic modeling to enhance the adaptability of digital twin-focused risk-assessment frameworks. However, the findings of this study establish a strong foundation for improving cyber-resilience in the increasingly complex digital-twin systems across various domains.

Acknowledgement

The authors would like to express gratitude to Ridwan Mustofa, currently pursuing a **Ph.D.** in **Systems Engineering** at **Boston University (BU)** in Boston, Massachusetts**,** for his guidance and support.

References

Abdullahi, S. M., & Lazarova-Molnar, S., *Toward A Unified Security Framework For Digital Twin Architectures*, In Proceedings Of The 2024 IEEE International Conference On Cyber Security And Resilience (CSR), Pp. 1–8, 2024, IEEE.

Al-Hawawreh, M., Sitnikova, E., & Aboutorab, N., *Securing The Industrial Internet Of Things Against Ransomware Attacks: A Comprehensive Framework*, IEEE Transactions On Industrial Informatics, 18(5), Pp. 3083–3092, 2022.

Andrea Cimolato, J. J., *EMG-Driven Control In Lower Limb Prostheses: A Topic-Based Systematic Review*, Journal Of Neuroengineering And Rehabilitation, Pp. 1–26, 2022.

Anda, I., Mishra, R., & Aliyu, A. M., *Data Security Management Framework For Digital Twins Of Industrial Pipelines*, In Proceedings Of The 2021 International Conference On Computer And Applications (CNA), Pp. 1–6, 2021, IEEE.

Anton, S. D., Kanoor, S., Fraunholz, D., & Schotten, H. D., *Evaluation Of Machine Learning-Based Anomaly Detection In Industrial Control Systems*, In Proceedings Of The 2021 IEEE International Conference On Cyber Security And Resilience (CSR), Pp. 1–8, 2021.

Biao Chen, C. C., *A Real-Time EMG-Based Fixed-Bandwidth Frequency-Domain Embedded System For Robotic Hand Control*, Frontiers, Pp. 1–15, 2022.

Cárdenas, A. A., Amin, S., & Sastry, S., *Research Challenges For The Security Of Control Systems*, In Proceedings Of The 3rd USENIX Workshop On Hot Topics In Security (Hotsec), Pp. 1–6, 2019.

Collaborators, G. B. D. 2019, *Global, Regional, And National Burden Of Stroke And Its Risk Factors, 1990–2019: A Systematic Analysis*, The Lancet Neurology, Pp. 795–820, 2021.

De Azambuja, A. J. G., Giese, T., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R., *Digital Twins In Industry 4.0: Opportunities And Challenges Related To Cybersecurity*, Procedia CIRP, 121, Pp. 25–30, 2024.

Fuller, A., Fan, Z., Day, C., & Barlow, C., *Digital Twin: Enabling Technologies, Challenges, And Open Research*, IEEE Access, 8, Pp. 108952–108971, 2020.

Grieves, M., & Vickers, J., *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior In Complex Systems*, In Transdisciplinary Perspectives On Complex Systems, Pp. 85–113, 2017, Springer, Cham.

Hussaini, A., Qian, C., Liao, W., & Yu, W., *A Taxonomy Of Security And Defense Mechanisms In Digital Twin-Based Cyber-Physical Systems*, In Proceedings Of The IEEE Ithings / Greencom / Cpscom / Smartdata Congress, Pp. 597–604, 2022, IEEE.

Kararslan, E., & Babiker, M., *Digital Twin Security Threats And Countermeasures: An Introduction*, In Proceedings Of The 14th International Conference On Information Security And Cryptology (ISCTURKEY), Pp. 1–5, 2021, IEEE.

Kaur, M. J., Mishra, V. P., & Maheshwari, P., *The Convergence Of Digital Twin, Iot, And Machine Learning: Transforming Business And Industries*, Wireless Personal Communications, 112(3), Pp. 1647–1669, 2020.

Khan, L. U., Saad, W., Han, Z., & Hong, C. S., *Digital Twin For 6G: Taxonomy, Research Challenges, And Future Directions*, IEEE Internet Of Things Magazine, 4(2), Pp. 70–77, 2021.

Lee, J., Bagheri, B., & Kao, H. A., *A Cyber-Physical Systems Architecture For Industry 4.0-Based Manufacturing Systems*, Manufacturing Letters, 3, Pp. 18–23, 2019.

Liu, Y., Zhang, L., Yang, Y., & Wang, Y., *A Novel Security Framework For Industrial Digital Twins In The 5G Era*, IEEE Transactions On Industrial Informatics, 18(9), Pp. 6231–6240, 2022.

Mohan, A., Singh, A., & Kumar, S., *Ddos Attack Detection In Iot Devices Using Machine Learning: A Comprehensive Survey*, Journal Of Network And Computer Applications, 212, 103571, 2023.

Otoom, S., *Risk Auditing For Digital Twins In Cyber-Physical Systems: A Systematic Review*, Journal Of Cyber Security And Risk Auditing, 2025(1), Pp. 22–35, 2025.

Sadeghi, M., Behnia, F., & Isazadeh, A., *A Survey On Security And Privacy Of Digital Twin*, Journal Of Network And Systems Management, 28(4), Pp. 1025–1054, 2020.

Suhail, S., Iqbal, M., Hussain, R., & Jurdak, R., *ENIGMA: An Explainable Digital Twin Security Solution For Cyber-Physical Systems*, Computers In Industry, 151, 103961, 2023.

Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C., *Digital Twin In Industry: State-Of-The-Art*, IEEE Transactions On Industrial Informatics, 15(4), Pp. 2405–2415, 2018.

Yurekten, O., & Demirci, M., *An SDN-Based Adaptive Defense Mechanism For Ddos Attacks In Iot Systems*, IEEE Transactions On Network And Service Management, 18(3), Pp. 3121–3135, 2021.

Zeng, Y.-P., Lin, C.-L., Dai, H.-M., Lin, Y.-C., & Hung, J.-C., *Multi-Performance Optimization In Electrical Discharge Machining Of Al_2O_3 Ceramics Using Taguchi-Based AHP Weighted TOPSIS Method*, Processes, 9(9), 1647, 2021.

Biographies

S M Julfiker Zahid is a Bangladeshi student from Kushtia, currently pursuing his MSc. in the Department of Industrial Engineering and Management (IEM) at Khulna University of Engineering and Technology (KUET). He completed his BSc. from the same department and institution about two years ago. Alongside his academic journey, he has developed a strong interest in Cyber Physical Systems and cybersecurity. Currently, he is doing research work on Blockchain Technology and Healthcare Engineering. Beyond this, he is enthusiastic about Industry 4.0, Smart Factories, Sustainable Manufacturing, and Circular Economy. Guided by a forward-looking mindset, he aspires to contribute to industrial systems that are sustainable and fundamentally more resilient.

Kazi Omar Faruk is an Industrial Engineering and Management (IEM) undergraduate student at Khulna University of Engineering & Technology (KUET), Bangladesh. His recent work focuses on Cyber Attacks on Digital Twins, exploring resilience and risk prioritization. Beyond coursework, his interests span Circular Economy, Smart Manufacturing, and the application of Artificial Intelligence, with a keen emphasis on data-driven optimization and sustainable operations. He has also participated in various co-curricular activities and served in multiple voluntary organizations.