Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/GC03.20260503
Published: February 2, 2026

Cybersecurity Risk Assessment for Digital Twins: AHP-TOPSIS Ranking of Critical DoS Attack Factors

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

Md. Saiful Islam
Professor
Department of Industrial Engineering and Management
Khulna University of Engineering and Technology
Khulna, Bangladesh
saifuliem@iem.kuet.ac.bd

Abstract

Digital Twins (DTs) are crucial uprising technologies within Industry 4.0, offering virtual representations dynamically for simulation, control, and real-time monitoring of physical systems. Their extensive integration with the Internet of Things (IoT) and Cyber-Physical Systems (CPS) results in major cybersecurity vulnerabilities, especially with regard to disruptive Denial of Service (DoS) attacks that endanger data integrity and operational continuity. This study methodically identifies and ranks the major causative factors of DoS cyber-attacks in digital twin systems. Applying an integrated Multi-Criteria Decision-Making (MCDM) technique, the Analytic Hierarchy Process (AHP) determines the weights of evaluation criteria on the basis of expert opinions, and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) ranks the detected attack factors. The final outcomes claim missing redundancy and load balancing, a lack of traffic throttling or rate-limiting systems, and flooding via exposed interfaces as the most vital attack factors. The robustness of these rankings is confirmed by a systematic sensitivity analysis, which provides a proven prioritization to direct focused security measures for improving the cyber-resilience of digital twin systems.

Keywords
Digital Twins, Cyber-Physical Systems (CPS), Cyber-attacks, Denial of Service (DoS), Cybersecurity.

1. Introduction
The growing advancement of Digital Twins as the fundamental components of Industry 4.0 faces significant cybersecurity challenges. These challenges especially come from Denial of Service (DoS) cyber-attacks that negatively affect data integrity and system availability. Such attacks can disrupt the real-time synchronization between physical and virtual entities, resulting in safety risks and operational interruptions. The urgent need to accurately evaluate and strengthen Digital Twin security is the driving force for this work. Therefore, finding and ranking the main operational and technical factors leading to DoS vulnerabilities can be considered the primary goal of this study. To improve the cyber resilience of crucial interconnected systems and develop specific defense mechanisms, it is important to establish this actionable, prioritized list of attack vectors.

1.1 Objectives

- Determining various causes of Denial of Service (DoS) cyber-attacks correlated with digital twin systems.
- Ranking determined causes using the AHP weighted TOPSIS method.
- Affirming the validity of the rankings through a systematic sensitivity analysis.

2. Literature Review

Digital Twins (DTs) serve as a core component of Industry 4.0, operating as agile, data- driven virtual representations of systems, processes, or physical assets that are constantly updated through simulation models and real-time data sources (Tao et al., 2018). This paradigm, with its intellectual origins in the three-part architecture of physical entities, virtual entities, and linking data figured by Grieves and Vickers (2017), has grown from a theoretical framework to a vital technology for operations. The Internet of Things (IoT) and Cyber-Physical Systems (CPS), which provide the required network of embedded computing, actuators, and sensors, enable two-way flow of data between the physical and virtual worlds and are essential to the practical implementation and enormous value of DTs (Lee et al., 2019). Because of this synergy, a tightly integrated closed-loop system is created, which allows formerly unusual capabilities in remote process control, operational optimization, and predictive maintenance. DTs' application domain has quickly grown beyond its manufacturing roots to include aerospace, energy, healthcare, and smart cities, highlighting its potential to revolutionize the economy (Fuller et al., 2020). However, the cyber-attack surface is significantly increased by this deep integration and dependence on high-fidelity and constant data synchronization. As stated by Kaur et al. (2020), the data stream's confidentiality, availability, and integrity are so crucial that any compromise may force the physical system to function using an out-of-date or inaccurate virtual model, which leads to disastrous financial and safety consequences. The complicated architecture of current DT deployments frequently incorporates various data sources, different communication protocols, and hybrid cloud-edge computing, which presents several inherent vulnerability points from their respective IoT and CPS layers (Khan et al., 2021). These vulnerabilities involve, but are not limited to, vulnerable edge computing nodes, insufficient encryption in communication channels, and unsecured device authentication. As a result, while this interconnection gives Digital Twins their power, it also makes them attractive targets for powerful cyber-attacks, mandating a security-by-design mindset from the start of development. (Hussaini et al., 2022).

Among the various types of cyber threats, Denial of Service (DoS) attacks are specifically dangerous and pose direct risks to the business continuity and operational integrity of Digital Twin environments. A DoS attack attempts to affect a service's availability by flooding its vital resources (memory, compute power, and network bandwidth) with fraudulent requests, making it unable to react to actual traffic. In the overall setting of a DT, such a type of attack may target the model's processing resources, the communication link between virtual model and physical sensor network, or the data intake endpoints (Sadeghi et al., 2020). The major consequence is the disruption in critical real-time synchronization, resulting in a digital model drifting situation in which the virtual representation gets more desynchronized from the physical environment, thus denying the twin's core goal (Anton et al., 2021). For example, a DoS attack on a DT in charge of a chemical processing plant can stop the virtual model from obtaining real-time data of pressure and temperature, preventing predictive warnings for possible failures and causing environmental and safety concerns. The effect is compounded in critical infrastructure sectors such as water treatment systems or smart grids, where the absence of control and visibility caused by a DoS attack might turn into significant widespread disruption and public safety risks (Cárdenas et al., 2019). According to research, the growth of vulnerable IoT devices has given rise to massive botnets that may be used to conduct massive DoS attacks on industrial CPS, which serve as the foundation for many DT implementations (Al-Hawawreh et al., 2022). While standard IT security has evolved several mitigation measures, they are frequently ill-suited for the severe safety-critical, high-reliability, and low-latency needs of DT and CPS systems (Mohan et al., 2023). Recent scientific work has begun to identify general security concerns for DTs, with Denial of Service (DoS) routinely highlighted as the primary threat to service and data availability (Liu et al., 2022). Studies have gone further into technical remedies like Software-Defined Networking (SDN) for adaptable filtering of traffic, ultimately to improve resilience (Yurekten & Demirci, 2021).

However, a major gap remains in the existing literature. Numerous studies reliably identify the presence of the DoS attack and suggest detection mechanisms and high-level prevention frameworks. But there is a noticeable lack of targeted research that methodically identifies and, more importantly, prioritizes the particular procedural, architectural, and technical factors within a DT system that most significantly increase the vulnerability to a strong DoS attack. Security allocation of resources can be ineffective and inefficient without a specific, concretely supported perception of which vulnerabilities are most critical, including insufficient system redundancy, the absence of resource throttling,

the cloud API gateway's request handling, and the edge device communication stack, or others. In order to close this gap, this study first identifies these causative factors, which are described in Table 1, and then uses an integrated methodology called AHP-weighted TOPSIS. This Multi-Criteria Decision-Making (MCDM) technique ranks the previously determined factors according to their criticality, and the rankings are further verified by an extensive sensitivity analysis. The outcomes offer a useful, prioritized structure for directing cybersecurity resources to successfully strengthen Digital Twin schemes against one of their most severe operational vulnerabilities.

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

Alternative	Causes of DoS Attacks	References
A1	Lack of traffic throttling or rate-limiting systems	Alcaraz and Lopez, 2022
A2	Poor filtering of malformed or high-volume requests	Alcaraz and Lopez, 2022
A3	Flooding via exposed interfaces	Otoom et al., 2025
A4	Missing redundancy and load balancing	Otoom et al., 2025
A5	Exploitable network services	Shaikh et al. 2023
A6	Lack of resource threshold policies	Kararslan et al., 2021
A7	Absence of DoS-specific safeguards in the communication stack	Varghese et al. 2022
A8	Weak scalability of system resources	Zemskov et al. 2024
A9	Exploiting processing power gaps across distributed systems	Abdullahi et al. 2024
A10	Poorly optimized web application architecture	Adilzhanova et al. 2025
A11	Absence of traffic anomaly detection	Sirigu et al. 2022
A12	Lack of synchronized data across DT layers	Abdullahi et al. 2024

3. Methods

AHP Weighted TOPSIS is an effective integrated framework of the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). This approach delivers a more accurate and complete final result by beginning with AHP to objectively determine the importance of each criterion and then applying TOPSIS to evaluate and rank the potential solutions on the basis of those weights (Zeng et al., 2021). The procedure is described 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 = λ_{max}w
b. Compute the eigenvalue: $\lambda_{max} = \frac{1}{n}\sum\frac{(Aw)_i}{w_i}$
c. Compute Consistency Index (CI) = (λ_{max}-n)/(n-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 DoS Key Factors

We have collected 12 alternatives of DoS attack factors on digital twin systems, which are shown in Table 1 of the literature review section. In order to perform the factor ranking, the key evaluation criteria or dimensions selected from the expert judgement of relevant fields are described in the following Table 2.

Table 2. Evaluation criteria for DoS attack factor ranking

ID	Criterion	Definition
C1	Exploitability	Technical ease in launching the attack (access, tools, skill)
C2	Impact on Physical Synchronization	Interruption of two-sided real-time communication in DT
C3	Impact on Data Integrity	Attacks that cause data loss, corruption, or mis-sequencing
C4	Resource Consumption	Exhaustion of host resources (CPU, RAM, bandwidth)
C5	Detection Difficulty	Difficulty in distinguishing between malicious and legitimate traffic
C6	Recovery Time (RTO)	Time to synchronize or restore the 'Golden Image.'
C7	Scalability	The attack's capacity to spread over DT nodes or layers

Experts compare each of the criteria 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) establishes the corresponding importance of the seven criteria for evaluation, applying Saaty's 1–9 scale. Table 3 and Table 4 show the pairwise comparison matrix and the normalized matrix (N), respectively.

Table 3. Pairwise Comparison Matrix (Synthetic Expert Judgement)

	C1	C2	C3	C4	C5	C6	C7
C1	1.00	0.33	0.33	0.50	2.00	2.00	1.00
C2	3.00	1.00	1.00	2.00	3.00	2.00	2.00
C3	3.00	1.00	1.00	2.00	3.00	2.00	2.00
C4	2.00	0.50	0.50	1.00	2.00	1.00	1.00
C5	0.50	0.33	0.33	0.50	1.00	1.00	0.50
C6	0.50	0.50	0.50	1.00	1.00	1.00	1.00
C7	1.00	0.50	0.50	1.00	2.00	1.00	1.00

Column Sums: [11.00, 4.16, 4.16, 8.00, 14.00, 10.00, 8.5].

Table 4. Normalized Matrix (N)

	C1	C2	C3	C4	C5	C6	C7
C1	0.091	0.079	0.079	0.063	0.143	0.200	0.118
C2	0.273	0.240	0.240	0.250	0.214	0.200	0.235
C3	0.273	0.240	0.240	0.250	0.214	0.200	0.235
C4	0.182	0.120	0.120	0.125	0.143	0.100	0.118
C5	0.045	0.079	0.079	0.063	0.071	0.100	0.059
C6	0.045	0.120	0.120	0.125	0.071	0.100	0.118
C7	0.091	0.120	0.120	0.125	0.143	0.100	0.118

Average of rows gives the weight vector: Weights (W) = [0.110, 0.236, 0.236, 0.130, 0.071, 0.100, 0.117]
Consistency Check:
Weighted Sum Vector: WSV=A × W = [0.7897, 1.7090, 1.7090, 0.9452, 0.5052, 0.7087, 0.8348]
Consistency Vector: WSV ÷ W = [7.1551, 7.2370, 7.2370, 7.2891, 7.1174, 7.0875, 7.1545]
Eigenvalue: λmax = (7.1551+7.2370+7.2370+7.2891+7.1174+7.0875+7.1545) ÷ 7 = 7.1825
Consistency Index Calculation: CI = (λmax - n) ÷ (n - 1) = (7.1825- 7) ÷ 6 = 0.0304
Consistency Ratio: RI (Random Index for n=7) = 1.32
CR = CI ÷ RI = 0.0304÷ 1.32 = 0.0230 < 0.10
Hence, the pairwise comparison matrix is consistent (CR = 0.0230 < 0.10).

Step 2: Construct the Decision Matrix 9Table 5 and Table 6)

Table 5. Decision Matrix

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

Step 3: Normalized decision matrix (R)

Table 6. Normalized Decision Matrix (R)

	C1	C2	C3	C4	C5	C6	C7
A1	0.360	0.328	0.299	0.334	0.355	0.336	0.267
A2	0.315	0.281	0.349	0.287	0.296	0.280	0.213
A3	0.315	0.328	0.299	0.287	0.296	0.280	0.320
A4	0.360	0.375	0.349	0.334	0.355	0.392	0.320
A5	0.315	0.281	0.299	0.287	0.296	0.280	0.267
A6	0.270	0.234	0.249	0.334	0.237	0.280	0.213
A7	0.270	0.234	0.249	0.287	0.296	0.280	0.213
A8	0.225	0.281	0.249	0.287	0.237	0.224	0.373
A9	0.270	0.234	0.299	0.239	0.237	0.224	0.320
A10	0.225	0.234	0.249	0.239	0.237	0.224	0.267

A11	0.270	0.281	0.249	0.287	0.296	0.280	0.320
A12	0.225	0.328	0.299	0.239	0.296	0.336	0.320

Step 4: Weighted Normalized Matrix
V = diag(W) × R, where W = [0.110, 0.236, 0.236, 0.130, 0.071, 0.100, 0.117]. Table 7 shows the weighted normalized matrix.

Table 7. Weighted Normalized Matrix

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
A1	0.0396	0.0774	0.0705	0.0435	0.0252	0.0336	0.0312
A2	0.0346	0.0664	0.0823	0.0373	0.0210	0.0280	0.0249
A3	0.0346	0.0774	0.0705	0.0373	0.0210	0.0280	0.0374
A4	0.0396	0.0885	0.0823	0.0435	0.0252	0.0392	0.0374
A5	0.0346	0.0664	0.0705	0.0373	0.0210	0.0280	0.0312
A6	0.0297	0.0553	0.0588	0.0435	0.0168	0.0280	0.0249
A7	0.0297	0.0553	0.0588	0.0373	0.0210	0.0280	0.0249
A8	0.0247	0.0664	0.0588	0.0373	0.0168	0.0224	0.0437
A9	0.0297	0.0553	0.0705	0.0311	0.0168	0.0224	0.0374
A10	0.0247	0.0553	0.0588	0.0311	0.0168	0.0224	0.0312
A11	0.0297	0.0664	0.0588	0.0373	0.0210	0.0280	0.0374
A12	0.0247	0.0774	0.0705	0.0311	0.0210	0.0336	0.0374

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 8 shows the positive ideal solution and the negative ideal solution.

Table 8. Positive Ideal Solution and Negative Ideal Solution

Solution Type	C1	C2	C3	C4	C5	C6	C7
Positive Ideal (A^+)	0.0396	0.0885	0.0823	0.0435	0.0252	0.0392	0.0437
Negative Ideal (A^-)	0.0247	0.0553	0.0588	0.0311	0.0168	0.0224	0.0249

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 9 shows the distance to the positive and negative ideal solution.

Table 9. Distance to Positive Ideal Solution and Negative Ideal Solution

Alternative	S^+ (Positive Ideal)	S^- (Negative Ideal)
A1	0.0281	0.0303
A2	0.0345	0.0251
A3	0.0307	0.0285
A4	0.0239	0.0346
A5	0.0348	0.0244
A6	0.0375	0.0217
A7	0.0369	0.0221
A8	0.0364	0.0229
A9	0.0370	0.0221
A10	0.0388	0.0203
A11	0.0319	0.0278
A12	0.0326	0.0271

Step 7: Compute Closeness Coefficient and Final Ranking

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

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

5. Sensitivity Analysis

This sensitivity analysis evaluates how stable the resultant DoS attack factor rankings are when AHP weights are slightly changed. This aids in confirming the resilience of the model.

Step 1: Define the Sensitivity Scenarios
We will generate 7scenarios, each of which increases one criterion weight by +10%, beginning from criterion 1 to criterion 7, while correspondingly decreasing the others so that the entire sum equals 1. In mathematical perception,

$$w_k' = w_k \times (1 + 0.1)$$
$$w_j' = w_j \times \frac{1 - w_k'}{1 - w_k}, \forall j \neq k$$

Step 2: Recalculate TOPSIS for Each Scenario
For each of the scenarios, replace the old AHP weight vector W_0 with the new W_k' and calculate:

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')

Each one of the seven criteria (C1–C7) for assessing DoS attacks was changed by ±10% on its own. All criteria weights were normalized following each variation in order to keep the total weights equal to one. The TOPSIS method was used again with altered weights for computing the weighted normalized decision matrix, ideal and negative-ideal solutions, Euclidean distances, and relative closeness (C_i) for each of the alternatives. Table 10 and Table 11 show the changes in the closeness coefficient and ranking of the alternatives under each criterion variation, respectively.

Table 10. Changes in the closeness coefficient of the alternatives in all criteria variation scenarios

Alternative	Original C_i	C1+10%	C1-10%	C2+10%	C2-10%	……	C7+10%	C7-10%
A1	0.519	0.524	0.516	0.528	0.513	……	0.520	0.514
A2	0.421	0.424	0.419	0.427	0.417	……	0.422	0.418
A3	0.482	0.486	0.480	0.487	0.479	……	0.483	0.479
A4	0.592	0.595	0.590	0.600	0.586	……	0.594	0.585
A5	0.412	0.414	0.411	0.415	0.410	……	0.414	0.410
A6	0.366	0.367	0.365	0.369	0.364	……	0.367	0.364
A7	0.375	0.376	0.374	0.378	0.373	……	0.376	0.373
A8	0.386	0.388	0.385	0.389	0.383	……	0.388	0.383
A9	0.374	0.376	0.373	0.378	0.372	……	0.375	0.372
A10	0.342	0.344	0.342	0.345	0.341	……	0.343	0.341
A11	0.466	0.468	0.464	0.470	0.463	……	0.468	0.463
A12	0.454	0.457	0.452	0.458	0.450	……	0.456	0.450

Table 11. Compact summary of changes in the ranking of the alternatives in all criteria variation scenarios

Alternative	Original Rank	C1±10%	C2±10%	C3±10%	C4±10%	C5±10%	C6±10%	C7±10%
A1	2	2-2	2-2	2-2	2-3	2-3	2-2	2-2
A2	6	6-6	6-6	6-6	6-6	6-6	6-6	6-6
A3	3	3-3	3-3	3-3	3-1	3-1	3-3	3-3
A4	1	1-1	1-1	1-1	1-2	1-2	1-1	1-1
A5	7	7-7	7-7	7-7	7-7	7-7	7-7	7-7
A6	11	11-11	11-11	11-11	11-11	11-11	11-11	11-11
A7	9	9-9	9-9	9-9	9-10	9-10	9-9	9-9
A8	8	8-8	8-8	8-8	8-9	8-9	8-8	8-8
A9	10	10-10	10-10	10-10	10-8	10-8	10-10	10-10
A10	12	12-12	12-12	12-12	12-12	12-12	12-12	12-12
A11	4	4-4	4-4	4-4	4-4	4-4	4-4	4-4
A12	5	5-5	5-5	5-5	5-5	5-5	5-5	5-5

The resultant top cause and rank stability for all 7 scenarios are shown in the results and discussion section.

6. Results and Discussion

After implementing the AHP weighted TOPSIS methodology on the attack factors of DoS on digital twin systems, we gained Table 12, which represents the closeness coefficient and final ranking for each of the alternative prime factors of DoS attack. This table is computed from the equation shown in step 7 of the method section.

Table 12. Closeness Coefficient and Final Ranking

Alternative	DoS Causative Factors	Closeness Coefficient	Rank (C_i)
A4	Missing redundancy and load balancing	0.592	1
A1	Lack of traffic throttling or rate-limiting systems	0.519	2
A3	Flooding via exposed interfaces	0.482	3
A11	Absence of traffic anomaly detection	0.466	4
A12	Lack of synchronized data across DT layers	0.454	5
A2	Poor filtering of malformed or high-volume requests	0.421	6
A5	Exploitable network services	0.412	7
A8	Weak scalability of system resources	0.386	8
A7	Absence of DoS-specific safeguards in the communication stack	0.375	9
A9	Exploiting processing power gaps across distributed systems	0.374	10

A6	Lack of resource threshold policies	0.366	11
A10	Poorly optimized web application architecture	0.343	12

The integration of the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) in this study gives a useful structure for prioritizing the causes of Denial of Service (DDoS) attacks. These rankings are based on different technical and operational criteria. The rankings show that missing redundancy and load balancing (A4) is the most critical factor having a closeness coefficient of 0.592, contributing to DoS vulnerability. This is followed by a lack of traffic throttling or rate-limiting systems (A1, C_i= 0.519) and Flooding via exposed interfaces (A3, C_i= 0.482). These rankings highlight that the main shortcomings of digital twin networks are poor traffic management systems and deficiencies in design. The highest weight (0.236) assigned to both impact on Physical Synchronization (C2) and impact on Data Integrity (C3) reflects how crucial it is to keep cyber-physical systems operating continuously. The comparatively lower weights given to detection Difficulty (C5=0.071) and recovery Time (C6=0.100) imply that experts emphasize proactive defensive architectures and give prevention priority over reactive measures. Alternatives such as A11 (Absence of traffic anomaly detection) and A12 (Lack of synchronized data across DT layers) grab the fourth and fifth places, respectively. The sensitivity analysis in 7 scenarios presents the verification of these results. Table 13 shows the resultant top cause and rank stability after performing the sensitivity analysis. The leading contributing factor (A4) remained almost consistent through all ±10% weight-variation scenarios. Notably, the minor rank changes show that the AHP-weighted TOPSIS framework can withstand slight differences in expert judgments, boosting trust in applications of strategic decision-making (Table 13).

Table 13. Top Cause and Rank stability after Sensitivity Analysis

Scenario	Varied Criterion	Top Cause (Rank 1)	Rank Stability
S1	C1 (Exploitability)	A4	Stable
S2	C2 (Impact on Physical Synchronization)	A4	Stable
S3	C3 (Impact on Data Integrity)	A4	Stable
S4	C4 (Resource Consumption)	A3	Unstable
S5	C5 (Detection Difficulty)	A3	Unstable
S6	C6 (Recovery Time)	A4	Stable
S7	C7 (Scalability)	A4	Stable

The consistency ratio of 0.023 (<0.10) confirms the logical sense and authenticity of expert opinions. The model illustrates the contribution of each factor, providing decision-makers with a data-driven framework for resource allocation in cybersecurity planning. The final outcomes offer practical recommendations for the deployment of digital twin security. Investing in redundant architectures, putting in place thorough rate-limiting procedures, and protecting network interfaces against flooding attacks should all be top priorities for organizations. The proposed integrated solution exhibits scalability and applicability that extend beyond the evaluation of DoS attacks. The AHP weighted TOPSIS framework serves as a tool for evaluating a range of cyber risks by changing the criteria and options. This versatility highlights the potential as a spreading tool for MCDM in the field of cybersecurity.

7. Conclusion

This study focused on identifying and systematically prioritizing the critical factors that contribute to Denial of Service (DoS) cyber-attacks in Digital Twin (DT) systems by combining the Analytic Hierarchy Process (AHP) with the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). Through the design and implementation of this integrated AHP-weighted TOPSIS model, this research addressed the fundamental challenges of a lack of a comprehensive and quantitative structure for guiding resource allocation of cybersecurity among various potential attack vectors. The reliability of the final rankings was confirmed through a sequential sensitivity analysis. To further improve the versatility of DT security evaluations, future research may add other cybersecurity related tools such as, Cloud ERP for protecting data while migration and integration take place between real entity and virtual entity. Overall, the results of this work provide a useful basis for enhancing cyber-resilience in more complicated and interrelated Digital Twin settings across industrial applications.

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., Zare, A., and Lazarova-Molnar, S., Cybersecurity in Distributed Industrial Digital Twins: Threats, Defenses, and Key Takeaways, Proceedings of the First International Workshop on Distributed Digital Twins (DiDit 2024), CEUR Workshop Proceedings, vol. 3755, paper 2, Groningen, the Netherlands, June 17, 2024.

Adilzhanova, S. A., Iglimanov, A. N., Tyulepberdinova, G. A., Salmanova, A. S., and Amirkhanova, G. A., The Use of Log Analysis to Identify DDoS Attacks and Determine User Behavior in the Process of Developing a Digital Twin of a Food Industry Enterprise, The Bulletin of KazATC, vol. 136, no. 1, pp. 107–118, 2025.

Alcaraz, C. and Lopez, J., Digital Twin: A Comprehensive Survey of Security Threats, IEEE Communications Surveys & Tutorials, vol. 24, pp. 1475–1503, 2022.

Al-Hawawreh, M., Sitnikova, E. and Aboutorab, N., Securing the Industrial Internet of Things against Ransomware Attacks: A Comprehensive Framework, IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3083–3092, 2022.

Anton, S. D., Kanoor, S., Fraunholz, D., and Schotten, H. D., Evaluation of Machine Learning-based Anomaly Detection in Industrial Control Systems, Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, pp. 1–8, 2021.

Cárdenas, A. A., Amin, S., and Sastry, S., Research Challenges for the Security of Control Systems, Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec), pp. 1–6, 2019.

Fuller, A., Fan, Z., Day, C. and Barlow, C., Digital Twin: Enabling Technologies, Challenges and Open Research, IEEE Access, vol. 8, pp. 108952–108971, 2020.

Grieves, M. and Vickers, J., Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems, in Transdisciplinary Perspectives on Complex Systems, Springer, Cham, pp. 85–113, 2017.

Hussaini, A., Qian, C., Liao, W., and Yu, W., A Taxonomy of Security and Defense Mechanisms in Digital Twins-based Cyber-Physical Systems, Proceedings of the 2022 IEEE International Conferences on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom) and Smart Data (SmartData), IEEE, pp. 597–604, 2022.

Kallapudi, V., Praneel, A. S. V., Sindhu, P., and Amiripalli, S. S., Securing Digital Twins: Lightweight Protocol Vulnerabilities and Mitigation Strategies, Proceedings of the Third International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2025), IEEE, pp. 427–433, Visakhapatnam, India, 2025.

Karaarslan, E. and Babiker, M., Digital Twin Security Threats and Countermeasures: An Introduction, Proceedings of the 14th International Conference on Information Security and Cryptology (ISCTURKEY 2021), IEEE, pp. 7–11, Ankara, Turkey, 2021.

Kaur, M. J., Mishra, V. P., and Maheshwari, P., The Convergence of Digital Twin, IoT, and Machine Learning: Transforming Business and Industries, Wireless Personal Communications, vol. 112, no. 3, pp. 1647–1669, 2020.

Khan, L. U., Saad, W., Han, Z. and Hong, C. S., Digital Twin for 6G: Taxonomy, Research Challenges, and Future Directions, IEEE Internet of Things Magazine, vol. 4, no. 2, pp. 70–77, 2021.

Lee, J., Bagheri, B. and Kao, H. A., A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems, Manufacturing Letters, vol. 3, pp. 18–23, 2019.

Liu, Y., Zhang, L., Yang, Y., and Wang, Y., A Novel Security Framework for Industrial Digital Twins in the 5G Era, IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6231–6240, 2022.

Mohan, A., Singh, A. and Kumar, S., DDoS Attack Detection in IoT Devices using Machine Learning: A Comprehensive Survey, Journal of Network and Computer Applications, vol. 212, article 103571, 2023.

Otoom, S., Risk Auditing for Digital Twins in Cyber Physical Systems: A Systematic Review, Journal of Cyber Security and Risk Auditing, vol. 2025, no. 1, pp. 22–35, 2025.

Sadeghi, M., Behnia, F. and Isazadeh, A., A Survey on Security and Privacy of Digital Twin, Journal of Network and Systems Management, vol. 28, no. 4, pp. 1025–1054, 2020.

Shaikh, E., Al-Ali, A. R., Muhammad, S., Mohammad, N., and Aloul, F., Security Analysis of a Digital Twin Framework Using Probabilistic Model Checking, IEEE Access, vol. 11, pp. 26358–26374, 2023.

Sirigu, G., Carminati, B. and Ferrari, E., Privacy and Security Issues for Human Digital Twins, Proceedings of the IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2022), IEEE, pp. 1–9, 2022.

Soudan, B., Cybersecurity of Digital Twins in Industrial IoT Environments, Proceedings of the Advances in Science and Engineering Technology International Conferences (ASET 2024), IEEE, Sharjah, UAE, 2024.

Tao, F., Zhang, H., Liu, A., and Nee, A. Y. C., Digital Twin in Industry: State-of-the-Art, IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, 2018.

Varghese, S. A., Ghadim, A. D., Balador, A., Alimadadi, Z., and Papadimitratos, P., Digital Twin-based Intrusion Detection for Industrial Control Systems, Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), IEEE, pp. 611–617, 2022.

Yurekten, O. and Demirci, M., A SDN-based Adaptive Defense Mechanism for DDoS Attacks in IoT Systems, IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3121–3135, 2021.

Zemskov, A. D., Fu, Y., Li, R., Wang, X., Karkaria, V., Tsai, Y., Chen, W., Zhang, J., Gao, R., Cao, J., Loparo, K. A. and Li, P., Security and Privacy of Digital Twins for Advanced Manufacturing: A Survey, ACM Computing Surveys, vol. 1, no. 1, pp. 1–35, 2024.

Zeng, Y.-P., Lin, C.-L., Dai, H.-M., Lin, Y.-C., and Hung, J.-C., Multi-performance Optimization in Electrical Discharge Machining of Al_2O_3 Ceramics Using Taguchi-based AHP Weighted TOPSIS Method, Processes, vol. 9, no. 9, article 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. Guided by a forward-looking mindset, he aspires to contribute to industrial systems that are sustainable and fundamentally more resilient.

Dr. Md. Saiful Islam is an accomplished academic and researcher in the field of Industrial Engineering. He completed his Bachelor of Science (B.Sc.) in Industrial & Production Engineering, as well as his Master of Science (M.Sc.) in Industrial Engineering and Management, from Khulna University of Engineering & Technology (KUET), Bangladesh. Dr. Islam further pursued and obtained his Ph.D. in Mechanical Engineering from the same prestigious institution. Currently, Dr. Islam serves as a Professor in the Department of Industrial Engineering and Management at KUET. Dr. Islam's research expertise basically extends into **combinatorial optimization**, **heuristics**, and **metaheuristics**. These methods are particularly valuable in real-world applications where traditional approaches may be too slow or infeasible due to the complexity of the problems.