GMR
The Original

THREAT-AWARE INDUSTRY 5.0 ATTACK GRAPH FRAMEWORK FOR CICIDS2017-BASED CYBER-PHYSICAL RISK ASSESSMENT

[1]Varsha Prafull Patil, [2]Dr. Sharada Ohatkar

[1]Research Scholar, Cummins College of Engineering for Women, Pune, Maharashtra, India, Email: varsha.patil@cumminscollege.in
[2]Professor and Research Guide, Cummins College of Engineering for Women, Pune, Maharashtra, India,
Email: sharada.ohatkar@cumminscollege.in

ABSTRACT
The swift development of Industrial Internet of Things (IIoT), cyber-physical systems, artificial intelligence and smart manufacturing technologies, the cybersecurity issues in Industry 5.0 are growing. In this study, a Threat-Aware Industry 5.0 Attack Graph (TAI5-AG) Framework is proposed for cyber-physical risk assessment from CICIDS2017 dataset. The proposed system consists of data preprocessing, Information Gain-based feature selection, multi-class threat detection, attack graph generation, Time-to-Compromise (TTC) analysis, threat likelihood estimation and restoration factor evaluation, which are all combined to evaluate security risks in interconnected industrial infrastructure. The framework illustrates propagation of attacks between critical assets like smart sensors, PLC controllers, industrial gateways, edge servers and digital twins. Through experimental evaluation, the proposed model is shown to be more accurate (99.12%), precise (99%), precise (99%) and F1 (99%) than the conventional machine learning approaches. The critical attack paths found using TTC analysis had compromise times between 25 and 5 minutes, with the highest threat likelihood score of 0.94 coming from the Botnet attacks, and the highest cyber-physical risk score of 0.91 from the same attacks. In addition, the restoration factor rose from 1.12 in the case of low impact attacks to 2.36 in the case of severe attacks. The results have verified that the proposed framework effectively enhances the threat prioritization, cyber resilience, and proactive risk management of cyber-physical systems in Industry 5.0.

KEYWORDS: Industry 5.0, Cyber-Physical Systems (CPS), Attack Graph Analysis, CICIDS2017 Dataset, Cyber Risk Assessment, Intrusion Detection System (IDS)

1. INTRODUCTION

The convergence of the terms “operational technology (OT)”, “information technology (IT)”, artificial intelligence, “industrial Internet of Things (IIoT)”, and autonomous decision making systems have made the shift from Industry 4.0 to Industry 5.0 happen faster. While Industry 4.0 is mainly focused on automation and digitalization, Industry 5.0 is more interested in the human-centric, resilient and sustainable industrial ecosystem where intelligent machines work collaboratively with human operators [1]. But with increasing interdependency between cyber and physical aspects, the attack surface of cyber-physical systems (CPSs) has grown considerably, leading to increasingly complex cyber attacks to critical industrial assets. Infrastructure for industrial control systems, smart manufacturing plants, autonomous robotics, and production environments with connections are increasingly the victims of ransomware, denial-of-service attacks, reconnaissance, privilege escalation and advanced persistent threats [3]. Such attacks may affect continuity of operations, safety features, and result in significant economic and societal impacts [4].

Typical cybersecurity risk assessment strategies are static vulnerability evaluation and isolated security measures, which are not adequate to represent the dynamic propagation of attacks in Industry 5.0 settings [5]. To reach their goals, cyber adversaries often attempt to take advantage of several vulnerabilities in different interconnected devices, networks, and applications [6]. Therefore, it has become vital for proactive cyber-physical risk management to be aware of attack paths and the mechanisms of propagation of threats. Attack graph modeling has become a very effective method that can be used to represent attack sequences, pinpoint attack nodes, and assess the security exposure of the entire system [7]. An attack graph is a systematic mapping of attack relationship, which can be used to give the information of how adversarial may navigate through industrial infrastructure and how many critical assets may be compromised [8].

Figure 1: Industry 5.0 smart factory ecosystem emphasizing human-centricity, sustainability, and resilience [9]

New developments in threat intelligence and machine learning have also improved the analysis of attacks in the attack graph for data-driven threat detection and risk prioritization [10]. The CICIDS2017 dataset is one of the most popular datasets available in open source cybersecurity research, as it contains a wide variety of both benign and malicious network traffic, including Distributed Denial of Service (DDoS) attacks, brute force attacks, botnet attacks, infiltration attacks, web-based attacks, and port scanning attacks [11]. The dataset can be used for realistic network behavior patterns that closely emulate the present enterprise and industrial communication environment, which is useful for the development and validation of cyber threat assessment frameworks [12]. Combining the attributes of attacks with the attack graph modeling will provide a practical solution for assessing the cyber-physical risks in Industry 5.0 infrastructures and determining the attack graph's high-risk attack paths [13].

For this study, a Threat-Aware Industry 5.0 Attack Graph Framework for CICIDS2017-Based Cyber-Physical Risk Assessment [14] is proposed. The framework combines the attack graph generation, threat severity analysis, attack path prioritization and cyber-physical risk quantification to give the security assessment mechanism a holistic approach. The proposed model uses extracted patterns of attacks from the CICIDS2017 dataset to analyze possible attack propagation scenarios and estimate their probability and consequences for interconnected industrial assets [15]. This framework allows security decision-makers to make proactive decisions by being able to detect critical vulnerabilities, optimize defense strategies and improve industrial resilience against new security threats [16].

The rest of this paper is organized as follows: Section 2 includes a detailed literature review of the existing work on Industry 5.0 Cybersecurity, Attack graph modeling, Cyber-Physical Risk assessment and Intrusion detection datasets. In section 3, the proposed threat-aware attack graph framework is described, which includes data preprocessing, attack graph construction, Threat Scoring, and Risk evaluation mechanisms. The experimental setup and implementation on the CICIDS2017 dataset is discussed in section 4. The result and performance analysis of the proposed framework is given in Section 5. Lastly, in Section 6, the study will be summarized, and future research paths for cyber-physical security in Industry 5.0 will be proposed. The aims of the Study are:

- To develop a threat-aware attack graph framework for modeling cyber attack propagation in Industry 5.0 cyber-physical systems.
- To utilize the CICIDS2017 dataset for identifying and analyzing diverse cyber attack behaviors affecting interconnected industrial environments.
- To quantify cyber-physical risks through attack path evaluation, threat severity assessment, and critical asset impact analysis.
- To improve proactive cybersecurity decision-making by prioritizing high-risk attack scenarios and recommending effective mitigation strategies.

2. LITERATURE REVIEW

Nandiya et al. (2026) [17] introduced the BRIDG-ICS framework, a knowledge graph and AI-based threat intelligence integration for the attack path simulation and evaluation of cyber resilience in Industry 5.0 environments. Govindarajan et al., 2026 [18] proposed the Aegis-5 adaptive ensemble intrusion detection framework and obtained 99.98% accuracy and 99.96% F1 score on the datasets related to industrial IoT. Dasarla et al. (2026) [19] proposed to use Graph Neural Networks for IIoT intrusion detection by significantly reducing the feature dimensionality from 72 to 40 with competitive performance. To achieve this, Kanca et al. [20] created the GraphDL model with the combination of visibility graph and CNN which produced accuracy ranging from 75.81% to 96.73%. ZuraNet and GRiQ-Net hybrid IDS models were proposed by Sridevi et al. [21] for SCADA system and achieved an accuracy of 99.60% and a detection rate of more than 99.35%.

Mishra et al. (2026) [22] implemented deep learning, blockchain logging, and Zero Trust architecture, achieving 89-91% accuracy and macro F1-scores up to 0.91. Ogunmolu et al. (2025) [23] adopted ConvLSTM3D and GNN models in the context of Cyber-Mechanical security, achieving 88.86% accuracy and 0.89 AUC. Using data fusion from multiple sources and attack path prediction, Oladele et al. (2025) [24] designed an AI-based framework for cyber-physical security for smart cities. To detect anomalies in intelligent networks, Yang et al. [25] introduced GNN-NAD, which combines GraphSAGE and attack graphs. Chinthamu et al. (2025) [26] proposed a blockchain based adaptive CPS security architecture to enhance the resilience and scalability. The edge computing approach with KNN and Random Forest was used by Zhukabayeva et al. (2025) [27] and yielded almost perfect precision, recall and F1 scores. Chowdhury et al. (2025) [28] summarized 142 studies and emphasized the better performance of deep learning models in real-time cyber risk assessment.

Cherukuri et al. (2025) [29] proposed a CA-DSCNN framework which successfully classified the CICIDS2017 and UNSW-NB15 datasets with 99.5% and 96.7% accuracy, respectively. Azar et al. [30] implemented EMHDL-AD attack detection model based on hierarchical deep learning and quantum optimization. Gajula et al. (2024) [31] and Matta et al. (2024) [32] successfully applied GNNs to cyber risk prediction and threat propagation analysis. Raza et al. (2024) [33] was able to get accuracy of 97.86% and F1 score of 97.31% with CNN-Transformer architecture. To validate the effectiveness of neural-network-based risk prediction in smart hospitals, Islam et al. (2024) [34] analysed 112 studies. The transformer models for Industry 5.0 security have shown to be more effective at detecting intrusions, according to Salam et al. 2023 [35]. Kandhro et al. (2023) [36] introduced a GAN-based intrusion detection framework which demonstrated an accuracy rate of 95–97% for various categories of cyberattacks. Overall, the studies reveal the increasing success of AI, Deep Learning, Graph Analytics, and Attack Graph techniques, but a unified Attack graph framework to assess cyber-physical Risk of CICIDS 2017 data is relatively underexplored.

While there is remarkable advancement in both AI-based intrusion detection and graph neural networks and cyber-physical security frameworks, most studies have concentrated on the accuracy of attack detection without considering a thorough cyber-physical risk assessment. Most methods do not utilize the requirements of Industry 5.0, do not consider attack graph-based propagation modelling of threats, and have not incorporated quantitative risk assessment based on realistic attack datasets. Moreover, there is still limited research that integrates the attack behaviours used in CICIDS2017 with the threat-aware attack graph generation to uncover the critical attack paths and asset level risk exposure. This gap leads to the development of a uniform framework for a cyber-physical risk assessment in the Industry 5.0 context.

Table 1: Recent Studies on AI-Based Cyber-Physical Security and Intrusion Detection in Industry 5.0

Ref.	Author(s) & Year	Proposed Framework/Method	Dataset/Application	Key Results
[17]	Nandiya et al. (2026)	BRIDG-ICS framework integrating Knowledge Graph and AI-based threat intelligence	Industry 5.0 cyber resilience assessment	Enabled attack path simulation and cyber resilience evaluation
[18]	Govindarajan et al. (2026)	Aegis-5 Adaptive Ensemble Intrusion Detection Framework	Industrial IoT datasets	Accuracy: 99.98%, F1-Score: 99.96%
[19]	Dasarla et al. (2026)	Graph Neural Network (GNN)-based intrusion detection	IIoT environments	Reduced feature dimensions from 72 to 40 while maintaining competitive performance
[20]	Kanca et al. (2026)	GraphDL model combining Visibility Graph and CNN	Industrial intrusion detection	Accuracy ranged from 75.81% to 96.73%
[21]	Sridevi et al. (2026)	ZuraNet and GRiQ-Net Hybrid IDS	SCADA systems	Accuracy: 99.60%; Detection Rate: >99.35%
[22]	Mishra et al. (2026)	Deep Learning, Blockchain Logging, and Zero Trust Architecture	Cyber-physical security systems	Accuracy: 89–91%; Macro F1-score: up to 0.91
[23]	Ogunmolu et al. (2025)	ConvLSTM3D and GNN models	Cyber-Mechanical security	Accuracy: 88.86%; AUC: 0.89
[24]	Oladele et al. (2025)	AI-based cyber-physical security framework using multi-source data fusion	Smart cities	Improved attack path prediction and security assessment
[25]	Yang et al. (2025)	GNN-NAD integrating GraphSAGE and attack graphs	Intelligent networks	Enhanced anomaly detection capability

[26]	Chinthamu et al. (2025)	Blockchain-based adaptive CPS security architecture	Cyber-Physical Systems	Improved resilience and scalability
[27]	Zhukabayeva et al. (2025)	Edge computing with KNN and Random Forest	Intelligent networks	Achieved near-perfect Precision, Recall, and F1-score
[28]	Chowdhury et al. (2025)	Systematic review of AI-based cyber risk assessment	Review of 142 studies	Deep learning models outperformed traditional methods
[29]	Cherukuri et al. (2025)	CA-DSCNN framework	CICIDS2017 and UNSW-NB15 datasets	Accuracy: 99.5% and 96.7%, respectively
[30]	Azar et al. (2025)	EMHDL-AD attack detection model using hierarchical DL and quantum optimization	Intrusion detection systems	Demonstrated effective attack detection performance
[31]	Gajula et al. (2024)	Graph Neural Networks for cyber risk prediction	Cybersecurity applications	Improved cyber risk prediction accuracy
[32]	Matta et al. (2024)	GNN-based threat propagation analysis	Cyber-physical systems	Enhanced threat propagation analysis
[33]	Raza et al. (2024)	CNN-Transformer architecture	Intrusion detection	Accuracy: 97.86%; F1-score: 97.31%
[34]	Islam et al. (2024)	Review of neural network-based risk prediction	Smart hospitals (112 studies)	Validated effectiveness of neural-network-based risk prediction
[35]	Salam et al. (2023)	Transformer-based security models	Industry 5.0 environments	Superior intrusion detection performance
[36]	Kandhro et al. (2023)	GAN-based intrusion detection framework	Cyberattack detection	Accuracy: 95–97% across attack categories

3. RESEARCH METHODOLOGY

The proposed Threat-Aware Industry 5.0 Attack Graph Framework is presented in this section based on the CICIDS2017 dataset. The methodology involves data preprocessing, feature selection, threat detection, attack graph generation, Time-to-Compromise analysis, threat likelihood estimation, restoration factor evaluation and assessment of performance. Figure 2 represents the proposed work framework.

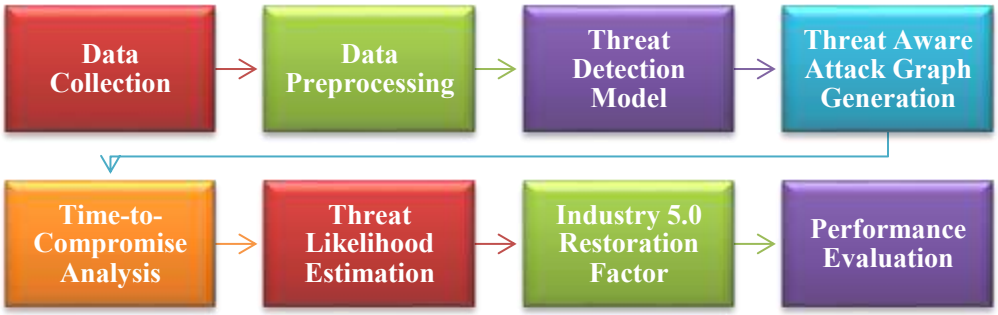

Figure 2: Framework of proposed work

3.1 Data Collection

The CIC-IDS2017 (Canadian Institute for Cybersecurity Intrusion Detection System 2017) dataset [37] is among the most popular standard datasets used in research on Network Intrusion Detection Systems. It was designed by the Canadian Institute for Cybersecurity at the University of New Brunswick with realistic benign and malicious network traffic captured over 5 days. Common Cyber Attack types that are present in the dataset are Distributed Denial of Service (DDoS), Denial of Service (DoS), Port Scanning, Brute Force, Infiltration and Web Attacks, Botnet. Offers more than 80 network flow features derived by CICFlowMeter such as packet statistics, flow duration and traffic behaviour metrics. CIC-IDS2017 is widely utilized in the field of machine learning and deep learning, cyber security analytics and risk assessment research.

3.2 Data Preprocessing

- **Missing Value Removal**

In the CICIDS2017 dataset there are some missing, undefined and infinite values created during the process of collecting network traffic. The behavior of these values can also impact the performance of machine learning models, and they may introduce biases into the model's predictions. Hence, all missing records are located and deleted prior to any other processing. Data cleaning helps ensure data consistency, minimizes data noise, and increases the accuracy of the model. Records with NaN, NULL or infinite values are removed, and the traffic

flows that contain valid data are kept for analysis. The cleaned dataset serves as a solid basis for attack detection, Cyber-physical risk assessment.

$$D_{clean} = D_{total} - D_{missing} \quad (1)$$

where D_{clean} is the cleaned dataset, D_{total} is the total number of records, and $D_{missing}$ represents records containing missing values.

• Data Normalization

The features presented in the CICIDS2017 have various scales and units. For instance, the Flow Duration is measured in millions but the counts of packets in the flows are relatively small. Min-Max normalization is used to avoid the domination of the learning process by large valued features. The idea is to transform all feature values into a range of [0,1] so that they all contribute equally in training the model. Normalization speeds up learning rates for classifiers, makes the numbers more stable and provides a uniform representation of features in intrusion detection models, which helps to raise the accuracy of the models.

$$X_{norms} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (2)$$

where X is the original feature value, X_{min} is the minimum value, and X_{max} is the maximum value.

• Feature Selection Using Information Gain

CICIDS2017 has over 80 features coming from the network traffic, many of which will be redundant or irrelevant. To find the most informative attributes to classify attacks, feature selection is carried out. Information Gain (IG) is defined as the decrease in uncertainty of the target class by observing a feature. The higher the IG higher the power of discrimination, so we choose features with these high values and train our model on them. This process helps to minimize the computational complexity, reduces overfitting, and enhances the efficiency of intrusion detection, and retains important information related to critical attacks.

$$IG(X) = H(Y) - H(Y|X) \quad (3)$$

where H(Y) represents the entropy of the class label and H(Y|X) denotes the conditional entropy after observing feature X.

3.3 Threat Detection Model

The threat detection model should classify the network traffic flows of CICIDS2017 dataset in to different classes such as Benign, DDoS, DoS, Port Scan, Botnet, and Web Attack. The network flow features extracted from the preprocessed data are given to the machine learning classifier for the purpose of training and testing after feature selection. The model is trained to recognize the patterns of normal and malicious traffic and detects suspicious activity in real-time. Behavioral traffic is considered benign when it is legitimate network traffic and attack classes are considered attack classes against network resources. The classifier facilitates accurate intrusion detection, helps to generate attack graphs, and forms the basis for cyber-physical risk assessment in Industry 5.0 environments.

3.4 Threat Aware Attack Graph Generation

The Threat-Aware Attack Graph Generation module simulates the potential attack path that an adversary can take to attack Industry 5.0 assets. After the attack graph methodology, the attackers proceed to multiple vulnerable nodes like IIoT devices, smart sensors, PLC controllers, industrial gateways, edge servers, and digital twins, to gain access to the target asset. Nodes are attack states, and edges are states that can be exploited between assets. The resulting attack graph allows the visualization of attack propagation, the identification of critical attack paths and the estimation of the cyber risk. The attack graph is mathematically represented as:

$$AG = (N, E) \quad (4)$$

where (N) denotes the set of attack states and (E) represents exploitable attack transitions. The total attack path cost is calculated using:

$$APC = \sum_{i=0}^{n} TTC_i \quad (5)$$

where (TTC_i) represents the Time-To-Compromise of each attack step along the attack path.

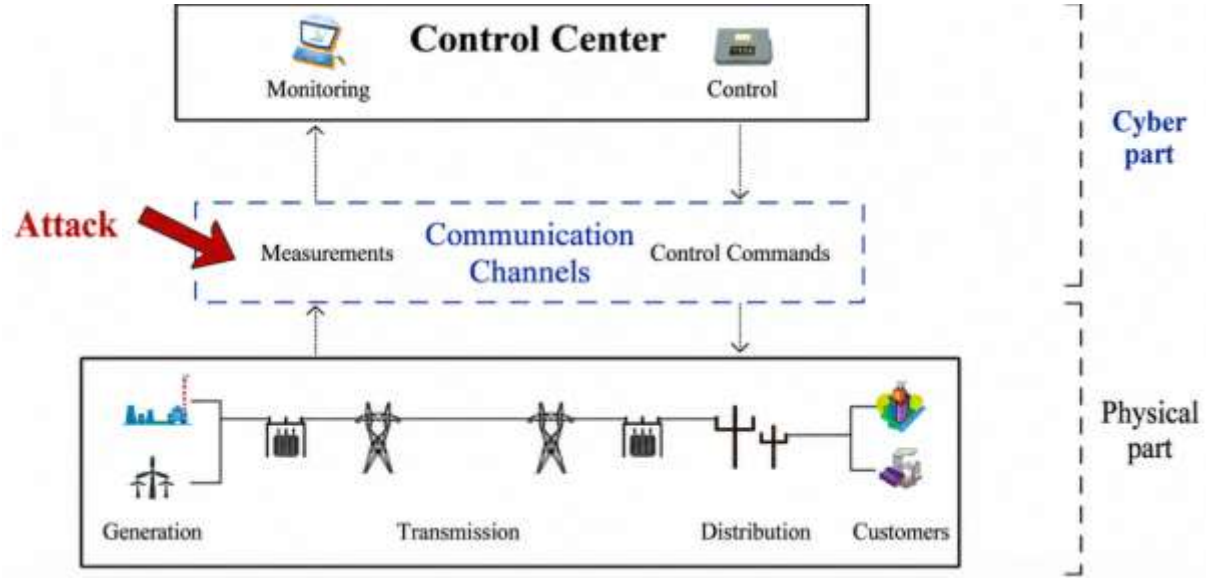

Figure 3: Cyber-Physical Attack on Communication Channel [38]

3.5 Time-to-Compromise Analysis

The time-to-compromise (TTC) analysis is a method of estimating the effort and time needed for an attacker to successfully compromise one or more critical assets in Industry 5.0 via a series of attacks. The attack graph analyzes vulnerabilities, attack paths and attacker capabilities to establish the speed at which a cyber threat can spread through the system. A lower TTC suggests the higher risk of security attacks since the attacker is able to reach the target assets faster. The Local TTC is the time that the individual attack step required, while the Global TTC is the overall compromise time for the entire attack path. Local TTC is defined as:

$$\mathrm{TTC_{local}} = \mathrm{f(V, K)} \quad (6)$$

where (V) denotes the number of vulnerabilities and (K) represents the attacker skill level. The overall compromise time is determined using:

$$\mathrm{TTC_{global}} = \max(\mathrm{TTC_1}, \mathrm{TTC_2}, \dots, \mathrm{TTC_N}) \quad (7)$$

where $(\mathrm{TTC_1}, \mathrm{TTC_2}, \dots, \mathrm{TTC_N})$ are the compromise times of individual attack stages.

3.6 Threat Likelihood Estimation

Threat likelihood estimation is used to estimate the likelihood of a successful attack on a target asset before the attack is detected. The probability is based on the relationship of Average Time to Compromise (TTC) and Mean Time To Detect (MTTD). When it takes attackers less time to break through a system than security teams to detect an attack, chances of a successful attack increase. On the other hand, the bigger the TTC, the lower the probability of success in attacking. This is a helpful indicator for identifying critical threats and for conducting a proper cyber-physical risk assessment in Industry 5.0 systems.

$$\mathrm{Likelihood(j)} = \frac{\mathrm{MTTD}}{\mathrm{TTC_{avg}+MTTD}} \quad (8)$$

The likelihood value ranges between 0 and 1, where higher values indicate greater attack success probability.

3.7 Industry 5.0 Restoration Factor

To measure the effort needed to put back to normal activity after a successful cyber attack, there is a measure of the Industry 5.0 Restoration Factor. It evaluates the resilience of a cyber-physical assets using the capacity of the affected components, the failure status of these components and the time required to recover. The larger a restoration factor, the more complex and disruptive it will be to restore. This metric helps organizations assess the costs associated with recovery following an attack, and add resilience to the cyber-physical risk assessment. The restoration factor is defined as:

$$\mathrm{F_r} = \mathrm{e}^{\frac{\sum \mathrm{a_i P_i}}{\mathrm{P_{total}}} \times \mathrm{T}} \quad (9)$$

where (P_i) represents the asset capacity, (a_i) denotes the asset failure status (0 or 1), (P_{total}) is the total system capacity, and (T) is the restoration time index. This formulation captures both the extent of asset damage and the recovery duration following a cyber incident. The figure 4 illustrates an Industry 5.0 framework where techno-functional principles and human-centric values integrate with emerging technologies such as AI, IoT, cobots, digital twins, and augmented reality to enhance engineering, training, maintenance, quality control, machine operations, assembly, and sustainable manufacturing processes.

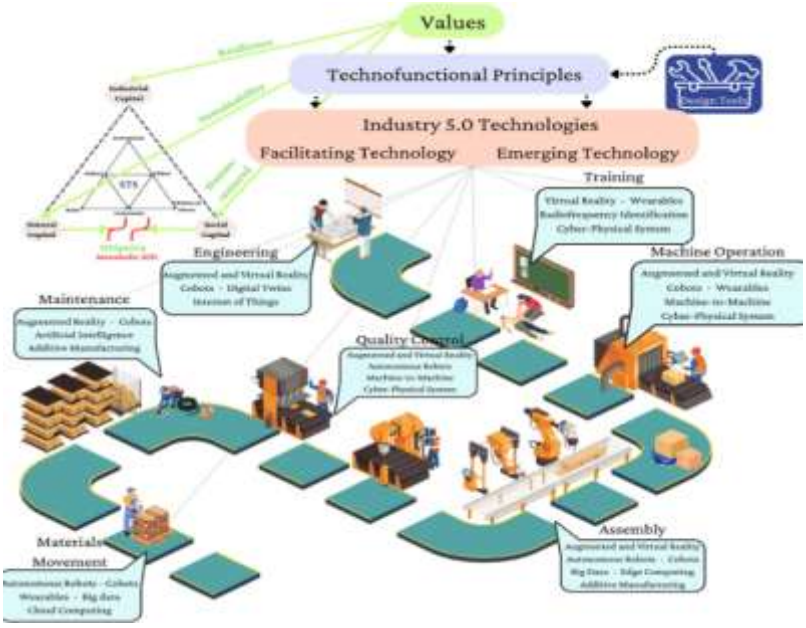

Figure 4: Industry 5.0 Smart Manufacturing Architecture [39]

3.8 Performance Evaluation

The proposed model is assessed for the effectiveness with the commonly used classification metrics.

- **Accuracy:**

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

- **Precision:**

$$\text{Precision} = \frac{TP}{TP+FP} \quad (11)$$

- **Recall:**

$$\textbf{Recall} = \frac{TP}{TP+FN} \quad (12)$$

- **F1-Score:**

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision}+\text{Recall}} \quad (13)$$

- **Area under Curve (AUC):**

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (14)$$

4. RESULT AND ANALYSIS

This section analyzes the effectiveness of the proposed framework by conducting several experiments. The framework is examined in terms of performance metrics, attack graph characteristics, threat likelihood, Time-to-Compromise values, restoration factors and cyber-physical risk scores, to validate the capability of the framework in performing security assessment in Industry 5.0. In the following figure 5, the performance of F1-score for three different framework architectures is compared in different scenarios A, B and C. The proposed TAI5-AG model has the highest performance with F1 score of 0.92, 0.96, and 0.93 for Scenarios A, B, and C, respectively. The Static AG framework, on the other hand, has lower scores of 0.73, 0.70 and 0.71, and the Feature-Only model scores 0.82, 0.84 and 0.83. The best performance is achieved in scenario B, where TAI5-AG reaches a score of 0.96, making a 26 percentage point improvement compared with Static AG and a 12 percentage point improvement compared with Feature-Only. The results show that the incorporation of threat-aware attack graph analysis can greatly improve attack detection capability and can increase the accuracy of cyber-physical risk assessments for various attack scenarios in Industry 5.0.

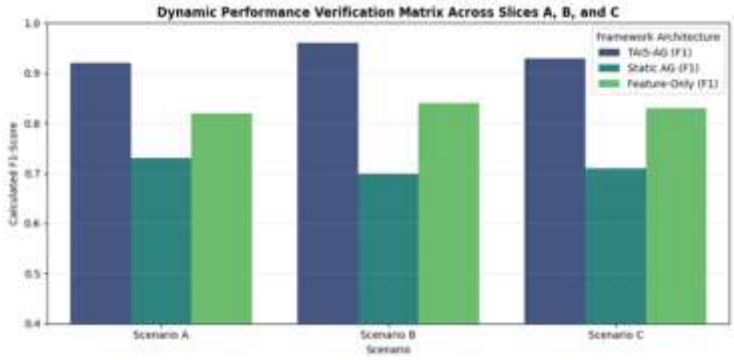

Figure 5: Dynamic Performance Verification across Different Attack Scenarios

The figure 6 shows the distribution of the network traffic classes in the dataset CICIDS2017. The majority of the network traffic is in the Benign class, which accounts for about 2.27 million records. In attack categories, there are approximately 252,673 records for DoS, 158,930 records for PortScan and 128,027 records for DDoS. The Botnet class is the least abundant class, consisting of only 1966 data records. This severely unbalanced distribution reflects the difficulty of correctly identifying minority attack classes and thus motivates the development of powerful threat detection and attack graph-based cyber-physical risk assessment models in Industry 5.0.

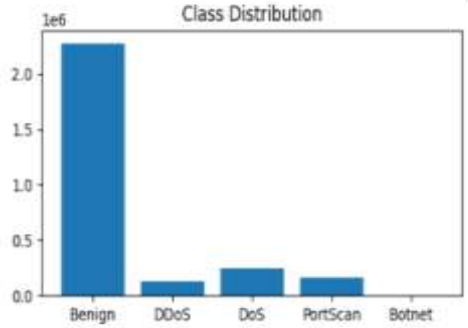

Figure 6: Class Distribution of CICIDS2017 Dataset

The figure 7 shows the number of missing values in the dataset CICIDS2017 before and after the data cleaning process. The data set had about 12,000 missing and/or invalid values at the very beginning which might affect the extraction of features, training the model and the accuracy of the classification. The missing value removal procedure resulted in no missing values (full data cleaning). This equates to a 100% reduction in the number of records missing, meaning a high quality dataset can be used for further analysis. The preprocessing helps to ensure consistency of the data, eliminate noise, increase the stability of the model and offer a solid basis for accurate threat detection and cyber-physical risk assessment.

Figure 7: Missing Values Before and After Data Cleaning

The figure 8 displays the Information Gain (IG) score of the most relevant features that were selected out of the CICIDS2017 dataset. The strongest contribution to attack classification is not only from Flow Duration with the highest IG value (0.91), but also from the impact of the same feature on the accuracy of attack classification.The impact of the same feature on the accuracy of attack classification is not only high for Flow Duration but also for the highest IG value of approximately 0.91. It is followed by Packet Length Mean (0.88), Flow Bytes/s (0.85), Flow Packets/s (0.82), Bwd Packet Length Standard Deviation (0.79), and Average Packet Size (0.76). The high IG scores indicate that these features include a significant amount of discriminative information that could be used to classify benign and malicious traffic. The choice of these features helps to lower the dimensionality, computational complexity and makes the proposed threat detection framework efficient and accurate.

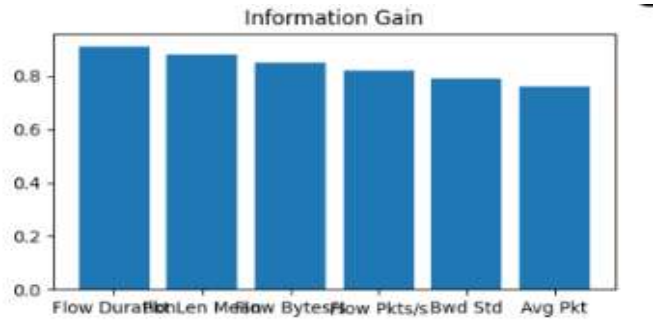

Figure 8: Information Gain-Based Feature Selection

The figure 9 shows the performance of various models on Accuracy, Precision, Recall, and F1-Score: Random Forest (RF), SVM, XGBoost, CNN, and TAI5-AG. The proposed TAI5-AG model has the best accuracy, precision, recall, and F1-score of 99.12%, 99%, 99%, and 99%, respectively, and outperforms the other models in terms of attack detection capability. CNN and XGBoost also show good accuracy of 98.67% and 98.23%, respectively. SVM has the lowest accuracy of 94.81% and F1 score of 92%. The results verify that the incorporation of threat-aware attack graph analysis greatly improves the classification effectiveness and Cyber-physical threat detection.

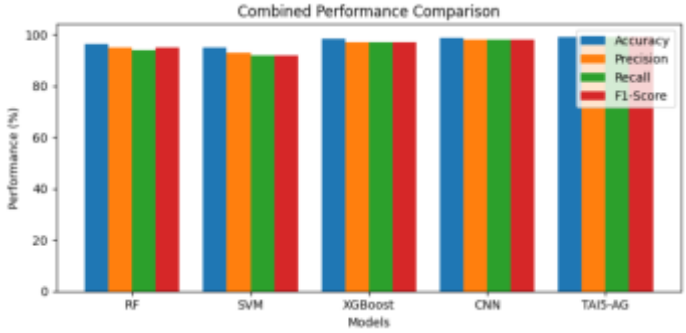

Figure 9: Combined Performance Comparison of Accuracy, Precision, Recall, and F1-Score across Different Models

The figure 10 shows some of the Time-to-Compromise (TTC) values determined based on the threat-aware attack graph for five attack paths. Path P1 is the most difficult of all paths to attack, with a TTC of 25 minutes. The values of the TTC's gradually decrease along the following paths: P2 = 18 minutes, P3 = 12 minutes, P4 = 8 minutes and P5 = 5 minutes. The lowest TTC observed for P5 indicates the weakest attack path and the greatest security threat. The degradation of the TTC trend reveals important attack pathways that must be designated as the focus of mitigation efforts to build up cyber resilience and enhance the cyber-physical risk management in Industry 5.0.

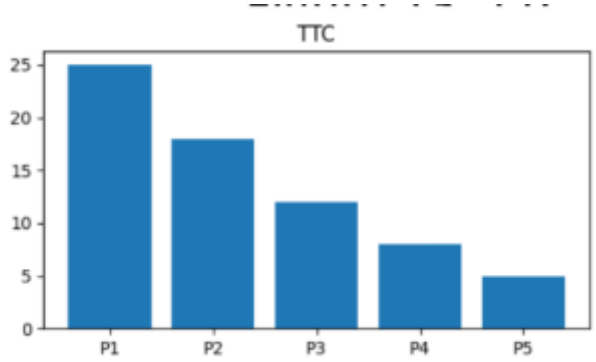

Figure 10: Time-to-Compromise (TTC) Analysis Across Attack Paths

Figure 11 shows the restoration factor that occurs at various impact levels of cyber attacks in an Industry 5.0 environment. The restoration factor rises from 1.12 for Low Impact scenario up to 1.45 for Medium Impact, 1.88 for High Impact and 2.36 for Severe Impact. Such an increase means that more serious attacks necessitate a much more elaborate recovery process, allocation of resources and recovery time. An operational disruption and recovery complexity is indicated by the highest restoration factor of 2.36 after severe cyber incidents. The findings show that resilience-aware risk assessment and proactively recovery planning should be important for the continuity of operational activities in cyber-physical industrial systems.

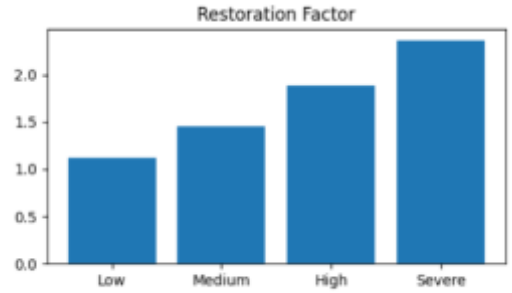

Figure 11: Industry 5.0 Restoration Factor Under Different Impact Levels

The 12 threat likelihood values of different cyber attacks in the CICIDS2017 dataset are shown in figure 12. The highest likelihood score is 0.94 for Botnet attacks, which have the highest likelihood of being able to compromise target assets before being detected among all attack categories. The probability of success of DDoS and DoS attacks are 0.91 and 0.87, respectively, which shows that Industry 5.0 systems are vulnerable to serious cyber threats. The moderate attacks include Web Attacks (0.82) and the lowest value is given to Port Scan attacks (0.79). The results show Botnet and DDoS attacks are the most critical attacks that must be given top priority in cyber-physical risk mitigation and security management.

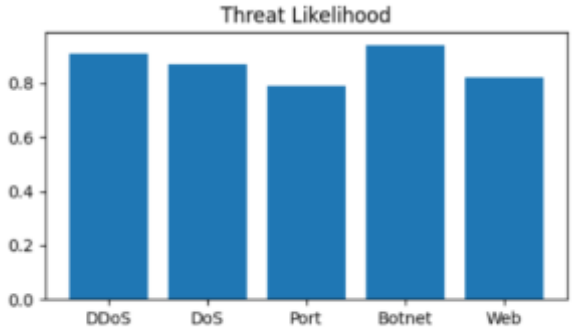

Figure 12: Threat Likelihood Analysis for Different Cyber Attack Types

Figure 13 shows the overall cyber-physical risk values of each attack category in the Industry 5.0 environment. Botnet attacks have the highest risk score (0.91), having the greatest impact on critical assets and system operations. Following the DDoS attacks is a risk of 0.84, and DoS attacks come in with a risk of 0.79. The Web Attacks have a moderate risk score of 0.74, while Port Scan attacks have the lowest risk score of 0.62. From the results, it can be concluded that Botnet and DDoS attack are the most hazardous attacks for CPI because of the high likelihood and operational impact. The results are in agreement with the success of the proposed threat-aware attack graph framework in terms of threat ranking and identifying critical threats for proactive security management and resilience planning.

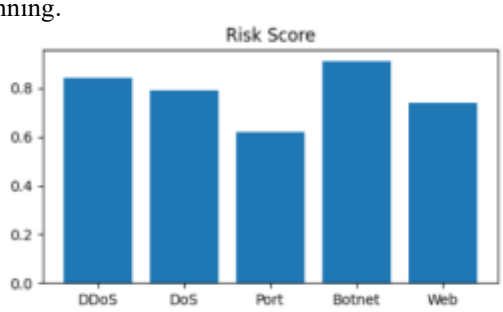

Figure 13: Cyber-Physical Risk Score Analysis for Different Attack Types

Table 2 presents the cyber-physical risk assessment results for different attack categories in the Industry 5.0 environment. The proposed threat-aware attack graph framework identifies Botnet (0.91) and DDoS (0.84) attacks as the most critical threats due to their high likelihood and severe operational consequences. In contrast, Port Scan attacks (0.62) exhibit the lowest risk level, indicating limited direct impact on cyber-physical infrastructure. These findings demonstrate the effectiveness of the proposed framework in threat prioritization, critical attack identification, and proactive resilience planning for Industry 5.0 systems.

Table 2: Cyber-Physical Risk Values for Different Attack Categories in Industry 5.0

Attack Category	Cyber-Physical Risk Value	Risk Level
Botnet Attack	0.91	Very High

DDoS Attack	0.84	High
DoS Attack	0.79	High
Web Attack	0.74	Moderate
Port Scan Attack	0.62	Low

5. CONCLUSION

In this study, a Threat-Aware Industry 5.0 Attack Graph (TAI5-AG) Framework for cyber-physical risk assessment was proposed, employing the CICIDS2017 dataset. The framework consists of threat detection, attack graph generation, Time-to-Compromise (TTC) analysis, threat likelihood estimation and restoration factor evaluation, and can be used to cover a comprehensive assessment of cyber risk in Industry 5.0 environments. Experimental results showed that the proposed TAI5-AG model outperformed the classical machine learning models like SVM (94.81% accuracy) and Random Forest (96.42% accuracy) with the highest detection performance of 99.12% accuracy, 99% precision, 99% recall and 99% F1-score. The attack graph analysis determined sensitive attack paths: TTC value dropped from 25 minutes (P1) to 5 minutes (P5) indicating vulnerable attack paths. Threat likelihood analysis showed that Botnet attacks (0.94) had the highest likelihood score, followed by DDoS attacks (0.91). Likewise, the cyber-physical risk assessment had the highest risk score (0.91) for Botnet attack. Restoration factor rose from 1.12 under low impact conditions to 2.36 under severe-impact conditions. The results validate the proposed framework's impact on enhancing threat prioritization, cyber resilience, and proactive security management in Industry 5.0 cyber-physical systems.

REFERENCES

[1] Agiollo, Andrea, Enkeleda Bardhi, Alessandro Palma, Riccardo Lazzeretti, Silvia Bonomi, and Fernando Kuipers. "SoK: Harmonizing Attack Graphs and Intrusion Detection Systems." arXiv preprint arXiv:2603.08295 (2026).

[2] Rahman, Md Arifur, Md Iqbal Hossan, Md Serajul Kabir Chowdhury, and BM Taslimul Haque. "NS-ZTFedIDS: A Neuro-Symbolic Federated Zero Trust Framework for Explainable Intrusion Detection in SDN and Optical Communication Networks."

[3] Behlim, Mohammed Ismail. "Adaptive Neuro-Symbolic Graph Networks with Differential Privacy for Real-Time Threat Intelligence in Software-Defined Industrial IoT." International Journal of Engineering and Computer Science 15, no. 05 (2026): 28497-28504.

[4] Fernández-Miguel, Andrés, Susana Ortíz-Marcos, Mariano Jiménez-Calzado, Alfonso P. Fernández del Hoyo, Fernando Enrique García-Muiña, and Davide Settembre-Blundo. "From Resilience to Cognitive Adaptivity: Redefining Human–AI Cybersecurity for Hard-to-Abate Industries in the Industry 5.0–6.0 Transition." Information 16, no. 10 (2025): 881.

[5] Haseltine, Carmen, and Laura A. Albert. "Modeling with Attack Graphs for Securing Cyber-Physical Systems." Tutorials in Operations Research: Advances in Analytics and Operations Research: Improving Decisions to Secure the Future (2025): 1-27.

[6] Huang, Shaofei, Christopher M. Poskitt, and Lwin Khin Shar. "From Incomplete Architecture to Quantified Risk: Multimodal LLM-Driven Security Assessment for Cyber-Physical Systems." arXiv preprint arXiv:2604.05674 (2026).

[7] Jbair, Mohammad, Bilal Ahmad, Carsten Maple, and Robert Harrison. "Threat modelling for industrial cyber physical systems in the era of smart manufacturing." Computers in Industry 137 (2022): 103611.

[8] Rosário, Albérico Travassos, and Ricardo Jorge Gomes Raimundo. "AI, Optimization, and Human Values: Mapping the Intellectual Landscape of Industry 4.0 to 5.0." Applied Sciences 15, no. 13 (2025): 7264.

[9] Rehman, Hafiz Muhammad Raza Ur, Saira Liaquat, Muhammad Junaid Gul, Muhammad Zeeshan Jhandir, Daniel Gavilanes, Manuel Masias Vergara, and Imran Ashraf. "A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions." Journal of Big Data 12, no. 1 (2025): 264.

[10] Presekal, Alfan, Alexandru Ştefanov, Vetrivel Subramaniam Rajkumar, and Peter Palensky. "Attack graph model for cyber-physical power systems using hybrid deep learning." IEEE Transactions on Smart Grid 14, no. 5 (2023): 4007-4020.

[11] Zhao, Jun, Xudong Liu, Qiben Yan, Bo Li, Minglai Shao, Hao Peng, and Lichao Sun. "Automatically predicting cyber attack preference with attributed heterogeneous attention networks and transductive learning." computers & security 102 (2021): 102152.

[12] Lallie, Harjinder Singh, Kurt Debattista, and Jay Bal. "A review of attack graph and attack tree visual syntax in cyber security." Computer Science Review 35 (2020): 100219.

[13] Pandey, Neeraj Kumar, Krishna Kumar, Gaurav Saini, and Amit Kumar Mishra. "Security issues and challenges in cloud of things-based applications for industrial automation." Annals of Operations Research 342, no. 1 (2024): 565-584.

[14] Pu, Hongyi, Liang He, Peng Cheng, Jiming Chen, and Youxian Sun. "CORMAND2: A deception attack against industrial robots." Engineering 32 (2024): 186-201.

[15] Li, Yansong, Qian Luo, Jiajia Liu, Hongzhi Guo, and Nei Kato. "TSP security in intelligent and connected vehicles: Challenges and solutions." IEEE Wireless Communications 26, no. 3 (2019): 125-131.
[16] Garg, Urvashi, Geeta Sikka, and Lalit K. Awasthi. "Empirical risk assessment of attack graphs using time to compromise framework." International Journal of Information and Computer Security 16, no. 1-2 (2021): 33-50.
[17] Nandiya, Padmeswari, Ahmad Mohsin, Ahmed Ibrahim, Iqbal H. Sarker, and Helge Janicke. "Bridg-ics: AI-grounded knowledge graphs for intelligent threat analytics in industry 5.0 cyber-physical systems." Cybersecurity 9, no. 1 (2026): 167.
[18] Govindarajan, Vijay, Faraz Ahmed, Zaid Bin Faheem, Muhammad Bilal, Manel Ayadi, and Jehad Ali. "Aegis-5: A Hybrid Ensemble Framework for Intrusion Detection in Industry 5.0 Driven Smart Manufacturing Environment." ACM Transactions on Autonomous and Adaptive Systems (2026).
[19] Dasarla, Mallikarjun. "Graph Neural Network-Based Intrusion Detection for Industrial Internet of Things Systems." Master's thesis, Ohio University, 2026.
[20] Kanca, Ali Melih, and İlker Türker. "GraphDL: A visibility graph-based structural representation framework for flow-based cyber-attack detection." Scientific Reports (2026).
[21] Sridevi, Kotari, Waseema Masood, Shahana Tanveer, Olfat M. Mirza, Nithya Rekha Sivakumar, and Shitharth Selvarajan. "ZuraNet: a hybrid rule-based intrusion detection system with deep learning for securing SCADA-driven cyber-physical systems." Scientific Reports (2026).
[22] Mishra, Shailendra, Tariq Saleh M. Aldafas, and Naif S. Alshammari. "A zero-trust digital twin framework for privacy-preserving multi-dataset intrusion detection in industrial IoT with lightweight blockchain auditing." Scientific Reports (2026).
[23] Ogunmolu, Akinde Michael. "A multiscale approach to cyber-mechanical threat modeling for predicting and preventing failures in critical energy infrastructure." (2025).
[24] Oladele, Oluwaseyi Kolawole. "Data-Driven Cyber-Physical Security Framework for Smart Cities." (2025).
[25] Yang, Guan-Yan, Farn Wang, and Kuo-Hui Yeh. "Gnn-enhanced traffic anomaly detection for next-generation sdn-enabled consumer electronics." IEEE Transactions on Consumer Electronics (2025).
[26] Chinthamu, Narender, Shobana Jayakumar, Manasa K, Revathi MP, and Syed Zahidur Rashid. "Cyber-Physical Systems Security Protecting Critical Infrastructure from Cyber Threats and Attacks." In ITM Web of Conferences, vol. 76, p. 03005. EDP Sciences, 2025.
[27] Zhukabayeva, Tamara, Zulfiqar Ahmad, Aigul Adamova, Nurdaulet Karabayev, and Assel Abdildayeva. "An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial iot." Sensors 25, no. 8 (2025): 2395.
[28] Chowdhury, Tonoy Kanti. "AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems." ASRC Procedia: Global Perspectives in Science and Scholarship 1, no. 01 (2025): 675-704.
[29] Cherukuri, Bangar Raju. "Advanced Multi Class Cyber Security Attack Classification in IoT Based Wireless Sensor Networks Using Context Aware Depthwise Separable Convolutional Neural Network." Journal of Machine and Computing 5, no. 2 (2025).
[30] Azar, Ahmad Taher, Syed Umar Amin, Mohammed Abdul Majeed, Ahmed Al-Khayyat, and Ibraheem Kasim. "Cloud-Cyber Physical Systems: Enhanced Metaheuristics with Hierarchical Deep Learning-based Cyberattack Detection." Engineering, Technology & Applied Science Research 14, no. 6 (2024): 17572-17583.
[31] Gajula, Sreenivasulu. "Cybersecurity risk prediction using graph neural networks." Journal of Information Systems Engineering and Management (2024).
[32] Matta, Sai Srinivas, and Manish Bolli. "AI-AUGMENTED CYBERSECURITY: GRAPH NEURAL NETWORKS FOR PREDICTING NATION-STATE CYBERATTACKS." International Journal of Business and Economics Insights 4, no. 4 (2024): 35-59.
[33] Raza, Aamir, Abdul Karim Sajid Ali, and Ali Abbas Hussain. "AI-driven approaches to cyber and information security: Machine learning algorithms for threat prediction and anomaly detection." Spectrum of Engineering Sciences (2024): 565-573.
[34] Islam, Md Tawfiqul, Sabbir Ahmad, Md Anikur Rahman, and Md Arifur Rahaman. "Neural Network–Based Risk Prediction And Simulation Framework For Medical IOT Cybersecurity: An Engineering Management Model For Smart Hospitals." International Journal of Scientific Interdisciplinary Research 5, no. 2 (2024): 30-57.
[35] Salam, Abdu, Faizan Ullah, Farhan Amin, and Mohammad Abrar. "Deep learning techniques for web-based attack detection in industry 5.0: A novel approach." Technologies 11, no. 4 (2023): 107.
[36] Kandhro, Irfan Ali, Sultan M. Alanazi, Fayyaz Ali, Asadullah Kehar, Kanwal Fatima, Mueen Uddin, and Shankar Karuppayah. "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures." IEEE Access 11 (2023): 9136-9148.
[37] https://www.kaggle.com/datasets/dhoogla/cicids2017/code
[38] Yu, Xue, Chengbin Gao, Yao Du, Bo Gao, Danyang Tian, and Tiantian Hou. "Adaptive residual observer-based detection and isolation framework against false data injection attack in large-scale power systems." Scientific Reports 15, no. 1 (2025): 41070.

[39] Agote-Garrido, Alejandro, Alejandro M. Martín-Gómez, and Juan Ramón Lama-Ruiz. "Manufacturing system design in Industry 5.0: Incorporating sociotechnical systems and social metabolism for human-centered, sustainable, and resilient production." Systems 11, no. 11 (2023): 537.