Interpretable and Adaptive Security Mechanism for Next-Gen Industrial Networks

V. Lalitha [1], A. Dhanasekhar Reddy [2*], R. R. Shantha Spandana [3] & T. Anil Kumar [4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
ORCID-ID: 0009-0002-3176-5586; E-mail: lalithavairam3@gmail.com,

[2] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
ORCID-ID: 0009-0008-6256-0405; E-mail: dhanasekhar918@gmail.com,

[3] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology,Puttur,
ORCID-ID: 0009-0003-4236-1250; E-mail: shanthaspandana@gmail.com,

[4] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
ORCID-ID: 0009-0003-3312-3031; E-mail: anil.thumburu@gmail.com,

Subject Area: Technology.
Type of the Paper: Regular.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.15789722
Google Scholar Citation: IJAEML

How to Cite this Paper:
Lalitha, V., Reddy, A. D., Spandana, R. R. S. & Kumar, T. A. (2025). Interpretable and Adaptive Security Mechanism for Next-Gen Industrial Networks. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *9*(1), 108-119. DOI: https://doi.org/10.5281/zenodo.15789722

International Journal of Applied Engineering and Management Letters (IJAEML)
A Refereed International Journal of Srinivas University, India.

Crossref DOI: https://doi.org/10.47992/IJAEML.2581.7000.0236

Received on: 18/04/2025
Published on: 28/06/2025

International Journal of Applied Engineering and Management Letters (IJAEML), ISSN: 2581-7000, Vol. 9, No. 1, June 2025

SRINIVAS PUBLICATION

Interpretable and Adaptive Security Mechanism for Next-Gen Industrial Networks

V. Lalitha [1], A. Dhanasekhar Reddy [2*], R. R. Shantha Spandana [3] & T. Anil Kumar [4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
ORCID-ID: 0009-0002-3176-5586; E-mail: lalithavairam3@gmail.com,

[2] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
ORCID-ID: 0009-0008-6256-0405; E-mail:dhanasekhar918@gmail.com,

[3] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology,Puttur,
ORCID-ID: 0009-0003-4236-1250; E-mail: shanthaspandana@gmail.com,

[4] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
ORCID-ID: 0009-0003-3312-3031; E-mail: anil.thumburu@gmail.com,

ABSTRACT

In the era of Industry 5.0, the evolution of smart and interconnected industrial environments calls for highly adaptive and interpretable security mechanisms. With the rapid proliferation of IoT devices, automation systems, and cloud-integrated platforms, industrial networks have become increasingly vulnerable to complex and evolving cyber threats. Ensuring the resilience of such environments requires the deployment of intelligent intrusion detection techniques capable of operating in real-time with high accuracy and interpretability. To address this necessity, an advanced security mechanism was developed using the CIC-DDoS 2019 dataset, which provides a comprehensive set of simulated Distributed Denial of Service (DDoS) attacks across multiple protocols in industrial network settings. The detection system was enhanced using prominent feature selection techniques such as SelectKBest, SelectPercentile, and Mutual Information. These techniques helped identify the most relevant attributes from the dataset, effectively reducing dimensionality while improving model generalization and training efficiency. The core of the detection system is a robust ensemble classification strategy, leveraging a voting-based classifier that integrates the strengths of bagging through Random Forest and boosting through Boosted Decision Trees. This hybrid ensemble architecture enables precise classification by combining the diversity and stability of multiple models. Among all tested configurations, the voting classifier demonstrated superior performance, achieving a high accuracy of 95.8%, thereby confirming the strength of ensemble learning in dynamic and heterogeneous network environments. The proposed detection system is scalable and adaptive, designed to function in real-time, and supports decision transparency—crucial for building trust in automated industrial defense systems. This mechanism offers a dependable layer of security against network intrusions and enhances the resilience of hyper-connected infrastructures, fulfilling the cybersecurity demands of next-generation industrial systems under the Industry 5.0 vision.

Keywords: Deep learning (DL), cyber-attacks, explainable artificial intelligence, Industry 5.0., intrusion detection system (IDS), Voting Classifier.

1. INTRODUCTION :

Merging human simplicity with a complex machine creates notable improvements and industrial solutions outside the industry more focused on consumers and more efficient sources, which is known as the fifth industrial revolution or industry meaning 5.0. Industry 5.0 seeks to combine the cognitive abilities of human specialists with the accuracy and performance of automated technologies for the development of goods and processes that are more flexible and sustainable. In contrast to its predecessor, which concentrated totally on automation and optimization, industry 5.0 prioritizes collaboration among people and machines to foster improved innovation, creativity, and personalization in production and service delivery [1], [2]. This paradigm shift is expected to

significantly influence consumer technology, expedite innovation, and alter the methods of product conception, manufacturing, and delivery to consumers.

In enterprise 5.0, "consumer Electronics (CE)" devices are essential for data collection and processing from various sensors and machines, in addition to facilitating remote monitoring and control. Facilities such as smartphones, smart watches and capsules act as an interface between human beings and machines, adding real facts, indicators and updates of operating status for industrial systems.3 by way of accumulating environmental records, such as temperature, air excellent, and humidity, CE devices can enhance industrial operations, resulting in extra intelligent and efficient manufacturing systems. These developments facilitate improved user experiences and the creation of more intuitive and resource-efficient systems, hence minimizing waste and energy usage.

Nonetheless, however the assurances of industry 5.0, the swift implementation and commercialization of these technology engender sizeable protection apprehensions. The escalating interconnectedness of devices and systems amplifies the hazards related to cyber threats and attacks. [5] Autonomous systems, including production robots, are susceptible to remote hijacking by hackers, which may disrupt operations and inflict considerable damage on enterprises. Facilities such as smartphones, smart watches and capsules act as an interface between human beings and machines, adding real facts, indicators and updates of operating status for industrial systems, the intricacy of enterprise 5.0 networks renders them vulnerable to cyber-attacks. Consequently, there is an urgent necessity for enhanced security protocols to safeguard these structures against growing threats [6].

An alternative alternative is the implementation of "intrusion detection systems (IDS)" that monitor network traffic to detect anomalous behavior indicating potential security violations.Although conventional IDS methodologies have been extensively employed, their efficacy against advancing and complex cyber threats is constrained. Consequently, it is vital to develop IDS systems that are more dynamic and adept at reacting to novel assault routes. In latest years, DL-based IDS have emerged as a promising study domain, with the promise for enhanced accuracy and real-time detection of cyber-attacks in complex and speedy dynamic environments characteristic of industry 5.0. Advanced IDS models, capable of learning and adapting to novel attack patterns, are increasingly stated as important factors in safeguarding the interconnected networks that help the industry 5.0 ecosystem [8].

2. OBJECTIVES :

To ensure cybersecurity in hyper-connected Industry 5.0 environments, this work focuses on creating an adaptive, accurate, and interpretable intrusion detection mechanism using ensemble machine learning models and feature optimization.

(1)Develop an adaptive intrusion detection mechanism

To construct a real-time detection system using the CIC-DDoS 2019 dataset, capable of classifying diverse network intrusions with high accuracy through optimized machine learning models.

(2)Enhance feature relevance and model performance

To apply feature selection methods—SelectKBest, SelectPercentile, and Mutual Information—to identify critical input features that significantly improve training efficiency and reduce computational complexity.

(3)Implement a robust ensemble-based classifier

To "integrate Random Forest (bagging) and Boosted Decision Trees (boosting)" in a voting classifier framework for precise, scalable, and interpretable intrusion detection in industrial network environments.

3. REVIEW OF LITERATURE/ RELATED WORKS :

Industry 5.0, defined by the amalgamation of human mind with sophisticated technology and intelligent systems, introduces novel opportunities and issues in industrial cybersecurity. As enterprises transform into hyper-connected ecosystems comprising intricate networked devices and systems, the risk of cyber threats escalates, requiring sophisticated techniques to safeguard these environments. Recent literature on (IDS) underscores the increasing interest in utilizing ML and DL models to tackle difficulties in industrial settings, especially within the framework of industry 5.0.

An important contribution is the research of Saba et al. [9], which represents a system of disruption detection based on anomaly adapted to IoT networks. They utilize DL models to identify anomalous actions that may represent a potential incursion. The solution seeks to bolster the security of industrial

IoT networks, which might be crucial to the interconnected devices of industry 5.0. The system utilizes deep learning techniques to adapt to the dynamic characteristics of IoT networks, providing an advanced method compared to conventional signature-based IDS answers. Their studies underscores the capability of deep learning to identify novel threats by recognizing intricate patterns in network traffic.

Similarly, Althobaiti et al. [32] concentrate on "intelligent cognitive computing for intrusion detection in industrial cyber-physical systems (CPS)". Their methodology entails the integration of cognitive computing with intrusion detection systems to augment the overall intelligence of the security framework. The cognitive model always learns and adjusts to emerging threats, rendering it a resilient solution for the swiftly changing domain of industrial cybersecurity. Their concept underscores the importance of cognitive abilities in IDS, stressing the necessity for structures that cannot only detect but also anticipate and react to emerging threats in real-time. This examine enhances the expanding corpus of research investigating the amalgamation of artificial intelligence with industrial safety systems.

Jeong et al. [11] advocate a semi-supervised methodology for network intrusion detection with "Generative adversarial Networks (GANs)", frequently hired in generative tasks, are repurposed for intrusion detection by producing adversarial samples to increase the possibility of the version to distinguish between normal and abnormal community activities.This method is in particular advantageous in contexts with little labeled data, as it allows the model to learn from both classified and unlabeled datasets. Their methodology highlights the significance of utilizing GANs to decorate the detection efficacy of IDS, specifically in eventualities when conventional supervised learning models may falter because of insufficient training data.

Fatani et al. [34] they propose a sophisticated approach for extraction and selecting elements that integrate deep learning with Aquila optimizer to increase the precision of the IoT disturbance detection systems.Characteristic selection and extraction are crucial for enhancing the efficacy of DL models, since they facilitate the identity of the most pertinent information from big datasets. The suggested technique seeks to beautify the efficiency and efficacy of "Intrusion Detection systems (IDS)" in figuring out complex assaults within IoT networks by mixing deep learning with optimization techniques such as Aquila. This examine highlights the significance of feature engineering and optimization in developing high-performance intrusion detection systems that can manage the extensive data produced by connected devices in industry 5.0.

Abdel-Basset et al. [13] investigate Deep-IFS, an "intrusion detection methodology tailored for industrial internet of things (IIoT)" communications inside a fog computing framework. Fog computing complements cloud computing by relocating computation closer to the community facet, which is especially advantageous in industrial environments where actual-time processing is essential. Deep-IFS integrates deep getting to know methodologies with fog computing to establish a system able to efficaciously identifying intrusions in IIoT networks while reducing latency. This approach emphasizes the want of using edge computing and deep learning to meet the real-time safety needs of industrial settings. The study illustrates that the integration of cloud and edge computing with sophisticated machine learning models can markedly strengthen the security and efficiency of Industry 5.0 systems.

Tang et al. [36] introduce DeepIDS, a DL-based methodology for intrusion detection in "software-defined networking (SDN)" contexts. SDN delineates the control plane from the data plane in networking, presenting advanced flexibility and scalability even as simultaneously presenting novel safety problems. DeepIDS employs deep learning methodologies to identify abnormalities and threats inside SDN settings, targeting the distinct vulnerabilities related to SDN's centralized manipulate. Their studies demonstrates how deep studying can be tailored to tackle the precise security issues of "software-defined Networking (SDN)", rendering it a viable strategy for safeguarding industrial networks that depend on this technology for adaptability and scalability.

Sahu et al. [15] concentrate on a hybrid model that integrates "long short-term memory (LSTM)" and "Fully Convolutional Neural Networks (FCNN)" for "multi-class intrusion detection" in business settings. LSTM, recognized for its functionality to deal with sequential facts, and FCNN, a convolutional neural community tailor-made for function extraction, are incorporated to pick out diverse types of intrusions inside a scalable framework. This hybrid paradigm is mainly effective for coping with intricate, multi-class intrusion detection tasks in real-time, rendering it appropriate for the

dynamic and developing characteristics of enterprise 5.0 networks. Their studies highlights the capability of integrating various deep learning models to attain enhanced accuracy and robustness in intrusion detection structures.

Moustafa et al. [16] provide a revolutionary danger intelligence framework for the protection of industry 4.0 systems, which is equally pertinent to industry 5.0. The initiative emphasizes the incorporation of risk intelligence with current safety protocols to enhance proactive protection in opposition to cyber threats. By integrating threat intelligence, the advised device can anticipate and alleviate capability dangers prior to their escalation into enormous assaults. This study emphasizes the significance of predictive security measures and the crucial role of threat facts in safeguarding the intricate and linked systems of enterprise 5.0. Their studies shows that integrating hazard intelligence with sophisticated detection models can markedly enhance the ability to ward off attacks in industrial environments.

Those works together emphasize the increasing fashion of incorporating deep getting to know, cognitive computing, and optimization techniques for decorating the efficiency of the detection detection systems in commercial and IoT settings. The literature identifies various interesting methodologies, including anomaly-based detection, semi-supervised learning, generative adversarial networks (GANs), feature selection, and the implementation of edge and fog computing. Each answer complements the security of business networks, tackling the distinct issues of industry five.0, which includes the complexity and scale of networked devices, the necessity for real-time processing, and the dynamic nature of cyber threats. Current research in this domain highlights the need of developing adaptive, clever systems that can learn from new data and react to rising threats, which is crucial for maintaining the security and resilience of industry 5.0 systems.

Table 1: Literature Survey Comparison Table

Sl. No	Area & Focus of the Research	The result of the Research	Reference
1	Anomaly-based intrusion detection using deep learning in IoT networks.	Effectively detected anomalies using adaptive deep learning for IoT.	T. Saba, A. Rehman, T. Sadad, H. Kolivand.Et.al.,(2022). [9]
2	Cognitive computing integration for smart industrial intrusion detection systems.	Improved real-time threat adaptation using cognitive learning models.	M. M. Althobaiti, K. P. M. Kumar, D. Gupta., et.al., (2021) [32]
3	Semi-supervised intrusion detection using GANs with limited labeled data.	Boosted detection in low-data settings using adversarial sample learning.	H. Jeong, J. Yu, and W. Lee (2021) [11]
4	Feature selection in intrusion detection using Aquila and deep learning.	Achieved better precision through optimization and deep learning fusion.	A. Fatani, A. Dahou, M. A. Al-Qaness, et.al., (2022) [34]
5	Intrusion detection for IIoT using deep learning in fog.	Enabled low-latency detection with edge-based learning architecture.	M. Abdel-Basset, V. Chang, H. Hawash. (2021) [13]

4. MATERIALS AND METHODS :

The suggested approach seeks to improve cybersecurity in the industry 5.0 framework by utilizing machine learning algorithms for intrusion detection. The CIC-DDoS 2019 dataset [22], comprising varied network traffic data, employs feature selection methods such as SelectKBest, Select Percentile, and Mutual information to ascertain the most pertinent factors for effective categorization. A variety of ML techniques are utilized, including decision trees [18], Random forest [19], “Bidirectional long short-term memory (BiLSTM), Bidirectional Gated Recurrent units (BiGRU) [17], Convolutional Neural Networks (CNN)” [20], and hybrid models like CNN + LSTM [21]. Moreover, ensemble learning is executed by a voting Classifier that integrates bagging with Random forest and Boosted

decision trees to decorate detection efficacy. This machine seeks to deliver a strong, real-time intrusion detection mechanism capable of managing intricate, hyper connected commercial networks, therefore assuring improved security and resilience in industry 5.0 settings.

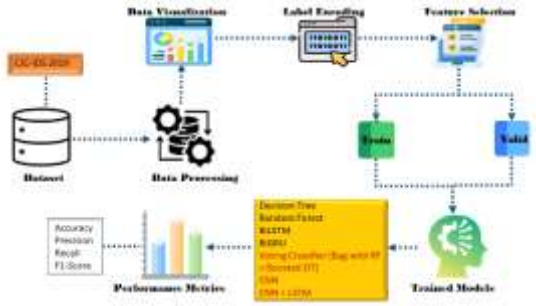


Fig 1: Proposed Architecture

The structure (fig. 1) illustrates a complete "Intrusion Detection system (IDS)" for industry 5.0. The machine initiates by analyzing the CIC-DDoS 2019 dataset [22], encompassing information visualization and label encoding. Eventually, feature selection is employed to determine the most pertinent features. The dataset is divided into training and testing subsets, and lots of device learning models are developed and assessed. The trained models classify network traffic as both normal and malicious, thereby safeguarding the security and resilience of industry 5.0 systems.

4.1 Dataset Collection:

This study utilizes the CIC-DDoS 2019 dataset, consisting of 125,170 entries and 78 attributes that represent several network traffic metrics. This dataset was meticulously built for research on intrusion detection systems (IDS) and incorporates a varied array of parameters such as packet lengths, flow durations, and flags, providing substantial insights into network behavior. Next to the use of feature selection methods, the dataset was condensed to the most pertinent features for intrusion detection, hence enhancing model performance and diminishing computational time. the chosen features include 'flow duration,' 'Fwd Packets length total,' 'Fwd Packet length Max,' 'Fwd Packet length Min,' 'Fwd Packet length mean,' 'flow Bytes/s,' 'flow Packets/s,' 'flow IAT mean,' 'flow IAT Std,' 'flow IAT Max,' 'Fwd IAT total,' 'Fwd IAT Max,' 'Fwd Packets/s,' 'Packet length Min,' 'Packet length Max,' 'Packet length mean,' 'Avg Packet size,' 'AvgFwd segment size,' and 'SubflowFwd Bytes.' These houses denote essential parameters including packet sizes, flow characteristics, and inter-arrival durations, which are vital for identifying anomalies and potential assaults in community traffic.

Table 2: Dataset Collection Table - CIC-DDoS 2019

	Protocol	Flow Duration	Total Fwd Packets	Total Backward Packets	Fwd Packets Length Total	Bwd Packets Length Total	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean
0	17	49	2	0	458.0	0.0	229.0	229.0	229.0
1	17	1	2	0	2944.0	0.0	1472.0	1472.0	1472.0
2	17	1	2	0	458.0	0.0	229.0	229.0	229.0
3	17	1	2	0	2944.0	0.0	1472.0	1472.0	1472.0
4	17	1	2	0	2944.0	0.0	1472.0	1472.0	1472.0

5 rows × 78 columns

4.2. Pre-Processing:

During the pre-processing phase, we concentrate on readying the dataset for modeling. This encompasses data processing, showing essential relationships, encoding specific labels, and executing feature selection to guarantee superior input for the predictive model.

4.2.1 Data Processing

The processing of this dataset entails numerous critical processes to guarantee its quality and preparedness for analysis. Initially, duplicate entries are detected and eliminated to preserve data integrity. Subsequently, any absent values are addressed by eliminating rows containing null entries, so guaranteeing the absence of incomplete data. Ultimately, normalization is implemented to normalize the data, guaranteeing that all numerical values fall within a comparable range. These preparation methods improve the dataset's consistency, reliability, and appropriateness for subsequent modeling and analysis.

4.2.2 Data Visualization

The data visualization technique entails generating a count plot to illustrate the prevalence of various categories inside the dataset's "Label" column. This visualization use separate colors to distinguish the categories, offering a clear representation of the distribution of each label within the data. This plot illustrates the frequency of each label, aiding in the comprehension of class distribution and the identity of potential class imbalances, that's crucial for informed decision-making in the modeling process.

4.2.3 Label Encoding

Label encoding is employed to transform categorical labels, expressed as strings, into numerical values. The label encoder allocates a unique integer to every separate category within the "Label" column. This translation lets in machine learning models to process the data, as the majority of algorithms necessitate numerical enter. Subsequent to encoding, the "Label" column is substituted with its numerical values, while the features (X) are delineated from the target variable (y) for subsequent model processing.

4.2.4 Feature Selection

Feature selection is an essential process for enhancing model efficiency and accuracy by minimizing the quantity of input features. The SelectPercentile method, utilizing mutual information as a criterion, is employed to identify the most pertinent attributes. This strategy identifies the top 25% of features according to their statistical correlation with the target variable. This method selects 19 important characteristics, ensuring that only the most useful variables are utilized for model training, hence improving performance.

4.3 Training & Testing

The data file is divided into training and test kit for assessing the model efficiency.Usually, 20% of the data is set aside for checking out; the last eighty% is used to train the version. This department guarantees that the version gains patterns from the vital facts even as it is assessed on new cases to gauge its generalization capacity. The random state is installed to offer uniformity in records splitting throughout several version executions.

4.4 Algorithms:

DecisionTree: This algorithm helps to decide on the basis of elements, construction of a structure similar to a tree for classification or prediction of the result. It is asked to grasp the selection -making process and explain the connections between features in categorization.

RandomForest:A compilation of decision trees, this approach enhances classification precision by averaging numerous models to mitigate overfitting. It is proficient at managing intricate datasets, delivering reliable forecasts and assessing feature significance.

BiLSTM: Bi-directional“long short-term memory networks” capture dependencies from each past and future data, therefore improving performance for sequential information. It is applied for applications such as time-series forecasting or collection annotation, enhancing contextual comprehension.

BiGRU: Bidirectional Gated Recurrent Unit networks, similar to BiLSTM, analyse data in both forward and backward orientations. It is effective for sequential obligations, providing expedited training while retaining comparable performance for context-aware sequence processing tasks.

Voting Classifier (Bag with RF + Boosted DT): This ensemble method integrates the forecasts of a Random forest and Boosted decision trees. It consolidates the outputs of many models to enhance classification accuracy, therefore improving resilience and generalization in tasks necessitating high predictive reliability.

CNN: Convolutional Neural Networks are utilized for pattern recognition in structured facts. They talented in extracting spatial features, particularly from photograph data, and are employed for classification tasks related to visual or geographic information, therefore improving feature extraction performance.

CNN + LSTM: The integration of CNN and LSTM capitalizes at the advantages of both architectures, with CNNs specializing in spatial feature extraction and LSTMs adept in capturing sequential dependencies. [21] This methodology is appropriate for applications necessitating both geographical and temporal data processing, enhancing predictive accuracy.

5. RESULTS AND DISCUSSION :

Accuracy: The correctness of the check is its ability to distinguish properly among the patient and healthy cases. Evaluating the correctness of the take a look at requires computing the ratio of actual positives to actual negatives in all assessed cases. Mathematically, this can be stated as:

"$Accuracy = \frac{\text{TP+TN}}{\text{TP+FP+TN+FN}}(1)$"

Precision: The accuracy evaluates the share of precisely classified cases among cases identified as positive. As a result, the formula for calculating accuracy is expressed:

"$Precision = \frac{\text{True Positive}}{\text{True Positive +False Positive}}(2)$"

Recall: The invocation is a meter in machine mastering that assesses the model's capacity to grasp all pertinent examples of a given class. It is the proportion of exactly expected high-quality observations of general genuine positives and provides insight into the efficiency of the version in detecting the frequency of a particular elegance.

"$Recall = \frac{\text{TP}}{\text{TP + FN}}(3)$"

F1-Score: The F1 score is a metric for evaluating the accuracy of the machine learning model. It integrates the metrics of accuracy and model. The metric of accuracy quantifies the frequency of real predictions of generated versions throughout the data file.

"$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall+Precision} * 100(1)$"

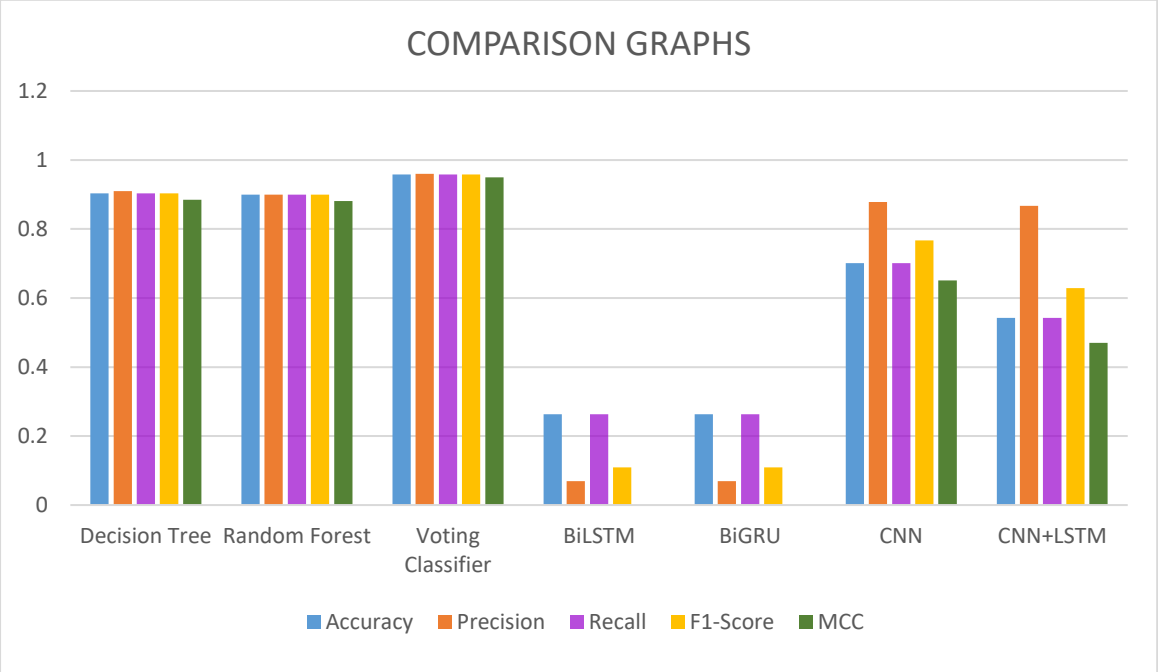
MCC: The Matthews coefficient, or Matthews correlation coefficient (MCC), is a performance indicator utilized for binary classifiers in machine learning. It assesses the correlation between expected and actual binary outcomes by evaluating all 4 components of a confusion matrix.

"$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN}}(5)$"

Table(3)assess the performance metrics—accuracy, precision, recall, F1-score, and MCC—for every method. The voting Classifier routinely surpasses all other algorithms across all metrics. The tables offer a comparative examination of the metrics for the alternative methods.

Table 3: Performance Evaluation Metrics

Model	Accuracy	Precision	Recall	F1-Score	MCC
DecisionTree	0.903	0.910	0.903	0.903	0.885
Random Forest	0.900	0.900	0.900	0.900	0.881
Voting Classifier	**0.958**	**0.960**	**0.958**	**0.958**	**0.950**
BiLSTM	0.263	0.069	0.263	0.109	0.000
BiGRU	0.263	0.069	0.263	0.109	0.000
CNN	0.701	0.878	0.701	0.767	0.651
CNN+LSTM	0.542	0.867	0.542	0.629	0.470



Graph 1: Comparison Graphs

In Graph (1), the accuracy is shown in blue, accuracy in orange color, remember in the purple, F1-score in the light yellow and MCC in green. In relation to other models, the voting classifier shows increased performance in all measures and reaches the highest values. The above graph clearly illustrates these findings.

6. CONCLUSION :

In short, the use of machine learning methodologies to detect disruption in framework of industry 5.0 shows considerable potential for enhancing cybersecurity in fairly interconnected industrial settings. The CIC-DDoS 2019 dataset [22] facilitated the examination of multiple feature selection techniques, including SelectKBest, SelectPercentile, and Mutual information, to ascertain the maximum pertinent features for intrusion detection. Optimizing the feature set enhanced the model's performance, facilitating more green and precise detection of network intrusions. Of the classification algorithms evaluated, the voting Classifier, which integrates bagging with Random forest [19] and Boosted decision trees [18], it achieved the highest accuracy of 95.8%. This result underlines the efficiency of the file approaches in dealing with complex concerns about cyber security in current business structures. This approach provides specific intrusion detection while guaranteeing the reliability and resilience crucial for safeguarding the linked and automated framework of industry 5.0. This work underscores the important function of powerful machine learning approaches in protecting industrial ecosystems from rising cyber threats.

The ***future scope***of this methodology involves the enhancement of “intrusion detection systems” by the use of sophisticated ML techniques, including DL models, to improve detection precision and minimize false positives. Furthermore, investigating the combination of real-time threat intelligence, adaptive learning systems, and ongoing model upgrades could enhance cybersecurity in industry 5.0. Augmenting the dataset to encompass a broader range of attack scenarios and evaluating the model's efficacy across diverse industrial contexts would enhance its robustness and scalability for practical applications.

REFERENCES :

[1] Grover, J. (2022). Security of vehicular ad hoc networks using block chain: A comprehensive review. *Veh. Commun*, 34(4), 124-126

[2] Viswanath, G. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary intelligence*, 14(2), 691-698.

[3] Wazid, M., Das, A. K., & Shetty, S. (2023). BSFR-SH: Blockchain-enabled security framework against Ransomware attacks for smart healthcare. *IEEE Trans. Consum. Electron.,* 69(1), 18–28.

[4] Viswanath, G. (2023). A Real-Time Case Scenario Based On URL Phishing Detection Through Login URLS. *Material science and technology,* 22(9), 103-108.

[5] Tidjon, L. N., Frappier, M., & Mammar, A. (2019). Intrusion detection systems: A cross-domain overview. *IEEE Commun. Surveys Tuts.,* 21(4), 3639–3681.

[6] Viswanath, G., & Sunil Kumar Reddy, T. (2014). Enhancing power unbiased cooperative media access control protocol in manets. *International Journal of Engineering Inventions*, 4(9), 8-12.

[7] Nguyen, A., et.al. (2021). System design for a data-driven and explainable cus tomer sentiment monitor using IoT and enterprise data. *IEEE Access*, 9(1), 117140–117152

[8] G Viswanath, G. (2024). Artificial Intelligence-driven Frameworks for Fostering Active Participation and Learning in Language Classrooms. *International Journal of Interpreting Enigma Engineers (IJIEE)*, 1(3), 23-32.

[9] Esposito, C., Ficco, M., & Gupta, B. B. (2021). Block chain-based authentication and authorization for smart city applications. *Inf. Process. Manage*, 58(2), 145631-145652.

[10] Viswanath, G. (2024). Improved LightGBM Model Performance Analysis and Comparison For Coronary Heart Disease Prediction. *International Journal of Information Technology and Computer Engineering,* 12(3), 658-672.

[11] Roy, S., Biswas, A., Shawon, M. T. A., Akter, S., & Rahman, M. M. (2024). Land use and meteorological influences on dengue transmission dynamics in Dhaka city, Bangladesh. *Bull. Nat. Res. Centre*, 48(1), 1–24

[12] Viswanath, G. (2024). Hybrid Feature Extraction With Machine Learning To Identify Network Attacks. *International Journal of HRM and Organizational Behavior*, 12(3), 217-228.

[13] M. Abdel-Basset, M., V. Chang, V., H. Hawash, H., R. K. Chakrabortty, R. K., &and M. Ryan, M. (2021). Deep-IFS: Intrusion detection approach for Industrial Internet of Things traffic in fog environment. *IEEE Trans. Ind. Informat.,* 17(11), 7704–7715.

[14] Viswanath, G. (2023). A Real Time Online Food Ording Application Based Django Restfull Framework. *Juni Khyat*, 13(9), 154-162.

[15] Abdualgalil, B., Abraham, S., & Ismael, W. M. (2022). Early diagnosis for dengue disease prediction using efficient machine learning techniques based on clinical data. *J. Robot. Control (JRC)*, 3(3), 257–268.

[16] Moustafa, N., Adi, E., Turnbull, B., & Hu, J. (2018). A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access*, 6(1), 32910–32924.

[17] Ullah, I., & Mahmoud, Q. H. (2022). Design and development of RNN anomaly detection model for IoT networks. *IEEE Access,* 10(2), 62722-62750.

[18] Ali, N. (2024). The recent burden of dengue infection in bangladesh: A serious public health issue. *J. Infection Public Health*, 17(2), 226–228.

[19] Resende, P. A. A., & Drummond, A. C. (2018). A survey of random forest based methods for intrusion detection systems. *ACM Computing Surveys (CSUR)*, 51(3), 1-36.

[20] Davi, C., Pastor, A., Oliveira, T., Neto, F. B. d. L., Braga-Neto, U., Bigham, A. W., Bamshad, M., Marques, E. T. A., & Acioli-Santos, B. (2019). Severe dengue prognosis using human genome data and machine learning. *IEEE Trans. Biomed. Eng.*, 66(10), 2861–2868.

[21] Tian, Q., Yan, L., Zhang, X., Zhang, X., Hu, Y., Han, Y., Liu, Z., Nan, H., Sun, Q., Sun, Y., Yang, Y., Yu, Y., Zhang, J., Hu, B., Xiao, G., Chen, P., Tian, S., Xu, J., Wang, W., & Cui, G. (2018). Radiomics strategy for glioma grading using texture features from multiparametric MRI. *J. Magn. Reson. Imag.*, 48(6), 1518–1528.

[22] Ouerghi, H., Mourali, O., & Zagrouba, E. (2022). Glioma classification via MR images radiomics analysis. *Vis. Comput*., 38(4), 1427–1441.

[23] Viswanath, G. (2024). Personalized Breast Cancer Prognosis through Data Mining Innovations. *Cuestiones de Fisioterapia*, 53(2), 538-548.

[24] Ding, F., Zhu, G., Alazab, M., Li, X., & Yu, K. (2022). Deep-learning empowered digital forensics for edge consumer electronics in 5G HetNets. *IEEE Consum. Electron. Mag.,* 11(2), 42–50.

[25] Viswanath, G. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. *Turkish Journal of Computer and Mathematics Education*, 12(9), 545-554.

[26] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learn ing techniques. *IEEE Commun. Surveys Tuts.,* 21(3), 2671–2701.

[27] Viswanath, G. (2023). A Real -Time Video Based Vehicle Classification Detection And Counting System. *Industrial Engineering Journal*, 52(9), 474-480.

[28] Dassanayake, P. M., Anjum, A., Bashir, A. K., Bacon, J., Saleem, R., & Manning, W. (2022). A deep learning based explainable control system for reconfigurable networks of edge devices. *IEEE Trans. Netw. Sci. Eng.,* 9(1), 7–19.

[29] Viswanath, G. (2025). Proactive Security in Multi-Cloud Environments: A Blockchain Integrated Real-Time Anomaly Detection and Mitigation Framework. *Cuestiones de Fisioterapia*, 54(2), 392-417.

[30] Hossain, M. S., Muhammad, G., & Guizani, N. (2020). Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics. *IEEE Netw.,* 34(4), 126–132.

[31] Viswanath, G. (2024). International Journal of Information Technology and Computer Engineering. *International Journal of Interpreting Enigma Engineers (IJIEE),* 12(3), 647-657.

[32] Jabeen, T., Ashraf, H., & Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. *J. Ambient Intell. Humanized Comput*., 12(2), 9841–9854.

[33] Viswanath, G. (2024). Machine Learning for IoT Device Anomaly Detection Attack Classification. *International Journal of Mechanical Engineering Research and Technology*, 16(9), 66-76.

[34] Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. Intrusion detection by machine learning: A review. *Expert Syst. Appl*., 36(10), 11994–12000.

[35] Viswanath, G. (2024). A Hybrid Particle Swarm Optimization And C4.5 For Network Intrusion Detection And Prevention System. *International Journal of Computing This link is disabled*, 23(1), 109-115.

[36] Khalid, S., Wu, S., & Zhang, F. (2021). A multi-objective approach to determining the usefulness of papers in academic search. *Data Technol. Appl*., 55(5), 734–748.

[37] Viswanath, G. (2014). Distributed Utility-Based Energy Efficient Cooperative Medium Access Control in MANETS. *International Journal of Engineering Inventions,* 4(2), 08-12.

[38] Bhaskar, K., et.al. (2025). Optimized Risk Assessment Model for Predicting Cardiac Disorders Using AI. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 9(1), 140-159. DOI: https://doi.org/10.5281/zenodo.15493550

[39] Dhanasekhar Reddy, A., et.al. (2025). Unveiling Hidden Risks in Medication Combinations with Graph-Based Adaptive Learning. *International Journal of Health Sciences and Pharmacy (IJHSP*), 9(1), 96-104. DOI: https://doi.org/10.5281/zenodo.15478353

[40] Shantha Spandana, R. R., et.al. (2025). A NovelHybrid Ensemble Framework for Thyroid Disease Diagnosis with Optimized Feature Selection. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 9(1), 115-125. DOI: https://doi.org/10.5281/zenodo.15486406

[41] Sunil Kumar Reddy, T., et.al. (2025). Interpretable AI for Precision Brain Tumor Prognosis: A Transparent Machine Learning Approach. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 9(1), 180-195. DOI: https://doi.org/10.5281/zenodo.15523628

[42] Bhaskar, K., et.al. (2025). Collaborative Intelligence for Securing Next-Generation Healthcare Systems Against Cyber Risks. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 9(1), 85-95. DOI: https://doi.org/10.5281/zenodo.15469623

[43] Yatheendra, K., et.al. (2025). Deep Learning-Powered Dental Diagnostics: Tooth Localization and Condition Assessment from Bitewing X-Rays. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 9(1), 105-114. DOI: https://doi.org/10.5281/zenodo.15479281

****