# CIRA-Cyber Intelligent Risk Assessment Methodology for Industrial Internet of Things Based on Machine Learning

Dr Rohita yamaganti
Associate professor
Department of Information Technology
Sreenidhi Institute of Science and Technology autonomous TS, Hyd, India
rohita.y@sreenidhi.edu.in

Dr Naga siva jyothi kompalli
Associate professor
Department of Information Technology
Sreenidhi Institute of Science and Technology autonomous TS, Hyd, India
sivajyothi.p@sreenidhi.edu.in

Mr. R. Ramesh
Assistant professor
Department of Information Technology
Sreenidhi Institute of Science and Technology autonomous TS, Hyd, India

Praharshith
Student,
Department of Information Technology
Sreenidhi Institute of Science and Technology Autonomous TS, Hyd, India
22311a12q3@it.sreenidhi.edu.in

Maggidi Rohith
Student,
Department of Information Technology
Sreenidhi Institute of Science and Technology Autonomous TS, Hyd, India
22311a12n1@it.sreenidhi.edu.in

Burla Karthik
Student,
Department of Information Technology
Sreenidhi Institute of Science and Technology Autonomous TS, Hyd, India
22311a12k4@it.sreenidhi.edu.in

***Abstract*— The IIoT makes it possible to implement Industry 4.0 applications to require industrial control systems to be more automated, efficient, and monitored in real-time. In spite of these benefits, IIoT infrastructures face high cybersecurity risks that jeopardize their availability, confidentiality, and integrity because of the extensive connections. This work introduces a machine learning-based system of cyber risk assessment to identify imminent threats in the IIoT environment in an active manner. A thorough evaluation is conducted of supervised models such as Multi-Layer Perceptron, XGBoost, LightGBM, RF, LR, KNN, DT, SVM, FSVM, FXGBoost, and ensemble voting classifiers. As per the experimental findings, the ensemble voting-based model has a high-accuracy of 99.3 and F1-score of 0.993 as compared to the individual learners. Explainable AI methods, both LIME and SHAP, are used together to enhance transparency by examining the influence of features on predictions. The trained model is constructed as a Flask-based web framework to enable a practical deployment of the model, where the risk can be evaluated in real-time, and the user can interact with it. To enable quick mitigation decision making, the system categorizes IIoT cyber risk into the outputs of Very Low, Low, Medium, High, and Very High. Overall, the proposed approach demonstrates a stable, understandable, and scalable approach that can effectively build IIoT cybersecurity resilience.**

***"Keywords— Industrial Internet of Things, cybersecurity, cyber threats, risk assessment, machine learning, federated learning, cyber threat intelligence, STRIDE threat modeling".***

## I. INTRODUCTION

The IoT explosive growth has drastically changed how people engage in a variety of fields, such as supply chain management, healthcare, transportation, industrial automation, and smart environments [1]. IoT technologies are transforming the operations by ensuring smooth connection, real-time data exchange, and smart decision-making, and it is estimated that by 2030, there will be 80 billion devices connected. This evolution has brought about the Industrial IIoT, a combination of cyber-physical systems, advanced analytics, and automated processes that facilitate Industry 4.0 in industrial settings [2]. The layered IIoT architecture, a sensing, network, application, and data/service activities, enables scalable, interoperable and secure industrial operations. This enhances efficiency and flexibility in production and manufacturing situations [3].

Notwithstanding these developments, the quick growth of IIoT ecosystems has also increased vulnerability to cybersecurity vulnerabilities, putting organizational assets, data integrity, and industrial processes at serious danger [4]. By exploiting the vulnerabilities of IIoT systems, including insecure communication protocols, lax device security, slow updates, and insufficient data protection mechanisms, attackers can lead to operational outages, financial losses, and safety hazards [5]. The necessity to improve the security challenges associated with large-scale IIoT implementations is explained by the increasing number of cyber attacks that target the industrial settings [6]. Such challenges highlight a major shortcoming of existing practices, which often do not have comprehensive frameworks to systematically identify, evaluate, and mitigate risks of the most interconnected IIoT systems [7].

These gaps require a thorough and proactive method of cyber risk evaluation in terms of threat detection, vulnerability analysis, and prioritization of mitigation [8]. By employing standard scoring systems and publicly available libraries of vulnerabilities, it will be possible to conduct a systematic evaluation of potential security gaps and make informed decisions to reduce exposure [9]. Scalable, privacy-preserving analytical models further enhance the ability to track and deal with emerging risks without compromising on important operations information [10]. Along with the ability to maintain operational continuity, reduce attack surfaces, and develop a more significant prioritization of cyber risks, the proposed method is centered around developing a safe, resilient, and flexible IIoT environment.

These programs are worthy as they can protect critical industrial infrastructure against the evolving cyberthreats as well as enable the complete benefits of IIoT implementation. Besides reducing financial losses, availability, confidentiality and integrity of industrial operations will ensure safety, legal skill, and trust in the interconnected technology. By establishing robust operational controls and comprehensive cyber risk evaluation, helping to promote sustainable development, enhancing operational efficiency, and fostering technological advancement in industries, industrial actors can enhance the security posture of IIoT installations, contribute to the sustainable expansion, and increase operational efficiency [1]–[10].

## II. Related Work

Focusing on the increasing complexity and vulnerability of interconnected systems, the recent literature has critically analyzed cybersecurity risk assessment and mitigation in the context of IoT and IIoT. Singla et al. [11] conducted a multidimensional analysis of the NVD and highlighted the usefulness of the database to track and prioritize the software vulnerabilities in various applications. Although this piece of work gives a lot of knowledge of vulnerability management, it fails to address how it can be integrated with real time industrial system and it is more about the analysis of databases. Vo et al. [12] demonstrated the benefits of decentralized learning in terms of data privacy as well as significantly higher scalability through contrasting centralized and asynchronous federated learning systems with predictive analytics of clinical data. However, the ways to apply these methods to industrial IoT contexts have much to be learned. Kalinin et al. [13] suggested a paradigm of cybersecurity risk assessment in the smart city infrastructures, identifying the most likely attack vectors and prioritized risks. However, the framework does not take into account the dynamic nature of emerging IIoT threats.

Flores et al. [14] analyzed the risk assessment of smart home IoT networks with Bayesian networks which provide a probabilistic approach to quantify the risk of security threats. This paradigm can hardly be generalized to large industrial systems because it has been limited to extremely small-scale situations though it may allow systematic thinking in the face of uncertainty. Kieras et al. [15] proposed a tool to evaluate the risk of supply chains in the IoT ecosystem RIoTS that emphasizes the interdependence of devices and the propagation of vulnerabilities. Although this work has a large scale coverage area, it does not have adaptive features to respond to threat dynamics on a real time basis. The significance of systematic evaluation was underscored by the thorough analysis of the cyber risk evaluation systems and process of prioritizing risks of IoT gadgets by Kandasamy et al. [16]. Nonetheless, instead of providing particular strategies to alleviate operations within industry environments, the paper mostly explores the existing frameworks.

George and Thampi [17] introduced combinatorial methods to defend Industry 4.0 applications against attacks based on vulnerabilities to offer a systematic method of reducing attack surfaces. Nevertheless, this approach is not sufficiently addressing the dynamic risks within IIoT networks, and it is based on unchanging environments. Arat and Akleylek [18] were keen to highlight the significance of active threat detection, focusing on detecting attack paths in IIoT-enabled cyber-physical systems. When it comes to combining risk assessment with adaptive mitigation techniques, the study has limitations. Abbass et al. [19] showed that automated detection methods were possible with the help of deep learning to categorize IoT security issues. However, such problems as data privacy, scalability, and real-time implementation in the industrial environment remain unaddressed. Finally, George and Thampi [20] explored the vulnerability-based risk assessment and mitigation of edge IoT devices and proposed the means of securing dispersed devices. The research fails to completely incorporate risk prioritization within multi-layer IIoT architectures, although it is effective in providing edge-level security.

## III. Materials And Methods

The suggested approach involves the development of a program to identify abnormalities and vulnerabilities that may happen in the future in the IIoT by learning about potential vulnerabilities and issues based on historical and [21] real-time IIoT network data, which is then used to develop an automated cyber risk assessment platform. To identify threats in a comprehensive manner, the model is a combination of multiple supervised learning algorithms, including MLP, XGBoost, LightGBM, RF, LR, KNN, DT, SVM, FSVM, and FXGBoost. To enhance accuracy and robustness via Bagged XGBoost, ensemble-based voting classifiers that locally combine Bagged Random Forest and MLP, and MLP with Bagged XGBoost are applied in a federated learning system [22] in distributed analysis. The system contains elucidable AI techniques, such as as LIME and SHAP, to provide interpretable insights to aid educated security choices and enhance cybersecurity resilience in industrial infrastructures. It is implemented on Flask to make real-time predictions at scale.

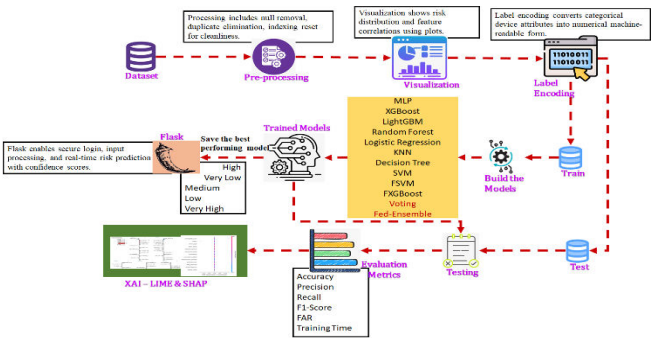


Fig. 1. System Architecture

Fig. 1 illustrates a full machine learning pipeline that predicts risks, starting with the capture of raw data up to the final deployment process. The categorical data are encoded as labels following pre-processing and visualization and the data is split into training and testing. A range of algorithms, such as ensemble methods such as Fed-Ensemble, are evaluated using metrics such as accuracy and F1-score. Finally, Flask is used to deploy the best model and explained with XAI (LIME/SHAP).

### *A) Dataset Collection:*

The dataset is 100,000 records of different devices, sensors, and network parameters and was designed to simulate IIoT situations. Each record contains the device characteristics, security settings, the metrics of vulnerability,

and the potential risk indicators. Exploitability, device risk factor and effect are used to create risk ratings which are then divided into risk levels. This large-scale data can provide a viable basis to evaluate cybersecurity risks and develop predictive risk assessment algorithms of industrial systems.

| | device_model | device_type | vulnerability_score | attack_frequency | patch_status | data_sensitivity | network_exposure | anomaly_score | authentication_strength | encryption_enabled | exploitability |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | Cisco 809 ISR | Raspberry Pi 3B | 3.833166 | 3 | unpatched | 5 | 0.188625 | 94.596642 | medium | yes | 7.833836 |
| 1 | Wind Sensor | Energy & Building Control Unit | 0.716479 | 1 | unpatched | 4 | 0.884995 | 48.166467 | strong | yes | 4.346861 |
| 2 | RH-632 Sensor | Solar Sensor SI V-10-TC | 0.046924 | 3 | up-to-date | 1 | 0.278040 | 12.129439 | strong | yes | 6.118609 |
| 3 | Wind Sensor | Cisco IR1101 Router | 9.294969 | 3 | outdated | 1 | 0.057195 | 29.519531 | strong | yes | 5.332706 |
| 4 | RH-632 Sensor | Tesla Powerwall II | 9.146527 | 2 | outdated | 1 | 0.959384 | 30.965030 | strong | no | 3.327246 |

Fig. 2. Dataset

*B) Pre-Processing:*

The pre-processing pipeline will prepare the IIoT dataset to machine learning by performing data collecting, cleaning, encoding, exploratory analysis, feature scaling, and train-test splitting, ensuring accurate and reliable prediction of cyber risks.

*i) Data preprocessing:* Data preprocessing refers to cleaning and pre-processing data, prior to being analyzed by machine learning. To preserve data integrity, duplicate entries and null values are found and eliminated. To encode them to be suitable in model training, categorical data such as device type, patch status, authentication strength, and encryption status is numerically encoded with label encoding. This kind of steps makes the data complete, uniform and error free to further analysis.

*ii) Exploratory Exploratory data analysis or EDA is performed to comprehend distribution, relationships and trends in the data.* To identify feature interactions, one can use techniques such as drawing correlation heatmaps, visualizing the number of times a given feature appears in counts, and visualizing risk values. To guide feature selection and preprocessing decisions, EDA helps to discover potential trends, imbalances, and correlations between features. It offers crucial insights that guide IIoT cybersecurity model creation, risk classification, and prediction techniques.

*iii) Feature Scaling:* In order to assure that the contribution of each feature in learning is equal, feature scaling normalizes numerical data. Constant variables such as the vulnerability scores, frequency of attacks, network exposure, exploitability and risk factor of a device are all standardized. The scaling enhances the performance of machine learning models, accelerates the convergence of the gradient-based algorithms, and prevents the use of features with larger magnitudes to dominate the model training. To ensure consistency in preparing when making an inference using new IIoT data, the fitted scaler is saved.

*C) Training and Testing:*

Exploratory data analysis or EDA is applied in order to objectively evaluate the work of models by splitting the data into training and testing parts. All the risk levels are equally represented in both groups; this is because it is stratified. The risk prediction machine learning models are trained and tested on the test data on their ability to generalize against the training data. To achieve multi-class evaluation, label binarization is employed in order to compute such metrics as accuracy, precision, recall, F1-score, and ROC-AUC, which ensures a strong and reliable cybersecurity risk assessment.ed to comprehend distribution, relationships and trends in the data.

*D) Algorithms*

*Multi-Layer Perceptron (MLP):* detects threats and anomalies, based on IIoT network traffic and device logs as well as sensor data [24]. It enables the ability to predict cyber risks accurately and helps to integrate into real-time monitoring so that to achieve proactive industrial cybersecurity.

$$\hat{y} = f\left(W^{L} f\left(W^{L-1} \cdots f(W^{1}X + b^{1}) + b^{(L-1)}\right) + b^{L}\right) \quad (1)$$

*XGBoost:* estimates network activity trends, traffic anomalies and device behaviour, providing the [25] fast and accurate detection through iterative error correction, reduction in false alarm and enable credible cyber risk assessment in the large, real time IIoT systems.

$$\hat{y}_i = \sigma\left(\sum_{k=1}^{K} f_k(x_i)\right), f_k \in F \quad (2)$$

*LightGBM:* identifies variants and successfully analyzes threats based on sensor, network, and device data. Scalable and precise detection for real-time industrial monitoring is made possible by its speed and memory optimization [26], which detects intricate patterns in IIoT datasets.

*Random Forest:* Reliable forecasts on high-dimensional IIoT data events are based on the use of multiple decision trees to analyze sensor values, traffic, and device activity. [27] Provides proactive detection of threats and anomalies and supports heterogeneous network inputs in industrial networks.

$$Gini = 1 - \sum_{i=1}^{C} (Pi)^2 \quad (3)$$

*Logistic Regression:* processes network and device data to generate predictions of the probability of security breaches, which are easy to interpret. [28] It complements current machine learning approaches on IIoT cybersecurity and can be used to conduct preliminary risk analysis, indicating feature associations with anomalies.

*K-Nearest Neighbors (KNN):* monitors the readings of current devices and network activities against previous data to detect abnormal activities. [29] It identifies potential anomalies and improves more advanced models within real-time monitoring, which seems to be effective with small to medium IIoT networks.

*Decision Tree:* Arranges normal and abnormal behavior by splitting IIoT data by feature attributes to enable quick vulnerability detection and proactive threat detection in industrial settings by making interpretable and hierarchical decisions [30].

*Support Vector Machine (SVM):* applies optimum hyperplanes in distinguishing between typical and atypical patterns of networks or devices. It provides definite, reliable classification to distinguish safe operations and risky situations of IIoT features spaces of high dimensions.

$$minimize\ \frac{1}{2}\ ||W||^2 + C\sum_{i=1}^{n}\xi_i \quad (4)$$

*Fuzzy Support Vector Machine (FSVM):* V

*FXGBoost:* Evaluates sensor, network and device data, using a combination of multiple boosted trees, which improves detection robustness and accuracy in high-dimensional or noisy IIoT settings, enabling the predictive control of anomalous sensor behaviour and novel cyberthreats.

*Extension Voting Classifier:* improves the accuracy of cyber risk detection in many IIoT devices to support real-time monitoring, reduces false alarms, and enhances detection reliability through the use of soft voting to combine the predictions of models like MLP and Bagged Random Forest.

$$\hat{y}\ = argmax_c\left(\sum_{i=1}^{n} II\ (\hat{y}_i = c)\right) \quad (5)$$

*Federated Extension Voting Classifier:* combines the models that were created on dispersed nodes and preserves privacy because it does not share raw data. allows collaborative threat detection in decentralized IIoT networks, ensuring the safety of risk assessment, high accuracy, and resilience in industrial environments.

*E) Integration of XAI and Flask Framework*

To implement the risk assessment of industrial cybersecurity, the Explainable Artificial Intelligence (XAI) with Flask framework will provide an effective, clear, and user-friendly interface. The XAI algorithms such as the LIME and SHAP are used to interpret the machine learning model predictions and provide data on risk classification, anomaly detection and feature contributions. This interpretability guarantees that the stakeholders in IIoT environments will have the ability to comprehend the rationale behind any forecast, which will lead to greater trust, responsibility, and responsible decision-making. XAI facilitates active cybersecurity and enables detecting possible threats and vulnerabilities in industrial equipment within the shortest time possible by converting the results of complex models into understandable explanations.

To deploy the system to monitor and analyze in real-time, Flask is used as a web application framework that is lightweight. Its seamless integration with underlying machine learning models allows users to input IIoT device data, view risk levels and obtain valuable insights. The combination of XAI and Flask offers an end-to-end platform that ensures safe, understandable, and responsive operations of industrial cybersecurity and ensures that predictions are understandable and transparent.

## IV. Experimental Results

*Accuracy:* Accuracy is the ability of a test to differentiate accurately between healthy cases and patients. To determine the accuracy of a test, the percentage of true positive and true negative in each case analyzed must be determined. This is mathematically given as:

$$Accuracy = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \quad (6)$$

*Precision:* Precision is a measure of the proportion of samples or incidences that are correctly detected to be positive. Thus, the precision can be calculated with the help of the following formula:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} \quad (7)$$

*Recall:* Recall is a measure used in machine learning to evaluate the ability of a model to identify all relevant examples of a certain type. It provides the data on how well a model can reflect the events of a particular type and is determined as a ratio between the number of correct positive instances, predicted by a model, and the number of the real positives.

$$Recall = \frac{\text{TP}}{\text{TP } + \text{ FN}} \quad (8)$$

*F1-Score:* The F1 score is a machine learning evaluation metric that is used to gauge the accuracy of a model. It combines recall and precision scores of a model. The accuracy measure is the count of times a model accurately predicted the entire dataset.

$$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall + Precision} * 100 \quad (9)$$

Table.1 Performance Evaluation Table

| ML Model | Accuracy | F1 Score | Recall | Precision | FAR |
|---|---|---|---|---|---|
| MLP | 0.984 | 0.984 | 0.984 | 0.985 | 0.005 |
| XGBoost | 0.983 | 0.983 | 0.983 | 0.983 | 0.003 |
| LightGBM | 0.983 | 0.983 | 0.983 | 0.983 | 0.037 |
| RF | 0.952 | 0.953 | 0.952 | 0.955 | 0.037 |
| LR | 0.893 | 0.893 | 0.893 | 0.893 | 0.014 |
| KNN | 0.748 | 0.750 | 0.748 | 0.754 | 0.033 |
| Decision Tree | 0.940 | 0.940 | 0.940 | 0.940 | 0.017 |
| SVM | 0.769 | 0.785 | 0.769 | 0.815 | 0.017 |
| FSVM | 0.766 | 0.748 | 0.766 | 0.757 | 0.071 |
| FXGBoost | 0.982 | 0.982 | 0.982 | 0.982 | 0.071 |
| Voting | 0.993 | 0.993 | 0.993 | 0.993 | 0.005 |
| Federated Voting | 0.985 | 0.985 | 0.985 | 0.985 | 0.004 |

To identify cybersecurity risks in IIoT, Voting (BagRF+MLP) model demonstrates the most effective results in Table 1, showing a higher degree of efficacy, robustness, and efficiency.

Fig. 3. Comparison Graph

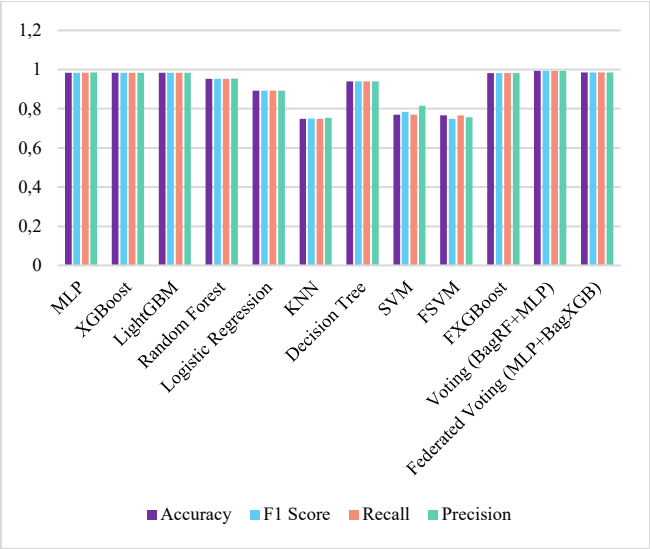


Fig. 3 shows the performance of the ML model best results were obtained with Voting (BagRF+MLP). The color codes are purple (accuracy), blue (F1-score), orange (recall), green (precision), and purple (training time).

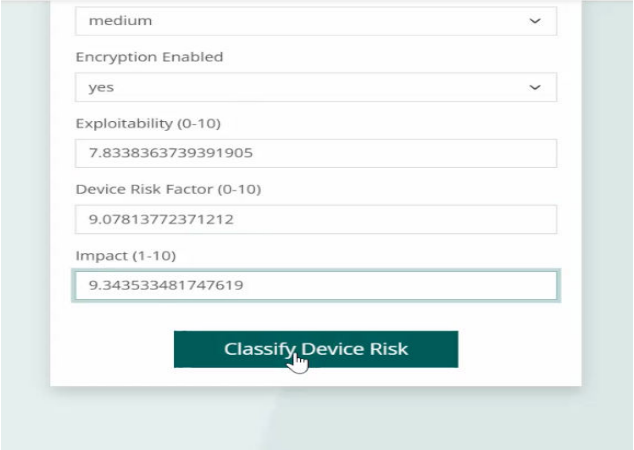


Fig. 4. Enter Input Data

An input interface that allows users to enter data from IIoT devices to automatically classify possible cybersecurity risk levels is shown in Fig. 4.

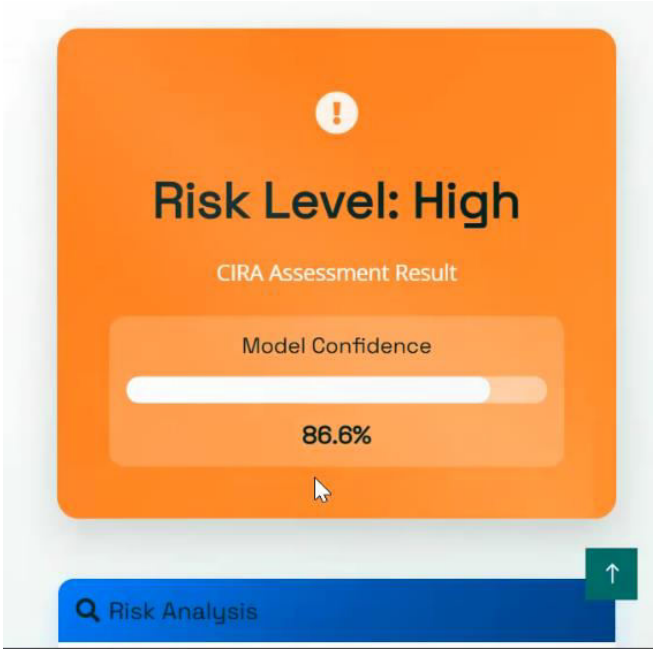


Fig. 5. Predicted Results

The outcome of CIRA assessment is presented in Fig. 5, where the model confidence is 86.6% and the risk level of the IIoT device is of the category High.

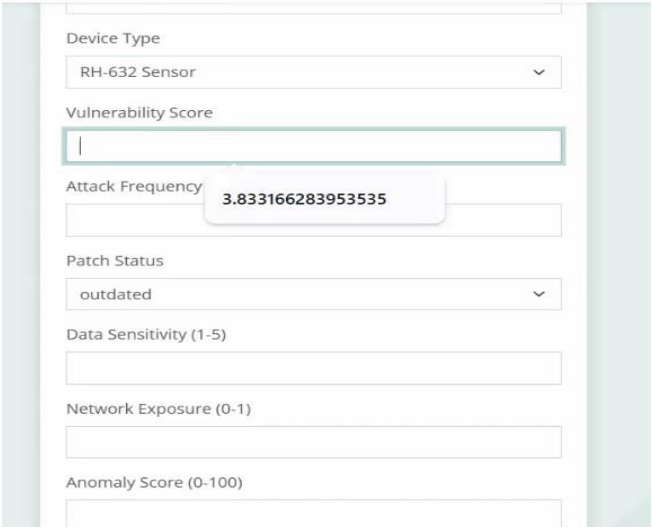


Fig. 6. Enter Input Data

To obtain real-time assessment and the identification of the corresponding risks in terms of cybersecurity, users will be able to enter the information about IIoT devices into the input interface displayed in Fig. 6.

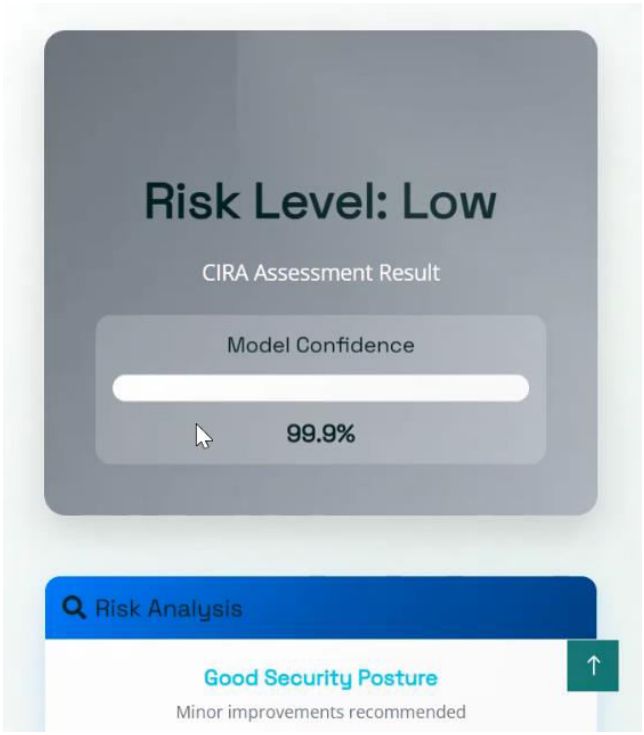


Fig. 7. Predicted Results

The CIRA assessment outcome, demonstrating a low risk rating of the IIoT device with a model confidence of 99.9 is presented in Fig. 7.

## V. Conclusion

The paper shows that ML-based cyber risk assessment can significantly enhance the security posture of Industrial Internet of Things infrastructures. Experimental results show that ensemble learning is more robust and more reliable in detection compared to individual models. Being 99.3% accurate and with a F1 score of 0.993, the voting-based ensemble classifier was very effective, which confirmed its effectiveness to detect many cyber risk patterns. The explainability of AI techniques, such as LIME and SHAP, can improve transparency by revealing the contribution of features and helping to make well-informed decisions by analysts. The optimized model is built on a lightweight Flask web framework, which can be used to implement an interactive monitoring of the system and real-time risk prediction. This interface classifies IIoT traffic into Very Low, Low, Medium, High and Very High risk levels enabling timely mitigation measures. The framework is suitable in continuous monitoring of industries as it is very reliable and able to control false alarms. The approach enables long-term viability and scalability towards safe, data-driven decision making in diverse industrial applications.

Future studies should improve machine learning risk assessment's scalability and applicability for various IIoT environments. Adaptive learning and real-time threat intelligence can be incorporated in zero-day detection. This can be done by making robust hybrids with probabilistic and deep learning architectures. Although multi-domain interoperability, secure communication, and continuous evaluation offers persistent resilience to dynamic industrial cyber threats on a global scale, efficiency optimization is beneficial to devices that have limited resources.

## References

[1] Allafi, R., & Alzahrani, I. R. (2024). Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model. IEEE Access, 12, 63282-63291.

[2] Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.

[3] Nadella, G. S., & Gonaygunta, H. (2024). Enhancing cybersecurity with artificial intelligence: Predictive techniques and challenges in the age of IoT. International journal of science and engineering applications, 13(04), 30-33.

[4] Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., & Silvestri, S. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. Journal of Reliable Intelligent Environments, 11(3), 12.

[5] Rele, M., & Patil, D. (2023). Examining the Impact of Artificial Intelligence on Cybersecurity within the Internet of Things.

[6] C. A. Gabrian, ‘‘Impact zones: How cybercrime disrupts and shapes the landscape of data security,’’ in Proc. Int. Conf. Mach. Intell. Secur. Smart Cities (TRUST), vol. 1, Jul. 2024, pp. 59–68.

[7] Kaspersky. (Mar. 1, 2022). Pushing The Limits: How to Address Specific Cybersecurity Demands and Protect IoT. Kaspersky Press Releases. [Online]. Available: https://www.kaspersky.com/about/press-releases/43-of-businesses-dont-protect-their-full-iot-suite

[8] T. AlSalem, M. Almaiah, and A. Lutfi, ‘‘Cybersecurity risk analysis in the IoT: Asystematic review,’’ Electronics, vol. 12, no. 18, p. 3958, Sep. 2023.

[9] P. Subhash, M. O. H. A. M. M. E. D. Qayyum, K. Mehernadh, K. J. Sahit, C. L. Varsha, and M.N.Hardeep,‘‘Risk assessment threat modelling using an integrated framework to enhance security,’’ J. Theor. Appl. Inf. Technol., vol. 102, pp. 3857–3867, May 2024.

[10] M. Sahinoglu, ‘‘Cyber security risk assessment and optimal risk manage ment of a national vulnerability database,’’ Int. J. Comput. Theory Eng., vol. 16, no. 4, pp. 104–126, 2024.

[11] R. Singla, N. Reddy, R. Bettati, and H. Alnuweiri, ‘‘Toward a multidimensional analysis of the national vulnerability database,’’ IEEE Access, vol. 11, pp. 93354–93367, 2023.

[12] V. T.-T. Vo, T.-H. Shin, H.-J. Yang, S.-R. Kang, and S.-H. Kim, ‘‘A comparison between centralized and asynchronous federated learning approaches for survival outcome prediction using clinical and PET data from non-small cell lung cancer patients,’’ Comput. Methods Programs Biomed., vol. 248, May 2024, Art. no. 108104.

[13] M. Kalinin, V. Krundyshev, and P. Zegzhda, ‘‘Cybersecurity risk assessment in smart city infrastructures,’’ Machines, vol. 9, no. 4, p. 78, Apr. 2021, doi: 10.3390/machines9040078.

[14] M. Flores, D. Heredia, R. Andrade, and M. Ibrahim, ‘‘Smart home IoT network risk assessment using Bayesian networks,’’ Entropy, vol. 24, no. 5, p. 668, May 2022.

[15] T. Kieras, M. J. Farooq, and Q. Zhu, ‘‘RIoTS: Risk analysis of IoT supply chain threats,’’ in Proc. IEEE 6th World Forum Internet Things (WF-IoT), Jun. 2020, pp. 1–6, doi: 10.1109/WF-IoT48130.2020.9221323.

[16] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, ‘‘IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process,’’ EURASIP J. Inf. Secur., vol. 2020, no. 1, pp. 1–18, Dec. 2020, doi: 10.1186/s13635-020-00111-0.

[17] G. George and S. M. Thampi, ‘‘Combinatorial analysis for securing IoT assisted industry 4.0 applications from vulnerability-based attacks,’’ IEEE Trans. Ind. Informat., vol. 18, no. 1, pp. 3–15, Jan. 2022.

[18] F. Arat and S. Akleylek, ‘‘Attack path detection for IIoT enabled cyber physical systems: Revisited,’’ Comput. Secur., vol. 128, May 2023, Art. no. 103174.

[19] W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih, ‘‘Classifying IoT security risks using deep learning algorithms,’’ in Proc. 6th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), Oct. 2018, pp. 1–6.

[20] G. George and S. M. Thampi, ‘‘Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things,’’ Pervas. Mobile Comput., vol. 59, Oct. 2019, Art. no. 101068.

[21] H. Razavi, M. R. Jamali, M. Emsaki, A. Ahmadi, and M. Hajiaghei-Keshteli, ‘‘Quantifying the financial impact of cyber security attacks

on banks: A big data analytics approach,'' in Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE), Sep. 2023, pp. 533–538.

[22] A.Ur-Rehman,I. Gondal, J. Kamruzzaman, and A. Jolfaei, ''Vulnerability modelling for hybrid industrial control system networks,'' J. Grid Comput., vol. 18, no. 4, pp. 863–878, Dec. 2020.

[23] J. S. Yuen, K. L. Choy, H. Y. Lam, and Y. P. Tsang, ''An intelligent risk management model for achieving smart manufacturing on the Internet of Things,'' in Proc. Portland Int. Conf. Manage. Eng. Technol. (PICMET), Aug. 2019, pp. 1–8.

[24] K. Raghunandan, ''Supervisory control and data acquisition (SCADA),'' in Introduction to Wireless Communications and Networks: A Practical Perspective. Cham, Switzerland: Springer, 2022, pp. 321–337.

[25] R. Sasaki, ''Reconsideration of risk communication and risk assessment support methods for security,'' in Proc. IEEE 23rd Int. Conf. Softw. Qual., Rel., Secur. Companion (QRS-C), Oct. 2023, pp. 516–523.

[26] S. Ksibi, F. Jaidi, and A. Bouhoula, ''A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach,'' Mobile Netw. Appl., vol. 28, no. 1, pp. 107–127, Feb. 2023.

[27] A. Mehmood, G. Epiphaniou, C. Maple, N. Ersotelos, and R. Wiseman, ''A hybrid methodology to assess cyber resilience of IoT in energy management and connected sites,'' Sensors, vol. 23, no. 21, p. 8720, Oct. 2023.

[28] P. Chhotaray, B. C. Behera, B. R. Moharana, K. Muduli, and F.-T.-R. Sephyrin, ''Enhancement of manufacturing sector performance with the application of industrial Internet of Things (IIoT),'' in Smart Technologies for Improved Performance of Manufacturing Systems and Services. Boca Raton, FL, USA: CRC Press, 2024, pp. 1–19.

[29] O. Saßnick, T. Rosenstatter, C. Schäfer, and S. Huber, ''STRIDE-based methodologies for threat modeling of industrial control systems: A review,'' in Proc. IEEE 7th Int. Conf. Ind. Cyber-Phys. Syst. (ICPS), May 2024, pp. 1–8.

M. F. Franco, E. Sula, A. Huertas, E. J. Scheid, L. Z. Granville, and B. Stiller, ''SecRiskAI: A machine learning-based approach for cybersecurity risk prediction in businesses,'' in Proc. IEEE 24th Conf. Bus. Informat. (CBI), vol. 1, Jun. 2022, pp. 1–10.