International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(16s) 2026 pp. 357-366
https://doi.org/10.70917/ijcisim-2026-4581
Article

Intelligent Cyber Risk Assessment Framework for Industrial IoT using Ensemble Learning and Explainable AI

Nimmala Bhavana[1], SK Mahaboob Basha[2]

[1]Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Sciences, Sheriguda, Hyderabad, Telangana, India.
Email: bhavananimmala19@gmail.com
[2]Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Sciences, Sheriguda, Hyderabad, Telangana, India.
Email: email2mahaboob@gmail.com

Abstract: — Industrial 4.0 is supported by the IIoT, which can enable increased automation, efficiency, and real-time monitoring of industrial control systems. Regardless of these benefits, the rise of connectivity makes the IIoT systems susceptible to some of the greatest cybersecurity threats, which undermine confidentiality, integrity, and availability. This paper presents a ML-based model of cyber risk assessment designed to identify a threat in IIoT proactively. Supervised models, such as Multi-Layer Perceptron, XGBoost, LightGBM, RF, LR, KNN, DT, SVM, FSVM,FXGBoost, and ensemble voting classifiers are fully evaluated. According to the experimental findings, the ensemble voting-based model is more effective as it reaches a higher accuracy of 99.3 percent, with a higher F1-score of 0.993, compared to the isolated learners. Using eAI methodologies, such as LIME and SHAP, to explain the impact of factors on the prediction improves transparency. The trained model is then deployed using the Flask web framework, enabling real-time risk assessments and interactions with users. The system categorizes the IIoT cyber risk levels as Very Low, Low, Medium, High and Very High which are immediately mitigated. The proposed solution provides an effective, interpretable and scalable treatment, and enhances the cybersecurity resilience of the IIoT.
Keywords: Industrial Internet of Things, cybersecurity, cyber threats, risk assessment, machine learning, federated learning, cyber threat intelligence, STRIDE threat modeling

1. Introduction

In the fast-changing world of IoT, human use patterns across multiple industries – including healthcare, transportation, smart environments, manufacturing, and supply chain management – have been transformed. By 2030, the density of connected devices will have risen to over 80 billion connected devices, as well as IoT technologies will change working conditions by ensuring free connectivity, real-time data exchange, and smart decision-making. Such a development in industrial settings has led to the development of the IIoT that supports Industry 4.0 through the incorporation of cyber-physical systems, improved analytics, and process automation. The IIoT architecture is an architecture of sensing, network, application and data /service layers that allow scalable, interoperable, and secure industrial processes that improve efficiency and flexibility of manufacturing and production environments [3].

Although such advantages are obtained, the rapid development of IIoT ecosystems has also introduced vulnerability to cybersecurity risks, which poses significant risks to the work of the industry, data integrity, and organizational resources [4]. Attackers might exploit exploitable vulnerabilities in IIoT systems, i.e., unsecured communication systems, insufficient device security, slow upgrades, ineffective data protection processes, and interfere with operations causing financial losses and safety hazards [5]. As the number of cyber attacks against industrial premises is growing, this makes it clear that the security issues of the implementation of large-scale IIoT are of critical importance to be addressed [6]. The key problems indicate a serious gap in the existing methodologies

that often do not have comprehensive schemes of detecting, evaluating, and mitigating risks in highly interdependent IIoT systems [7].

The mitigation efforts should take into account all these gaps and a proactive approach to assessment of cyber risks should include threat identification, vulnerability analysis, and prioritization of mitigation measures [8]. The systematic evaluation of the possible security flaws with the help of publicly available vulnerability databases as well as the predetermined grading systems can assist in making informed decisions to reduce exposure [9]. Privacy preserving, scalable analytical systems enhance the ability to track and respond to new threats without compromising important data on operations [10]. The proposed approach will establish a safe, resilient, and flexible IIoT environment that will guarantee that operations continue, minimize the attack surfaces, and prioritize cyber threats.

The significance of such initiatives lies in the fact that they will help protect crucial industrial infrastructure against the evolving cyber threats, as well as enhance the overall benefits of the IIoT deployment. The integrity and confidentiality of industrial operations and their accessibility help to reduce the economic damage and increase the safety, adherence to regulatory requirements, and the confidence in interconnected technology. By conducting a regular cyber risk assessment and putting in place effective operation safeguards, industrial stakeholders can strengthen the security position of IIoT deployments, promote sustainable growth, enhance operational efficiency, and drive technological innovation in most of the industries [1] -[10].

2. Related Work

Recent literature has explored in detail cybersecurity risk assessment and mitigation in the IoT and IIoT environments, and the increasing complexity and vulnerability of interconnected systems. Singla et al. [11] conducted a detailed analysis of the NVD with a particular focus on its efficiency in surveillance and prioritization of software vulnerabilities in different applications. The article provides a lot of information on the vulnerability management, but it mainly focuses on database analysis and fails to include the real-time industrial systems. Vo et al. [12] compared the centralized and asynchronous federated learning techniques in predictive analytics of clinical data and demonstrated the advantages of decentralized learning to maintain the confidentiality of data and support its scalability. However, the applicability of these methodologies in industrial internet contexts has still not been researched properly. Kalinin et al. The framework described in [13] was used to evaluate the cybersecurity risk of smart city infrastructures, where the type of attack vectors is defined, and the importance of hazards is prioritized. But the methodology does not consider the dynamics of the new IIoT threats.

Flores et al. [14] analyzed the risk assessment of smart home IoT networks by using Bayesian networks that provided an approach of a probabilistic approach of quantification of security threats. By allowing a systematic reasoning in unpredictable circumstances, this paradigm enables itself; but it is limited to extremely small-scale situations, and extension to large-scale industrial systems becomes a problemKieras et al. [15] introduced the RIoTS framework for analyzing the risk of IoT and focusing on the dependency that exists between devices and the propagation of vulnerabilities. But it is a work, and, no matter its size, it doesn't have any adaptive mechanisms to react to the dynamic of dangers in the real world. Kandasamy et al. give a detailed overview of the existing cyber risk assessment frameworks and priority ranking methods for IoT systems. [16] indicated that systematic examination is critical. The research does not provide particular methods of operational mitigation in the industrial environment, as it mainly assesses the current frameworks.

George and Thampi [17] suggested that combinatorial methods can be used to defend Industry 4.0 applications from vulnerability attacks. This gives a structured approach to minimise attack surfaces. This approach, nevertheless, assumes the unchanging environments and does not meet the challenge of dynamic threats of IIoT networks. The study by Arat and Akleylek [18] focused on the identification of attack pathways of IIoT-enabled cyber-physical systems with a focus on proactive threats identification. The study is limited to the capability of involving risk evaluation and mitigation through adaptive actions. DL was employed by Abbass et al. [19] to categorise IoT security issues, and it demonstrates how effective automated detection systems can be. However, such questions as scalability, data protection, the implementation in real-time in an industrial environment remain unsolved. George and Thampi [20] examined vulnerability-focused risk assessment and mitigation of edge IoT devices, where, the authors offer methods of ensuring the security of distributed devices. Though good at protecting the edges, the research does not fully incorporate risk prioritization within multi-layer IIoT designs.

3. Materials And Methods

The proposed system develops a smart system of cyber risk evaluation that is specifically tailored to the IIoT conditions and which uses the historical and current IIoT network statistics to predict the likely vulnerabilities and anomalies. The approach uses numerous supervised learning algorithms, including MLP, XGBoost, LightGBM, RF, LR, KNN, DT, SVM, FSVM, and FXGBoost, to provide a comprehensive threat detection approach. Ensemble-based voting classifiers are used to improve accuracy and stability by including Bagged RF and MLP in local mode and MLP with Bagged XGBoost in a federated learning model to perform distributed analysis. The system also uses Flask to make scalable real-time predictions, as well as the explainable AI techniques, including, but not limited to, LIME and SHAP, to provide interpretable forecasts that can support informed security decisions and enhance resilience towards cybersecurity threats in industrial infrastructures.

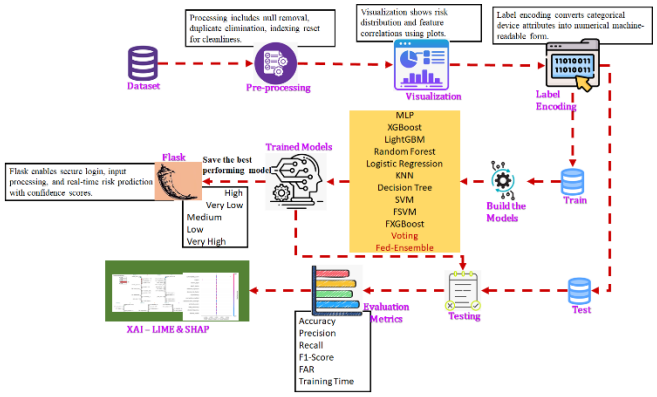


Fig. 1. System Architecture

Figure 1 illustrates a ML pipeline in detail of risk prediction, which includes the full process of raw data capture to the deployment. Categorical data is further encoded with labels before it is split into training and testing data after pre-processing and visualization. Several algorithms, including ensemble methods like Fed-Ensemble, are evaluated based on such measures as accuracy and F1-score. The best model can be explained with the help of XAI methods like LIME and SHAP and deployed with the help of Flask.

A) Dataset Collection:

The dataset was generated to simulate a scenario of the IIoT, and it contains 100,000 records with different devices, sensors, and network measurements. Each record includes characteristics of devices, security configurations, risk measurements, and possible risk signals. [23]. Risk ratings are then determined with the help of exploitability, device risk factor and impact and then divided into various risk levels. This rich data provides a feasible basis of evaluation of cybersecurity risks and developing predictive risk evaluation 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	0.048924	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:

To ensure accurate and reliable prediction of cyber risk, the pre-processing pipeline prepares the IIoT data to feed a ML model by data collection, data cleaning, feature encoding, exploratory data discovery, scaling of features, and train-test splitting.

i) Data preprocessing: Data Processing: Data preprocessing involves cleaning and organizing the data to be used in ML. Data integrity is maintained by identifying null values and duplicate records and deleting them. Numerical encoding through label encoding is used to encode categorical variables, such as device type, patch status,

authentication strength and encryption status, to enable them to be used in model training. These controls ensure that the data is consistent, complete and ready to be further analyzed, without bias or errors.

ii) EDA: EDA is carried out to understand how data are spread with regards to their pattern and relationships. Techniques include visualization of the risk level, the distribution of the values of categorical variables, and heatmap correlations to understand the interactions between the features. EDA indicates possible patterns, differences, and relationships between characteristics, which is used to determine features to be selected and preprocessed decisions. It provides crucial information that can be used to build models, classify risks, and predict in IIoT cybersecurity.

iii) Feature Scaling: The numeric data is scaled using feature scaling. This is to make sure all the features are equally used in the learning process. Continuous variables are standardized such as vulnerability scores, frequency of attacks, network exposure, exploitability and risk factors on devices. Scaling removes the impact of more significant characteristics on model training, improves convergence on gradient-based models, and maximizes the overall effectiveness of ML models. The calibrated scaler is maintained to prepare uniformly when inference is being made on new IIoT data.

C) Training and Testing:

The dataset has been separated into a training set and a testing set for the objective performance to be evaluated and stratified to ensure the training set and the testing set are proportionally represented across all risk levels. The ML predictors for the risk prediction are trained on the training data, and testing data is used to see how well the model generalises their learning. In multi-class assessment, binarization of labels is used, which makes the calculation of metrics like accuracy, precision, recall, F1-score and ROC-AUC easier. It's a reliable and effective measure of cyber risk.

D) Algorithms

Multi-Layer Perceptron (MLP): Assesses IIoT network traffic, device logs, and sensor data to detect threats, as well as abnormalities by identifying complex relationships between characteristics, which can be used to accurately predict cyber risks to support integration into real-time monitoring to implement 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: Processes device behavior, network traffic and network activity trends and allows fast and accurate identification of device behavior by correcting errors through iteration, reducing false alarms and provides reliable cyber risk analysis in large scale and real-time IIoT environments.

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

LightGBM: Interprets sensor, network and device data in order to detect anomalies and assess risks efficiently. Designed to be efficient in speed and memory, [26] is a model that determines complex trends in IIoT data and enables scalable and accurate detection of real-time surveillance of industries.

Random Forest: Aggregates multiple decision trees to assess how devices behave, and traffic and sensor measurements, which offer accurate predictions of the high-dimensional IIoT data. Enables active recognition of threats and abnormalities and effectively deals with various industrial network entries.

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

Logistic Regression: Makes measurable predictions of the probability of security breaches using data of devices and networks, which result in understandable estimates. It is effective to assess initial risk, and it focuses on contributions to anomalies made by features and complements other ML approaches to IIoT cybersecurity.

K-Nearest Neighbors (KNN): Detects abnormal behavior by comparing upcoming metrics of the device and network activity to the past data. It is appropriate to small to medium-scale IIoT networks and identifies the likely anomalies, as well as optimizing more advanced models during real-time monitoring.

Decision Tree: Categorizes IIoT data as normal and abnormal based on the feature criteria. Allows making of understandable, hierarchical decisions, with quick and easy faults identification, and proactive detection of threats in industry.

Support Vector Machine (SVM): Differentiates normal and problematic network/ device topologies based on the optimal hyperplanes. It is effective in highly dimensional IIoT feature space to give accurate and robust classification in order to discriminate between safe and potentially risky activities.

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

Fuzzy Support Vector Machine (FSVM): Incorporates the use of fuzzy membership to overcome ambiguity and inaccurate IIoT readings. Removes the influence of outliers to enhance classification accuracy and provide resilient risk assessment of inconsistent or partially unreliable device and sensor measurements.

FXGBoost: Combines multiple boosted tree to evaluate device, network and sensor data. Increases both accuracy and robustness in high-dimensional or noisy IIoT contexts, where reliable prediction of abnormal behavior and cyber threats of the future can be made.

Extension Voting Classifier: Soft voting Predictions made by the models like Bagged RF and MLP are consolidated. Enhances the accuracy of detection, reduces the number of false alarms, and ensures accurate detection of cyber threats in different IIoT devices to monitor in real-time.

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

Federated Extension Voting Classifier: Combines the models that are trained on the distributed nodes and protects raw data, therefore preserving the privacy. Gets decentralized IIoT networks to cooperatively and jointly identify hazards, ensuring high precision, resiliency, and secure risk analysis of industrial environments.

E) Integration of XAI and Flask Framework

The combination of XAI and the Flask framework offers a robust, clear and user-friendly interface to analyse the risk of cybersecurity threats in the industrial environment. ML model predictions are interpreted using XAI techniques like LIME and SHAP to understand the features contribution, detection of anomalies and risk classification. Such interpretability ensures that the stakeholders understand the basis of each of the predictions, which in turn adds to the trust, accountability, and informed decision-making in IIoT contexts. XAI allows preventing cybercrime issues proactively by transforming the complex model results into readable explanations, allowing the timely identification of potential threats and vulnerabilities of industrial devices.

Flask is a minimalist web application that can be used to deploy a system that was created to monitor and analyze in real time. It allows them to interact with the underlying ML schemes with ease, allowing customers to feed them with data collected by IIoT devices, analyze the risk likelihood, and receive recommendations on what to do. XAI and Flask integration ensure that predictions remain transparent and understandable and provide a unified system of safe, decipherable, and responsive industrial cybersecurity tasks.

4. Experimental Results

Accuracy: accuracy of a test The accuracy of a test in differentiating patients from healthy people. The percentage of true positive and true negative from total number of tests performed is a measure of the effectiveness of a test. This can be mathematically written as:

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

Precision: Precision is the proportion of positive cases which were classified correctly. So the formula to calculate precision is:

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

Recall: Recall in ML is a measure of the ability of a particular model to identify all the instances of a specific class. This will provide some indication of the quality of a model when it comes to identifying cases of a specific type. The ratio of the number of correct positive observations to the total number of positive observations is this.

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

F1-Score: The F1 score is an evaluation measure which checks the accuracy of an ML model. It is the mean of the precision and recall of the model. The more models that can accurately predict from the set of models, the more accurate is the model.

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

"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
Random Forest	0.952	0.953	0.952	0.955	0.037
Logistic Regression	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 (BagRF+MLP)	0.993	0.993	0.993	0.993	0.005
Federated Voting (MLP+BagXGB)	0.985	0.985	0.985	0.985	0.004

Table 1 suggests that the model, which has the highest performance, is Voting (BagRF+MLP), which is characterized by a high level of efficacy, robustness, and efficiency in the detection of IIoT cybersecurity risks.

Fig. 3. Comparison Graph

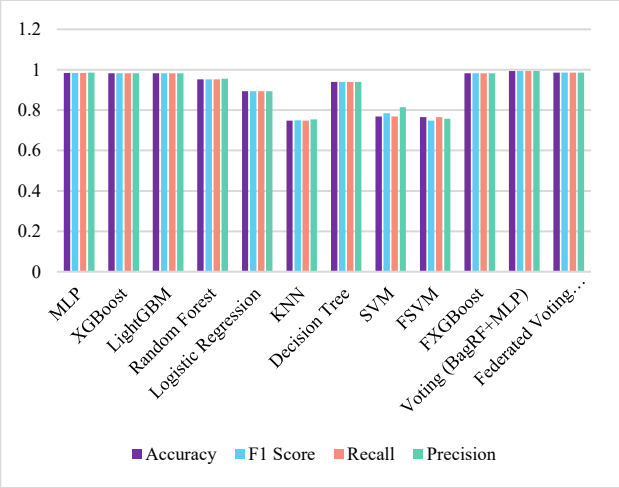
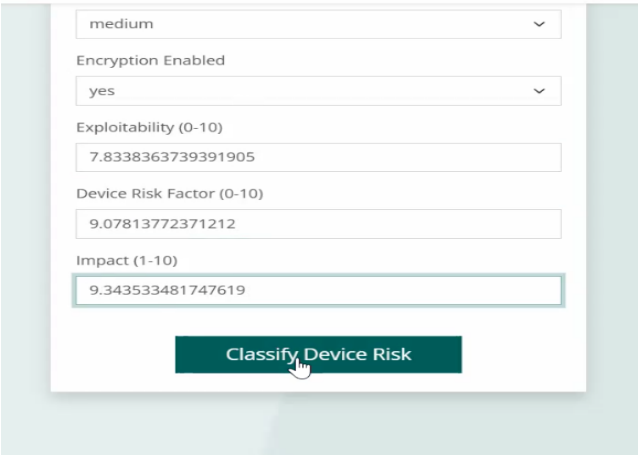


Figure 3 shows the work of the ML model, where Voting (BagRF+MLP) achieves the best results. The values in purple, blue, orange, green, and purple represent accuracy, F1-score, recall, precision, and training time respectively.



"Fig. 4. Enter Input Data"

Figure 4 illustrates an input interface where users can provide data of the IIoT devices in order to automatically evaluate the possible level of the cybersecurity risks.

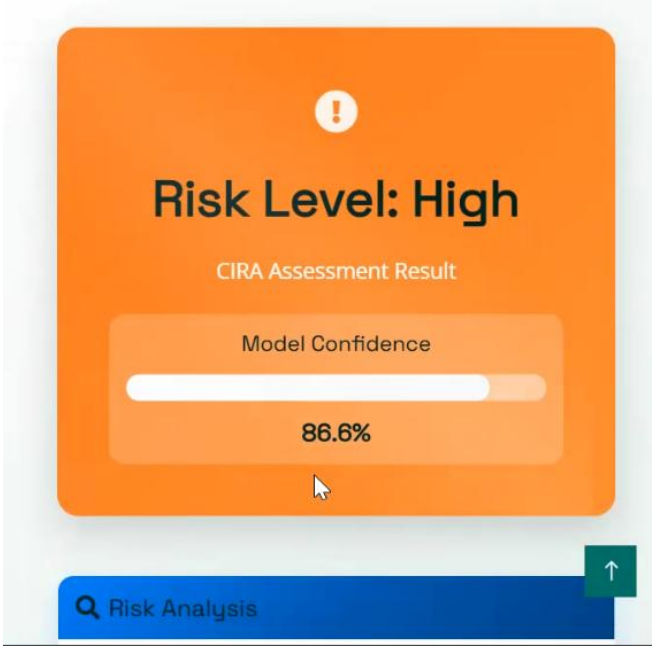
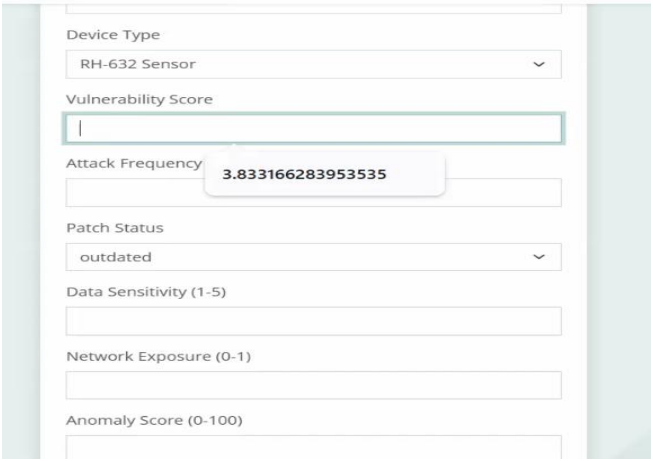


Fig. 5. Predicted Results

The Figure 5 shows the evaluation result of CIRA, which shows that the IIoT device has a high risk rating with a model confidence of 86.6%.



“Fig. 6. Enter Input Data”

Figure 6 demonstrates an input interface with which users can input the information about IIoT devices to the real-time evaluation and detection of the level of cybersecurity risk.

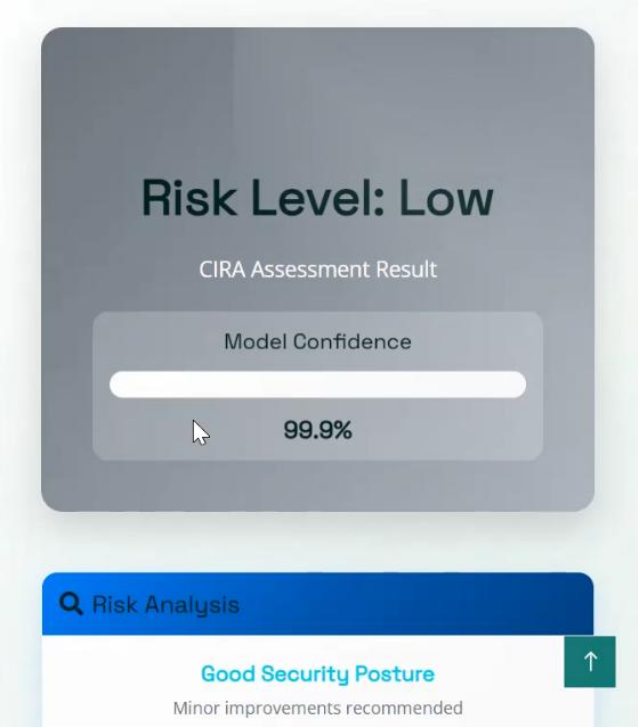


Fig. 7. Predicted Results

The CIRA assessment result shows in Figure 7 with a rating of a low risk of the IIoT device, and model confidence of 99.9%.

5. Conclusion

The study confirms that ML-based cyber risk evaluation makes a significant contribution to the security platform of Industrial IoT infrastructures. It has been shown that in cases of ensemble learning, the robustness and detection reliability is higher than that of individual models. The ensemble classifier using the voting-based classifier achieved excellent performance of 99.3 percent accuracy and 0.993 F1 score, and thus verifies its effectiveness in identifying different patterns of cyber risks. Inclusion of explainable artificial intelligence methods, i.e. LIME and SHAP, also increases the transparency by explaining the contribution of features as well as making informed decisions by the analysts. The optimised model is deployed with a lightweight Flask web framework to enhance the real-time prediction of dangers and interactive monitoring. The interface is linked to the IIoT traffic and categorises it into Very Low, Low, Medium, High and Very High risk categories, allowing hazards to be reduced more easily. The framework is very reliable and tries to reduce false alarms, which makes it suitable in constant monitoring of industries. The approach supports scalable application and long-term sustainability to make data-driven, secure decisions in the industrial environment.

The scalability and applicability of ML risk assessment in diverse IIoT environments ought to be enhanced in future studies. Real-time threat intelligence, together with adaptive learning, will help improve the zero-day detection. DL combined with probabilistic models could be more robust in the form of hybrid ensembles. Efficiency optimization supports the devices with resource constraints and multi-domain interoperability, secure communication, and continuous assessment ensure the long-term resilience against the rising global industrial cyber threats.

The data is divided into training data and testing data. First data set for training and Second data set for testing. The model is helpful if it is able to predict by naming the model data in the training set. The test set is used for testing the model with unknown data.

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.
30. 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.