A Machine Learning Driven Framework for Proactive Cyber Risk Detection and Classification in Industrial Internet of Things Systems

N Harini[1], Jithendra Kukutla[2], K Yatheendra[3]

[1]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: haraninandhi@gmail.com , ORC-ID: https://orcid.org/0009-0000-0927-5877

[2] Assistant Professor, Department of CSE(AI &ML), Santhiram Engineering College, Nandyal, Kurnool Dist, AP,E-mail:24x51d1304@srecnandyal.edu.in

[3]Assistant Professor, Department of CSE(AI & ML), Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: k.yatheendra84@gmail.com, ORC-ID: https://orcid.org/0009-0003-1382-8587

To Cite this Article

N Harini, Jithendra Kukutla, K Yatheendra, "A Machine Learning Driven Framework for Proactive Cyber Risk Detection and Classification in Industrial Internet of Things Systems", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 04, April 2026,pp: 298-307, DOI: http://doi.org/10.64771/jsetms.2026.v03.i04.pp298-307

Submitted: 28-02-2026 Accepted: 01-04-2026 Published: 08-04-2026

Abstract: The Industrial Internet of Things (IIoT) makes Industry 4.0 possible by making industrial control systems more automated, efficient, and able to watch things in real time. Even with these benefits, IIoT infrastructures that are highly connected are open to major cybersecurity threats that can compromise their privacy, integrity, and availability. This paper shows a cyber risk assessment method based on machine learning that can be used to find threats before they happen in IIoT environments. A lot of different supervised models are tested, such as Decision Tree, Support Vector Machine, XGBoost, LightGBM, Random Forest, Logistic Regression, K-Nearest Neighbors, Decision Tree, FSVM, FXGBoost, and ensemble vote classifiers. The experimental results show that the group voting-based model works best, with a score of 0.993 and a 99.3% accuracy rate, doing better than individual learners. Artificial intelligence methods that can be explained, like LIME and SHAP, are used to improve clarity by figuring out how features affect predictions. For real-world use, the trained model is put together using a Flask-based web framework that lets users connect and assess risks in real time. The system sorts IIoT cyber risk levels into outputs that are Very Low, Low, Medium, High, and Very High. This helps people make quick choices about how to reduce the risk. Overall, the suggested method shows a strong, clear, and expandable answer that effectively boosts IIoT cybersecurity resistance.

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

1. INTRODUCTION

The fast growth of the Internet of Things (IoT) has completely changed many areas of human life, such as transportation, healthcare, smart environments, workplace automation, and supply chain management [1]. It is expected that by 2030, there will be 80 billion connected gadgets. IoT technologies are changing the way things are done by allowing seamless connectivity, real-time data exchange, and smart decision-making. The Industrial Internet of Things (IIoT) was created because of this change in the business world. It helps with Industry 4.0 by combining cyber-physical systems, advanced analytics, and automatic processes [2]. The layered IIoT architecture, which is made up of sensing, network, application, and data/service layers, makes industrial processes scalable, interoperable, and safe. This increases efficiency and flexibility in production and manufacturing settings [3].

Even with these improvements, the fast growth of IIoT ecosystems has also made them more vulnerable to cyber threats, which can seriously harm business processes, data integrity, and company property [4]. Attackers can take advantage of flaws in IIoT systems, such as communication methods that aren't secure, devices that aren't secure, updates that are late, and data protection systems that aren't strong enough. This can cause problems with

operations, cost money, and put people in danger [5]. The growing number of cyberattacks on industrial settings makes it even more important to deal with the security issues that come with large-scale IIoT deployments [6]. These problems show a major weakness in the way things are done now: they don't always include complete plans for finding, analyzing, and reducing risks in IIoT systems that are highly connected [7].

To close these holes, we need to look at cyber risk assessment as a whole and be proactive. We need to focus on finding threats, analyzing vulnerabilities, and setting priorities for prevention [8]. Using freely available vulnerability databases and consistent scoring methods lets you check for possible security holes in a planned way and helps you make smart choices to lower your risk [9]. Scalable analytical frameworks that protect privacy make it even easier to keep an eye on new threats and act to them without putting sensitive operational data at risk [10]. The suggested method focuses on creating a safe, strong, and flexible setting for IIoT systems while keeping operations going, lowering attack surfaces, and making it easier to decide which security risks are most important. These attempts are important because they could protect important industrial infrastructure from new cyber threats while also letting IIoT users get the most out of the technology. Making sure that industrial processes are safe, private, and available not only cuts down on economic losses, but it also helps with safety, following the rules, and trust in connected technologies. Industrial stakeholders can improve the security of IIoT deployments, encourage long-term growth, boost operational efficiency, and encourage technological innovation across all fields by putting in place a systematic cyber risk assessment and strong operational protections [1–10].

2. LITERATURE REVIEW

A lot of new research has been done on how to measure and reduce cybersecurity risks in IoT and IIoT environments. This research shows that connected systems are getting more complicated and vulnerable. Singla et al. [11] did a multidimensional study of the National Vulnerability Database (NVD) to show how useful it is for keeping track of and ranking software vulnerabilities in a wide range of applications. This work gives a lot of information about managing vulnerabilities, but it mostly just looks at databases and doesn't connect to real-time industrial systems. Vo et al. [12] looked at centralized and asynchronous federated learning methods for predictive analytics in clinical data. They showed that decentralized learning is better for keeping data private and making it easier to scale. But it's still not clear how these kinds of methods can be used in industrial IoT settings. Kalinin et al. [13] suggested a way to evaluate the cybersecurity risks in smart city infrastructures by finding possible attack paths and ranking the risks. However, the approach doesn't take into account how IIoT threats change over time.

Flores et al. [14] looked into how to rate risk for IoT networks in smart homes using Bayesian networks, which give a probabilistic way to measure security risks. This method allows for structured reasoning when there is doubt, but it only works in small settings, which makes it hard to apply to large, complicated industrial systems. Kieras et al. [15] introduced RIoTS, a way to look at supply chain risks in IoT ecosystems that focuses on how devices are linked together and how vulnerabilities spread. Even though this work covers a lot of ground, it doesn't offer any ways to change to changing threats in real time. Kandasamy et al. [16] looked at cyber risk assessment frameworks and risk ranking processes for IoT systems as a whole. This shows how important it is to do a thorough review. However, the study mostly looks at current frameworks and doesn't suggest any new ways to make industrial environments safer.

Combinatorial methods were first presented by George and Thampi [17] as a way to protect Industry 4.0 apps from vulnerability-based attacks. They provide a structured way to lower attack surfaces. Still, this method is based on the idea that settings stay the same, and it doesn't fully account for how threats change in IIoT networks. Arat and Akleylek [18] studied how to find attack paths for IIoT-enabled cyber-physical systems. This showed how important it is to find threats before they happen. The study doesn't look into how to combine risk assessment with flexible ways to reduce risks. Abbass et al. [19] used deep learning to sort IoT security risks into groups, showing how useful automatic detection systems can be. But problems like scalability, data privacy, and real-time application in industrial settings haven't been solved yet. Lastly, George and Thampi [20] looked into vulnerability-based risk assessment and mitigation for edge IoT devices and came up with ways to keep spread devices safe. The study only looks at risk prioritization across single-layer IIoT systems, but it does work well for protecting the edge.

3. MATERIALS AND METHODS

The suggested system creates a smart method for assessing cyber risks in Industrial Internet of Things (IIoT) settings. It does this by using historical and [21] real-time IIoT network datasets to guess possible weaknesses and strange behavior. For full threat identification, the method uses many supervised learning algorithms, such as

Multi-Layer Perceptron (MLP), XGBoost, LightGBM, Random Forest, Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), FSVM, and FXGBoost. To make the system more accurate and reliable, ensemble-based voting models are used. These combine Bagged Random Forest and MLP locally, and MLP with Bagged XGBoost in a federated learning setup for distributed analysis [22]. The system is set up using Flask to make scalable real-time predictions. It uses explainable AI methods, like LIME and SHAP, to give us understandable insights that help us make better security decisions and make industrial infrastructures safer.

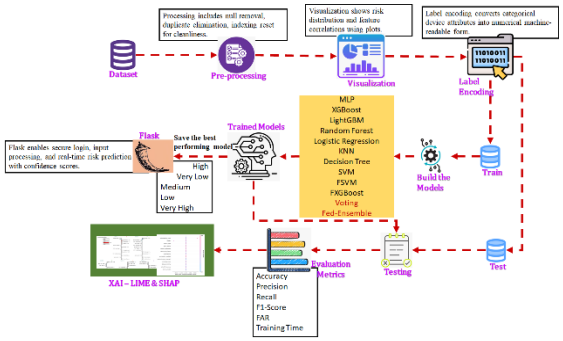

Fig.1 Proposed Architecture

Figure 1 shows a full machine learning process for predicting risk, from getting the raw dataset to putting it into use. Categorical data goes through Label Encoding after Pre-processing and Visualization. It is then split into groups for training and testing. Metrics like precision and F1-score are used to judge different algorithms, such as ensemble methods like Fed-Ensemble. Finally, XAI (LIME/SHAP) is used to explain the best model, which is then put into use using Flask.

a) Dataset Collection:

The dataset, which has 100,000 records with different devices, sensors, and network parameters, was made to model Industrial Internet of Things (IIoT) environments. Each record has information about the gadget, how it is secured, how vulnerable it is, and possible risk indicators. [23] Risk scores are made up of three parts: exploitability, device risk factor, and effect. These scores are then put into different risk levels. This large dataset gives us a solid foundation for looking at cyber threats and creating models that predict how dangerous industrial systems might be.

	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	0.188623	94.596642	medium	yes	7.833836
1	Wind Sensor	Energy & Building Control Unit	0.716479	1	unpatched	4	0.884995	46.166467	strong	yes	4.346861
2	RH-632 Sensor	Solar Sensor SI-V-10-TC	0.048824	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 collects, cleans, encodes, explores, features scales, and splits the IIoT dataset so that it is ready for machine learning. This makes sure that the cyber risk prediction is accurate and dependable.

i) Data preprocessing: Cleaning up and getting the information ready for machine learning analysis is what data preprocessing is all about. To keep the data's integrity, null values and duplicate records are found and gotten rid of. Label encoding turns categorical traits like device type, patch status, authentication strength, and encryption status into numbers so that they can be used to train models. These steps make sure that the dataset is full, consistent, and ready for more analysis without any mistakes or bias.

ii) Exploratory Data Analysis (EDA): Exploratory Data Analysis (EDA) is used to figure out how the data is distributed, how it is related to other data, and what trends it shows. Some techniques are showing risk levels visually, looking at value counts for categorical features, and making association heatmaps to see how features interact with each other. EDA helps find possible patterns, imbalances, and connections between features, which guides choices about which features to use and how to prepare the data. It gives important information that is used to make models, classify risks, and make predictions in IIoT hacking.

iii) Feature Scaling: Feature scaling makes numerical data more uniform so that all features add equally to the learning process. Standardization is used on continuous factors like device risk factor, network exposure, attack frequency, vulnerability scores, and how easy it is to exploit. Scaling stops features with bigger sizes from controlling model training, speeds up convergence for gradient-based algorithms, and makes machine learning

models work better overall. The fitted scaler is saved so that it can be used for uniform preprocessing when new IIoT data is used for inference.

c) Training and Testing:

To get an objective look at how well the model works, the dataset is split into training and testing groups. A tiered split makes sure that both sets have an equal number of people with each risk level. Training data is used to make machine learning models that can predict risks, and testing data makes sure that the models can work in real life. Label binarization is used for multi-class evaluation, which lets you figure out measures like F1-score, ROC-AUC, accuracy, precision, and recall. This makes sure that the cybersecurity risk assessment is strong and reliable.

d) Algorithms:

Multi-Layer Perceptron (MLP): Looks at IIoT network traffic, device logs, and sensor data to [24] find threats and oddities by figuring out how complex relationships between features work. This lets you accurately predict cyber risks and supports integrating into real-time tracking for 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: Looks for patterns in how devices act, how networks work, and strange traffic patterns. This helps find problems quickly and correctly by fixing mistakes over and over again. This lowers the number of false alarms and supports accurate cyber risk assessment in big, 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: handles data from sensors, networks, and devices to find problems and quickly evaluate risks. It captures complex patterns in IIoT datasets and is optimized for speed and memory [26]. This makes it possible for scalable and accurate detection for real-time industrial tracking.

Random Forest: Combines several decision trees to look at how devices behave, how traffic flows, and sensor readings, making accurate guesses for large amounts of IIoT data. [27] Helps find threats and strange behavior before they happen, and handles different types of network data well.

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

Logistic Regression: Models the likelihood of security breaches using data from devices and networks, making predictions that can be understood. [28] It works well for quick risk assessment, shows how features contribute to outliers, and works well with other machine learning methods for IIoT security.

$$\hat{y}_i = \sigma(w^T x + b) = \frac{1}{1 + e^{-(w^T x + b)}} \quad (4)$$

K-Nearest Neighbors (KNN): Compares present device readings and network activity with past data to find strange behavior. [29] It works for small to medium-sized IIoT networks, finds possible problems, and works with more advanced models for real-time tracking.

$$distance(x, X_i) = \sqrt{\sum_{j=1}^{d} \left(x_j - X_{i_j}\right)^2} \quad (5)$$

Decision Tree: Splits IIoT data into groups based on feature criteria to tell the difference between normal and unusual behavior. Hierarchical decision-making that is easy to understand helps find vulnerabilities quickly and supports proactive threat detection in industry settings.

$$I\,(i) = 1 - \sum_{i=1}^{k} p_i^2 \quad (6)$$

Support Vector Machine (SVM): Using optimal hyperplanes, it tells the difference between normal and abnormal network or device trends. It works well in IIoT feature spaces with a lot of dimensions and gives accurate, reliable classification to tell the difference between safe activities and possible threats.

$$minimize\ \frac{1}{2}\ ||W||^2 + C \sum_{i=1}^{n} \xi_i \quad (7)$$

Fuzzy Support Vector Machine (FSVM): It uses fuzzy membership to deal with uncertainty and noisy IIoT data. Lowers the impact of outliers, which improves the accuracy of classification and gives a strong risk assessment for device and sensor data that are inconsistent or partly unreliable.

FXGBoost: Boosted trees are used to look at data from devices, networks, and sensors. It makes detection more accurate and reliable in IIoT settings with a lot of dimensions or noise, so it's possible to reliably predict strange behavior and new cyber risks.

Extension Voting Classifier: Using soft voting, it brings together results from models like Bagged Random Forest and MLP. Improves the accuracy of detection, cuts down on fake alarms, and makes sure that cyber risks are correctly identified across a wide range of IIoT devices for real-time monitoring.

$$\hat{y} = argmax_c \left(\sum_{i=1}^{n} II\ (\hat{y}_i = c) \right) \quad (8)$$

Federated Extension Voting Classifier: Brings together models that were learned on different nodes without sharing raw data, which protects privacy. Allows multiple autonomous IIoT networks to work together to find threats, making sure that risk assessment is accurate, reliable, and safe in industrial settings.

e) Integration of XAI and Flask Framework

Explainable Artificial Intelligence (XAI) and the Flask framework work together to make a strong, clear, and easy-to-use interface for evaluating hacking risks in businesses. XAI methods, like LIME and SHAP, are used to understand what machine learning models are saying, giving us more information about how features work, finding outliers, and figuring out risk. This interpretability makes sure that everyone involved can see how each prediction was made. This builds trust, holds people accountable, and helps people make better decisions in IIoT settings. XAI helps with proactive cybersecurity management by turning complicated model outputs into explanations that are easy to understand. This lets potential threats and weaknesses in industrial devices be found quickly.

Flask is a simple web application framework that lets you set up the system for tracking and analyzing in real time. It lets users easily connect with the machine learning models underneath, so they can send data from IIoT devices, see how risky they are, and get insights they can use. When you combine XAI and Flask, predictions are clear and easy to reach. This creates a complete system for safe, understandable, and quick industrial cybersecurity operations.

4. EXPERIMENTAL RESULTS

Accuracy: How well a test can tell the difference between sick and healthy people is called its accuracy. To get an idea of how accurate a test is, we should figure out what percentage of cases are true positives and true negatives. In terms of math, this can be written as

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} \quad (9)$$

Precision: Precision is the percentage of correctly classified cases or samples compared to those that were correctly classified as positives. So, here is the method to figure out the precision:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (10)$$

Recall: In machine learning, recall is a metric that shows how well a model can find all the important instances of a certain class. It shows how well a model captures instances of a certain class. It is calculated by dividing the number of correctly predicted positive observations by the total number of real positives.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \quad (11)$$

F1-Score: The F1 score is a way to rate the correctness of a machine learning model. It takes a model's accuracy and recall scores and adds them together. The accuracy metric counts how many times, across the whole dataset, a model made a correct guess.

$$F1\ Score = 2 * \frac{Recall\ \mathrm{X}\ Precision}{Recall + Precision} * 100 \quad (12)$$

Table.1 Performance Evaluation Table

ML Model	Accuracy	F1 Score	Recall	Precision	FAR	Training Time
MLP	0.984	0.984	0.984	0.985	0.005	6.250
XGBoost	0.983	0.983	0.983	0.983	0.003	6.810
LightGBM	0.983	0.983	0.983	0.983	0.037	19.478
Random Forest	0.952	0.953	0.952	0.955	0.037	41.483

Logistic Regression	0.893	0.893	0.893	0.893	0.014	4.673
KNN	0.748	0.750	0.748	0.754	0.033	0.238
Decision Tree	0.940	0.940	0.940	0.940	0.017	0.540
SVM	0.769	0.785	0.769	0.815	0.017	35.384
FSVM	0.766	0.748	0.766	0.757	0.071	86.255
FXGBoost	0.982	0.982	0.982	0.982	0.071	63.448
Voting (BagRF+MLP)	**0.993**	**0.993**	**0.993**	**0.993**	**0.005**	**137.398**
Federated Voting (MLP+BagXGB)	0.985	0.985	0.985	0.985	0.004	157.097

The Voting (BagRF+MLP) model has the best performance (Table.1), showing that it is the most effective, stable, and efficient way to find IIoT cybersecurity risks.

Fig.3 Comparison Graph

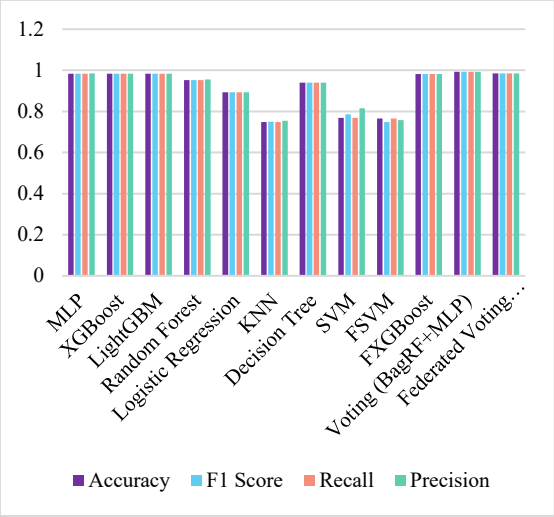

Figure 3 displays the success of ML models, with Voting (BagRF+MLP) showing the best results. F1-score is shown in blue, accuracy is shown in purple, recall is shown in orange, precision is shown in green, and training time is shown in purple.

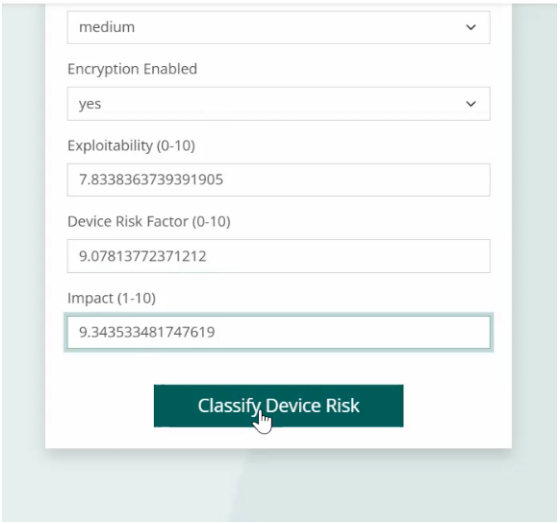

Fig.4 Enter Input Data

Figure 4 shows an input interface where IIoT device data can be entered to get an automatic list of possible cybersecurity risk levels.

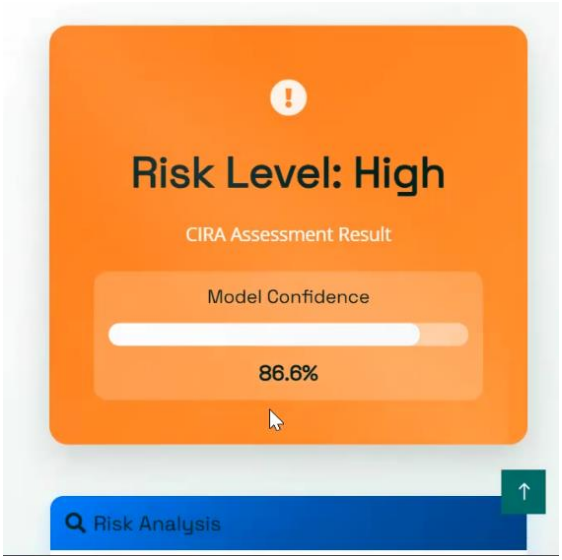

Fig.5 Predicted Results

The CIRA report (Fig.5) shows that the IIoT device has a "High" risk level, with an 86.6% model trust.

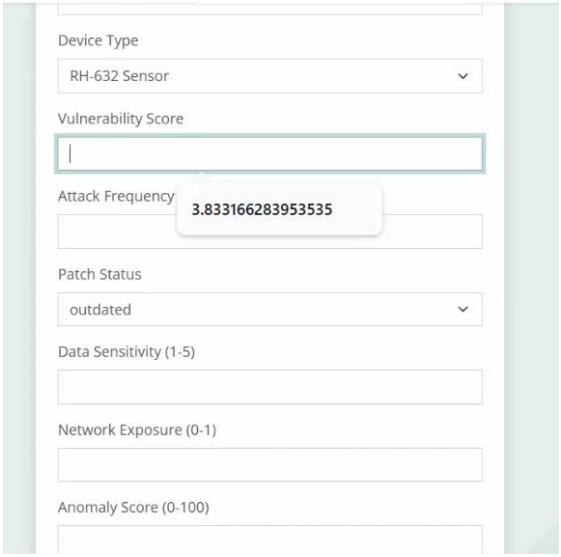

Fig.6 Enter Input Data

Figure 6 shows an input interface where users can enter information about IIoT devices to get a real-time evaluation and amount of cybersecurity risk for those devices.

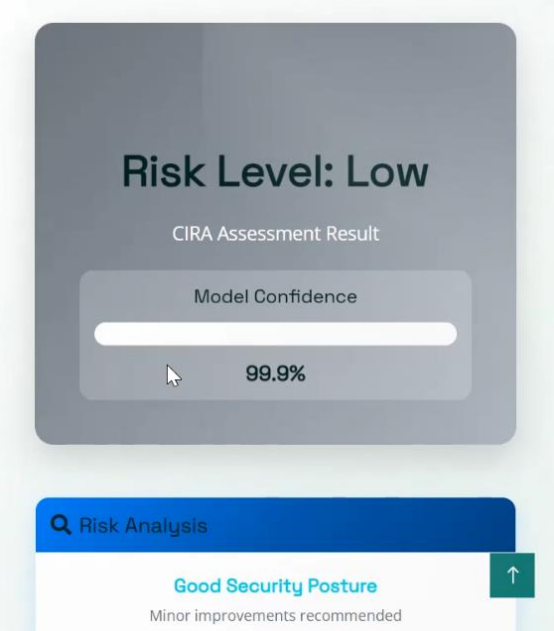

Fig.7 Predicted Results

The CIRA assessment result, shown in Fig.7, shows that the IIoT device has a "Low" risk level, with a model confidence of 99.9%.

5. CONCLUSION

According to the study, cyber risk assessment that is driven by machine learning makes Industrial Internet of Things systems much safer. The results of experiments show that ensemble learning is better at being stable and reliable at detecting problems than standalone models. In particular, the voting-based ensemble classifier did the best, with an F1-score of 0.993 and a 99.3% success rate, showing that it is good at finding different cyber risk trends. Adding explainable AI techniques like LIME and SHAP increased transparency by making feature contributions more clear. This built trust among analysts and helped them make better security choices. So that it can be used in the real world, the optimized model is put into use using a Flask-based web framework. This lets cyber risk predictions happen in real time and user contact go smoothly. This interface sorts IIoT data into levels of actionable risk, such as Very Low, Low, Medium, High, and Very High. This lets timely responses be made to lower the risk. The framework is very reliable and keeps false alarms under control, so it can be used for constant industrial monitoring. Overall, the results show that using a lightweight Flask deployment along with an approach that is interpretable and ensemble-driven is a scalable, reliable, and useful way to handle cybersecurity risks in IIoT environments that are changing.

The machine learning-based risk assessment framework can be made more scalable and flexible for different IIoT environments through future study. It is possible to make the system better at finding new and unknown attacks by adding real-time threat intelligence and adaptive learning methods. More research into hybrid ensemble methods that use both deep learning and probabilistic models could lead to more accurate predictions that hold up in changing network conditions. Optimizing model efficiency to lower computational overhead while keeping high detection performance can also make adoption easier in IIoT devices with limited resources. Industrial networks can be made more reliable by looking into secure communication methods and multi-domain interoperability. The cyber risk assessment method will stay reliable and useful as long as it is evaluated regularly and attack scenarios are changed.

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] Lakshmi, J. M., Prasad, K. K., & 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.

[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] G, Viswanath., N, Madhvik., K, Bhaskar., K, Supriya. (2024). Machine-Learning-Based Cloud Intrusion Detection. International Journal of Mechanical Engineering Research and Technology, 16(9), 38–52.

[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 multidi mensional 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] Viswanath, G., Prasad, K. K., Lakshmi, J. M., & Swapna, G. (2025). Diabetes Diagnosis Using Machine Learning with Cloud Security. Cuestiones De Fisioterapia, 54(2), 417–431. https://doi.org/10.48047/r2mhn978

[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] Gudditti, V., & Krishna, P. V. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 545–554.

[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 toWireless 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