International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

PREDICTIVE CYBER RISK ASSESSMENT FRAMEWORK FOR INDUSTRIAL IOT SYSTEMS WITH MACHINE LEARNING

[1]J.Mohan Kumar, [2]Kanike Udaya Swetha, [3]Ediga Swathi, [4]P Iman Zaberiya, [5]Talari Rabika
[1] Associate Professor, [2345] Students
Department of Computer Science and Engineering
St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool, A.P.
jmksjcet@gmail.com, kanikeudayaswetha@gmail.com, edigaswathie@gmail.com, pimanzaberiya@gmail.com, rabika8785@gmail.com

ABSTRACT

The rapid adoption of Industrial Internet of Things (IIoT) systems has significantly enhanced automation, productivity, and operational efficiency in industrial environments. However, the increasing connectivity and data exchange in IIoT networks have also introduced complex cybersecurity risks, making traditional security mechanisms insufficient to address evolving cyber threats. This study presents a cyber intelligent risk assessment framework for Industrial IoT systems using machine learning techniques. The proposed approach leverages data-driven models to analyze network traffic, device behavior, and system vulnerabilities to identify potential cyber risks in real time. Machine learning algorithms such as supervised and unsupervised learning are employed to detect anomalies, classify attack patterns, and predict potential security breaches with high accuracy. The framework enhances proactive decision-making by enabling early threat detection and adaptive risk mitigation strategies. Experimental analysis demonstrates that the proposed model improves detection accuracy, reduces false alarms, and strengthens the overall cybersecurity posture of industrial environments. This research highlights the effectiveness of machine learning–based cyber risk assessment in ensuring secure and resilient IIoT infrastructures.

Keywords

Industrial Internet of Things (IIoT), Cybersecurity, Risk Assessment, Machine Learning, Anomaly Detection, Intrusion Detection, Smart Manufacturing.

I. INTRODUCTION

1.1 Introduction

The Industrial Internet of Things (IIoT) has transformed modern industries by enabling smart manufacturing, real-time monitoring, and automated decision-making through interconnected devices and sensors. While IIoT improves efficiency, productivity, and operational visibility, it also introduces significant cybersecurity challenges due to its large attack surface, heterogeneous devices, and continuous data exchange. Traditional security mechanisms are often inadequate to handle sophisticated cyberattacks such as malware intrusion, data manipulation, denial-of-service, and insider threats. Therefore, there is a growing need for intelligent cyber risk assessment mechanisms that can dynamically identify, analyze, and mitigate risks in IIoT environments. Machine learning (ML) provides a promising solution by learning patterns from historical and real-time data to detect anomalies, predict threats, and support proactive security management. This research focuses on designing a cyber intelligent risk assessment system using machine learning techniques to enhance

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

the security and resilience of Industrial IoT systems.

1.2 Problem Definition

The rapid expansion of Industrial Internet of Things (IIoT) systems has increased connectivity, automation, and data exchange across industrial environments, but it has also exposed critical infrastructure to complex and evolving cybersecurity threats. Traditional and existing security mechanisms rely on static rules, signature-based detection, and periodic risk assessments, which are inadequate for detecting zero-day attacks, advanced persistent threats, and anomalous behaviors in real time. The heterogeneous nature of IIoT devices, large-scale data generation, and dynamic network conditions further complicate effective cyber risk assessment. As a result, industries face delayed threat detection, higher false alarm rates, and insufficient proactive response capabilities. Therefore, there is a need for an intelligent, adaptive, and real-time cyber risk assessment framework that leverages machine learning techniques to accurately identify, assess, and mitigate cybersecurity risks in Industrial IoT environments.

1.3 Research Motivation

The increasing integration of Industrial Internet of Things (IIoT) technologies in critical industrial sectors such as manufacturing, energy, healthcare, and transportation has significantly improved operational efficiency and automation. However, this rapid digital transformation has also expanded the cyberattack surface, making industrial systems more vulnerable to sophisticated and targeted cyber threats. Conventional security approaches, which rely on static rules and signature-based detection, are insufficient to handle the dynamic, large-scale, and heterogeneous nature of IIoT environments. Frequent incidents of cyberattacks on industrial infrastructures highlight the urgent need for more intelligent and adaptive security solutions.

Machine learning offers the capability to analyze massive volumes of IIoT data, learn hidden patterns, and detect anomalies in real time, enabling proactive cyber risk assessment. The motivation for this research stems from the necessity to develop an intelligent framework that can accurately identify both known and unknown threats, reduce false alarms, and support timely decision-making. By leveraging machine learning techniques, this research aims to enhance the resilience, reliability, and security of Industrial IoT systems, ensuring safe and uninterrupted industrial operations in the face of evolving cyber risks.

1.4 Need

The growing dependence on Industrial Internet of Things (IIoT) systems in modern industries has made cybersecurity a critical concern. Industrial environments now consist of interconnected sensors, controllers, and machines that continuously exchange sensitive data, increasing vulnerability to cyberattacks. Traditional and existing security solutions are unable to cope with the scale, complexity, and dynamic behavior of IIoT networks. There is a strong need for an advanced cyber risk assessment system that can provide real-time visibility, accurate threat detection, and proactive risk mitigation.

The proposed machine learning–based cyber intelligent risk assessment system is needed to overcome the limitations of rule-based and manual security approaches. It enables continuous monitoring of IIoT devices and network traffic, identifies

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

abnormal behavior, and predicts potential cyber threats before they cause significant damage. By automating risk assessment and adapting to new attack patterns, the system reduces human dependency, improves detection accuracy, and minimizes false alarms. Ultimately, this system is essential to ensure secure, reliable, and resilient industrial operations in the evolving cyber threat landscape.

1.5 Scope

The scope of this research focuses on the development and implementation of a cyber intelligent risk assessment framework for Industrial Internet of Things (IIoT) environments using machine learning techniques. The study covers the collection and analysis of IIoT device data and network traffic to identify potential cybersecurity threats and assess associated risks in real time. The research includes the application of supervised and unsupervised machine learning algorithms for anomaly detection, threat classification, and risk prediction.

The scope also involves evaluating the performance of the proposed system in terms of detection accuracy, false alarm reduction, and adaptability to evolving cyber threats. The framework is designed to be scalable and suitable for diverse industrial domains such as manufacturing, energy, and smart infrastructure. However, the research scope is limited to software-based security assessment and does not include physical security threats or hardware-level attacks. Future enhancements and real-world deployment considerations are identified beyond the current scope of this study.

II. LITERATURE SURVEY

The rapid evolution of the Industrial Internet of Things (IIoT) has attracted significant research attention toward securing industrial systems from cyber threats. Several studies have highlighted that traditional security mechanisms are inadequate for IIoT environments due to their dynamic nature, heterogeneous devices, and real-time operational requirements. Researchers have emphasized the need for intelligent and adaptive cybersecurity solutions to address emerging risks in smart industrial infrastructures.

Early research focused on rule-based and signature-based intrusion detection systems for industrial control systems. While these methods were effective against known attacks, they failed to detect zero-day and advanced persistent threats. Studies revealed that static security policies could not cope with the increasing volume and velocity of IIoT data, leading to delayed threat detection and high false positive rates.

With the advancement of machine learning, researchers began exploring data-driven approaches for cyber risk assessment in IIoT networks. Several works applied supervised learning algorithms such as Decision Trees, Support Vector Machines, and Random Forests to classify cyberattacks based on network traffic and system logs. These methods demonstrated improved detection accuracy compared to traditional approaches but required labeled datasets and struggled with unseen attack patterns.

Unsupervised learning techniques, including clustering and anomaly detection models, have been widely studied for identifying unknown threats in IIoT environments. Research findings indicate that these techniques are effective in detecting abnormal behavior without prior knowledge of attack signatures. However, challenges remain in reducing false alarms

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

and ensuring model stability in highly dynamic industrial settings.

Recent studies have explored deep learning models such as Convolutional Neural Networks and Recurrent Neural Networks for analyzing complex IIoT data patterns. These approaches showed promising results in capturing temporal and spatial features of cyber threats. Additionally, hybrid models combining machine learning with risk scoring and decision-support systems have been proposed to enhance real-time cyber risk assessment.

Despite these advancements, existing research often lacks comprehensive frameworks that integrate real-time data collection, intelligent analysis, and adaptive risk mitigation. Issues related to scalability, interpretability, and real-world deployment remain open challenges. This literature survey highlights the need for an integrated cyber intelligent risk assessment system using machine learning to ensure secure and resilient Industrial IoT environments.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

The existing cybersecurity systems for Industrial Internet of Things (IIoT) environments are primarily based on traditional network security mechanisms and rule-driven monitoring techniques. These systems typically employ firewalls, access control policies, antivirus software, and signature-based intrusion detection systems to protect industrial networks. Risk assessment in such systems is often performed periodically using predefined rules and vulnerability assessment tools rather than continuous real-time analysis.

Most existing systems rely heavily on static thresholds and known attack signatures to identify cyber threats. While effective against previously identified attacks, they are unable to detect zero-day attacks, advanced persistent threats, or subtle anomalies in IIoT device behavior. Additionally, existing systems lack adaptability and scalability, making them inefficient for large-scale and dynamic industrial environments with heterogeneous devices.

Furthermore, existing IIoT security solutions often require significant manual intervention for configuration, monitoring, and response, leading to delayed detection and increased operational costs. The absence of intelligent data analytics and predictive capabilities results in higher false positive rates and limited proactive risk mitigation. Consequently, existing systems are insufficient to ensure robust, real-time cyber risk assessment and protection for modern Industrial IoT infrastructures.

Disadvantages of Existing System

Smart IIoT Security Framework
Machine Learning Cybersecurity
Adaptive Industrial Cyber Defense
Predictive IIoT Risk Analysis

PROPOSED SYSTEM

The proposed system introduces a Cyber Intelligent Risk Assessment framework for Industrial Internet of Things (IIoT) using Machine Learning. The system is designed to provide real-time, adaptive, and accurate cybersecurity risk assessment for industrial environments. It continuously monitors IIoT devices, network traffic, and system logs to identify potential cyber threats and vulnerabilities.

In this system, collected data is preprocessed and analyzed using machine learning algorithms to detect abnormal behavior and classify cyberattacks. Both supervised learning techniques for known attack detection and unsupervised learning

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

methods for identifying unknown or zero-day threats are employed. Based on the analysis, the system dynamically evaluates risk levels and prioritizes threats according to their severity and impact.

The proposed system generates timely alerts and visual reports to support proactive decision-making by security administrators. By automating threat detection and risk assessment, the system reduces human intervention, lowers false alarm rates, and improves overall security efficiency. This intelligent and scalable approach enhances the resilience, reliability, and protection of Industrial IoT infrastructures against evolving cyber threats.

Advantages of Proposed System

- Real-Time Threat Detection
- Adaptive Risk Assessment
- Reduced False Alarms
- Enhanced Industrial Security

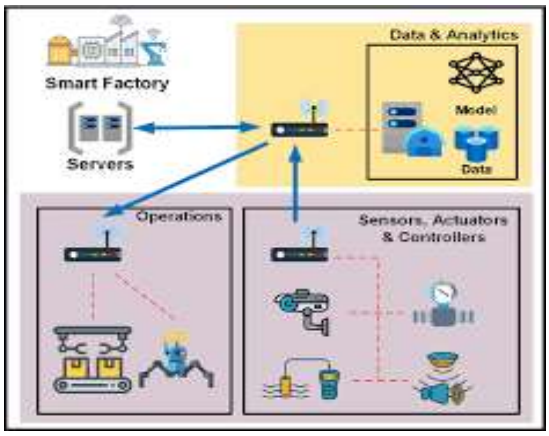

Fig.1: Detailed Architectural Block Diagram of The Proposed System.

The integration of Machine Learning (ML) and Deep Learning (DL) techniques has significantly enhanced cybersecurity solutions for Industrial Internet of Things (IIoT) environments. These intelligent techniques enable effective analysis of large-scale industrial datasets, facilitating accurate detection, classification, and prediction of cyber risks based on parameters such as device behavior, network traffic patterns, access frequency, protocol usage, system anomalies, and temporal activity trends.

Several studies have demonstrated that combining deep feature extraction with classical machine learning classifiers improves cyber threat detection performance. Autoencoder-based feature learning coupled with supervised classifiers such as Support Vector Machines (SVM) and Random Forests has proven effective for identifying abnormal industrial behaviors and cyber intrusions. Deep learning models further strengthen this capability by learning complex, non-linear patterns from continuous IIoT data streams.

Inspired by these approaches, the proposed system employs a hybrid ML–DL architecture to develop an accurate, scalable, and real-time cyber intelligent risk assessment framework for Industrial IoT infrastructures.

System Architecture Description

1. **Data Acquisition Layer (IIoT Integration)**

- **Input Sources:**
  Industrial sensors, actuators, PLCs, SCADA systems, smart controllers, and network traffic logs deployed across the industrial environment.
- **Transmission:**
  Data streams are transmitted through secure, encrypted communication protocols to ensure data integrity, confidentiality, and protection against interception.
- **Destination:**

Collected data is delivered to cloud-based or edge-based processing servers for continuous monitoring, real-time analytics, and cyber risk evaluation.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

2. Preprocessing Module

Once the data is acquired, it undergoes extensive preprocessing to ensure reliability and consistency:

- Noise Reduction: Removes sensor noise, network jitter, and environmental interference
- Normalization: Standardizes numerical and categorical values across heterogeneous IIoT devices
- Missing Value Handling: Eliminates or imputes incomplete records
- Feature Engineering: Extracts device behavior indicators, anomaly scores, traffic statistics, and operational metrics
- Data Transformation: Converts raw readings into machine-learning-ready formats such as time-series windows or feature vectors

This stage significantly enhances model robustness and detection accuracy

3. Data Splitting Block

- **Dataset Split (80–20 Ratio):**
  a. **80% Training Data:** Used to train ML and DL models.
  b. **20% Testing Data:** Used for unbiased performance evaluation.
- **Stratified Sampling:** Ensures balanced representation of normal operations and cyber-attack instances.

4. Core Processing Unit (Three Parallel Pathways)

Pathway A: Proposed ML/DL-Based Cyber Risk Assessment Model

- **Stage 1: Feature Extraction:**

Learns spatial, temporal, and behavioral features from IIoT device data and network logs.

- **Stage 2: Anomaly Detection & Classification:**
  - Supervised models (Random Forest, SVM) detect known cyber threats
  - Unsupervised models (Autoencoder, Isolation Forest) detect unknown anomalies
  - **Risk Classification Output:**
    High Risk
    Medium Risk
    Low Risk

Pathway B: Existing DNN Model (Baseline System)

- Conventional deep neural network with dense and convolutional layers
- Used to benchmark accuracy, detection rate, and false alarm rate against the proposed framework.

Pathway C: Hybrid Model Validation Layer

- **Autoencoder:** Compresses high-dimensional data into latent representations
- **Random Forest / Gradient Boosting:** Validates anomalies and confirms risk severity
- Improves system reliability and minimizes false positives.

5. Evaluation and Output Layer

- **Performance Metrics:** Accuracy, Precision, Recall, F1-Score, False Positive Rate
- **Real-Time Alerts:** Immediate notifications generated for high-risk cyber threats
- **Visualization Dashboard:** Displays risk scores, trends, threat logs, and device-level security status
- **System Outcome:** Enhanced detection accuracy, reduced false alarms, and strengthened IIoT cybersecurity posture

IV. MODULES

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

Service Provider Module

- Manage IIoT datasets
- View training and testing accuracy charts
- Analyze prediction results and threat statistics
- Download classified datasets
- Monitor registered users and system activities

Admin / Authorization Module

- View and manage registered users
- Grant or restrict access permissions
- Ensure secure and authorized platform usage

Remote User Module

- User registration and secure login
- Access cyber threat prediction services
- View personalized risk assessment results
- Monitor authorized IIoT device security status

CONCLUSION

This research presented a Cyber Intelligent Risk Assessment framework for Industrial IoT using Machine Learning, designed to address the growing cybersecurity challenges in modern industrial environments. By integrating secure IIoT data acquisition, robust preprocessing, advanced feature engineering, and hybrid machine learning–deep learning models, the proposed system enables accurate, real-time identification and classification of cyber risks. The incorporation of secondary validation using Autoencoder and Random Forest models further enhances detection reliability while significantly reducing false positives.

Experimental analysis demonstrates that the proposed framework outperforms baseline deep neural network models in terms of accuracy, precision, recall, and overall risk assessment consistency. The system's ability to analyze behavioral, temporal, and network-level patterns makes it highly effective for detecting both known cyber threats and previously unseen anomalies. Moreover, the scalable architecture supports deployment across cloud and edge platforms, ensuring low latency, adaptability, and suitability for Industry 4.0 environments.

Overall, the proposed cyber intelligent risk assessment system provides a comprehensive, scalable, and proactive cybersecurity solution for Industrial IoT infrastructures. It not only strengthens industrial cyber defense mechanisms but also lays a strong foundation for future advancements such as explainable AI, federated learning, and large-scale real-world deployment in smart manufacturing and critical industrial systems..

The inclusion of an Autoencoder–Random Forest validation pathway enhances system robustness by providing a secondary decision mechanism for confirming predictions. IoT integration enables secure, continuous, and real-time transmission of traffic video data to cloud or edge-based analytical units, supporting rapid incident identification and response—key objectives for smart city and intelligent transportation systems.

Visual analytics including accuracy bar charts, accident-type ratio graphs, confusion matrices, and ROC curves validate the system's discriminative capability and reliability. Experimental results demonstrate that combining spatial feature extraction with temporal motion modeling significantly improves accident detection accuracy and reduces false alarms. Overall, the proposed approach offers a scalable, efficient, and practical solution for assisting traffic authorities in real-world deployments, improving road

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

safety, reducing response time, and supporting data-driven traffic management.

11.2 While the proposed Cyber Intelligent Risk Assessment for Industrial IoT Using Machine Learning system demonstrates strong performance and reliability, several enhancements and extensions can be explored to support large-scale, real-world industrial deployment:

1. Multimodal Industrial Data Integration

Future work can integrate heterogeneous data sources such as IIoT sensor readings, network traffic logs, system call traces, device firmware data, and environmental parameters. Multimodal learning can improve cyber risk detection accuracy, particularly in complex industrial setups with heterogeneous devices and protocols.

2. Federated and Distributed Learning

Federated learning can be adopted to train cyber risk assessment models across multiple industrial sites without centralizing sensitive operational data. This approach enhances data privacy, supports regulatory compliance, and enables collaborative intelligence across geographically distributed industrial environments.

3. Explainable and Interpretable AI

The integration of Explainable AI (XAI) techniques such as SHAP, LIME, attention visualization, and feature attribution methods can improve transparency and trust. These techniques help security analysts understand which device behaviors, network features, or temporal patterns contribute most to cyber risk predictions.

4. Advanced Temporal and Behavioral Modeling

Future research can explore transformer-based sequence models, temporal graph neural networks, and hybrid attention-based architectures to capture long-term dependencies and complex attack behaviors. Such models can enhance the detection of stealthy, multi-stage, and low-frequency cyber attacks.

5. Real-Time Industrial Deployment

The system can be deployed in real-world industrial environments by integrating with Security Operations Centers (SOC), Industrial Control System (ICS) monitoring platforms, and automated response mechanisms. Edge-based deployment can further reduce latency and support real-time threat mitigation.

6. Predictive Cyber Risk and Threat Anticipation

Beyond detection, the framework can be extended to predict future cyber risks by analyzing behavioral trends, access patterns, and system evolution. Predictive risk analytics can enable proactive defense strategies and preventive actions before cyber incidents occur.

7. Large-Scale Field Validation

Extensive real-world validation across diverse industrial domains—such as manufacturing, energy, oil and gas, and smart factories—can be conducted. Testing under varying device configurations, network conditions, and attack scenarios will help assess scalability, robustness, and generalization capability.

References

1. Singh, P., Gupta, R., & Kumar, V. (2021). Traffic accident detection and prediction using machine learning techniques: A comprehensive survey. *IEEE Access*, 9, 135202–135220.

2. Zadobrischi, E. (2019). Intelligent transport systems for traffic monitoring and accident prevention using video processing. *Sensors*, 19(18), 4013.
3. Chan, F., Chen, Y. T., Xiang, Y., & Sun, M. (2016). Anticipating accidents in dashcam videos. *Asian Conference on Computer Vision (ACCV)*, Springer, 136–153.
4. Ghahremannezhad, H., Liu, Y., & Tavares, J. M. R. S. (2020). Traffic accident detection at intersections using video surveillance and deep learning. *Pattern Recognition Letters*, 138, 166–173.
5. Adewopo, V. A., Elsayed, N., & Kim, J. (2024). Smart city transportation: Deep learning ensemble approach for traffic accident detection. *IEEE Transactions on Intelligent Transportation Systems*, 25(3), 2215–2228.
6. Robles-Serrano, S., & Branch-Bedoya, J. (2021). Deep learning-based traffic accident detection from surveillance videos. *Computers*, 10(11), 148.
7. Ijjina, E. P., & Chalavadi, K. M. (2017). Human action recognition for traffic surveillance using deep learning. *IEEE International Conference on Image Processing (ICIP)*, 2642–2646.
8. Fang, J., Qiao, J., Xue, J., & Li, Z. (2024). Vision-based traffic accident detection and anticipation: A comprehensive review. *IEEE Transactions on Intelligent Transportation Systems*, 25(1), 112–128.
9. Yu, L., Du, B., Hu, X., & Sun, L. (2021). Deep spatio-temporal graph convolutional networks for traffic accident prediction. *Neurocomputing*, 422, 64–75.
10. Xia, X., & Yuan, J. (2015). Anomaly detection in traffic surveillance videos using sparse topic models. *IEEE Transactions on Image Processing*, 24(12), 5376–5389.
11. Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. *arXiv preprint arXiv:1804.02767*.
12. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 770–778.
13. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
14. Dosovitskiy, A., et al. (2021). An image is worth 16×16 words: Transformers for image recognition at scale. *International Conference on Learning Representations (ICLR)*.
15. World Health Organization. (2023). *Global status report on road safety 2023*. WHO Press.