AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

Machine Learning-Based Detection of Anomalies, Intrusions and Threats in Industrial Control Systems

Mr. V Koteswara Rao Pokuri, M.Tech, Assistant Professor, Department of MCA, Bapatla Engineering College Bapatla, pvkr415@gmail.com, ORCID: 0009-0009-1860-3073

Ms. Gundreddi Nandini, (Reg No: Y25MC23026), Mr. Bonigala Chinnu, (Reg No : Y25MC23013)
Mr. Janni Venkatesh, (Reg No: Y25MC23027), Mr. Sarimalla Suresh, (Reg No: Y25MC23073)
Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh, India

***Abstract*—Industrial Control Systems are a part of the infrastructure we use today. They are used in power grids, manufacturing systems, water treatment facilities and transportation networks. As we use digital technologies and connect things to the internet, these systems are more at risk of being hacked. This means that Industrial Control Systems are vulnerable to cyber threats like people getting in without permission, malware attacks and system intrusions. The old ways of keeping them safe, like using signature-based detection and rule-based monitoring, are not good enough to stop complicated and changing cyber attacks. So we need security solutions that can adapt and learn to protect Industrial Control Systems.**

This paper is about using machine learning to detect anomalies, intrusions and threats in Industrial Control Systems. The idea is to use data-driven techniques to look at network traffic, system logs and sensor data from Industrial Control Systems. By using machine learning algorithms like Decision Trees, Random Forest, Support Vector Machines and Neural Networks, the system can learn what normal operations look like and find things that do not seem right. This can help us find activities.

To do this, we need to collect data from networks, clean it up to remove mistakes and find the important parts like communication patterns, command sequences and system behaviours. Then we train models to sort system activities into abnormal groups. This helps us find cyber threats early. We also use anomaly detection to find attacks that we have not seen before.

We tested this approach. It works really well. It can detect threats with accuracy, precision and recall and it can find both known and unknown threats without giving too many false alarms. The system can also monitor things in time so we can respond quickly to potential security incidents.

Using machine learning in Industrial Control Systems security makes it better at detecting cyber threats. It also makes the systems more resilient. Ensures that critical industrial infrastructure works safely and reliably. In the future, we might work on making the models bigger using learning and creating adaptive defence mechanisms for industrial environments that change. Industrial Control Systems will be safer with these security solutions.

Keywords: Industrial Control Systems (ICS), Machine Learning, Anomaly Detection, Intrusion Detection, Cybersecurity, Threat Detection

I. INTRODUCTION

Industrial Control Systems play an important role in managing and automating critical infrastructure like power generation and distribution, oil and gas pipelines, manufacturing plants, water treatment facilities and transportation systems. These Industrial Control Systems rely on a combination of hardware, software, sensors and communication networks to monitor and control processes in real time.

With companies using digital technologies, remote connectivity and Industrial Internet of Things devices, Industrial Control Systems environments have become more interconnected and efficient. However this increased connectivity has also introduced cybersecurity challenges and vulnerabilities. Industrial Control Systems are now more connected to systems and this has made them more vulnerable to cyber attacks.

In the past, Industrial Control Systems were designed as isolated systems with exposure to external networks, which provided a level of inherent security. In modern industrial environments, the integration of enterprise networks, cloud platforms and remote access capabilities has expanded the attack surface. As a result Industrial Control Systems are increasingly targeted by cyber threats such as malware attacks, unauthorised access, data manipulation and distributed denial-of-service attacks. These threats can disrupt operations, cause financial losses and even endanger public safety.

Therefore, ensuring the security and reliability of Industrial Control Systems has become a concern for industries and governments worldwide. Conventional security approaches in

...

Industrial Control Systems environments primarily rely on signature-based intrusion detection systems and rule-based monitoring techniques. While these methods are effective in detecting known threats, they often fail to identify evolving attack patterns, including zero-day attacks and sophisticated intrusions.

Machine learning has emerged as a tool for enhancing cybersecurity in industrial systems. Machine learning techniques enable systems to learn patterns from data and automatically detect anomalies that deviate from normal behaviour. By analysing network traffic, system logs and sensor data, machine learning models can identify activities that may indicate potential intrusions or cyber threats.

Various machine learning algorithms, such as Decision Trees, Random Forest Support Vector Machines and Neural Networks, have been widely applied for anomaly detection and intrusion detection in environments. These models can classify system behaviour into abnormal categories, enabling early detection of threats and reducing response time.

This paper focuses on the development of a machine learning-based framework for detecting anomalies, intrusions and threats in Industrial Control Systems. The proposed approach aims to enhance the security of Industrial Control Systems by leveraging data-driven techniques to monitor system behaviour, identify threats and support timely mitigation strategies.

The remainder of this paper is organised as follows.

* Section II presents a review of work in Industrial Control Systems security and machine learning-based threat detection.
* Section III describes the proposed methodology and system architecture.
* Section IV discusses the results and performance analysis.
* Section V concludes the paper. Outlines future research directions.

II. LITERATURE SURVEY

The security of Industrial Control Systems is a deal these days. Industrial Control Systems are used in lots of places like power grids, manufacturing systems, oil and gas industries and water treatment plants. With communication technologies and the Industrial Internet of Things Industrial Control Systems are more open to cyber attacks. So researchers are working hard to find ways to detect anomalies, intrusions and cyber threats in Industrial Control Systems.

Traditional ways to detect intrusions are not that great. They use signature-based and rule-based intrusion detection systems. These systems look at network activity. Compare it to known attack signatures or rules. They are good at finding known threats. They are not good at finding new threats. Also it is hard to keep the signature databases up to date in industrial environments that are always changing.

Another old way is to use anomaly detection. This is where normal system behavior is modeled using statistics. If something does not fit the model it is considered an anomaly. This method can find attacks but it often has a lot of false positives and may not work well with complex systems.

A. Machine Learning-Based Approaches

Machine learning is being used more and more to secure Industrial Control Systems. Machine learning models can learn from data and find patterns that might be cyber threats. Some machine learning algorithms like Decision Trees, Random Forest Support Vector Machines and k-Nearest Neighbors are often used for intrusion detection.

These models are trained on data that has malicious activities labeled. Once they are trained they can tell if new data is normal or an attack. Studies have shown that these methods can be very accurate. They need good data to work well and that can be hard to get in industrial environments.

B. Unsupervised and Semi-Supervised Learning

Unsupervised learning is also being used to detect anomalies in Industrial Control Systems. Methods like clustering, Principal Component Analysis and autoencoders are used to model system behavior without labeled data. These methods are good at finding threats.

Semi-supervised learning uses both labeled and unlabeled data to improve detection. This is helpful in Industrial Control Systems where labeled attack data's limited. However these methods may still have trouble telling the difference between variations and actual attacks.

C. Deep Learning Techniques

Deep learning is a way to detect intrusions. Deep Neural Networks, Convolutional Neural Networks and Recurrent Neural Networks are being used to analyze network traffic and system behavior. These models can automatically find features and improve detection accuracy.

For example Recurrent Neural Networks are good at finding patterns in time-series data from Industrial Control Systems sensors. Convolutional Neural Networks are good at finding patterns in network traffic data. However deep learning models often need a lot of data and computational power which can be a problem in time industrial systems.

D. Hybrid and Ensemble Methods

To improve detection researchers are combining machine learning techniques. Ensemble methods like Random Forest

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 19-04-2026 | www.ajaccm.com

and Gradient Boosting combine the predictions of models to improve accuracy and robustness. Hybrid systems combine signature-based detection with machine learning to get both accuracy and adaptability.

These methods have shown results in reducing false positives and improving detection rates. However they can make the system more complex. Need careful tuning.

E. Challenges and Research Gaps

There are still some challenges in using machine learning for Industrial Control Systems security.

* There is a lack of data for training models.
* There are a lot of positives in anomaly detection.
* It is hard to detect attacks.
* There are constraints in real-time industrial environments.
* There is a need for models that can be explained and interpreted.

F. Motivation for Proposed Work

Based on what has been done far it is clear that machine learning has improved intrusion detection but there is still a need for solutions that are efficient, accurate and scalable for industrial environments. Many existing methods focus on accuracy. Are not efficient or they are not good at adapting to new threats.

So this research proposes a machine learning-based framework for detecting anomalies, intrusions and threats in Industrial Control Systems. The goal is to balance detection accuracy, computational efficiency and adaptability. The proposed approach builds on existing methods and addresses challenges, in Industrial Control Systems cybersecurity.

III. **ALGORITHM**

The proposed algorithm focuses on detecting anomalies, intrusions, and cyber threats in Industrial Control Systems (ICS) using a machine learning-based framework. The system analyzes network traffic, sensor data, and system logs to identify abnormal behavior and ensure secure industrial operations.

A. ML-Based ICS Threat Detection Framework

Input: Dataset D containing network traffic, sensor data, and system logs

Output: Detection and classification of anomalies, intrusions, and cyber threats

Step 1: Data Collection: Data is collected from various ICS components including:

- Network traffic data
- Sensor readings
- Control commands
- System logs

The dataset is represented as:

$$D = \{N, S, C\} \tag{1}$$

where N represents network data, S represents sensor data, and C represents control system logs.

Step 2: Data Preprocessing: The collected data is preprocessed to improve quality and consistency.

- Remove duplicate and irrelevant data
- Handle missing values
- Normalize feature values
- Convert raw data into structured format

Step 3: Feature Extraction: Important features are extracted from the dataset such as packet size, protocol type, command sequences, sensor value patterns, and time-based behavior.

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \tag{2}$$

where f_i represents system behavior features.

Step 4: Model Training: The dataset is divided into training and testing sets. Machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and Neural Networks are used to learn normal and abnormal patterns.

$$Y = f(F) \tag{3}$$

where Y represents the predicted class (Normal or Attack).

Step 5: Anomaly Detection: Real-time system behavior is compared with trained models to detect deviations from normal patterns. If the deviation exceeds a threshold, it is identified as an anomaly.

Step 6: Intrusion Classification: Detected anomalies are classified into different types of cyber threats:

- Denial-of-Service (DoS) attacks
- Malware or ransomware attacks
- Unauthorized access
- Data manipulation attacks

Step 7: Alert and Response Mechanism: The system generates alerts and initiates defense actions:

- Block suspicious IP addresses
- Isolate affected systems
- Update firewall rules
- Log incidents for further analysis

Step 8: Performance Evaluation: The performance of the model is evaluated using standard metrics.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

$$Recall = \frac{TP}{TP + FN} \tag{6}$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{7}$$

where TP , TN , FP , and FN represent true positives, true negatives, false positives, and false negatives respectively.

The proposed algorithm enables early detection of cyber threats, improves system security, and supports automated response mechanisms in Industrial Control Systems.

IV. METHODOLOGY

The proposed methodology presents a machine learning-based framework for detecting anomalies, intrusions, and cyber threats in Industrial Control Systems (ICS). The approach focuses on analyzing system behavior, identifying deviations from normal operations, and enabling timely detection of potential security threats. The methodology consists of multiple stages including data collection, preprocessing, feature extraction, model training, anomaly detection, threat classification, and performance evaluation.

A. Data Collection

The first step involves collecting data from various components of Industrial Control Systems. The collected data includes network traffic data, sensor readings, control commands, and system logs.

$$D = \{N, S, C\} \tag{8}$$

where N represents network traffic data, S represents sensor data, and C represents control and system logs.

B. Data Preprocessing

The collected data is preprocessed to improve data quality.

- Remove duplicate and irrelevant records
- Handle missing values
- Normalize and scale feature values
- Convert categorical data into numerical format

C. Feature Extraction

Feature extraction identifies important attributes that represent system behavior.

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \tag{9}$$

where f_i represents features such as packet size, protocol type, sensor patterns, and time-based behavior.

D. Model Training

The dataset is divided into training and testing sets. Machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and Neural Networks are used for training.

$$Y = f(F) \tag{10}$$

where F represents the feature vector and Y represents the predicted class (normal or attack).

E. Anomaly Detection

The trained model monitors real-time data and detects deviations from normal behavior. If the deviation exceeds a predefined threshold, the activity is marked as an anomaly.

F. Intrusion and Threat Classification

Detected anomalies are classified into different types of cyber threats:

- Denial-of-Service (DoS) attacks
- Malware and ransomware attacks
- Unauthorized access
- Data manipulation attacks

G. Alert Generation and Response

The system generates alerts and initiates response mechanisms:

- Block suspicious IP addresses
- Isolate compromised systems
- Update firewall rules
- Log incidents for further analysis

H. Performance Evaluation

The effectiveness of the model is evaluated using standard metrics.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{14}$$

where TP , TN , FP , and FN represent true positives, true negatives, false positives, and false negatives respectively.

The proposed methodology enables early detection of cyber threats, improves system security, and supports automated response mechanisms in Industrial Control Systems.

V. RESULT ANALYSIS

This section presents the experimental evaluation of the proposed machine learning-based framework for detecting anomalies, intrusions, and cyber threats in Industrial Control Systems (ICS). The objective is to analyze the effectiveness of the model in identifying malicious activities while maintaining high accuracy and low false alarm rates.

The dataset used for experimentation consists of network traffic data, sensor readings, control commands, and system logs collected from ICS environments. The dataset is divided into training data (80%) and testing data (20%) for performance evaluation.

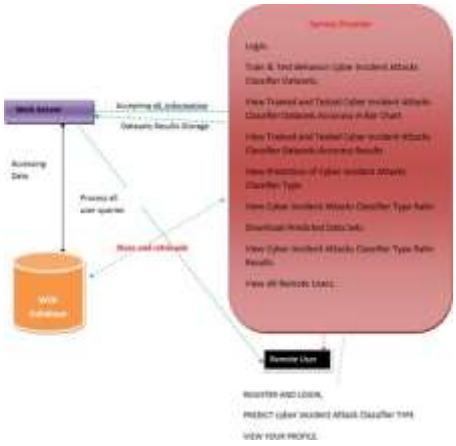

Fig. 1. Architecture Overview

A. Model Performance Evaluation

Machine learning algorithms such as Decision Trees, Random Forest, Support Vector Machines (SVM), and Neural Networks are used to classify system behavior as normal or malicious. These models learn patterns of normal operations and identify deviations indicating cyber threats.

The performance of the model is evaluated using standard metrics such as accuracy, precision, recall, and F1-score.

B. Accuracy Analysis

Accuracy measures the proportion of correctly classified instances.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (15)$$

where TP represents true positives, TN represents true negatives, FP represents false positives, and FN represents false negatives.

The results show that the proposed system achieves high accuracy in detecting cyber threats.

C. Precision and Recall Analysis

Precision and recall evaluate the reliability of the detection system.

$$Precision = \frac{TP}{TP + FP} \quad (16)$$

$$Recall = \frac{TP}{TP + FN} \quad (17)$$

Precision indicates how many detected threats are correct, while recall measures how many actual threats are detected. The system achieves high precision and recall values.

D. F1 Score Evaluation

The F1-score provides a balance between precision and recall.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (18)$$

A high F1-score indicates effective detection performance.

E. Anomaly Detection Performance

The proposed system effectively detects anomalies by identifying deviations from normal system behavior. This allows detection of unknown or zero-day attacks and unusual system activities.

F. Intrusion Classification Analysis

Detected anomalies are classified into categories such as:

- Denial-of-Service (DoS) attacks
- Malware or ransomware attacks
- Unauthorized access attempts
- Data manipulation attacks

The model accurately distinguishes between different types of cyber threats.

G. Comparative Analysis

Compared to traditional signature-based systems, the proposed approach provides improved detection of unknown threats, reduced false positives, and better adaptability to evolving attack patterns.

H. Real-Time Detection Capability

The proposed framework supports real-time monitoring of ICS environments. It can detect threats quickly and enable timely response, which is critical for industrial systems.

I. Overall System Performance

The experimental results demonstrate that the proposed machine learning- based system achieves high detection accuracy, reliable anomaly detection, and efficient classification of cyber threats. It reduces false alarms and enhances the overall security and resilience of Industrial Control Systems.

Visualization and Output:

Fig. 2. wed page

Fig. 3. login page

Fig. 4. Prediced value

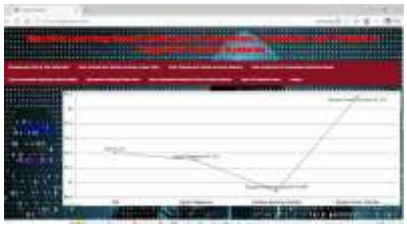

Fig. 5. Prediced graph

VI. CONCLUSION

The security of Industrial Control Systems (ICS) has become increasingly critical with the rise of interconnected industrial environments and the growing sophistication of cyber threats. Traditional security mechanisms, which rely primarily on signature-based detection and static rules, are no longer sufficient to handle evolving and unknown attack patterns. This research addressed these challenges by proposing a machine learning-based framework for detecting anomalies, intrusions, and cyber threats in ICS environments.

The proposed approach leverages machine learning algorithms to analyze network traffic, sensor data, and system logs, enabling the system to learn normal operational behavior and identify deviations that indicate potential threats. By incorporating techniques such as anomaly detection and classification, the framework is capable of detecting both known and unknown attacks, including zero-day threats. This significantly enhances the capability of industrial systems to respond to emerging cybersecurity risks.

The experimental results demonstrate that the proposed system achieves high accuracy, precision, recall, and F1-score, indicating strong performance in detecting malicious activities while minimizing false positives. The system also supports real-time monitoring and rapid response, which are essential for maintaining the reliability and safety of critical industrial operations.

Furthermore, the integration of machine learning techniques improves adaptability and scalability, allowing the system to evolve with changing threat landscapes. The ability to classify different types of cyber attacks enables targeted mitigation strategies, thereby strengthening the overall defense mechanism of ICS environments.

In conclusion, the proposed machine learning-based detection framework provides an effective and intelligent solution for enhancing cybersecurity in Industrial Control Systems. It improves threat detection accuracy, reduces response time, and increases system resilience against cyber attacks. Future work may focus on integrating advanced deep learning models, improving model interpretability, and developing lightweight solutions for deployment in resource-constrained industrial environments.

REFERENCES

[1] F. Song, Y. Lei, S. Chen, L. Fan, and Y. Liu, “Advanced Anomalies, Intrusions Attacks and mitigations on practical ML-based phishing website classifiers,” Int. J. Intell. Syst., vol. 36, no. 9, pp. 5210–5240, Sep. 2021.

[2] B. Sabir, M. A. Babar, and R. Gaire, “An evasion attack against ML-based phishing URL detectors,” Tech. Rep., 2020.

[3] H. Shirazi, B. Bezawada, I. Ray, and C. Anderson, “Adversarial sampling attacks against phishing detection,” in Proc. IFIP Annu. Conf. Data Appl. Secur. Cham, Switzerland: Springer, Jul. 2019, pp. 83–101.

[4] S. Anupam and A. K. Kar, “Phishing website detection using support vector machines and nature-inspired optimization algorithms,” Telecommun. Syst., vol. 76, no. 1, pp. 17–32, Jan. 2021.

[5] A. K. Jain and B. B. Gupta, “Towards detection of phishing websites on client-side using machine learning based approach,” Telecommun. Syst., vol. 68, no. 4, pp. 687–700, Aug. 2018.

[6] S. Chen, M. Xue, L. Fan, S. Hao, L. Xu, H. Zhu, and B. Li, “Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach,” Comput. Secur., vol. 73, pp. 326–344, Mar. 2018.

[7] I. Vayansky and S. Kumar, “Phishingchallenges and solutions,” Comput. Fraud Secur., vol. 2018, no. 1, pp. 15–20, Jan. 2018.

[8] Z. Abaid, M. A. Kaafar, and S. Jha, “Quantifying the impact of adversarial Anomalies, Intrusions Attacks on machine learning based Android malware classifiers,” in Proc. IEEE 16th Int. Symp. Netw.

Comput. Appl. (NCA), Oct. 2017, pp. 1–10.

[9] I. Corona, B. Biggio, M. Contini, L. Piras, R. Corda, M. Mereu, G. Mureddu, D. Ariu, and F. Roli, "DeltaPhish: Detecting phishing webpages in compromised websites," in Proc. Eur. Symp. Res. Comput. Secur. Cham, Switzerland: Springer, Sep. 2017, pp. 370–388.

[10] Log Files - Book of Zeek [Online]. Available: https://docs.zeek.org/en/master/script-reference/log-files.html, Accessed on: Dec. 1, 2023