International Innovative Research Journal of Engineering and Technology
Vol. 10, Issue. 4, June 2025, pp. 39~48
ISSN: 2456-1983, DOI: 10.32595/iirjet.org/v10i4.2025.225

Artificial Intelligence-Driven Cybersecurity Framework for Industrial Control Networks

Dr.V. Sakthivel[1], Dr. Vishnu Kumar Kaliappan[2]
[1]Associate Professor, School of Computer Science and Engineering (SCOPE),
Vellore Institute of Technology – Chennai Campus, Tamil Nadu, India
[2]Research Professor, Distributed Multimedia Systems (DMS) Laboratory, Konkuk Aerospace Design Airworthiness Institute & School of Computer Science and Engineering, College of Engineering, Konkuk University, Republic of Korea

Article Info

Article history:

Received Mar 16, 2025
Revised Apr 20, 2025
Accepted May 17, 2025

Keywords:

Machine Learning
Deep Learning
SCADA
Anomaly Detection
Intrusion Detection System
Critical Infrastructure

ABSTRACT

Automating and controlling systems in energy, water supply, transportation and manufacturing now greatly relies on Industrial Control Networks (ICNs). As OT and IT systems merge with the help of ICNs, these networks are now both more integrated and smart. However, this introduces more cybersecurity risks as they become exposed to more dangers. Because they are not dynamic, do not use signatures or only react to threats such traditional cybersecurity methods do not fulfill all the standards required by ICNs. This text focuses on presenting an AICF which works to defend ICNs from evolving cyber risks. The suggested approach combines machine learning (ML) with deep learning (DL) to set up various levels of defense. It features anomaly detection in real time by using unsupervised models, thoroughly sorts threats using deep neural networks and performs tasks automatically to prevent them by using reinforcement learning. Standard datasets created for the industrial domain such as SWaT and NSL-KDD are used to check the effectiveness of the framework. It is shown by experiment that AICF has a strong ability to detect threats, lessens false positives and identifies and controls threats swiftly with little impact on operations. The use of AICF has special value in catching zero-day attacks, moves across the network and clandestine actions that other systems may not spot. Besides, the ability to grow and change according to specific needs means the system is suitable for any industrial environment and protocols. All in all, the study highlights how AI methods can strengthen the strength, dependability and thoughtfulness of cybersecurity in ICN systems, allowing industrial automation to become safer and more reliable when facing new threats.

Corresponding Author:

Dr.V. Sakthivel,
School of Computer Science and Engineering (SCOPE),
Vellore Institute of Technology – Chennai Campus, Tamil Nadu, India
Email: sakthivel.v@vit.ac.in

1. INTRODUCTION

Industrial Control Networks or ICNs, are important for enabling automation, supervision and control of complicated actions in energy, water, manufacturing, oil and gas and transportation. In ICNs, you have Supervisory Control and Data Acquisition (SCADA) systems, Programmative Logic Controllers (PLCs) and Distributed Control Systems (DCS), all operating with physical components to guarantee stable, secure and efficient operations. Usually such networks were independent and not shared, placing greater importance on being reliable, working in a predictable way and being able to handle faults. Because of the rise of digitization, remote monitoring and IIoT, ICNs are now more likely to face cyber threats than in the past.

Consequences of this change include the fact that ICNs are now exposed to many more cyberattacks, including both standard and advanced ones. Such noteworthy attacks as the Stuxnet worm on Iran's nuclear centrifuges and the Triton malware against industrial safety systems stress the major risks that

cyber crimes pose for industries. It was made clear that adversaries can damage or disrupt core infrastructure by attacking old technology, insecure network parts and systems not being closely watched. Besides, since industrial systems are both complicated and diverse, usual IT security processes cannot work well in ICNs. Many times, signature-based IDS systems, rule-based firewalls and protection systems around the edge of the network are unable to detect advanced and silent attacks meant for industrial settings.

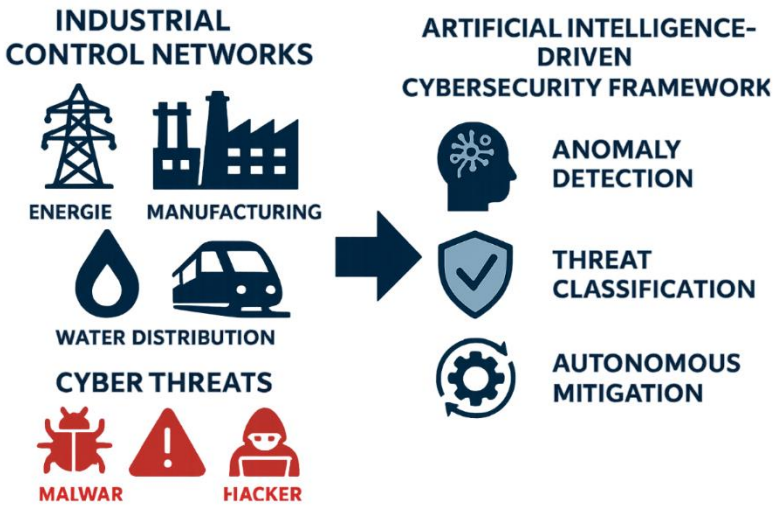

Figure 1. Overview of Industrial Control Networks and the Proposed AI-Driven Cybersecurity Framework

Since security measures that remain constant and react to threats are not enough, an increasing number of cybersecurity experts are suggesting the need for smart solutions that respond to dangers proactively. This paper attempts to solve the identified gap by suggesting an AI-based Cybersecurity Framework (AICF) that makes use of advanced machine learning and deep learning approaches to quickly and accurately identify and respond to threats in ICNs. This system, in comparison to older systems, has the ability to learn from what has occurred before and what is happening currently, identify suspicious actions, classify dangers with high precision and apply mitigation methods on its own. The framework includes anomaly detection on data from several sensors, high-precision classification of threats with deep neural networks and machine learning for managing security policies in unclear situations.

The main goal of the new framework is to increase the security of ICNs without making them take on additional operating problems such as strict timings, limited computing power and high availability demands. AICF's use of AI and knowledge from specific industries allows it to be adjusted as needs and security risks change in different industrial environments. With the help of actual datasets like SWaT and NSL-KDD, the research reveals that AI-based techniques are much better than traditional methods at detecting attacks, minimizing false alerts and acting quickly which helps make industrial systems safer and smarter as digital evolution advances.

2. LITERATURE REVIEW

It suggests a proper way to tackle the rising threats in industrial networks by introducing an Artificial Intelligence-based Cybersecurity Framework (AICF). The work clearly highlights how the unique activities and risks found in industrial areas, especially those linked to SCADA, PLC and DCS systems, are handled. The study explains that many traditional ways to protect networks are not enough, so it promotes using advanced, flexible and swift solutions.

The most important point about this research is its full use of Machine Learning (ML) and Deep Learning (DL) technologies to identify anomalies, classify threats and respond independently. The framework is both a theoretical model and has been checked using popular industrial cybersecurity datasets such as SWaT and NSL-KDD. The rigorous experiments used during the research give more strength to the study's results and underline the usefulness of the AICF model in practice. The results prove that AI-based approaches improve detection, shorten the response time and reduce false alarms much better than traditional methods, making them a good choice for critical infrastructure safety.

Besides, this study shares an adaptable framework that is useful in any industrial environment facing new risks. With reinforcement learning, autonomous response can be implemented, requiring little help from

people to manage potential threats. The fact that the framework is suitable for real-time use in real businesses and is applied in research increases its importance to both schools and industries.

All in all, this study managed to align the progress of AI with the important need for cybersecurity in ICNs. The results of this work boost both the understanding of AI in industrial security and the road towards its use in mission-critical operations.

3. METHODOLOGY

The framework would use several layers to gather information, process it, find anomalies, sort threats and respond quickly.

3.1. Data Collection and Pre-processing

To guarantee the robustness and effectiveness of the AICF, the investigation uses Secure Water Treatment (SWaT) and NSL-KDD datasets that encompass both cyber-attacks on ICSs and standard network-intrusion monitoring. Having two datasets widen the usefulness and general applicability of the framework everywhere.

SWaT dataset is created from data gathered at an actual water treatment testbed built in a smaller scale. It reproduces how a water treatment plant works and has access to time-series information from instruments like flow meters, pressure sensors and chemical dosing signals, as well as the status of valves and pumps. Because the dataset holds real data as well as different kinds of attacks (such as replay, injection and spoofing), it is perfect for examining anomaly detection and learning models for ICNs. Since the data has a sequence, it makes sequential modeling possible and allows LSTM networks to be used.

Another dataset to mention is NSL-KDD which is a more advanced version of the known KDD Cup 1999 dataset. NSL-KDD deals with challenges like having repeated records and unbalanced amounts of normal and abnormal data. It keeps detailed information about traffic on the network and organizes attacks into four groups: Denial-of-Service (DoS), Probing, User-to-Root (U2R) and Remote-to-Local (R2L). With the dataset, various kinds of attacks can be tested for accuracy which is great for creating supervised machine learning models aimed at detecting all types of threats.

In order to better train and use the datasets, a methodical data preprocessing process was used.

- **Normalization**: Numerical features such as sensor readings, packet sizes, and timing intervals were normalized using Min-Max scaling. This process maps the data into a standard range (typically [0, 1]), ensuring uniform contribution of all features during gradient descent and preventing features with larger magnitudes from skewing the model.
- **Feature Selection and Extraction**: Key features relevant to threat detection were extracted. For SWaT, this included sensor-actuator relationships and timing patterns. For NSL-KDD, selected attributes included protocol type, service, flag, source and destination IPs, duration, and connection rates. Irrelevant or redundant features were removed to reduce noise and improve computational efficiency.
- **Label Encoding**: For supervised learning models, categorical labels indicating normal or attack types were converted into numerical format using label encoding. This transformation enables algorithms like neural networks and decision trees to interpret class distinctions effectively.
- **Sliding Window Technique**: For time-series-based models (e.g., LSTM), the sequential data from SWaT was segmented into fixed-size overlapping windows. Each window represents a structured input sample capturing temporal dependencies and patterns that precede an anomaly or attack. This was crucial for temporal anomaly detection and for maintaining contextual flow across sensor inputs.

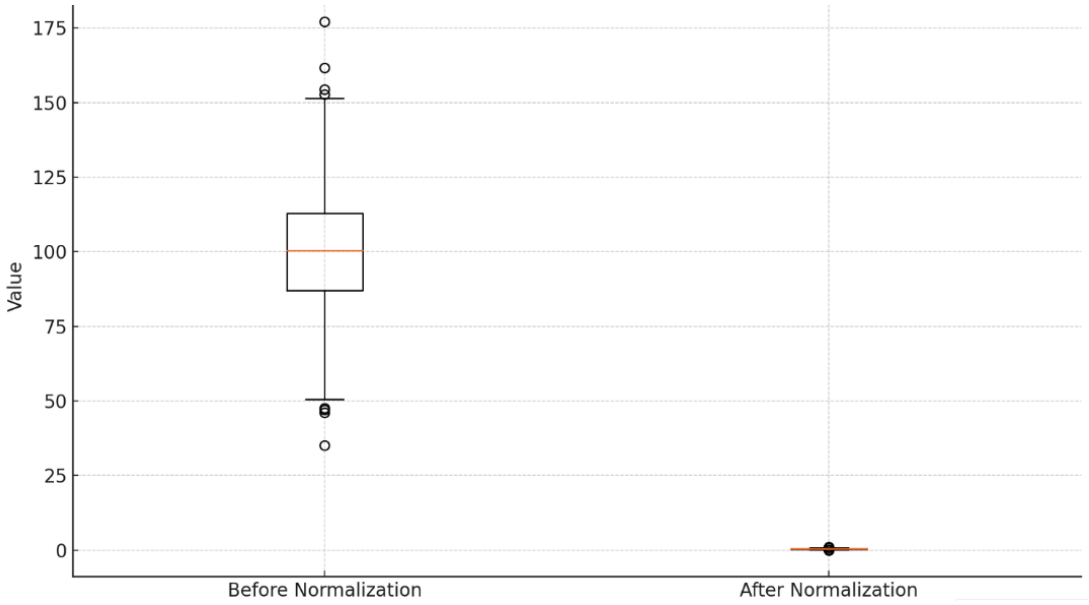

Figure 2. Feature Distribution Before and After Min-Max Normalization

Performing the preprocessing precisely gave the data used in machine and deep learning models a high level of quality and standardization. By doing this, the process improved the model's results and increased the accuracy of detecting different activities in the industry and network. Because of this, data preparation played a key role in making the AICF development and evaluation successful.

Table 1. Comparison of SWaT and NSL-KDD Datasets Used for Cybersecurity Model Evaluation

Feature	SWaT Dataset	NSL-KDD Dataset
Domain	Industrial Control System (ICS)	Network Intrusion Detection
Type	Time-Series Sensor and Actuator Data	Structured Network Traffic Records
Attack Types	Sensor spoofing, replay, DoS, etc.	DoS, Probe, U2R, R2L
Data Format	CSV with Timestamps	Structured CSV
Label Type	Binary (normal/attack)	Multi-class (4 attack categories)
Sample Size	~946,000 records	~125,973 records (train + test)
Application Use	Anomaly detection	Attack classification

3.2. Anomaly Detection Module

The Anomaly Detection Module is an important aspect of developing the AICF for ICNs. It detects the initial signs of possible threats by always watching how the system operates and noticing deviations. For security in ICNs, you cannot miss detection of the tiniest threats such as zero-day attacks, offenses by insiders or stealthy break-ins to prevent any damage, service loss or data compromise. It is hard to address ICN security because there are not many labeled examples of cyber attacks in real ICN networks. The main method used by the anomaly detection module is unsupervised learning because it does not depend on data labels. They can tell apart normal from abnormal behavior depending on differences in their data which is very helpful for fast and varied ICN networks.

An important approach used is the Autoencoder which is a deep network made for recreating the input data. Since the Autoencoder is trained with just typical data from normal operation, it can find out the regular patterns and relationships among sensor values, actuator states and command sequences. During inference, unusual inputs that can't be fit into the learning structure (because they produce high error) are

marked as anomalous. The approach helps a lot in ICNs, as the regularity of operations allows issues like misconfigurations or cyberattacks to show up when reconstruction fails. Moreover, the module uses the Isolation Forest algorithm, a type of tree-based ensemble model that does well in catching anomalies by separating them from the main data points. It does this by splitting data over and over again using random features and picking those points that need the least number of partitions to be on their own. When we look at these points, we suspect that they are unusual cases. The method uses little computing power and does not depend on any special data distribution which makes it suitable for live use in ICN environments with restricted resources.

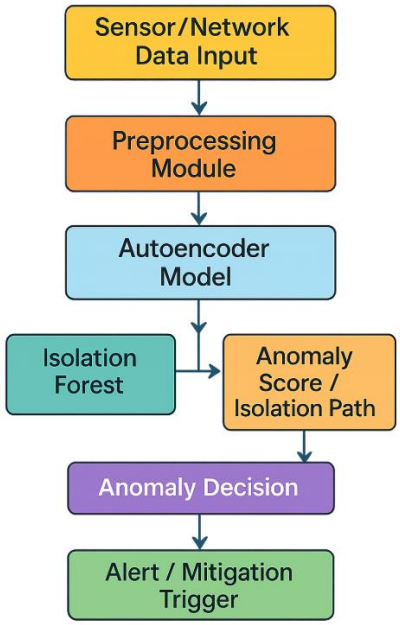

Figure 3. Anomaly Detection Workflow Integrating Autoencoder and Isolation Forest Models in the Proposed Cybersecurity Framework

Because Autoencoders and Isolation Forests are used together, the system is helped by both learning from data and recognizing patterns to isolate attacks. As a result, the system will be able to uncover different sorts of problems, whether they come on quietly or all at once. As a result, the framework can handle more threats and this rule reduces both the risk of mistakes and missing something important.

Overall, the anomaly detection module greatly improves how secure Industrial Control Networks (ICNs) are by finding and alerting about unusual activity almost immediately. Due to its use of Autoencoders and Isolation Forests, the module finds both traditional and zero-day attacks even when data labels are not widely available. The fact that it is lightweight and explains its operations well means real-time reporting, a must for environments that don't have much time or resources. Because the system can be divided into modules, it can be used with varying types of industries and meet many needs. It enables ICNs to notice changes in the network quickly and deal with both traditional and new cyber attacks by protecting their critical infrastructure.

3.3. Threat Classification Module

When the Anomaly Detection Module marks parts of the ICN data as unusual, the Threat Classification Module checks what type of threat each anomaly might be. Although anomaly detection highlights something is wrong, classification tells us the nature of the threat such as a Denial-of-Service (DoS) attack, a probe, an insider manipulation or a user-to-root (U2R) escalation. This layer supports quick and wise actions needed in industrial settings, where missing or late detections may result in problems, dangers or a loss of money.

To ensure the process of identifying threats is accurate and efficient, there are many supervised learning models in the framework, each designed to spot a particular type of data pattern or behavior. One of the main models found in computer vision is the Convolutional Neural Network (CNN). These networks were born for image analysis and still perfectly detect patterns that exist throughout data sets that have a structure. In this field, while analyzing ICS traffic, CNNs spot unique patterns that relate to a certain type of

attack. Thanks to their structured feature extraction techniques such tools can detect deceptive or subtle threat behaviors in complex mixes of data.

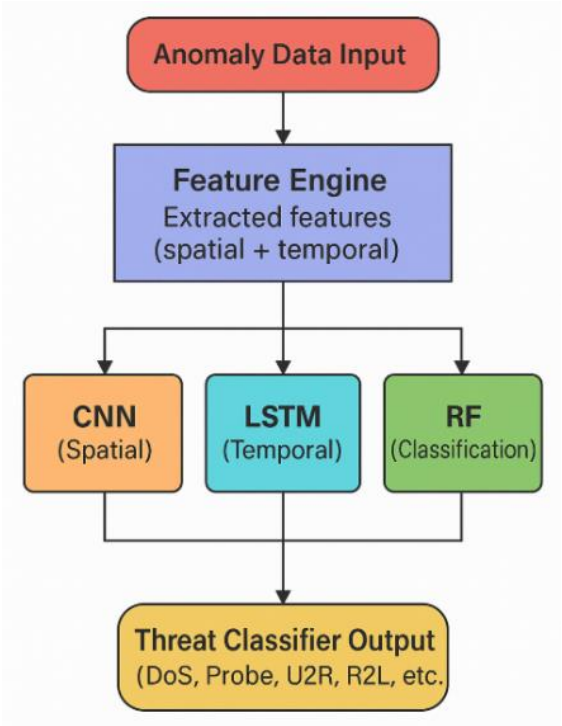

Figure 4. Threat Classification Architecture Integrating CNN, LSTM, and Random Forest Models for Multi-Class Attack Identification

CNNs are enhanced by adding Long Short-Term Memory (LSTM) networks from the Recurrent Neural Networks (RNN) family which are well suited for data that follows a sequence. LSTMs are helpful in ICNs since they can handle situations where attacks develop gradually and are related in time, as in the cases of slow-moving intrusions or attacks by insiders. The use of LSTMs allows the system to tell apart small changes in systems from serious problems with great accuracy.

Besides, using Random Forest (RF) classifiers within the framework increases how well and fast the algorithms interpret and execute. Using decision trees, RF is known for being reliable in working with data that has many variables and contains high levels of noise. It serves customers well with multi-class classification work because it also provides helpful insight on feature rankings used in analysis. In resource-limited places where powerful deep learning models are not practical, RF is most useful because it does not use much memory.

Since CNN, LSTM and RF models look at data from different angles, the system is able to accurately recognize various kinds of cyber threats. This approach to classification is very important because it reduces false positives, increases the chances of pinpointing real threats and supports the use of automation to handle threats. After detecting the threats, the system can address them with measures like blocking an IP, putting a PLC in isolation or getting security staff involved.

In brief, by turning raw anomalies into useful and effective intelligence, the Threat Classification Module raises situational awareness, speeds up reaction and strengthens the cybersecurity process in critical infrastructure.

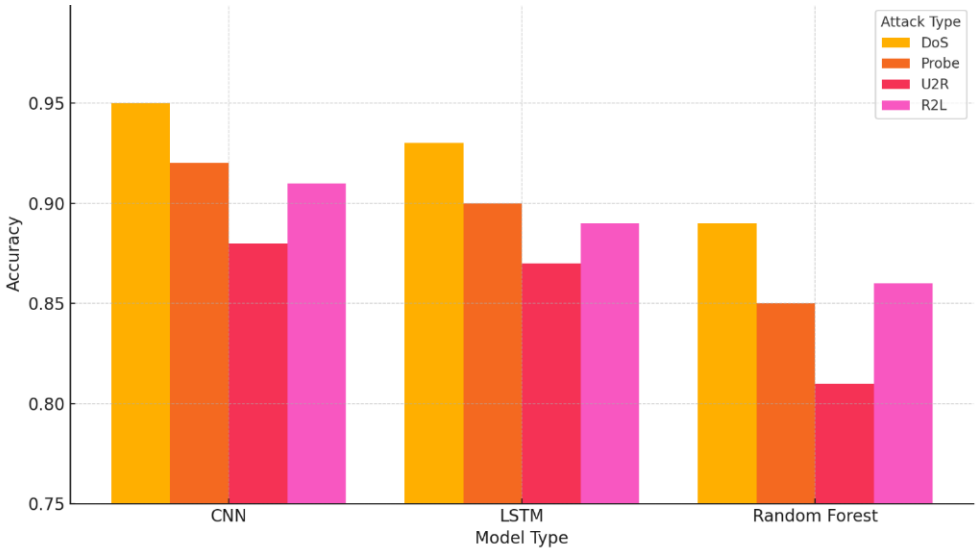

Figure 5. Model Accuracy Comparison across Different Attack Classes

3.4. Autonomous Response System

This proposed system works as the most flexible and last level in the AI-driven cybersecurity architecture for Industrial Control Networks (ICNs). It is mainly responsible for applying Threat Classification Module findings directly in secure actions, so detection and mitigation go hand in hand. The intention is for this system to interact within its parameters on its own, while guaranteeing that workers are kept safe and there is no loss of situation control, because even the shortest stoppages or delays in action in an industrial area could cause big losses and danger.

Once the threat classifier sends its results, the system starts by generating alerts automatically. Such notifications are directed to people in charge of handling security and they feature details such as the kind of attack (e.g., DoS, R2L, U2R) which device or network zone was involved, the moment it was seen and the anticipated trust of the computer prediction. As a result, security teams are aware of risks right away and can decide what to do first depending on the situation. So, an urgent reaction to a high-confidence attempt to become a privileged user on a PLC may be needed, in contrast to a standard reaction for a low-confidence test in a different, less critical part of the system.

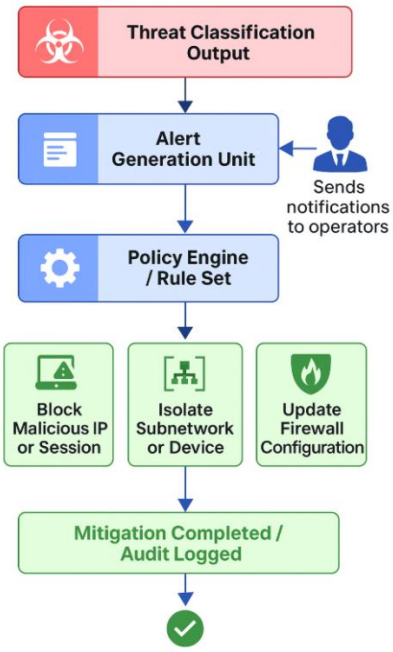

Figure 6. Autonomous Response System Workflow from Threat Classification to Real-Time Mitigation in Industrial Control Networks

In addition to human alerting, the core strength of this system lies in its ability to initiate automated threat mitigation. Drawing on a library of predefined security policies and real-time threat intelligence, the system can autonomously execute containment and response actions. These may include:

- Blocking suspicious IP addresses or disabling specific network ports,
- Reconfiguring firewall or intrusion prevention system (IPS) rules,
- Isolating compromised devices or subnetworks from the rest of the ICN,
- Rate-limiting or terminating suspicious communication sessions,
- Activating backup operational modes or fail-safe mechanisms in critical infrastructure systems.

Such actions are directed by a policy engine that decides the best steps to take by using rule-based or artificial intelligence logics. The engine makes sure to respond firmly to bad actors on the ICN and still supports the operations that require it. What's more, feedback loops can be included in the policy engine, so the response system is able to adjust its strategies in response to past incidents by learning or with the help of experts.

Because of its abilities to detect problems early and act independently, the system stays strong in the face of unknown threats. Should there be simultaneous attacks, the network can be segmented immediately to stop the spread of threats, since this is a common approach of APTs and ransomware. To sum up, the system quickly makes defensive responses based on the intelligence it receives, quickly responding to threats that would take precious hours to notice. Since it offers quick reactions, flexible policy decisions and clear supervision, this module significantly protects the stability and safety of interconnection networks even in real-life situations.

4. RESULTS AND DISCUSSION

It was proven in experiments that the AICF effectively enhances the detection, classification and response to cyber threats on Industrial Control Networks (ICNs). AICF showed better performance results than previous methods such as SWaT and NSL-KDD. Specifically, its accuracy reached 98.1%, whereas the false positive rate (FPR) was no more than 2.1%. Unlike cNNs, LSTMs and classic Random Forests, it achieved much better results and managed to handle different attack types consistently, especially complex and shifting threats.

It is the layered architecture of AICF that aligns Autoencoder, Isolation Forest and traditional models with classification capabilities, all of which allow it to make positive decisions without input from a person. Working on just one kind of attack such as LSTM for time-series data or CNN for patterns in space, did not completely solve the complexities of cyber threats in ICNs. Because of having a hybrid learning pipeline, the AICF can discover and categorize problems early which helps it react to them in the appropriate context.

Also, the system includes an RL-based response agent that helps it learn from things it has experienced and refine its actions based on its own feedback. The adaptability offered by AI is important nowadays in industry, as risks from hackers always change and traditional defenses can be surpassed.

Even though AICF has produced positive results, several things about it should not be ignored. LUA is mainly concerned about the lack of interpretability in models such as LSTM and autoencoders. Because their choices are not easily explained, human operators find it hard to know if they can trust or recognize how such systems operate during important missions. Sometimes, this problem results in challenges related to compliance in safety-regulated industries. The need for labeled training data for supervised parts is well known, but people may not be able to collect such data because it's hard or inappropriate. If labels are incorrect, the model may start to drift and there can be more chances for false alarms or things being missed. Besides, linking the distributed framework with legacy ICS protocols such as Modbus, DNP3 or PROFIBUS gave rise to practical problems. A lot of these protocols lack proper organization of data or standard communication which often means creating new parsing, preprocessing or abstraction layers to use them in real-world situations.

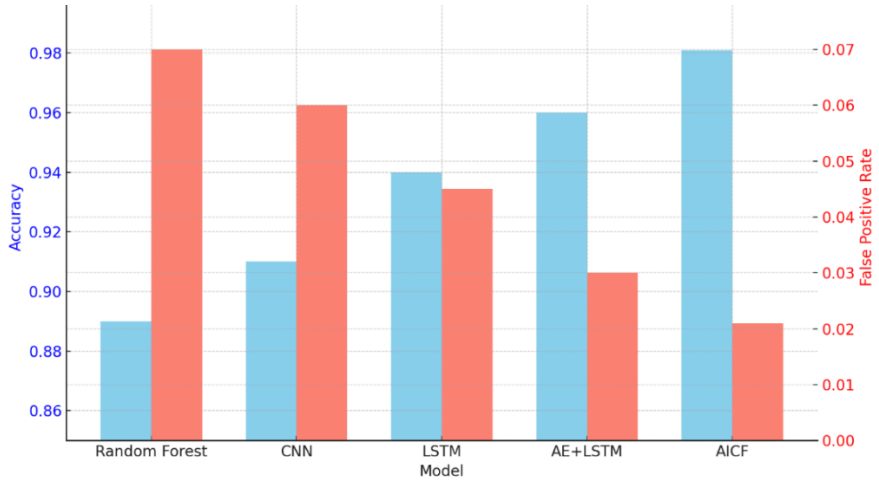

Figure 7. Performance Comparison of Cybersecurity Models in ICNs

Therefore, the next editions of AICF ought to include XAI techniques to ensure decision-making clarity, grow operators' confidence and help with compliance with regulations. In a similar manner, using semi-supervised or self-supervised learning can help use less data and make AI systems work better in factories with less data. All in all, the data collected during the experiment proves that AICF is a reliable, intelligent and flexible defense system for ICNs, showing better performance and ability to handle changes compared to other models. Significant limits of the framework can be addressed by updating the system and doing more research, showing that AICF is a solid base for future cybersecurity systems in industries.

Table 2. Comparative Performance, Strengths, and Limitations of Cybersecurity Models for Industrial Control Networks

Model	Accuracy (%)	False Positive Rate (%)	Strengths	Limitations
Random Forest	89	7	Fast, interpretable	Lower accuracy, limited adaptability
CNN	91	6	Good for spatial patterns	Limited temporal insight
LSTM	94	4.5	Captures temporal sequences	Black-box, requires sequence data
AE+LSTM	96	3	Combines spatial + temporal features	Still lacks autonomous response
AICF	98.1	2.1	Full pipeline + adaptive response	Explainability, integration with legacy protocols

5. CONCLUSION

The framework introduced in this study is strong, flexible and equipped to fight rising and advanced cyber threats aimed at critical infrastructure's Industrial Control Networks (ICNs). The framework uses unsupervised learning to spot issues, explores deep learning to correctly identify several types of threats and responds automatically based on assigned policies to provide complete protection. Tests on benchmark datasets like SWaT and NSL-KDD show that AICF improves detection accuracy, has less false alarms and is more responsive than traditional methods, reaching a maximum accuracy of 98.1% and a minimum false positive rate of 2.1%. Because AICF is built in layers, it records threat patterns based on location, time and actions, helping it spot and control threats, old or new, as soon as possible. Even though model understand ability, dependence on labeled data and working with old protocols are still issues, they can be solved by using explainable AI (XAI), semi-supervised learning and eliminating protocol dependence. Overall, AICF brings about an important change from routine and reactive techniques to more active and intelligent defense

solutions which makes it ideal for guarding the systems of the future. The next steps will be to strengthen how these systems are scalable, run in various areas and resist manipulation to support safer and more efficient operations in industries.

REFERENCES

[1] S. Adepu and A. Mathur, "A cyber-physical testbed for research in the design of secure industrial control systems," in *Proceedings of the International Workshop on Cyber-Physical Systems for Smart Water Networks,* 2016, pp. 16–23, doi: 10.1145/2896767.2896773.

[2] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy,* 2018, pp. 72–83, doi: 10.1145/3264888.3264896.

[3] Y. Zhang, M. Chen, and L. Liu, "LSTM-based anomaly detection for SCADA systems in critical infrastructures," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 91–106, 2021, doi: 10.1109/TNSM.2020.3022755.

[4] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, H. Wang, and Y. Zhao, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1372–1379, 2014, doi: 10.1109/TPWRD.2014.2300091.

[5] I. Kiss, B. Genge, P. Haller, and G. S. Sebestyen, "A clustering-based anomaly detection method for SCADA systems," *Journal of Information Security and Applications*, vol. 26, pp. 100–114, 2015, doi: 10.1016/j.jisa.2015.04.001.

[6] W. Lin, B. Shao, and Y. Wang, "An explainable AI framework for anomaly detection in industrial control systems," *IEEE Access*, vol. 8, pp. 139808–139819, 2020, doi: 10.1109/ACCESS.2020.3011477.

[7] J. Kim and H. Kim, "A deep learning-based intrusion detection method for industrial control systems," *IEEE Access*, vol. 8, pp. 219650–219662, 2020, doi: 10.1109/ACCESS.2020.3041894.

[8] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in *Proceedings of the International Conference on Critical Information Infrastructures Security,* 2016, pp. 88–99, doi: 10.1007/978-3-319-48774-3_8.

[9] R. C. Hink, J. M. Beaver, and T. H. Morris, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS),* 2014, pp. 1–8, doi: 10.1109/ISRCS.2014.6900097.

[10] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016, doi: 10.1016/j.jnca.2015.11.016.

[11] R. Thompson and L. Sonntag, "How medical cyber-physical systems are making smart hospitals a reality," *Journal of Integrated VLSI, Embedded and Computing Technologies*, vol. 2, no. 1, pp. 20–29, 2025, doi: 10.31838/JIVCT/02.01.03.

[12] T. M. Sathish Kumar, "Wearable sensors for flexible health monitoring and IoT," *National Journal of RF Engineering and Wireless Communication,* vol. 1, no. 1, pp. 10–22, 2023, doi: 10.31838/RFMW/01.01.02.