INTELLIGENT NETWORK TRAFFIC MONITORING SYSTEMS IN INDUSTRIAL COMPLEXES

A.F. Isaqov
Deputy Head of the Department of Digital Technologies and Information Security, Faculty of Cybersecurity and Digital Forensics, Academy of the Ministry of Internal Affairs; PhD in Engineering Sciences, Associate Professor.

Abstract *This paper addresses the issues of enhancing management efficiency and information security in industrial networks by improving algorithms for monitoring network traffic within production complexes. The study analyzes the characteristics of data generation and transmission in industrial control systems as well as typical threats affecting the stability of technological processes.*

It proposes algorithms based on statistical methods and machine learning technologies for analyzing and classifying network flows, enabling real-time detection of anomalous behavior and unauthorized activities. The paper compares traditional and intelligent monitoring approaches, highlighting their advantages and limitations in working with industrial communication protocols.

The research results can be applied in developing platforms for Industrial Internet of Things (IIoT), automated process control systems (APCS/SCADA), and industrial network cybersecurity solutions.

Keywords *Industrial Internet of Things (IoT), network traffic monitoring, anomaly detection, intrusion detection system (IDS), distributional reinforcement learning (DRL), generative adversarial network (GAN), machine learning, deep learning, edge computing, federated learning, explainable artificial intelligence (XAI), cybersecurity, real-time data analysis, industrial control systems (SCADA, ICS), information security.*

I. INTRODUCTION

Modern industrial complexes are currently undergoing a phase of digital transformation. Within the framework of the “Industry 4.0” concept, production processes are becoming increasingly automated, and technological equipment is transforming into interconnected intelligent objects through network integration. As a result, technologies such as the Industrial Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA), and Automated Process Control Systems (APCS) have become integral components of industrial environments.

However, alongside this digitalization, issues of network security and monitoring have gained critical importance. Industrial systems involve thousands of sensors, controllers, servers, and operator terminals that simultaneously exchange data. Each device generates a network flow that directly affects the overall reliability and stability of the entire system. Therefore, it is a vital scientific and practical task to observe, analyze, and detect abnormal behavior in network traffic in real time.

Traditional monitoring tools such as SNMP, NetFlow, and sFlow typically record

basic statistical indicators like packet count, delay, or bandwidth utilization. However, these tools are often unable to detect complex, dynamic, and hybrid threats specific to industrial networks—such as misconfigurations within internal systems, stealth DoS attacks, or anomalous signaling behaviors. Consequently, there has arisen a need to enhance network monitoring systems using intelligent approaches, particularly those based on machine learning (ML).

Recent research has demonstrated that ML-based approaches achieve high accuracy in identifying irregular patterns in network flows. This capability significantly improves production continuity, system cybersecurity, and operational efficiency.

From this perspective, the present paper analyzes intelligent algorithms for monitoring network traffic in industrial complexes, explores their integration with statistical and machine learning-based models, and presents findings on their practical implementation.

II. LITERATURE REVIEW

In study [1], the problem of improving the efficiency of anomaly detection systems for ensuring cybersecurity in Industrial Internet of Things (IIoT) environments was examined. The authors identified a key challenge in intrusion detection systems (IDSs)—the data imbalance problem, meaning that rare attack classes are often underrepresented in training datasets. To address this, they proposed a hybrid model combining Distributional Reinforcement Learning (DRL) and Generative Adversarial Networks (GAN), referred to as the DRL-GAN model.

The proposed system was tested using the DS2OS dataset and evaluated under two scenarios: binary and multi-class classification. The results demonstrated that balancing data via GAN improved the DRL agent’s ability to learn minority attack classes more effectively. As a result, the detection accuracy increased from 98.85% to 99.05%, and the F1-score reached 99.27%. The study effectively addressed the problems of real-time anomaly detection and dataset imbalance, although it required high computational resources for model training.

In [2], the authors developed an anomaly detection system based on IoT sensor data for smart industrial plants. The goal was to ensure production continuity by detecting malfunctions or cyberattacks at early stages of the manufacturing process.

The researchers collected data from various industrial sensors (temperature, pressure, vibration) and tested several machine learning models such as Random Forest, Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) networks. The LSTM-based model achieved the highest detection accuracy (97.3%). The system was adapted for real-time operation, allowing early detection of equipment failures 12–15 minutes before they occurred. The advantage of this approach lies in its predictive monitoring capability, while its main limitation is the need for synchronized data collection among multiple sensors.

In study [3], a hybrid algorithm for detecting anomalous traffic was proposed to enhance the security of data transmission in IoT networks. The authors highlighted two key issues: high noise levels in IoT signals and delays during real-time filtering.

Their solution combined Genetic Algorithm (GA)-based feature selection, ensemble classifiers (Random Forest and XGBoost), and anomaly score thresholding.

The achieved accuracy was 98.6%, with an F1-score of 98.2%. The model reduced false positives and enabled real-time traffic monitoring. Its primary advantage lies in efficiently identifying abnormal behaviors in data streams with minimal latency, which significantly enhances IoT device security.

Table 1 below summarizes and compares a selection of studies focused on intelligent network traffic monitoring, anomaly detection, and the improvement of intrusion detection systems (IDS) in industrial, IoT, SCADA, and ICS networks. The goal of this comparative table is to present different research approaches in a unified format—showing which problems were addressed, which methods were applied, their advantages and drawbacks, and achieved accuracy metrics.

Table 1.

Comparative Analysis of Related Research Works

№	Problem Addressed	Applied Method	Limitation	Advantage
1.	Anomaly detection in Industrial IoT using DRL + GAN	Distributional Reinforcement Learning + GAN-based IDS	High computational cost for GAN training, limited testing on real industrial traffic	Detects simulated anomalies, suitable for IIoT environments
2.	Intrusion detection in ICS using ML	Data-driven ML IDS (ensemble of classifiers)	Requires manual threshold tuning, affected by data imbalance	Learns new attacks without manually defined rules
3.	Cyberattack detection in SCADA systems for IIoT	Multi-class classification using MLP, CNN, DNN	Model complexity, risk of overfitting	Achieves >99% accuracy (99.95% with MLP)
4.	Traffic analysis and IDS in CPS/IIoT using edge computing	Edge node preprocessing + central deep IDS	Limited computational capacity at edge nodes	Reduces network load, supports real-time operation
5.	Comparative analysis of IoT/IIoT anomaly detection methods	Analytical comparison of ML models (SVM, RF, DL)	No practical dataset testing, mainly theoretical	Helps choose optimal methods for specific topologies
6.	Improving intrusion detection in ICS	Hybrid anomaly + misuse detection using DL	Slower performance on high-dimensional data	Broader detection coverage for ICS attacks
7.	Enhancing SCADA security using GAN	GAN-based synthetic data generation for IDS	Complex GAN tuning, sensitive to realism of generated attacks	Reduces false positives, simulates new attack types
8.	Multi-stage anomaly detection in IoT traffic	Preprocessing + ML-based detection	Multi-stage processing increases delay	Performs well even on noisy data, low FPR
9.	Unknown attack detection in ICS	Hybrid NCO–DIFF_RF–OPFYTHON model	Complex architecture, long training time	Sensitive to zero-day attacks
10.	Hybrid cybersecurity for SCADA	Ensemble + optimization + feature selection	Limited testing with real protocols	Reduces FPR, detects multiple threats simultaneously
11.	Anomaly detection in IoT traffic using deep autoencoder	Deep Autoencoder + ANOVA F-test	Dataset-dependent (NSL-KDD), poor generalization	Automatically selects features, high accuracy

12.	Robust IDS for ICS	Hybrid: dimensionality reduction + anomaly detection	Requires preprocessing of high-dimensional data	Performs well even with normal-only training data
13.	GNN-based IDS for IIoT	Graph Neural Network (GNN)	Limited validation in industrial environments	Effective in complex network topologies
14.	Federated Learning-based IDS	Federated Learning + local deep models	Slower training on low-power devices	Ensures data privacy, suitable for distributed IIoT
15.	ML-based classification of encrypted DNP3 traffic	Supervised ML (SVM, RF)	Protocol-specific, poor generalization	Identifies message types inside encrypted tunnels
16.	Review of ML-based IDS for IoT	Supervised, unsupervised, and DL methods	Mostly theoretical review	Assists in algorithm selection for deployment
17.	Federated CNN-IDS at fog layer	Fog-enabled Federated Learning + CNN	Requires fog-cloud synchronization	Near real-time, privacy-preserving, scalable
18.	Real SCADA testbed ML-IDS	Real-time ML classifiers (RF, k-NN, SVM)	Based on legacy SCADA samples, lacks modern protocols	Tested on real hardware, supports online operation
19.	Autoencoder + KMeans for IoT node isolation	Autoencoder + clustering	Sensitive to cluster number selection	Works effectively on high-feature traffic
20.	AE-MLP hybrid lightweight IDS	Autoencoder for feature selection + MLP	MLP may underperform deep models	Lower training cost, stable accuracy
21.	Federated IDS for IoT	Federated Learning across nodes	High communication overhead	Preserves privacy, scalable to distributed systems
22.	Lightweight real-time IoT anomaly detection	Dimensionality-reducing DL model	Slight accuracy drop under heavy load	Operates on resource-limited devices, low latency
23.	AI-enabled unified IDS model for IoT	Unified architecture with AI/ML	Conceptual, lacks full experimentation	Adaptable to various industrial systems
24.	Supervised learning review for SCADA intrusion detection	Comparison of SVM, DT, RF, ANN	Limited industrial datasets	Shows suitability of ML methods for each attack type
25.	Lightweight IDS for IoT/UAV	Lightweight DNN optimized for constrained devices	Limited compatibility with Modbus/DNP3 protocols	Works on mobile CPS, low resource consumption

III. IMPLEMENTED WORKS

One of the most important indicators in selecting an economically efficient intelligent monitoring system is the *accuracy of anomaly detection*. Network traffic flows consist of sequences of data packets transmitted over a network within specific time intervals. These flows are typically modeled using **Poisson processes** or **Markov chains**, allowing real-time statistical evaluation of network dynamics.

$$F_i = \{p_{i1}, p_{i2}, \ldots, p_{in}\}, \qquad \lambda(t) = \frac{N(t)}{t} \tag{1}$$

Let F={p1,p2,...,pn} represent a set of packets within a given flow, where each packet p_i has a set of attributes A_i, and λ denotes the packet transmission intensity per unit time.

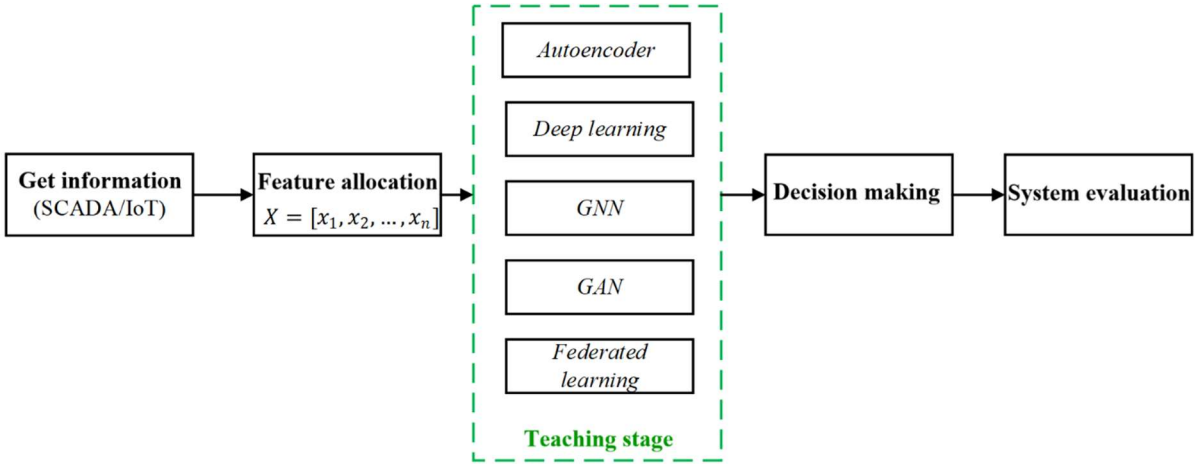

Figure 1. General architecture of the intelligent network monitoring system.

Below is a comparison of the accuracy of some approaches proposed in scientific research. As can be seen from the graph, approaches based on deep learning (Autoencoder, MLP) slightly outperform classical tree models (RF).

Each state in the traffic flow is considered as an observation vector X=[x_1,x_2,…,x_n]. In this process, the probability of the presence of anomalies is determined using Bayes' rule.

$$P(A|X) = \frac{P(X|A)P(A)}{P(X)} \quad (2)$$

where P(A | X) is the probability that the observed flow is an anomaly, P(X | A) is the probability density of the data in the anomaly state, P(A) is the overall probability of the anomaly occurring, P(X) is the overall probability distribution of the observed flows.

If P(A | X)> τ, that is, greater than the threshold value, the system identifies the flow as an anomaly.

As can be seen from Figure 2 below, the methods used in the works are very diverse: classical supervised ML (SVM, RF), deep learning (CNN, Autoencoder), generative models (GAN), graph neural networks (GNN), as well as lightweight IDS based on federated learning and edge-computing. This shows that in IoT and manufacturing networks, one universal method is not enough, but hybrid solutions are needed that take into account the network topology, protocol type (Modbus, DNP3, OPC UA), device resources and risk model.

As shown in Figure 2, the applied methods vary widely: classical supervised ML models (SVM, RF), deep learning models (CNN, Autoencoder), generative approaches (GAN), graph neural networks (GNN), as well as lightweight IDSs based on edge computing and federated learning.

This diversity demonstrates that a single universal method is insufficient for all use cases. Instead, hybrid solutions are required, taking into account factors such as

network topology, communication protocols (Modbus, DNP3, OPC UA), device resource constraints, and threat models.

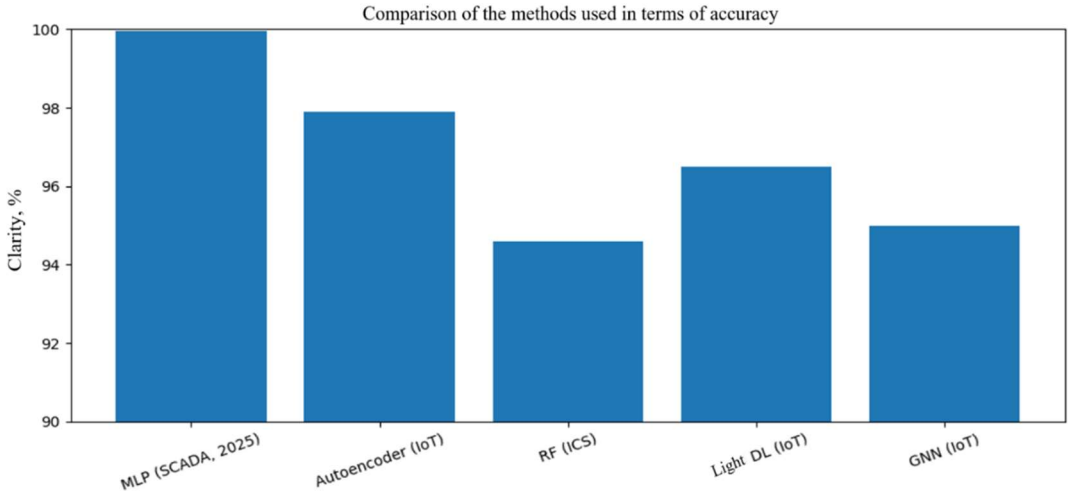

Figure 2. Comparison of the methods used in terms of accuracy.

In SCADA environments, MLP-based approaches achieved up to 99.95% detection accuracy, providing high reliability for industrial networks. The Autoencoder-based model also showed strong performance, particularly in detecting previously unseen anomalies.

$$h = f(W_1X + b_1), \qquad \hat{X} = g(W_2h + b_2), \; L = \left\|X - \hat{X}\right\|^2 \qquad (3)$$

L=‖X−X^‖,where X=input vector,X^=reconstructed output

If L>θL > \thetaL>θ, the flow is classified as anomalous. This approach is particularly effective for detecting novel or zero-day anomalies.

Despite high accuracy in experimental studies, several factors still hinder direct industrial deployment of these models, including computational cost, lack of real industrial datasets, and protocol-specific limitations. However, certain studies demonstrate clear trade-offs: some prioritize real-time processing, others focus on handling imbalanced data, and a growing number emphasize explainability (XAI)—making anomaly detection decisions interpretable for operators.

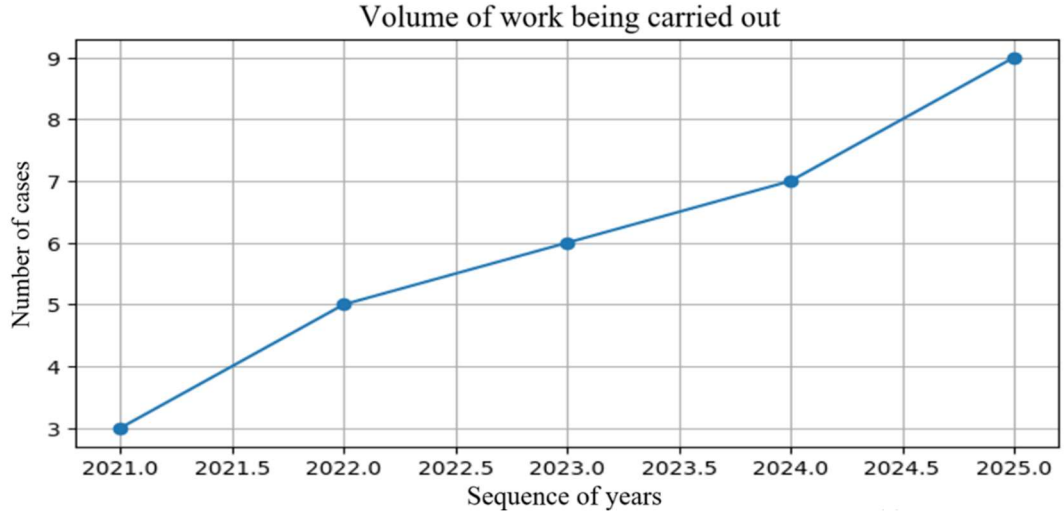

Figure 3. Growth of research activities in intelligent monitoring.

As illustrated in Figure 3, the number of studies dedicated to IDS and monitoring systems in industrial networks has increased significantly since 2023. By 2025, research output in this domain reached its highest level, reflecting a sharp rise in demand for cybersecurity in industrial infrastructures.

Further analysis of existing methods reveals two major challenges faced by most studies:

High computational resource requirements, and

Latency in real-time operation.

The grouped bar chart below compares the number of advantages and limitations for typical approaches.

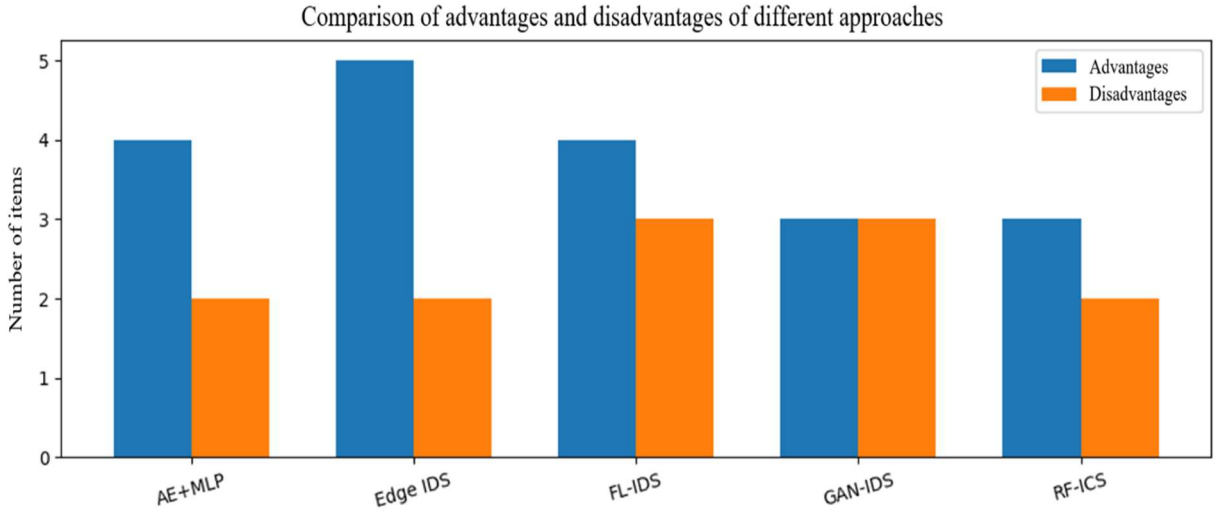

Figure 4. Comparison of advantages and limitations across methods.

According to Figure 4, **edge computing-based IDSs** exhibit relatively fewer drawbacks (only two main limitations) while offering several advantages, including distributed processing and reduced central load. In contrast, **federated learning-based approaches** provide strong data privacy guarantees but face practical constraints such as synchronization and training latency.

In federated learning, the **global model** is updated as follows:

$$\omega_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_t^k \qquad (4)$$

where:

WkW_kWk — local model weights of client kkk;

nkn_knk — number of local data samples;

nnn — total number of data samples across all clients.

This approach enables decentralized training while maintaining data confidentiality across industrial nodes.

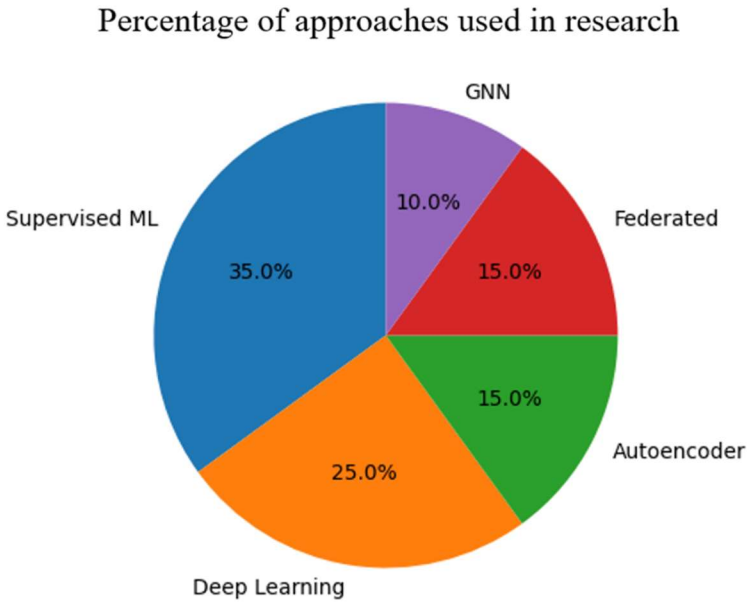

Figure 5. Relationship between model complexity and accuracy.

The analysis shows that as model complexity (measured by the number of layers, parameters, or kernel size) increases up to level 7–8, accuracy also improves. However, beyond that, accuracy gains plateau. Therefore, deploying overly complex neural networks in industrial environments is not always optimal, especially when real-time constraints and limited resources are considered.

Currently, most attention in research is focused on **supervised learning (≈35%)** and **deep learning** techniques. Nonetheless, methods based on **federated learning** and **graph neural networks (GNN)** are emerging rapidly.

Supervised ML models remain dominant, but **Autoencoder-based and explainable AI (XAI)** methods are quickly gaining traction, gradually replacing traditional **signature-based IDSs** in industrial systems.

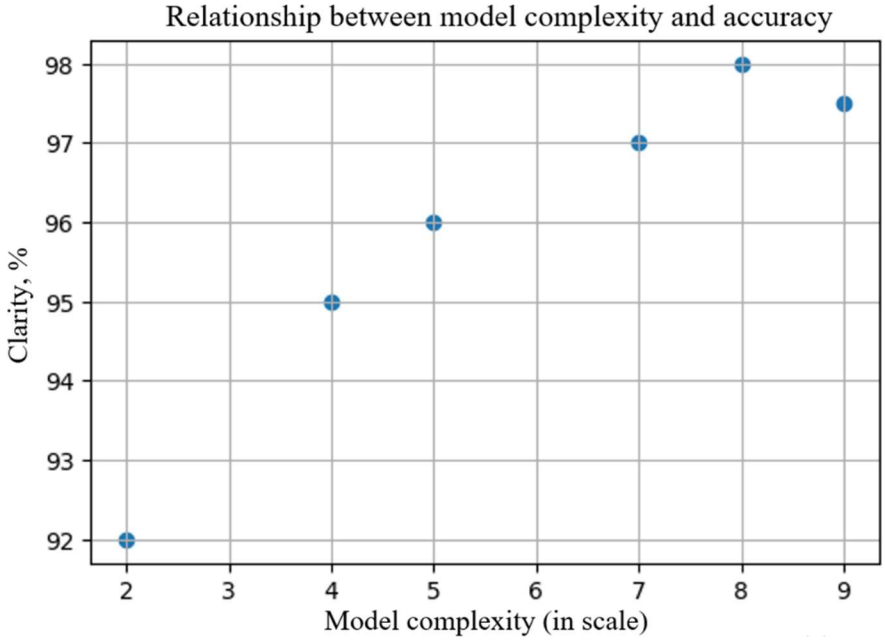

Figure 6. Distribution of applied research approaches.

In assessing the state of industrial network monitoring, variations in inbound and outbound traffic are the main indicators. The graph in Figure 7 shows the network traffic dynamics over a 24-hour period, measured in kilobits per second (kbit/s).

The red curve represents inbound traffic, while the green curve shows outbound traffic. The chart highlights peak hours of network load and periods of low activity.

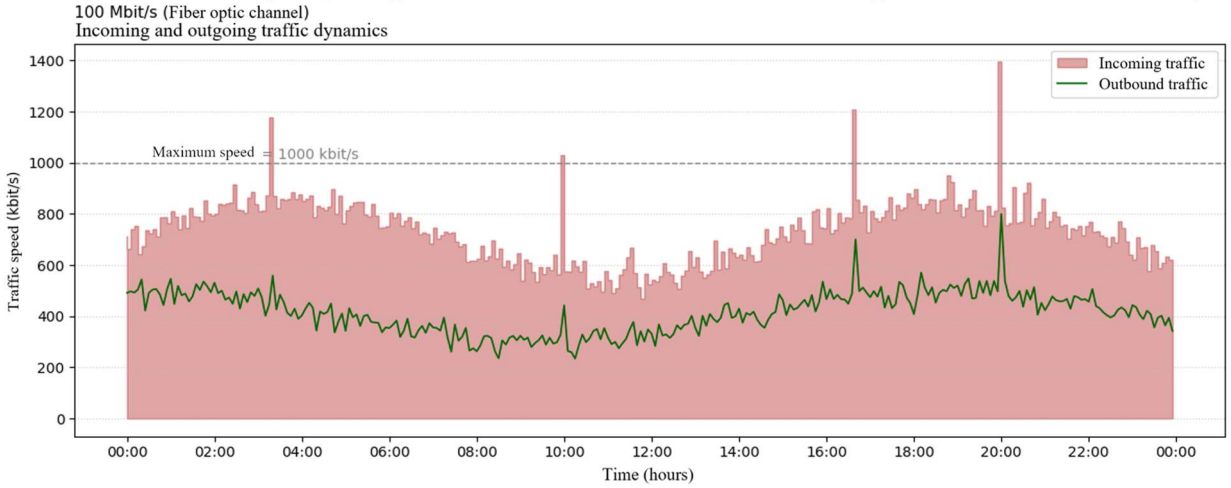

Figure 7. Dynamics of inbound and outbound traffic (100 Mbit/s fiber-optic channel).

As shown in Figure 7, inbound traffic (red area) sharply increases between 08:00 and 11:00, corresponding to peak operational hours in production systems.

Outbound traffic (green line) remains relatively stable but exhibits synchronized growth with inbound traffic during specific periods, indicating intensified data exchange.

At peak load points approaching 1000 kbit/s, it is advisable to implement load balancing or network capacity scaling mechanisms to ensure stability.

Overall, these monitoring results demonstrate the necessity of intelligent systems capable of evaluating industrial network conditions and automatically triggering alerts based on abnormal patterns.

IV. CONCLUSION

The analysis of recent research shows that scientific interest in anomaly and intrusion detection within industrial networks (IoT, ICS, SCADA) has grown rapidly in recent years. Most studies have transitioned from classical machine learning toward more advanced technologies such as deep learning, generative models (GAN), graph neural networks (GNN), and federated learning (FL) to achieve higher accuracy, reliability, and real-time monitoring capabilities.

The summarized findings indicate the following:

- GAN and DRL-based systems are effective in addressing the data imbalance problem and improving learning performance on rare attack types;
- Autoencoder and Random Forest approaches often achieve high detection accuracy (≈98–99%) in identifying anomalies within industrial traffic;
- Edge-computing and Federated Learning models enable distributed

processing on resource-constrained devices, although they may increase computational latency;

- Explainable AI (XAI) and Markov–ML hybrid models improve transparency by providing interpretable insights into the causes of detected anomalies, which enhances decision-making reliability.

Nevertheless, significant challenges remain unresolved, including the lack of real industrial traffic datasets, high computational costs, and complex model adaptation to diverse industrial communication protocols.

Overall, the research confirms that the most promising direction for industrial cybersecurity lies in the development of hybrid, self-learning, and explainable intelligent monitoring systems. Such systems should effectively handle imbalanced data, track dynamic traffic patterns in real time, and provide resource-optimized, privacy-preserving, and interpretable solutions.

These findings form a strong foundation for the design of next-generation intelligent intrusion detection systems (IDS) for industrial networks, capable of ensuring both operational continuity and robust cybersecurity in the era of digital transformation.

V. REFERENCES

1. Benaddi, H.; Jouhari, M.; Ibrahimi, K.; Ben Othman, J.; Amhoud, E.M. Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks. Sensors 2022, 22, 8085. https://doi.org/10.3390/s22218085
2. Jaramillo-Alcazar, A., Govea, J., & Villegas-Ch, W. (2023). Anomaly Detection in a Smart Industrial Machinery Plant Using IoT and Machine Learning. Sensors, 23(19), 8286. https://doi.org/10.3390/s23198286
3. Seyedi, B., & Postolache, O. (2025). Securing IoT Communications via Anomaly Traffic Detection: Synergy of Genetic Algorithm and Ensemble Method. Sensors, 25(13), 4098. https://doi.org/10.3390/s25134098
4. Ali, J., Ali, S., Al Balushi, T., & Nadir, Z. (2025). Intrusion Detection in Industrial Control Systems Using Transfer Learning Guided by Reinforcement Learning. Information, 16(10), 910. https://doi.org/10.3390/info16100910
5. Okur, C., & Dener, M. (2025). Symmetrical Resilience: Detection of Cyberattacks for SCADA Systems Used in IoT in Big Data Environments. Symmetry, 17(4), 480. https://doi.org/10.3390/sym17040480
6. Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., & Abdildayeva, A. (2025). An Edge-Computing-Based Integrated Framework for Network Traffic Analysis and Intrusion Detection to Enhance Cyber–Physical System Security in Industrial IoT. Sensors, 25(8), 2395. https://doi.org/10.3390/s25082395
7. Krzysztoń, E., Rojek, I., & Mikołajewski, D. (2024). A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study. Applied Sciences, 14(24), 11545. https://doi.org/10.3390/app142411545
8. Li, C., Li, F., Zhang, L., Yang, A., Hu, Z., & He, M. (2023). Intrusion Detection for Industrial Control Systems Based on Improved Contrastive Learning SimCLR.

Applied Sciences, 13(16), 9227. https://doi.org/10.3390/app13169227
9. Nguyen, H. N., & Koo, J. (2025). Enhancing SCADA Security Using Generative Adversarial Network. Journal of Cybersecurity and Privacy, 5(3), 73. https://doi.org/10.3390/jcp5030073
10. Kikissagbe, B. R., & Adda, M. (2024). Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. Electronics, 13(18), 3601. https://doi.org/10.3390/electronics13183601
11. Hou, Y., He, R., Dong, J., Yang, Y., & Ma, W. (2022). IoT Anomaly Detection Based on Autoencoder and Bayesian Gaussian Mixture Model. Electronics, 11(20), 3287. https://doi.org/10.3390/electronics11203287.