Machine Learning-Based Security Strategies in the IIoT: A Systematic Review

César A. Flores C.[1]; David Yauri Q.[2]; Walter R. Marzal M.[3]; Luis C. Rada M.[4]
[1,3]Universidad Tecnológica del Perú, Perú, *c.a.flores8@hotmail.com*, *C22314@utp.edu.pe*
[2,4]Universidad Tecnológica del Perú, Perú, *david.yq.3014@gmail.com, C18380@utp.edu.pe*

Abstract — **This Systematic Literature Review (SLR) aimed to analyze the applications of machine learning (ML) in the security of the Industrial Internet of Things (IIoT), identifying current advances, challenges and gaps. To structure the research questions, the PICO methodology was first used, which allowed the review to be oriented towards risks, applied strategies, comparisons with traditional methods and improvements achieved. Subsequently, the PRISMA protocol was applied for the process of selection and refinement of studies, obtaining a total of 31 scientific articles from the Scopus and Web of Science. The results show that ML has significantly improved the detection of threats such as ransomware, zero-day attacks and APTs, outperforming traditional strategies in accuracy, adaptability and efficiency. Strategies such as neural networks, federated learning, hybrid models and edge architectures were identified. However, limitations such as poor validation in real environments, lack of interpretability and vulnerability to adversarial attacks persist. In conclusion, ML represents a key advance in the protection of IIoT infrastructures, although further applied research, development of explainable solutions and adoption of common standards are required to strengthen its effective implementation.**

Keywords—Network Security, Industrial Internet of Things (IIoT), Machine Learning, Threat Detection and Access Control, Cybersecurity.

I. Introduction

Digital transformation in industry has promoted the large-scale adoption of the Industrial Internet of Things (IIoT), enabling unprecedented connectivity between devices, sensors, and distributed control systems. This transformation has brought significant benefits in terms of operational efficiency, real-time monitoring, and predictive maintenance. However, it has also significantly increased the attack surface, leaving industrial environments vulnerable to increasingly sophisticated cyber threats [1]. In response to the challenges posed by the complexity and variety of these contexts, machine learning (ML) based strategies have emerged as promising solutions for early intrusion detection, anomaly classification, and attack mitigation [2], [3]. Specifically, models such as decision trees, Random Forest, XGBoost, and deep neural networks have achieved accuracy levels above 99% in simulated and real-world situations [1], [2].

Currently, techniques such as deep learning, ensemble learning, and combined tools have been shown to promote the formation of robust and versatile defense systems, even against adversarial attacks or data poisoning [4], [5], [6]. However, these advances face considerable limitations due to the low computing power and low energy consumption required by IIoT devices, as well as challenges in scalability and model interpretation [7], [8].

Despite advances in the creation of smart devices for security in IIoT contexts, significant gaps remain in their effective implementation. Although most of the suggested models achieve high accuracy in controlled environments, they often fail when deployed in real-world situations due to computational limitations, unbalanced data, and advanced attacks that modify the expected behavior of systems [6], [8]. Currently, IIoT cybersecurity solutions do not have a unified architecture that facilitates the timely, flexible, and energy-efficient identification of threats. Similarly, many models do not adequately account for attacks targeting the training process, such as data poisoning, which can compromise system integrity [9], [10]. This discrepancy between expected performance and actual behavior limits the security of industrial organizations when it comes to fully adopting ML based solutions.

Given this situation, it is essential to further research robust and flexible ML strategies that not only achieve high detection rates but are also compatible with the limitations of the IIoT environment. Progress must be made toward solutions that combine accuracy, resilience, computational efficiency, and ease of maintenance, with the goal of ensuring constant and reliable defense in these essential systems [3], [5], [9], [10]. It should be noted that the latest research on ML-based security strategies for IIoT environments points to the need to continue developing and evaluating security strategies, especially those based on ML, to address emerging vulnerabilities in IIoT environments [11].

Further research on ML techniques is also needed to improve real-time intrusion detection and address the specific challenges of industrial IoT environments [12]. Similarly, gaps in current security measures remain, suggesting the need to develop new strategies, including those based on ML, to improve the security posture of IIoT systems [13]. In this regard, the research question of this RSL is: What are the applications of ML in IIoT security that identify current advances, challenges, and gaps? For this reason, there is an urgent need to conduct and discuss a new RSL that updates trends in new strategies that minimize security risks in the IIoT.

Considering this situation, the present RSL aims to analyze the current applications of ML in IIoT security. It should be noted that this review article is divided into five sections, namely: a) the methodology section, which explains the systematic development of this review; b) the results section, which presents the key findings, including the performance of various hybrid strategies; c) the discussion section, which contrasts the use of ML with traditional methods, highlighting strengths, limitations, and challenges in its real-world application in IIoT environments, d) the conclusions section, which summarizes the main results and future research, and, finally, the references section, which details the articles discussed in this study.

II. METHODOLOGY

A. Study

Table 1 shows the application of the PICO methodology [14], used to structure in a clear, logical and focused way the search for relevant information on ML-based security strategies in IIoT environments. This methodology facilitated the formulation of concise and well-defined research questions, focused on critical aspects such as the security risks present in IIoT systems, the application of ML techniques for threat detection and mitigation, the comparison between traditional solutions and those based on artificial intelligence, as well as the benefits achieved in terms of accuracy, adaptability and responsiveness to cybersecurity incidents.

In addition, specific search equations were developed for each component of the PICO (Population, Intervention, Comparison and Outcome) scheme, using Boolean operators (“AND”, “OR”) and a selection of key terms such as “industrial”, “internet of things ", " vulnerability ", " Machine Learning " and " threat detection ”. This structured search strategy enabled more precise information retrieval, focusing on studies highly relevant to the research objectives. By properly delimiting the terms and relationships between concepts, the identification of relevant scientific literature was optimized, and the quality of the systematic review process was strengthened, providing a solid foundation for the analysis of security strategies in IIoT environments.

TABLE I.
PICO METHOD

Component	Motivation	Question	Search Equation
P (Population / Problem)	Security in the context of the Internet of Things (IoT) in industrial environments.	What security risks have been identified using ML in industrial IoT environments ?	(“industrial" OR "manufacturing" OR "production" OR "factory “) AND (" IoT" OR "internet of things" OR "connected devices" OR "smart devices “) AND (" risk*" OR "threat*" OR "vulnerability* “)
I (Intervention)	Application of ML techniques in IIoT threat detection and protection mechanisms.	What ML-based security strategies have been implemented to strengthen the security of industrial IoT devices?	(“Machine Learning " OR "ml" OR "algorithm" OR "artificial intelligence" OR "deep learning “) AND (" data analysis" OR "anomaly detection" OR "monitoring" OR "risk assessment “)
C (Comparison)	Traditional security strategies and those based on ML in the context of IIoT.	How does the use of ML compare to traditional security methods in industrial IoT environments ?	(“strategy" OR "approach" OR "method" OR "framework “) AND (“protection" OR "security" OR "safety" OR "risk management")
O (Result)	Increased capacity to detect, respond to, and adapt to threats.	What improvements have been identified through the application of ML in the protection of industrial IoT-based infrastructures?	(“vulnerability*" OR "threat detection" OR "attack detection" OR "risk mitigation" OR "security “)

B. Prisma Protocol

To ensure the methodological rigor, thematic coherence, and scientific relevance of the studies included in this SLR, clearly defined inclusion and exclusion criteria were established, which are detailed in Table 2. These criteria were designed to precisely delimit the analysis corpus, selecting only research that explicitly addressed the application of ML techniques in cybersecurity in IIoT environments, within a specific temporal, disciplinary, and methodological framework. The application of this filtering process made it possible to minimize potential selection biases, ensure alignment with the research objectives, and focus the analysis on empirically validated, up-to-date studies with a high academic impact. Overall, this strategy contributes to optimizing the quality of the review and strengthening the internal validity of the results obtained.

TABLE II.
INCLUSION AND EXCLUSION CRITERIA

INCLUSION CRITERIA	EXCLUSION CRITERIA
IC1: Articles should address the use of ML applied to the security of IoT devices in industrial environments	**EC1:** Term 2021-2025 **EC2:** Engineering **EC3:** Original and conference papers **EC4:** Languages English and Spanish **EC5:** Open Access **EC6:** Unrelated Titles **EC7:** Systematic Reviews **EC8:** Unrelated Abstracts **EC9:** Inaccessible Articles
IC2: Research articles indexed in Scopus or Web of Science (WOS)	
IC3: Studies that present empirical results or practical validations of ML techniques applied to security in IIoT devices.	

Figure 1 illustrates the flowchart of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [1]. Its incorporation aims to ensure methodological transparency, accurately document each phase, from the initial identification of records to final inclusion, and provide a traceable justification for the decisions made during screening. The main purpose of this flowchart is to clearly and transparently visualize the stages of the study selection process, from the initial identification of articles to their final inclusion. This flowchart demonstrates the decisions made at each stage of screening and also justifies the exclusion of certain documents, ensuring the rigor, traceability, and reproducibility of the review process. It also visualizes the scope of the search, the purification of sources, and the consistency of the eligibility criteria applied, which are key aspects for the credibility and robustness of the findings presented in this SLR.

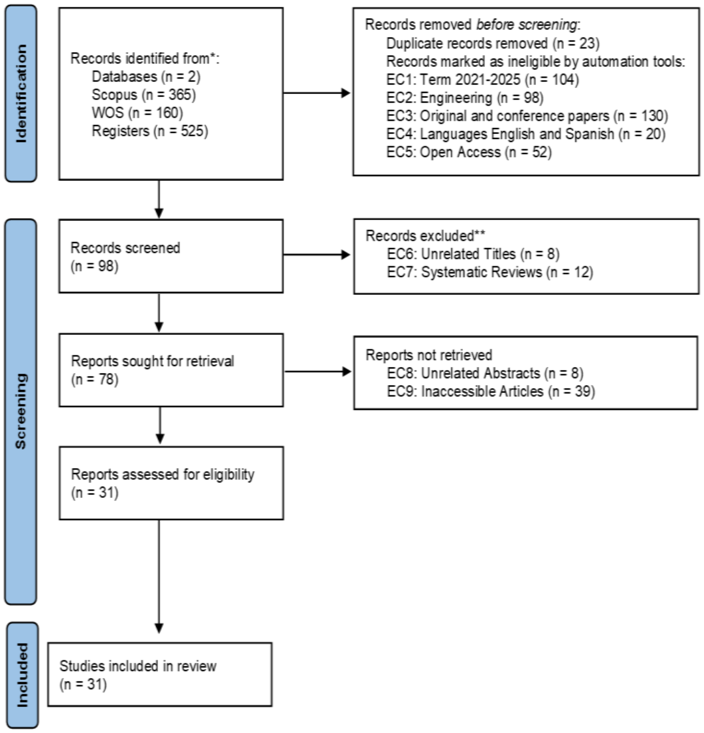
Identification
Records identified from*:
Databases (n = 2)
Scopus (n = 365)
WOS (n = 160)
Registers (n = 525)
Records removed *before screening*:
Duplicate records removed (n = 23)
Records marked as ineligible by automation tools:
EC1: Term 2021-2025 (n = 104)
EC2: Engineering (n = 98)
EC3: Original and conference papers (n = 130)
EC4: Languages English and Spanish (n = 20)
EC5: Open Access (n = 52)
Screening
Records screened
(n = 98)
Records excluded**
EC6: Unrelated Titles (n = 8)
EC7: Systematic Reviews (n = 12)
Reports sought for retrieval
(n = 78)
Reports not retrieved
EC8: Unrelated Abstracts (n = 8)
EC9: Inaccessible Articles (n = 39)
Reports assessed for eligibility
(n = 31)
Included
Studies included in review
(n = 31)

Fig. 1. PRISMA flowchart

Figure 2 presents the temporal evolution of scientific production related to the use of ML in the security of the IIoT. This visualization allows us to observe how the volume of publications has changed in recent years, which in turn reflects the growing interest of the academic community in this field. Through a chronological representation, it is possible to identify patterns of increase or stability in the number of research studies, which indicates the level of maturity and attention that this topic has received. Furthermore, this figure provides a quantitative basis that supports the validity of the present study, since it shows that the use of ML techniques in the protection of IIoT systems is not only a current topic, but also an expanding one. The sustained increase in the number of publications demonstrates that this field continues to generate research questions, emerging solutions, and application opportunities in real industrial contexts.

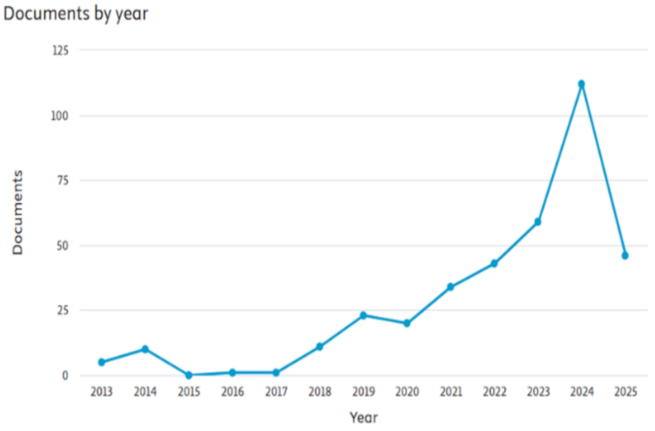

Fig. 2. Research Articles per year

The initial breakdown of the collected articles, shown in Figure 3, from the Scopus and Web of Science plays a critical role in the systematic review process, allowing for the assessment of the breadth, diversity, and balance of scholarly source selection. This segmentation not only provides a quantitative estimate of the volume of scientific literature available on the use of ML in IIoT security but also acts as a check to ensure that results are not influenced by an overreliance on a single source. Considering the complementarity of both platforms strengthens the study's methodological validity, favoring a more representative coverage of the current state of research in the field addressed.

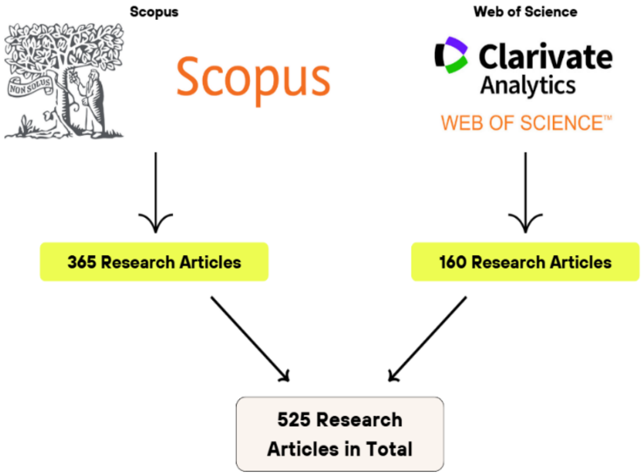

Fig. 3. Total Research Articles Collected

III. Results

A. *Bibliometric Analysis*

The studies compiled within the framework of this SLR have enabled the extraction and analysis of key metadata, providing a broad overview of the interrelationships of the main topics addressed in the field of study. As part of the semantic analysis of the reviewed literature, a co-occurrence map was developed, demonstrating the cognitive structure of the field of study around security in IIoT environments using ML. Figure 4 visualizes the most relevant associations between key concepts, revealing well-defined thematic clusters such as anomaly detection, federated learning, industrial control systems, and cybersecurity.

Its importance lies not only in showing the frequency of terms, but also in highlighting how they interact within scientific discourse, facilitating the identification of dominant areas, emerging links, and potential research gaps. This type of analysis is crucial to empirically support the methodological and theoretical decisions of this systematic review and more precisely guides future interdisciplinary lines of research. In this context, the figure provides empirical support for the direction of the analysis, reinforcing the identification of gaps, interdisciplinary challenges, and potential avenues for future research in the application of ML for the protection of critical industrial infrastructures.

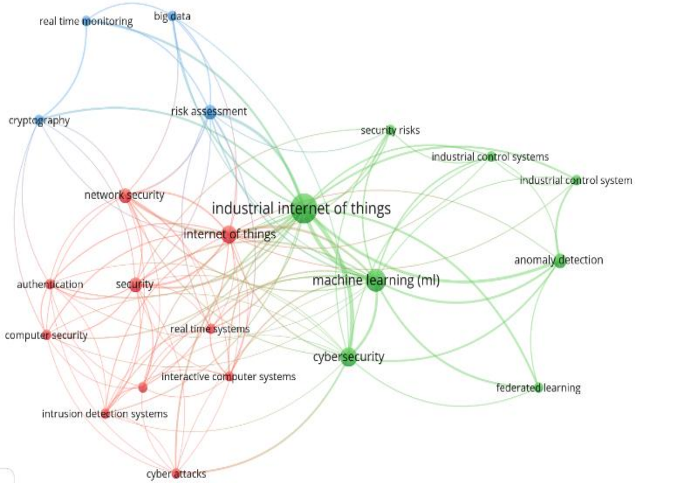

Fig. 4. Co-occurrence diagram of the study selection process for review.

This highlights the central themes of the research, such as Industrial Internet of Things, Machine Learning, and cybersecurity, which are frequently addressed. It also allows us to identify how these terms cluster into interrelated thematic communities.

In addition, a Treemap visualization was created to identify the relative frequency and thematic relevance of the most frequently discussed concepts in the scientific literature on security in the IIoT using ML techniques, as represented in Figure 5. This hierarchical representation helps to clarify the dominant semantic structure of the reviewed studies, revealing patterns of thematic concentration that allow us to infer the priorities of the field. By visualizing the relative weight of certain concepts, it is possible to identify how research agendas have favored strategies focused on IIoT and ML, while terms linked to emerging technologies or specific techniques maintain a more fragmented presence. This configuration suggests not only the consolidated lines of research, but also the theoretical and practical gaps that still require greater attention, especially regarding interoperability, protection in distributed environments, and risk assessment in complex industrial contexts. Thus, this analysis is not limited to quantifying terms but rather guides critical reflection on the current state and projections of cybersecurity applied to the IIoT.

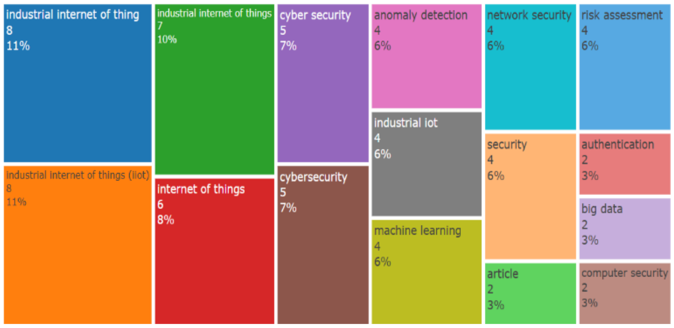

Fig. 5. Treemap diagram on the thematic relevance of the review.

B. *Content analysis*

After conducting a general review of the articles collected for analysis, they will be used to answer the PICO questions posed.

P: Security risks used in ML in industrial IoT environments

The use of ML in IIoT environments has made it possible to identify multiple security risks that exceed the capabilities of traditional methods. Among the most relevant are ransomware attacks, zero-day threats, APTs and physical sabotage, which affect both data integrity and operational continuity and physical security of infrastructures [2], [3], [4], [5], [6], [7]. Various publications [4], [8], [9] warn about the use of IIoT devices as attack vectors, exploiting vulnerabilities such as outdated firmware, default passwords and weak communication protocols (Modbus, MQTT). These weaknesses are exploited by attackers to carry out actions such as data manipulation, generation of persistent backdoors or serious operational interruptions.

In the field of ML itself, emerging risks are identified such as model poisoning, label-flipping attacks, parameter leakage in federated learning and adversarial attacks that degrade system performance or compromise data privacy [10], [11], [12]. Likewise, the heterogeneity and large volume of data generated by industrial sensors can make it difficult to detect faults or cyberattacks, especially in the absence of intelligent real-time analysis mechanisms. Risks such as data falsification, supply chain manipulation and unauthorized access are common in critical sectors such as agri-food, healthcare, energy or transport [13], [14], [15], [16], [17].

Finally, it is highlighted that traditional strategies based on predefined signatures or rules are insufficient against these dynamic threats, generating numerous false positives or failures in the detection of unknown attacks [18], [19], [20], [21]. This reinforces the need to adopt adaptive ML-based strategies that identify anomalous patterns, prevent complex intrusions, and strengthen the resilience of industrial infrastructures.

The classification presented in Table 3 organizes the most relevant security risks identified in IIoT environments that have been addressed using ML techniques, grouping them according to their technical or strategic nature. Beyond the threats considered individually, the analysis highlights three key dimensions that concentrate the sector's main concerns: persistent structural vulnerabilities, increasingly sophisticated attacks, and challenges associated with the management and protection of sensitive data.

This scenario demonstrates that, despite technological advances in artificial intelligence linked to cybersecurity, critical gaps persist in terms of infrastructure and data governance. The consistent presentation of certain risks underscores the importance of defense strategies that are not only accurate but also flexible in changing, diverse contexts with operational constraints. This information is essential for guiding the creation of more robust intelligent solutions aligned with the industry's real challenges.

TABLE III.
MAIN SECURITY RISKS IDENTIFIED

TYPE OF RISK	DESCRIPTION	FREQUENCY
Technical and structural vulnerabilities	Use of default passwords, outdated software, insecure protocols such as Modbus or MQTT, and devices with limited resources that don't support traditional security measures.	4
Expanded attack surface through massive connectivity	Massive connectivity, public networks and heterogeneous environments allow attacks such as DoS, DDoS, replay, hijacking and MiTM .	4
Sophisticated and zero-day attacks	Hard-to-detect threats using signatures such as zero-day attacks, APTs, ransomware, command injection, and targeted sabotage.	4
Model manipulation in federated learning	Gradient leakage, label-flipping and malicious nodes (Byzantines) that alter model training or leak sensitive information.	3
Privacy and sensitive data compromised	Leakage or interception of critical data, especially in sectors such as healthcare, transportation, or energy. Exposure of personal data or critical infrastructure.	4
Limitations in data quality	Noisy, unbalanced, unlabeled, and heterogeneous data reduce ML accuracy, generating false positives or detection failures.	3
Failures in anomaly detection	If anomalies are not detected correctly, they can lead to industrial failures, erroneous decisions, or sabotage.	4
Cloud dependency and critical latency	In cloud-based CNN applications, risks of latency, insufficient bandwidth, and sensitive data transmission are identified.	2
Lack of certification and standards	Introduction of technologies without security validation, use of legacy systems exposed to attacks because they are connected to external networks.	2

I: Machine Learning based security strategies implemented to strengthen the security of industrial IoT devices

Various ML-based security strategies have been implemented in industrial IoT environments to address emerging and complex threats. These strategies integrate deep, federated, and supervised learning techniques, as well as hybrid models and intelligent architectures embedded at the edge. One of the most notable solutions is the CCSOA-OWKELM system, which combines chaotic optimization algorithms with wavelet-based classifiers, enabling accurate intrusion detection at low computational cost [21]. Hybrid models such as DNNs combined with autoencoders and decision trees have also been implemented, effectively identifying attacks in unbalanced datasets [8].

Federated learning with differential privacy has been employed to protect data confidentiality in heterogeneous IIoT networks, complemented by cloud detection to identify malicious nodes [10], [12]. In mission-critical systems, LSTM neural networks are used to detect anomalies in traffic patterns or physical signals, even without requiring labeled data or manual intervention [3], [5].

In addition, structured strategies such as directed acyclic graphs (DAGs) have been adopted to model and prioritize attack paths, enabling proactive defense through topological analysis [22]. Models such as SAMKNN and GAAINet demonstrate adaptive capabilities for online classification and sophisticated intrusion response [19], [23]. Other strategies employ techniques such as Gradient Boosting Machine and Lasso Regression to select relevant features and improve detection accuracy, especially in embedded systems like Zephyr OS [2], or frameworks like PBDL that integrate blockchain and deep learning to authenticate devices and detect complex attacks [24].

Likewise, ML has been integrated into edge architectures, such as ABM- SpConv -SIMD and IIoL , which allow inferences to be run directly on devices, eliminating cloud dependency and reducing latency and exposure [25]. [26]Also, a functional categorization of ML-based security tactics applied in IIoT environments is shown (as in Table 4). This systematization facilitates the identification of the different objectives for which ML techniques have been used, as well as their correspondence with the particular protection demands in interrelated industrial systems.

The study shows a notable bias toward identifying irregularities and cyberattacks as a priority, with a wide range of models used, including deep neural networks, autoencoders, and sequential algorithms. However, significant applications are also recognized in fields such as authentication, privacy protection through federated learning, operational error anticipation, and structural-scale model improvement.

Similarly, there is an increase in the inclusion of complementary technologies, such as blockchain, remote computing, specialized systems, and sophisticated simulations, demonstrating a trend toward more integrated and context-specific solutions. This categorization provides a comprehensive view of the level of maturity and innovation present in current strategies and becomes a valuable framework for identifying potential synergies, gaps, or emerging paths in the creation of cybersecurity solutions for the IIoT.

TABLE IV.
CLASSIFYING SECURITY STRATEGIES WITH ML IN IIOT

Strategy Category	Applied ML Strategy	Main objective	Frequency
Anomaly and cyberattack detection	LSTM, RF, DBN, CNN, SAMKNN, Autoencoders, SACNN	Identification of malicious/anomalous patterns	8
Intrusion Detection System (IDS)	IF + PCC + Ensemble, decision trees, MLP	Binary classification of intrusions	3
Authentication and access control	Biometric matching, blockchain + DL	Identity verification, secure access	2
Federated learning and privacy	FL with ALDP, TSA-FL, homomorphic encryption	Preserve privacy, protect distributed model	3
Prediction of risks and operational failures	Time prediction with DL, linear regression	Predictive maintenance, threat prediction	2
Model optimization and improvement	Gradient Boosting, Lasso, Shapley + genetics	Feature selection, ML efficiency	2
Routing and resource management	EDM-ML, game theory + wolf colony	Resource allocation, network trust	2
Integrated intelligent architectures	DNN + trees + attack attribution	Multi-level classification and attack attribution	1
Secure execution infrastructure	ABM- SpConv - SIMD, IIoL framework	Secure inference at the edge, reduced latency	2
Hybrid and adaptive expert systems	ML + rules, RL, hybrid expert systems	Continuous monitoring and adaptive response	2

C: Effects of using ML compared to traditional security methods in industrial IoT environments

The reviewed literature shows that ML-based strategies significantly outperform traditional methods in various critical aspects of security in IIoT environments. Classic techniques, such as signature-based systems or static rules, present significant limitations in the face of advanced threats, zero-day attacks, and dynamic environments, since they depend on previously known patterns and require constant manual updates [10], [5], [8].

In contrast, ML models offer proactive detection, adaptability to new threats, and a greater ability to identify complex anomalous patterns. In particular, strategies such as LSTM neural networks, SACNNs, and hybrid architectures based on DNNs, autoencoders, or Random Forests have been shown to outperform traditional techniques in accuracy, speed, and false positive rate [3]. [27]Furthermore [20], [16]the use of algorithms such as Gradient Boosting Machine, Lasso Regression or encrypted federated models allow maintaining data privacy, scaling analysis to large volumes and offering more resilient solutions [10], [14], [12].

In order to visually and comparatively synthesize the performance of traditional security strategies versus those based on ML, a radar-type chart has been developed that integrates multiple key dimensions associated with the protection of interconnected industrial environments. The values used in Figure 6 derive from a quantitative and qualitative analysis of the empirical evidence presented in the reviewed studies. In this sense, ML-based solutions consistently show superior performance in all the evaluated metrics. For example, the average accuracy in threat detection with ML is close to 97%, while traditional methods barely reach 75%, according to the results reported in [2], [9], [19], [28]. Likewise, a significant difference is observed in the ability to adapt to unknown threats, where ML achieves 94% versus 60% for classical methods, highlighting its ability to address non-predefined scenarios through continuous learning mechanisms [11], [16].

In terms of privacy protection, metrics such as federated learning with differential encryption or the use of frameworks like blockchain -DL demonstrate considerable improvements over traditional centralized techniques, reaching 92% effectiveness, as evidenced in [4], [12], [29]. Other dimensions, such as computational efficiency and scalability, also reflect substantial benefits from the use of optimized ML models [30].

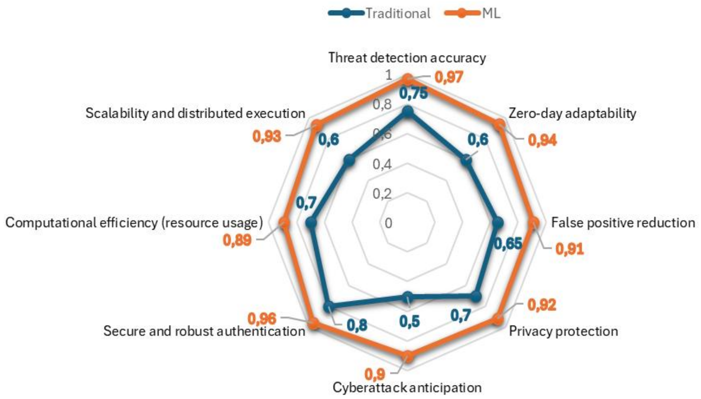

Fig. 6. Relative performance of traditional and ML-based strategies in IIoT.

Other methods, such as integrating game theory, blockchain , edge Computing or inference on edge devices using SIMD, as well as authentication and cryptographic protection mechanisms based on physical and environmental characteristics, have been shown to significantly improve operational efficiency and reduce data exposure by eliminating dependence on the cloud [31], [29], [25], [26]. These solutions not only increase the accuracy of threat detection, but also reduce latency, energy consumption and computational complexity [17], [19], [25].

The representation shown in Figure 7 summarizes the most relevant benefits provided by the use of ML techniques compared to traditional security methods employed in IIoT environments. Beyond a simple quantification, the study reveals that the differential value of ML is most strongly manifested in its ability to detect unknown threats, reduce false positives, and adapt to dynamic operating environments—essential characteristics in complex and highly variable industrial systems.

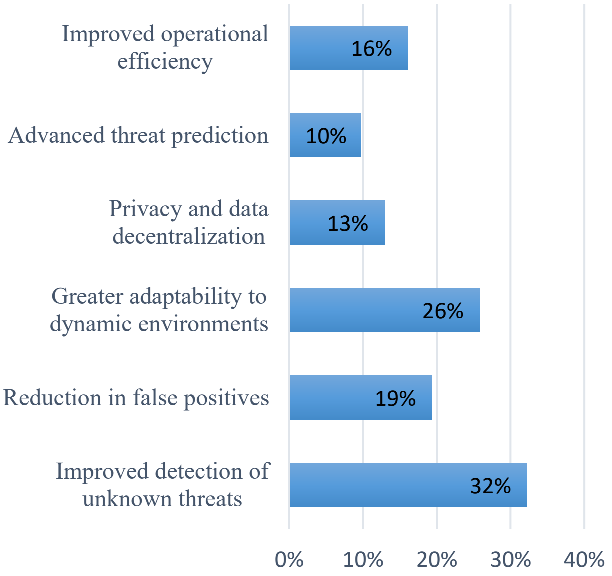

Fig. 7. Influence of ML versus traditional methods in IIoT environments

This finding demonstrates the scientific community's growing inclination toward proactive and adaptive solutions that not only respond to known events but can also anticipate irregular behavior in real time, even if it has not been previously identified or documented. Similarly, the identification of additional benefits such as increased operational efficiency and decentralized data management indicates a shift toward more holistic perspectives, in which security is perceived as an essential component of the IIoT 's intelligent architecture.

It is worth noting that the analyzed sources not only present a solid consensus regarding the superiority of ML over traditional methods but also show significant evolution in the sophistication of the proposed solutions. For example, [10]it shows that models such as Gradient Boosting Machine and Lasso Regression not only increase detection accuracy but also achieve better adaptation to new ransomware variants, greatly overcoming the rigidity of signature-based methods. Furthermore, works such as [3] and [13] emphasize how the incorporation of LSTM models and multivariate strategies allow for the dynamic analysis of industrial data streams, something that conventional strategies with static thresholds cannot effectively handle. Other sources, such as [4] and [14], show the value of graph-based modeling and the use of ML to mitigate uncertainty, representing a methodological transition toward more autonomous, accurate, and resilient systems.

O: Improvements identified through the application of ML in the protection of industrial IoT- based infrastructures

The studies analyzed show a sustained evolution in the improvements implemented through ML to protect IIoT infrastructures, highlighting progress in efficiency, accuracy, and adaptability. One of the most relevant improvements has been the ability to detect attacks early and accurately, as demonstrated by [2], by detecting ransomware with 92% effectiveness, and [20], by identifying multivariate botnet attacks with 99.94% accuracy. These figures have been accompanied by notable reductions in false positives and an improvement in response speed [19], [8]. Another greatly improved aspect is computational efficiency, which has allowed models to be implemented on devices with limited resources, without compromising their performance. In this sense, improvements in local data processing are reported, such as in edge environments, where inference times and latency are reduced [25], as well as energy consumption and operational costs [6], [28]. The reduction of false positives and negatives is also a constant improvement, facilitating a more precise and timely response to potential threats.

Figure 8 consolidates the main achievements reported in the scientific literature over time as a result of the implementation of ML algorithms in IIoT environments. The improvements have been classified into ten functional categories, ranging from accurate threat detection and strong authentication to computational efficiency and operational resilience of the systems.

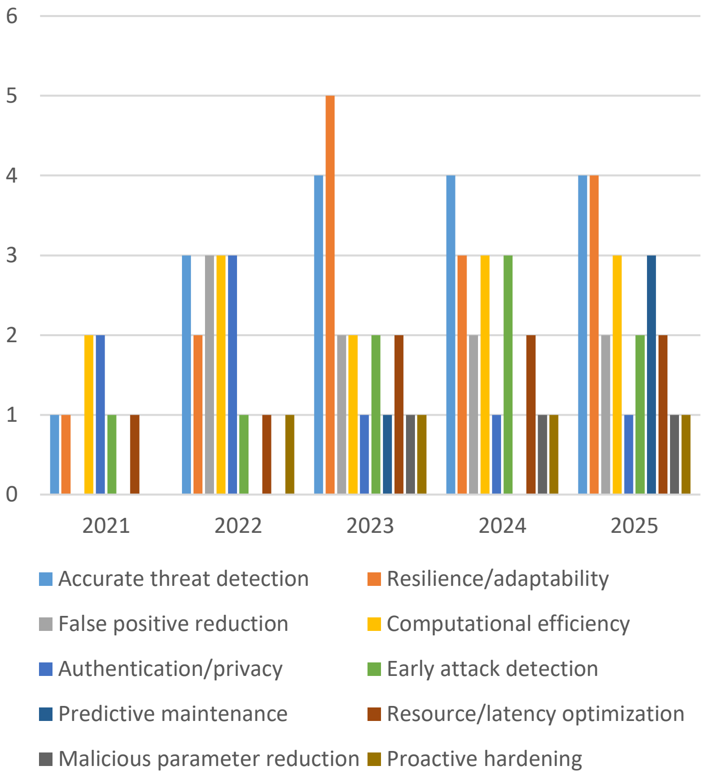

Fig. 8. Improvements identified through ML over time.

Beyond the annual count, the graph shows a sustained evolution in the breadth and specificity of the benefits achieved, with a notable increase in the years 2023, 2024 and 2025. This behavior suggests an acceleration in the technological maturity of the field and a growing prioritization of the use of intelligent techniques to face emerging challenges in industrial cybersecurity. Studies provide models that combine techniques such as correlation analysis, advanced normalization or hybrid architectures have managed to stabilize detection, adjusting to changing and dynamic environments [3], [17], [19]. On the other hand, from the point of view of resilience and adaptability, intelligent systems have improved the capacity for recovery and continuous protection, including mechanisms for autonomous detection, threat prediction and proactive risk management [18], [12], [23]. This includes improvements in the protection of sensitive data through biometric authentication, blockchain or federated learning [32], [24], [10], [12]. In critical sectors such as healthcare, energy and manufacturing, improvements have also been observed in operational stability, event traceability and predictive monitoring, key factors for service continuity and the prevention of catastrophic failures [14], [26], [15].

IV. Discussion

This systematic review confirms that the use of ML techniques in IIoT environments constitutes a relevant advance with respect to traditional security methods. One of the most notable findings is the clear disadvantage that conventional tools, such as signature-based systems, static rules or whitelists, present against dynamic and sophisticated threats, such as zero-day attacks, APTs (Advanced Persistent Threats) and modern ransomware variants. These traditional methods depend on previously known patterns and require constant manual updates, which makes them ineffective against unexpected behavior [24], [19], [22]. In contrast, ML-based models, particularly those using architectures such as LSTM, SACNN or Random Forest, have demonstrated a greater capacity to detect anomalous patterns, adapt to changing industrial environments and significantly reduce the false positive rate [17], [30], [34], [40]. Such models are not only more sensitive to subtle attack signals but can also learn and evolve as new threats emerge. However, model calibration and explainability remain inconsistent; attaching calibrated confidence scores and feature-level attributions to alerts is key for operator trust and auditability in Industrial Control Systems (ICS) environments.

Additionally, the incorporation of strategies such as federated learning and edge Computing has strengthened critical aspects such as data privacy and operational efficiency by enabling local processing of information and minimizing cloud dependency [24], [26], [38], [43]. However, these advances are not without risks. There are emerging vulnerabilities associated with the use of ML itself, such as model poisoning attacks, training manipulation in distributed environments, and the leakage of sensitive parameters. Mitigations like secure aggregation, client reputation/robust aggregation, signed model artifacts, and provenance tracking help, but they must operate within strict production controls that cover training data, artifacts, and deployments. These technical challenges have not yet been comprehensively solved by current solutions, highlighting the need to develop more robust protection mechanisms, especially in federated and self-training systems [25], [26].

While some studies report highly promising results, with accuracy rates above 99% in detecting threats such as botnet attacks or ransomware [46], [34], [31], it is important to note that most of these results come from controlled or simulated environments. This represents a major limitation for their practical implementation, since real industrial environments usually present much more complex conditions: unbalanced data, incomplete information, operational noise, and computational constraints. Consequently, evaluations should prioritize imbalance-aware metrics (PR, F1, AUCPR, MCC) over raw accuracy, and report latency, processing rate, and energy per inference alongside detection quality. Furthermore, notable heterogeneity was detected among the reviewed studies in terms of the metrics used, the datasets employed, and the validation methodologies, which makes direct comparison between strategies and the generalization of results difficult. This lack of uniformity also reflects the absence of consolidated standards in the evaluation of ML-based security strategies for IIoT. Therefore, it is recommended that future research prioritize the validation of models in real industrial environments, where their performance is evaluated under authentic operating conditions. Likewise, it is crucial to advance the design of more interpretable solutions for system users and operators, and to promote the use of standardized metrics that allow for objective comparisons of the effectiveness and robustness of the various proposed strategies.

V. Conclusions

In conclusion, various applications of ML in IIoT security were identified, highlighting its ability to detect complex threats, adapt to changing environments, and reduce false positives, aspects in which it significantly outperforms traditional methods. A review of the studies shows progressive progress in the implementation of techniques such as LSTM, federated learning, and mixture models, along with a trend toward combined and contextualized solutions for industrial environments.

Persistent challenges were also found, such as low model interpretability, vulnerability to adversarial attacks, and poor algorithm validation in real-world scenarios, factors that limit the effectiveness of these strategies in operational contexts. Despite improvements in computational efficiency and privacy, these obstacles reflect that the use of ML in IIoT still faces significant gaps in its robust and reliable implementation.

With such significant results, it is necessary to continue developing research that includes validations in real industrial environments, with noisy data and realistic operating conditions. This will allow for more accurate measurement of the effectiveness of the proposed models and facilitate their practical adaptation. Furthermore, it is recommended to advance the design of explainable and resilient models capable of operating on devices with limited resources, and to promote common standards that allow for a homogeneous evaluation of approaches. Only in this way will sustainable and effective security solutions be consolidated for the growing IIoT ecosystem.

References

[1] R. Ch, S. Nimmala, I. Batra, and A. Malik, “A Comparative Study of ML Techniques for Threat Detection and Enhancing Security in Industrial IoT,” 2025, ch. 4, pp. 295–310. doi :10.4018/979-8-3693-6135-1.ch011.

[2] T. Zhukabayeva , Z. Ahmad, N. Karabayev , D. Baumuratova , and M. Ali, “An Intrusion Detection System for Multiclass Classification Across Multiple Datasets in Industrial IoT Using ML and Neural Networks Integrated with Edge Computing,” 2025. doi : 10.3233/ATDE250012.

[3] K. Hassini and M. Lazaar, "Enhancing Industrial-IoT Cybersecurity Through Generative Models and Convolutional Neural Networks," 2024, pp. 543–558. doi :10.1007/978-3-031-74491-4_41.

[4] R. Golchha , A. Joshi, and GP Gupta, "Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things," *Procedia Comput Sci* , vol. 218, pp. 1752–1759, 2023, doi : 10.1016/j.procs.2023.01.153.

[5] O. Gungor, T. Rosing, and B. Aksanli , "STEWART: STacking Ensemble for White-Box AdversaRial Attacks Towards more resilient data-driven predictive maintenance," *Comput Ind* , vol. 140, p. 103660, Sep. 2022, doi : 10.1016/j.compind.2022.103660.

[6] N. Baracaldo, B. Chen, H. Ludwig, A. Safavi, and R. Zhang, "Detecting Poisoning Attacks on ML in IoT Environments," in *2018 IEEE International Congress on Internet of Things (ICIOT)* , IEEE, Jul. 2018, pp. 57–64. doi : 10.1109/ICIOT.2018.00015.

[7] AS Lalos, AP Kalogeras, C. Koulamas , C. Tselios, C. Alexakos, and D. Serpanos , "Secure and Safe IIoT Systems via Machine and Deep Learning Approaches," in *Security and Quality in Cyber-Physical Systems Engineering* , Cham: Springer International Publishing, 2019, pp. 443–470. doi :10.1007/978-3-030-25312-7_16.

[8] KK Wankhade, S. Dongre, R. Chandra, KV Krishnan, and S. Arasavilli , "ML-Based Detection of Attacks and Anomalies in IIoT(IIoT) Networks," 2024, pp. 91–109. doi :10.1007/978-981-97-2004-0_7.

[9] D. Hamouda, MA Ferrag , N. Benhamida, and H. Seridi , "Intrusion Detection Systems for Industrial Internet of Things: A Survey," in *2021 International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS)* , IEEE, Dec. 2021, pp. 1–8. doi : 10.1109/ICTAACS53298.2021.9715177.

[10] Kapil Keshao Wankhade, "Mathematical Approach towards Adaptive ML Models for Dynamic Security Threats in Industrial IoT," *Advances in Nonlinear Variational Inequalities* , vol. 27, no. 3, pp. 80–101, Aug. 2024, doi : 10.52783/ anvi.v 27.1359.

[11] AA Oliva Olazábal , C. Llanos, F. Alarcón, and C. León-Velarde, "Cybersecurity for the Protection of IOT Devices in the Industrial Sector," in *Proceedings of the 22nd LACCEI International Multi-Conference for Engineering, Education and Technology: "Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0.,"* Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi : 10.18687/LACCEI2024.1.1.1206.

[12] F. Alwahedi , A. Aldhaheri , M.A. Ferrag , A. Battah, and N. Tihanyi, "ML techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems* , vol. 4, pp. 167–185, 2024, doi : 10.1016/j.iotcps.2023.12.003.

[13] AA Alli, K. Kalinaki , M. Fahadi , and L. Ibrahim, "Securing IIoT(IIoT)," in *Artificial Intelligence Solutions for Cyber-Physical Systems* , Boca Raton: Auerbach Publications, 2024, pp. 244–263. doi :10.1201/9781032694375-14.

[14] B. Kitchenham, O. Pearl Brereton, D. Budgen , M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Inf Softw Technol* , vol. 51, no. 1, pp. 7–15, Jan. 2009, doi : 10.1016/j.infsof.2008.09.009.

[15] MJ Page *et al.* , "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ* , p. n71, Mar. 2021, doi : 10.1136/ bmj.n 71.

[16] U. Tariq, "Combatting ransomware in ZephyrOS -enabled industrial IoT environments," *Heliyon* , vol. 10, no. 9, p. e29917, May 2024, doi : 10.1016/j.heliyon.2024.e 29917.

[17] J. Kim, J. Shin, K.-W. Park, and J. Taek Seo, "Improving Method of Anomaly Detection Performance for Industrial IoT Environment," *Computers, Materials & Continua* , vol. 72, no. 3, pp. 5377–5394, 2022, doi : 10.32604/cmc.2022.026619.

[18] F. Arat and S. Akleylek , "Modified graph-based algorithm to analyze security threats in IoT," *PeerJ Comput Sci* , vol. 9, p. e1743, Dec. 2023, doi : 10.7717/peerj-cs.1743.

[19] S. Kim *et al.* , "Two-Phase Industrial Control System Anomaly Detection Using Communication Patterns and Deep Learning," *Electronics (Basel)* , vol. 13, no. 8, p. 1520, Apr. 2024, doi : 10.3390/electronics13081520.

[20] P.R. Agbedanu , S.J. Yang, R. Musabe , I. Gatare , and J. Rwigema , "A Scalable Approach to Internet of Things and IIoTSecurity: Evaluating Adaptive Self-Adjusting Memory K-Nearest Neighbor for Zero-Day Attack Detection," *Sensors* , vol. 25, no. 1, p. 216, Jan. 2025, doi : 10.3390/s25010216.

[21] E. Seid, O. Popov, and F. Blix, "Towards Security Attack Event Monitoring for Cyber Physical-Systems," in *Proceedings of the 9th International Conference on Information Systems Security and Privacy* , SCITEPRESS - Science and Technology Publications, 2023, pp. 722–732. doi :10.5220/0011803400003405.

[22] C. Atheeq , R. Sultana, S.A. Sabahath , and MAK Mohammed, "Advancing IoT Cybersecurity: Adaptive Threat Identification with Deep Learning in Cyber-Physical Systems," *Engineering, Technology & Applied Science Research* , vol. 14, no. 2, pp. 13559–13566, Apr. 2024, doi : 10.48084/etasr.6969.

[23] G. Karacayılmaz and H. Artuner , "A novel detection approach for IIoT attacks via artificial intelligence," *Cluster Comput* , vol. 27, no. 8, pp. 10467–10485, Nov. 2024, doi : 10.1007/s10586-024-04529-w.

[24] SK Poorazad , C. Benzaïd , and T. Taleb, "A Novel Buffered Federated Learning Framework for Privacy-Driven Anomaly Detection in IIoT ," in *GLOBECOM 2024 - 2024 IEEE Global Communications Conference* , IEEE, Dec. 2024, pp. 1725–1730. doi :10.1109/GLOBECOM52923.2024.10901786.

[25] AK Takele and B. Villányi, "Two-Stage Aggregation based Federated Learning (TSA-FL) for Industrial Internet of Things," *Journal of Engineering Research* , Mar. 2025, doi : 10.1016/j.jer.2025.03.003.

[26] Y. Liu, R. Zhao, J. Kang, A. Yassine, D. Niyato , and J. Peng, "Towards Communication-Efficient and Attack-Resistant Federated Edge Learning for Industrial Internet of Things," *ACM Trans Internet Technol* , vol. 22, no. 3, pp. 1–22, Aug. 2022, doi : 10.1145/3453169.

[27] H.Gupta *et al.* , "Variance-driven security optimization in industrial IoT sensors," *IET Networks* , vol. 14, no. 1, Jan. 2025, doi : 10.1049/ntw2.12139.

[28] K. Haseeb, T. Saba, A. Rehman, I. Ahmed, and J. Lloret, "Efficient data uncertainty management for health IIoTusing ML," *International Journal of Communication Systems* , vol. 34, no. 16, Nov. 2021, doi : 10.1002/dac.4948.

[29] S. Halder, M. Rafiqul Islam, Q. Mamun, A. Mahboubi, P. Walsh, and M. Zahidul Islam, "A comprehensive survey on AI-enabled secure social IIoTin the agri-food supply chain," *Smart Agricultural Technology* , vol. 11, p. 100902, Aug. 2025, doi : 10.1016/j.atech.2025.100902.

[30] M. Al Qathrady *et al.* , "SACNN-IDS: A self-attention convolutional neural network for intrusion detection in industrial internet of things," *CAAI Trans Intell Technol* , vol. 9, no. 6, pp. 1398–1411, Dec. 2024, doi : 10.1049/cit2.12352.

[31] M. Ragab *et al.* , "Artificial intelligence driven cyberattack detection system using integration of deep belief network with convolution neural network on industrial IoT," *Alexandria Engineering Journal* , vol. 110, pp. 438–450, Jan. 2025, doi : 10.1016/j.aej.2024.10.009.

[32] A. Javed, M. Lakoju , P. Burnap, and O. Rana, "Security analytics for real-time forecasting of cyberattacks," *Softw Pract Exp* , vol. 52, no. 3, pp. 788–804, Mar. 2022, doi : 10.1002/spe.2822.

[33] A. Sezgin and A. Boyacı, "Enhancing Intrusion Detection in IIoTthrough Automated Preprocessing," *Advances in Science and Technology Research Journal* , vol. 17, no. 2, pp. 120–135, Apr. 2023, doi : 10.12913/22998624/162004.

[34] T. Hasan *et al.* , "Securing IIoTAgainst Botnet Attacks Using Hybrid Deep Learning Approach," *IEEE Trans Netw Sci Eng* , vol. 10, no. 5, pp. 2952–2963, Sep. 2023, doi : 10.1109/TNSE.2022.3168533.

[35] R. Gopi *et al.* , "Intelligent Intrusion Detection System for IIoTEnvironment," *Computer Systems Science and Engineering* , vol. 44, no. 2, pp. 1567–1582, 2023, doi : 10.32604/csse.2023.025216.

[36] SP Sithungu and EM Ehlers, " GAAINet : A Generative Adversarial Artificial Immune Network Model for Intrusion Detection in Industrial IoT Systems," *Journal of Advances in Information Technology* , vol. 13, no. 5, 2022, doi : 10.12720/jait.13.5.456-461.

[37] R. Kumar, P. Kumar, R. Tripathi, GP Gupta, AKMN Islam, and M. Shorfuzzaman , "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems,"

IEEE Trans Industr Inform , vol. 18, no. 11, pp. 8065–8073, Nov. 2022, doi : 10.1109/TII.2022.3161631.

[38] X. Li *et al.* , "ABM- SpConv -SIMD: Accelerating Convolutional Neural Network Inference for Industrial IoT Applications on Edge Devices," *IEEE Trans Netw Sci Eng* , vol. 10, no. 5, pp. 3071–3085, Sep. 2023, doi : 10.1109/TNSE.2022.3154412.

[39] J. Qin *et al.* , "Industrial Internet of Learning (IIoL): IIoT based pervasive knowledge network for LPWAN—concept, framework and case studies," *CCF Transactions on Pervasive Computing and Interaction* , vol. 3, no. 1, pp. 25–39, Mar. 2021, doi : 10.1007/s42486-020-00050-2.

[40] Bhupal Naik DS, V. Dondeti , and S. Balakrishna, "Comparative Analysis of ML-Based Algorithms for Detection of Anomalies in IIoT ," *International Journal of Information Retrieval Research* , vol. 12, no. 1, pp. 1–55, May 2022, doi : 10.4018/IJIRR.298647.

[41] S. Ruiz-Villafranca, J. Carrillo- Mondéjar , JM Castelo Gómez, and J. Roldán-Gómez, " MECInOT : a multi-access edge computing and IIoTemulator for the modeling and study of cybersecurity threats," *J Supercomput* , vol. 79, no. 11, pp. 11895–11933, Jul. 2023, doi : 10.1007/s11227-023-05098-2.

[42] H. Feng, D. Chen, H. Lv , and Z. Lv , "Game theory in network security for digital twins in industry," *Digital Communications and Networks* , vol. 10, no. 4, pp. 1068–1078, Aug. 2024, doi : 10.1016/j.dcan.2023.01.004.

[43] L. Ren, Z. Jia, Y. Laili, and D. Huang, "Deep Learning for Time-Series Prediction in IIoT : Progress, Challenges, and Prospects," *IEEE Trans Neural Network Learn Syst* , vol. 35, no. 11, pp. 15072–15091, Nov. 2024, doi : 10.1109/TNNLS.2023.3291371.

[44] E. Hong, S. Lee, M.-K. Oh, and S.-H. Seo, "Two-Factor Device DNA-Based Fuzzy Vault for Industrial IoT Device Security," *IEEE Access* , vol. 9, pp. 99009–99023, 2021, doi : 10.1109/ACCESS.2021.3095348.

[45] A. Bedari , S. Wang, and W. Yang, "A Secure Online Fingerprint Authentication System for Industrial IoT Devices over 5G Networks," *Sensors* , vol. 22, no. 19, p. 7609, Oct. 2022, doi : 10.3390/s22197609.

[46] M. Mohy-Eddine, A. Guezzaz , S. Benkirane, M. Azrour , and Y. Farhaoui , "An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security," *Big Data Mining and Analytics* , vol. 6, no. 3, pp. 273–287, Sep. 2023, doi : 10.26599/BDMA.2022.9020032.