International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Attack Detection Time in Industrial Systems Using Machine Learning Techniques

[1]Mussaveer Tungal, [2]Dr. Meena Chaudhary

Submitted:08/07/2023 **Revised**: 17/09/2023 **Accepted:** 12/10/2023

Abstract: Sophisticated cyber-harsh are aimed at rapid industrial systems, which asks for sharp and accurate intrusion detection devices. Delayed attack detection period can cause major operational disturbances and financial losses, so traditional security methods typically struggle with them. This paper examines the methods of machine learning to increase the time to detect attacks in industrial systems to resolve the issue. “The main goal is to improve the discrepancy-based infiltration by suggesting the maximum posterior dicotomus dicotomous discriminatory jaccardized rocchio loud (MPDQDJREB)” classification structure. This innovative approach reduces the processing load when detecting discrepancy by combining probable classification with geometry and equality-based learning. The decision limit refinement is done using the maximum backward-devious quadratic analysis (mpdqd) by the suggested model, the similarity-propelled discrepancy classification is done using jaccardized rocchio emphasis boost (JREB), and accurateness is increased using an adaptive learning technique. Using the benchmark industrial infiltration dataset, the evaluation of the approach was shown to detect a 16% sharp attack than the traditional machine learning model. Classification with processing speeds the ability of framework to balance the classification accuracy, so guarantee the reaction to real -time danger, responsible for promoting this efficiency. By greatly reduced the delay in detecting discrepancies, the results suggest how mpdqdjreb can improve the cyber security flexibility of industrial systems. Research has found that hybrid classification methods in industrial cyber security systems can be added to maximize maximum accuracy and efficiency. Future studies can emphasize modifying the model for dynamic industrial environments' real-time deployment, hence strengthening the proactive protection mechanisms against changing cyber threats.

Keywords: *Attack detection; Detection Time; Industrial Systems; Machine Learning Models*

Introduction:

While technology has also created major cyber security issues, increasing digitization of industrial systems has operated more efficiency and production. Sophisticated cyber attacks that can intervene in operations, compromise sensitive data, and cause major financial losses, often “industrial control systems (ICS), supervisory control and data acquisition (SCADA) system, and Industrial Internet of Things (IIOT) Network (Al-Abasi et al., 2020; Sagezchi et al, 2022)”. An attack detection time is one of the major issues in industrial cyber security as there may be cascading failures in industrial operations associated with delay in spotting and

[1]Department of Computer Science and Engineering,

Institute of engineering and technology, Mangalayatan University, Beswan,

Aligarh - 202146

20200969_mussaveer @mangalayatan.edu.in

[2]Assistant professor, Research Guide

Department of Computer Science and Engineering,

Institute of engineering and technology, Mangalayatan university, Beswan ,

Aligarh - 202146.

meenachaudhary9350@gmail.com

reduced risk. Due to their dependence on pre-degraded patterns, traditional “rules-based and signed-based infiltration systems (IDs) often recall zero-day attacks and advanced persistent dangers (APT) (Elonor et al., 2023; Slavas et al, 2021). As a result, machine learning (ML) -Driven anomali detection has become more prominent as a strong replacement for real -time cyber security monitoring.”

Although ML-based infiltration has improved, current models often have significant computational load and poor response time, which disrupts their practical use in time-sensitive industrial settings. Efficient, low-lonely ML technologies that can move into the attack detection when preserving great accuracy, thus needs rapidly (Alshab et al., 2023; Alonor et al., 2023). This work offers a new categorization system meant to improve anomaly detection performance and greatly shorten attack detection time. The suggested model seeks to increase detection speed while maintaining classification accuracy by combining probabilistic decision-making with geometric similarity-based learning, hence providing a feasible option for industrial cybersecurity in real time. The following section elaborates the past literatures related to this study in detail.

Literature Review:

The table 1 discussed in depth the prior literatures connected to enhancing attack detection time in industrial systems using machine learning techniques.

Table 1: Related Works

AUTHORS AND YEAR	METHODOLOGY	FINDINGS
Mokhtari et al., (2021)	Proposed a novel solution to this problem based on measurement data in the supervisory control and data acquisition (SCADA) system	The results showed that the random forest is performing better than other classifier algorithms in detecting anomalies based on measured data in the testbed.
Umer et al., (2022)	The SCADA system's measurements information was used to propose a new approach to this challenge. The four main categories of automated learning techniques used for abnormality and penetration detection—supervised, semi-supervised, uncontrolled, and reinforcing learning—were the subject of this review.	When compared to other encoder methods, random forest performed the best in identifying outliers in the testing ground data.
Chakir et al., (2023)	Using each of the most serious datasets currently available, this work compares only one classifier to different types of ensemble algorithms for the latest generation of web-based attack detection. It is the first actual analysis of its kind.	Cyber-adversaries should be prevented from compromising ICS because of its importance to a nation's economy and infrastructure. According to the datasets, bagging—specifically Random Forest—performed better than each classifier in terms of accuracy “(99.597%), resolution (98.274%), F-value (99.129%), FPR (0.523%),

		and ROC curve area (99.867%), respectively.”
Alam et al., (2023)	Improving the smart grid's safety and efficiency in operations using AI-driven analytics for prediction was the primary goal of this project	The advantages and disadvantages of using AI for smart grid cybersecurity are discussed in this article, which provides valuable insight into the technology's uses in practice.

Research Gap

Most of the time, current machine learning-based intrusion detection systems for industrial systems emphasize enhancing classification accuracy while neglecting the vital element of attack detection time. High computational needs of traditional techniques like deep learning and ensemble classifiers cause delayed threat identification in real-time industrial settings. Moreover, traditional anomaly detection methods find it difficult to strike a balance between detection speed and precision, which reduces their efficacy against time-sensitive cyber-attacks. Although hybrid methods have been investigated, there is little study on combining probabilistic classification with geometric similarity-based learning to maximize both speed and accuracy in intrusion detection. This paper fills in this vacuum by presenting the mpdqdjreb classification system, which means to reduce the time to detect the attack, preserving the accuracy of high discrepancy detection, which improves the real -time cyber security flexibility of industrial systems.

Methodology

To improve the attack time in the system of exploiting industrial infiltration, this paper presents the paper “maximum posterior dicotomus dickelus discriminatory jaccardized rocchio loudly boost (mpdqdjreb)” classification structure. The approach guarantees potential accuracy in classification by the use of maximum posterior dicotyum quadrulary discrimination (MPDQD), so the decision refines limitations. Jaccardized Rocchio emphasis boost (JREB) is also used to improve equality-based discrepancy identity, so maximizing computational efficiency. Using benchmark industrial cyber security dataset, framework is trained and tested; At the time of detecting performance, is judged at accuracy and false positive rates.

Results And Discussion:

Attack detection time denotes the period necessary to classify data for the recognition of malicious attacks, contingent upon the overall volume of input data. Utilizing relevant attributes from the dataset, data are classified efficiently in a short duration. It is measured in milliseconds (ms). The time required to classify data for predicting normal or anomalous occurrences is diminished, although the proposed method is considered more effective.

Table 2: Tabulation for attack detection time

nber of data	Attack detection time (ms)			
	Existing HDRaNN	Existing DRaNN- AD-IoT	Proposed MPDQDJREBC	Proposed WDGMS-MCP- ELM-AD-IOT
5000	19	21	18	16
10000	25	28	20	18
15000	27	34	23	21
20000	30	34	26	24

25000	33	37	30	27
30000	36	39	33	30
35000	39	43	35	32
40000	42	46	37	35
45000	46	49	40	37
50000	48	53	42	40

The experimental results about the duration required to classify input data for predicting dangerous information, obtained via both the proposed and existing approaches, are displayed in the table above. The table provides a comparative study of the proposed and existing methodologies based on various input data from the IIoT network traffic dataset. A data range of 5,000 to 50,000 entries is analysed for experimental reasons. The categorization duration fluctuates among all methodologies as the input data expands, as indicated by the table values. The tabulated results juxtapose the suggested MPDQDJREBC approach and the WDGMS-MCP-ELM-AD-IoT technology against existing methodologies, including the "Hybrid Deep Random Neural Network and the Deep Random Neural Network model, for attack detection in industrial IoT". The testing results demonstrate that the proposed WDGMS-MCP-ELM-AD-IoT technique attained the minimal data categorization duration. A graph has been created based on the data from the aforementioned table to assess the effectiveness of the proposed techniques.

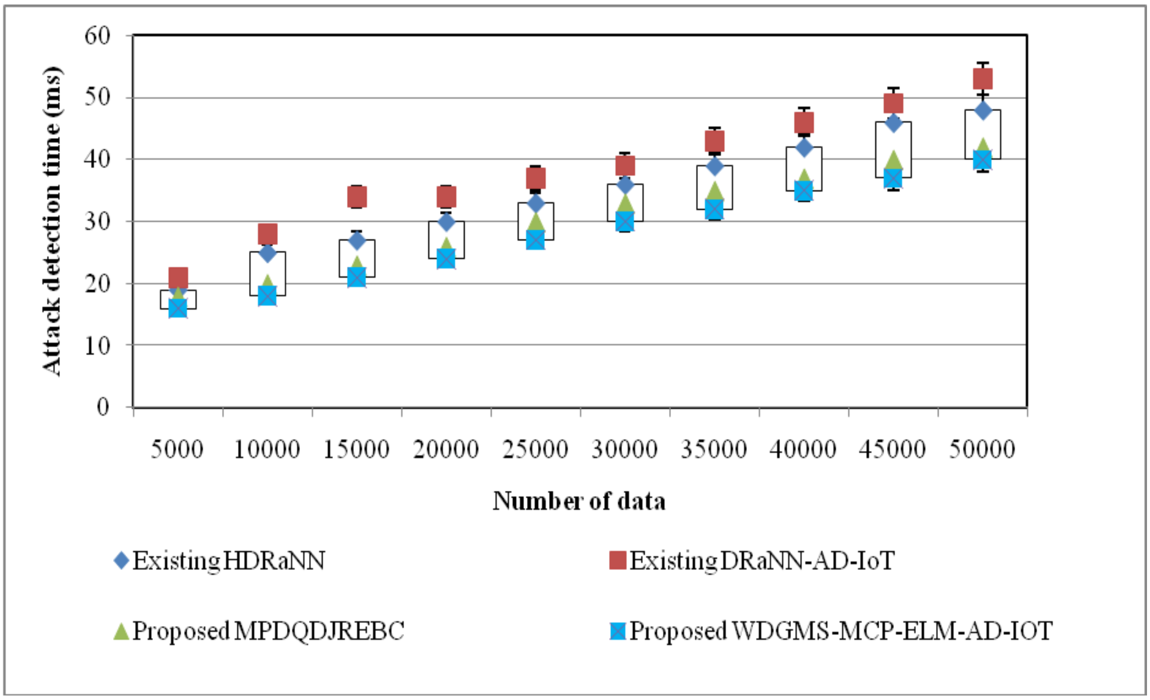

Figure 1: Measure of attack detection time

The performance metrics for attack detection time with varying data quantities are illustrated in the aforementioned figure. The quantity of input data is derived from the IIoT network database for experimental purposes. The aforementioned figure illustrates that the time required for data classification utilizing the proposed technique demonstrates superior performance. Furthermore, when the volume of input data increases, the duration required for classifying data for attack detection fluctuates. For instance, 5,000 distinct data points are selected from the dataset for experimental purposes. The performance investigation indicates that the current HDRaNN and DRaNN-AD-IoT achieve attack detection times of 19 ms and 21 ms, respectively. The proposed MPDQDJREBC technique achieves a time of 18 ms, whereas the WDGMS-MCP-ELM-AD-IoT technique achieves 16 ms. The results indicate that the suggested WDGMS-MCP-ELM-AD-IoT technique achieves a shorter attack detection time compared to other established strategies.

The proposed method executes pre-processing to eliminate redundant data. The Weibull distribution output is utilized to pick pertinent features and exclude irrelevant ones. Data is accurately classified based on the chosen features. The classified data facilitates the efficient prediction of attack data with minimal time expenditure. As a result, MPDQDJREBC function is reduced by 16%, while the WDGMS-MCP-ElM-AD-IOT strategy reduces it by 23% compared to state-of-the-art technologies. Consequently, the duration required for data classification using WDGMS-MCP-Elm-AD-IOT techniques gives better results than the existing HDrann produced by Zil Hama et al. (2021) and the drama-ed-aquet was clarified by Shahid Latif et al. (2020).

Conclusion

Industrial cyber threats are becoming more complex, requiring intrusion that algorithm detecting algorithms that prefer accuracy and attack speed. While effective in discrepancy classification, traditional machine learning-based infiltration system detects a considerable processing overhead, delaying the danger response. “The maximum posterior dicotomum was introduced in this study to reduce the detection of detection and improving the classification accuracy. When potential decision making (MPDQD) is combined with geometrical equality-based learning (JREB),” detection of discrepancy is faster and more efficient. Experimental results suggest that mpdqdjreb performs better than the traditional model, reduces the attack time 16%. This deficiency improves real - time cyber security monitoring, allowing industrial systems to respond rapidly for hazards and reduce operating disruption and security risks. Conclusions suggest that hybrid classification framework can adapt to the detection of industrial infiltration by scalable and computably efficient methods. Mpdqdjreb should be tested in dynamic industrial networks to see how it optimized for cyber hazards. Additionally, reinforcement learning and incorporating federated learning can improve its genuine -time admirement and flexibility of increased attacks.

References

[1] Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *Ieee Access*, *8*, 83965-83973.

[2] Saghezchi, F. B., Mantas, G., Violas, M. A., de Oliveira Duarte, A. M., & Rodriguez, J. (2022). Machine learning for DDoS attack detection in industry 4.0 CPPSs. *Electronics*, *11*(4), 602.

[3] Elnour, M., Noorizadeh, M., Shakerpour, M., Meskin, N., Khan, K., & Jain, R. (2023). A machine learning based framework for real-time detection and mitigation of sensor false data injection cyber-physical attacks in industrial control systems. *IEEe Access*, *11*, 86977-86998.

[4] Vargas, H., Lozano-Garzon, C., Montoya, G. A., & Donoso, Y. (2021). Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach. *Electronics*, *10*(21), 2662.

[5] Alashhab, A. A., Zahid, M. S., Isyaku, B., Elnour, A. A., Nagmeldin, W., Abdelmaboud, A., ... & Maiwada, U. D. (2023). Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. *IEEE access*, *12*, 51630-51649.

[6] Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *International Journal of Critical Infrastructure Protection*, *38*, 100516.

[7] Mokhtari, S., Abbaspour, A., Yen, K. K., & Sargolzaei, A. (2021). A machine learning approach for anomaly detection in industrial control systems based on measurement data. *Electronics*, *10*(4), 407.

[8] Chakir, O., Rehaimi, A., Sadqi, Y., Alaoui, E. A. A., Krichen, M., Gaba, G. S., & Gurtov, A. (2023). An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0. *Journal of King Saud University-Computer and Information Sciences*, *35*(3), 103-119.

[9] Alam, K., Imran, M. A., Mahmud, U., & Fathah, A. A. (2023). Cyber Attacks Detection and Mitigation Using Machine Learning in Smart Grid Systems. *Journal of Science and Engineering Research*, *1*(01), 38-55.

[10] Huma, Z. E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., ... & Baothman, F. (2021). A hybrid deep random neural network for cyberattack detection in the industrial internet of things. *IEEE access*, *9*, 55595-55605.

[11] Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020). A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE access*, *8*, 89337-89350.