Improving Anomaly Detection with Adaptive Dynamic Threshold: A Review and Enhanced Method

Arman Aghaei Attar*
Institute for Automation and Applied Informatics (IAI)
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
arman.attar@kit.edu

Tagir Fabarisov
Institute of Industrial Automation and Software Engineering (IAS)
University of Stuttgart
Stuttgart, Germany
tagir.fabarisov@ias.uni-stuttgart.de

Kaibin Bao, Veit Hagenmeyer
Institute for Automation and Applied Informatics (IAI)
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
{kaibin.bao, veit.hagenmeyer}@kit.edu

Andrey Morozov
Institute of Industrial Automation and Software Engineering (IAS)
University of Stuttgart
Stuttgart, Germany
andrey.morozov@ias.uni-stuttgart.de

***Abstract*—In fast-growing modern cyber-physical systems, reliability plays a vital role. Effective anomaly detection, which identifies security and safety issues at early stage, is essential for ensuring system reliability. While much research has focused on anomaly detection techniques, fewer studies address a key challenge, setting precise and responsive thresholds for anomaly detection. In this study, we conduct a comprehensive review of current threshold setting methods. Thereafter, we introduce a novel approach for adaptive threshold setting. Our method is tailored for diverse safety and security tasks and is tested on a safety-critical exoskeleton model and a cybersecurity scenario for energy systems. The results demonstrate that our approach could enhance the threshold setting for anomaly detection in CPS.**

***Index Terms*—Anomaly Detection, Threshold Setting, Cyber-Physical Systems, Time Series**

I. Introduction

The rapid development of complex and safety-critical cyber-physical systems (CPS) underscores the need for reliability. Safety-critical CPS applications, such as medical robots, autonomous vehicles, and energy grids, rely heavily on consistent performance [1], [2]. The tight coupling of computational algorithms with physical processes can result in complex behaviors that are challenging to predict and manage. This complexity, coupled with the heterogeneous structure of CPS, makes them prone to failure scenarios with severe physical consequences [3], posing a high risk of causing harm or damage in the event of failure [4]. Anomaly detection, one of the key reliability measures, is crucial for the early identification of internal faults and intrusions. It helps prevent significant physical consequences and maintains system integrity and security [5].

Researchers have been exploring various techniques to enhance safety. Technically, it needs to be accurate and fast. Approaches such as model-based diagnosis [6], expert knowledge [7], and data-driven error detection, including deep learning (DL), are being investigated to enable fast and effective anomaly detection and failure recovery in safety-critical CPS [8], [9]. On the other hand cybersecurity in CPS is equally important. These systems are targets for cyber-attacks that can lead to catastrophic failures [10]. Ensuring both safety and security requires robust anomaly detection systems capable of identifying both internal faults and external intrusions [9].

Advancements in data-driven methods, particularly artificial intelligence (AI) and machine learning (ML), have opened new possibilities for anomaly detection in CPS [5]. Deep learning (DL), a subset of ML, is especially effective in processing large volumes of data to identify anomalies [11], [12]. However, proper threshold setting is vital in this process, as it determines when a deviation is classified as an anomaly [13]. Recent advancements focus on improving anomaly detection methods, particularly in enhancing fast and robust prediction models [14], [15]. Despite these advances, optimizing threshold setting methods, which are equally important, has received less attention. Without proper optimization, high false alarm rates can persist even with accurate DL models. Optimizing threshold setting methods is important for improving detection performance and enhancing CPS reliability and security through timely and accurate detection of errors and intrusions [16]. **Contribution:** In this paper, various threshold setting methods are studied, and an improvement on the prevalent dynamic threshold setting method is proposed. The adaptive dynamic threshold setting mechanism offers a context-

This research is supported by the Bundesanstalt fuer Arbeitsschutz und Arbeitsmedizin (BAuA, Germany) funds, project F 2497, and by the Helmholtz Association under the programs 'Energy System Design (ESD)' (topic number 37.12.01) and 'Engineering Digital Futures (EDF)' as part of the KASTEL Security Research Labs, Karlsruhe (topic number 46.23.02).

sensitive system that adjusts its sensitivity based on real-time data, improving the accuracy and reliability of detection. The next sections of the paper are organized as follows: Section II provides a comprehensive literature review on threshold setting methods. Section III details the proposed method. Section IV implements and evaluates the proposed method in the safety and security of two sample CPS. Finally, Section V concludes and discusses prospective future work.

II. Literature Review

The threshold setting method is essential in balancing accuracy and speed in anomaly detection. As threshold computing influence both the sensitivity and the computational load of an anomaly detection system [17]. Therefore, understanding the various threshold setting methods is crucial for selecting the optimal one. These methods can be broadly categorized into static and dynamic approaches.

Static thresholds: There are fixed values that do not change over time. They are simple to implement and computationally efficient. However, static thresholds often fail to accommodate the dynamic nature of real-world data, leading to high false alarm rates or missed anomalies. They require detailed prior knowledge of normal behavior, which may not always be available in complex CPS. In [18] comprehensive survey of anomaly scoring methods aimed at mitigating false alarms is provided. The main limitation of static thresholds is their rigidity, making them unsuitable for environments with variable data patterns.

Dynamic thresholds: There are adjusted based on the characteristics of the data stream over time. These thresholds are more flexible than static ones and can adapt to changes in the underlying data distribution. Common approaches include using moving averages or exponentially-weighted moving averages (EWMA) to smooth error values and set thresholds that reflect the current state of the data. In [19] a dynamic threshold method for anomaly detection using time series segmentation is proposed. it showed improved accuracy over static methods. However, the complexity of implementation can pose significant challenges.

Another conventional categorization is parametric vs. non-parametric methods [13].

Parametric methods: They rely on statistical models that assume a specific distribution for the data. Gaussian-based methods [20] are common, using the mean and standard deviation to set thresholds. These methods are efficient but may struggle with non-Gaussian data or when the data distribution changes over time. An improved method is the application of Gaussian mixture models (GMM) for this purpose [21]. It can handle multi-modal distributions by modeling the data as a mixture of several Gaussian distributions. The primary drawback of parametric methods is their dependency on the assumption of a known distribution, which may not always be accurate.

Non-parametric methods: They do not assume a specific data distribution and offer greater flexibility in handling various types of data. Techniques such as the leverage principle and center offset measurement can dynamically adjust thresholds based on observed data. In [22], an anomaly detection algorithm based on the leverage principle is presented, using adaptive threshold setting to reduce subjectivity in distinguishing normal instances from anomalies. This method achieved high detection performance and proved practical for unsupervised anomaly detection, though it may increase computational complexity and processing time.

One of the pioneering studies in this field, [23], demonstrates non-parametric dynamic thresholding for detecting spacecraft anomalies using Long Short-Term Memory networks (LSTMs). This approach combines LSTM models with a dynamic thresholding technique that does not rely on predefined distributions, making it highly adaptable to varying data patterns. The study showed that this method effectively detects anomalies in spacecraft telemetry data, achieving high accuracy and low false positive rates. The widespread adoption of this method for dynamic threshold setting in anomaly detection highlights its effectiveness and adaptability. However, its reliance on predefined coefficients, determined through a trial-and-error process, can limit performance when applied to different data contexts. In [14], a hybrid deep learning model based on a prediction method is implemented. It compares three threshold setting method. These included conventional methods include Gaussian distribution [20], the Gaussian mixture model [21], and a dynamic non- parametric model [23]. The results demonstrate the superiority of the popular dynamic non-parametric model. Despite their effectiveness, adaptive thresholds can be sensitive to the quality and accuracy of the underlying statistical measures used for adjustment. Similarly, in [13], both a Gaussian distribution method and a non-parametric dynamic threshold setting method are compared. The results indicate that while the Gaussian distribution method achieves slightly higher precision, the dynamic threshold method performs better in terms of recall.

Adaptive thresholds, are adjusted dynamically based on observed data and are often used in environments where data characteristics change frequently [19]. These methods utilize various statistical measures, such as the mean and standard deviation of smoothed residuals, to continuously update the threshold. In [16], an adaptive threshold method for intrusion detection systems is proposed, highlighting its effectiveness in improving detection accuracy in dynamic environments. In [24], an adaptive threshold adjustment method integrated with a Temporal Attention Network (TAN-ATA) for anomaly detection in Electrical Submersible Pumps (ESP) is proposed. This approach enhances detection by incorporating a temporal attention mechanism, which reinforces the hidden states that contribute most to dynamic modeling performance. While the TAN-ATA method shows significant promise in reducing false alarms and improving anomaly detection accuracy, its complexity and potential sensitivity to variations in ESP data can present challenges, especially when applied to different CPS contexts.

In recent research, deep learning and reinforcement learning approaches have been explored for anomaly detection. Deep reinforcement learning can adaptively learn optimal detection strategies based on the system's dynamics. A deep Q-network is employed to develop a real-time error detection policy that effectively managed complex interactions between CPS components [25]. This method provided low delay, high coverage, and low redundancy, which are necessary for many CPS applications. Another agent-based dynamic thresholding (ADT) framework is dynamically adapting thresholds to detect anomalies in complex systems [26]. However, this approach can be sensitive to isolated data points that deviate from the norm, potentially affecting detection accuracy.

As shown, each method has its strengths and limitations. It is essential to choose the most adaptable approach based on the specific characteristics of the data in various safety and security anomaly detection scenarios in CPS.

III. Proposed Method

To improve adaptability of the non-parametric dynamic threshold setting model, we propose an adaptive dynamic threshold setting method. The high-level implementation of the method is presented in Figure 1. It is based on the prediction method for anomaly detection, where the residual data is calculated as the difference between predicted and actual data. The method is implemented in Python.

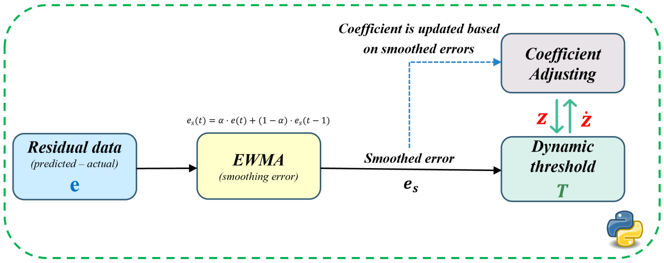

Fig. 1. High-level abstraction novel adaptive dynamic threshold

Figure 1 shows the flow of residual data through the EWMA filter, coefficient adjustment, and dynamic threshold setting. Additionally, the algorithm below describes the detailed steps of this method. This method enhances the original non-parametric dynamic threshold [23] by making the coefficient adaptive based on the data stream, allowing for more effective fault detection across diverse scenarios. Our approach employs the Exponentially-Weighted Moving Average (EWMA) to smooth residuals [23]. The smoothed residuals are then used to dynamically adjust the threshold. The improvement in our approach lies in the adaptive coefficient, which adjusts itself based on the data stream, rather than relying on a static multiplier. This adjustment is made within a predefined range, making the threshold setting more responsive to changes in the data and in the next place residual statistical properties. Mathematically, the threshold T is determined by the mean μ and standard deviation σ of the smoothed residuals e_s with an adaptive coefficient z:

$$T = \mu(e_s) + z \cdot \sigma(e_s) \tag{1}$$

The coefficient z plays a crucial role in balancing the influence of the mean and standard deviation on the final threshold. According to [23], a range between 2 and 10 has been shown to effectively balance sensitivity and stability in anomaly detection. In our study, we dynamically adjust z based on the behavior of the data stream within this range, ensuring that the threshold adapts to variations in fault types and domains. The process involves calculating the smoothed errors using the EWMA [23]:

$$e_s(t) = \alpha \cdot e(t) + (1-\alpha) \cdot e_s(t-1) \tag{2}$$

where α is the smoothing factor. The adaptive coefficient z is then updated based on the data stream's distribution and the observed anomaly rate.

$$z = \frac{\Delta\mu(e_s)/\mu(e_s) + \Delta\sigma(e_s)/\sigma(e_s)}{|e_a| + |E_{seq}|} \tag{3}$$

Here:

$$\Delta\mu(e_s) = \mu(e_s) - \mu(\{e_s \mid e_s < T\}) \tag{4}$$

$$\Delta\sigma(e_s) = \sigma(e_s) - \sigma(\{e_s \mid e_s < T\}) \tag{5}$$

$$e_a = \{e_s \mid e_s > T\} \tag{6}$$

$$E_{seq} \quad \text{continuous sequences of } e_a \tag{7}$$

- $\Delta\mu(e_s)$ represents the change in the mean of the smoothed residuals.
- $\Delta\sigma(e_s)$ represents the change in the standard deviation of the smoothed residuals.
- e_a is the set of smoothed residuals above the threshold.
- E_{seq} represents continuous sequences of e_a, which are consecutive data points from $e_s$that exceed the threshold.

The described method is formalized in Algorithm 1.

IV. Preliminary Evaluation

To evaluate the performance of the proposed detection method, we investigate two different CPS case studies. First, we consider the safety analysis of an exoskeleton model. The proposed adaptive dynamic threshold is used as the threshold in the comprehensive deployment of hybrid DL-based error detection models as described in [14], [27]. The second case study focused on CPS security in distributed energy resources (DERs), a critical safety concern. Network data from a smart inverter, which was also used by [28], are analyzed. This monitored network traffic is utilized to detect anomalies and potential attacks, ensuring the security and reliability of the CPS. For evaluating, two key metrics are utilized: precision and recall. Precision measures the correctness of detected anomalies, while recall assesses a model's ability to identify all positive instances in a dataset. Combining these metrics into a single score determines overall error detection performance. This study prioritizes both precision and recall equally, using the F1 score, as shown in Equation 8 [29]. to evaluate error detection performance. While it is true that the F1 score assumes that the costs of false positives and false negatives are equal, it remains a suitable metric in this general evaluation of threshold setting methods. Given that we are not focused on

Algorithm 1 Calculation of the Adaptive Dynamic Threshold

```
Require: Stream of smoothed residuals $e_s$
Ensure: Threshold $T$, coefficient $z \in [2, 10]$
  function CalculateThreshold($e_s, z$)
      $\mu_{\text{all}} \leftarrow \mu(e_s)$
      $\sigma_{\text{all}} \leftarrow \sigma(e_s)$
      $\mu_{\text{below}} \leftarrow \mu(\{e_s \mid e_s < T\})$
      $\sigma_{\text{below}} \leftarrow \sigma(\{e_s \mid e_s < T\})$
      $\Delta\mu \leftarrow \mu_{\text{all}} - \mu_{\text{below}}$
      $\Delta\sigma \leftarrow \sigma_{\text{all}} - \sigma_{\text{below}}$
      $e_a \leftarrow \{e_s \mid e_s > T\}$
      $E_{\text{seq}} \leftarrow$ continuous sequences of $e_a$
      $z \leftarrow \frac{\Delta\mu/\mu(e_s)+\Delta\sigma/\sigma(e_s)}{|e_a|+|E_{seq}|}$
      if $z < 2$ then
          $z \leftarrow 2$
      else if $z > 10$ then
          $z \leftarrow 10$
      end if
      $T \leftarrow \mu(e_s) + z \cdot \sigma(e_s)$
      return $(T, z)$
  end function
  while receiving new data point $e_{s,\text{new}}$ do
      Update $e_s$ with $e_{s,\text{new}}$
      $(T, z) \leftarrow$ CalculateThreshold($e_s$)
      Output $(T, z)$
  end while
```

a specific application where one type of error (false positive or false negative) is more critical than the other, the F1 score provides a balanced assessment of both aspects.

$$\begin{aligned} \text{Precision} &= \frac{\text{True Positives}}{\text{True Positives + False Positives}} \\ \text{Recall} &= \frac{\text{True Positives}}{\text{True Positives + False Negatives}} \\ \text{F1 Score} &= \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision + Recall}} \end{aligned} \tag{8}$$

True Positive (TP) is the number of actual injected errors detected. True Negative (TN) is the number of injected errors not detected. False Positive (FP) is the number of false errors detected without any fault injected. The F1 score ranges from 0 to 1, with higher values indicating better performance. With this evaluation tool in mind, we conducted a preliminary implementation of the proposed detection method. We evaluated the method in both case studies.

A. Safety Case Study

Effective error detection is a key requirement for CPS safety. This case study focuses on a prediction-based method for detecting errors in safety-critical CPS [14]. In prediction based models, the choice of threshold-setting model significantly impacts the performance of prediction-based error detection. An appropriate threshold can effectively keep optimized balance between false positives and false negatives. The case study here is an exoskeleton prototype, recognized as a safety-critical system. The exoskeleton model is highly exposed to various types and domains of errors. To address these challenges, we adopt the adaptive threshold model. To conduct the test, actual sensor data from an exoskeleton prototype was used to train the DL-based prediction model, followed by applying the threshold method. Various safety-related fault types based on [6]were injected into the last 20% of the test data.

Table 1 presents the results of three conventional threshold-setting methods compared to the adaptive dynamic model. The conventional methods include baseline Gaussian-based, Gaussian Mixture Model (GMM), and Gaussian Distribution. The adaptive dynamic model demonstrated superior performance in the experiment. It is particularly effective in detecting drift faults. Drift faults occur when a system's behavior gradually shifts from its expected state. Unlike sudden faults, they develop slowly, making them harder to detect.

TABLE I
COMPARISON OF THRESHOLD SETTING METHODS

	Baseline Gaussian Based	**GMM**	**Non-parametric Dynamic Threshold**	**Adaptive Dynamic Threshold**
F1 Score (Fault type)	67.8%	71.7%	79.1%	84.7%

B. Network Cybersecurity Case Study

The second case study focuses on cybersecurity in CPS, specifically targeting distributed energy resources (DERs), which are critical infrastructure. Cybersecurity is addressed by detecting anomalies and potential cyber attacks using network data from an experimental DER setup [28].

Packet capture (pcap) files were processed to extract the UDP packet rate, as UDP is used for communication between DER components. The packet rate was resampled at 15-second intervals, and the adaptive threshold method was applied to standardized error values. The results show that anomalies can occur across different domains, highlighting the effectiveness of the adaptive dynamic threshold.

Figure 2 shows the UDP packet rate across different emulated attack scenarios. Figure 3 illustrates the adaptive dynamic threshold applied to the smoothed error data. The anomalies detected by the adaptive threshold achieves an F1 score of 92.7%.

V. CONCLUSION

In this paper, threshold setting methods in the context of CPS reliability were investigated. We proposed an enhanced adaptive dynamic threshold method as part of anomaly detection models. The method is evaluated through implementation in two CPS case studies: the safety analysis of an assistive exoskeleton system and the network security measures of a distributed energy resource (DER) system. Preliminary results show the strong performance of the method. Its strength is its adaptability to streamed data without predefined coefficients. Future work will focus on evaluating the proposed method with more critical intrusion emulations in energy

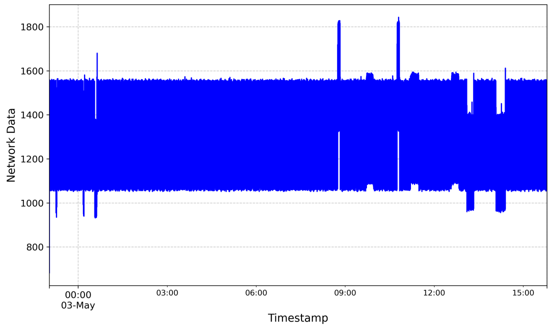

Fig. 2. UDP rates showing anomalies

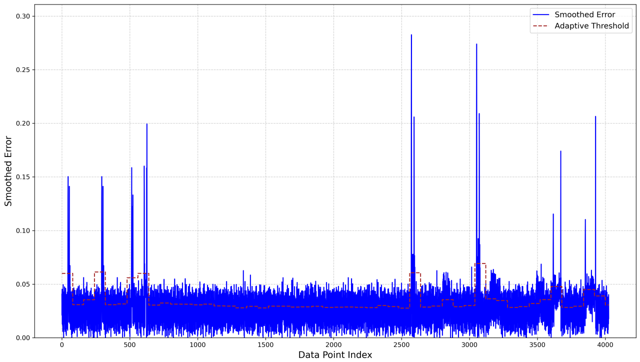

Fig. 3. Adaptive Dynamic Threshold on Network Data

infrastructure. The goal would be to generalize the method for automation systems for energy systems, to enhance reliability across various applications.

References

[1] H. Koc, S. S. Shaik, and P. P. Madupu, “Reliability modeling and analysis for cyber physical systems,” in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0448–0451.

[2] B. W. S. Y. Yang Liu, Yu Peng and Z. Liu, “Review on cyber-physical systems,” *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[3] N. Jazdi, “Cyber physical systems in the context of industry 4.0,” in *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, 2014, pp. 1–4.

[4] T. K. N. P. Seppo Sierla, Bryan O’Halloran and I. Tumer, “Common cause failure analysis of cyber–physical systems situated in constructed environments,” *Research in Engineering Design*, vol. 24, 2013.

[5] A. K. T. K. Alshaibi Ahmed Jamal, Mustafa Majid Al-Ani and A. Shelupanov, “A review on security analysis of cyber physical systems using machine learning,” *Materials Today: Proceedings*, 2021.

[6] T. Fabarisov, I. Mamaev, A. Morozov, and K. Janschek, “Model-based fault injection experiments for the safety analysis of exoskeleton system,” 01 2020.

[7] A. Q. Khan, S. El Jaouhari, N. Tamani, and L. Mroueh, “Knowledge-based anomaly detection: Survey, challenges, and future directions,” *Engineering Applications of Artificial Intelligence*, vol. 136, p. 108996, 2024.

[8] K. Ding, S. Ding, A. Morozov, T. Fabarisov, and K. Janschek, “On-line error detection and mitigation for time-series data of cyber-physical systems using deep learning based methods,” in *2019 15th European Dependable Computing Conference (EDCC)*, 2019, pp. 7–14.

[9] Y. D. Xiaorong Lyu and S. Yang, “Safety and security risk assessment in cyber-physical systems,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 221–232, 2019.

[10] L. H. Nguyen and V. R. Prasad, “Cyber-physical system security: A review of the state of the art,” *Journal of Software: Evolution and Process*, 2016.

[11] J. Audibert, P. Michiardi, F. Guyard, S. Marti, and M. A. Zuluaga, “Do deep neural networks contribute to multivariate time series anomaly detection?” *Pattern Recognition*, vol. 132, p. 108945, 2022.

[12] G. Pang, C. Shen, L. Cao, and A. Hengel, “Deep learning for anomaly detection: A review,” *ACM Computing Surveys*, vol. 54, pp. 1–38, 2021.

[13] S. V.-M. W. Sheng Ding, Andrey Morozov and K. Janschek, “Model-based error detection for industrial automation systems using lstm networks,” 2020.

[14] A. A. Attar, T. Fabarisov, A. Morozov, M. Artelt, and I. Mamaev, “Hybrid lightweight deep learning-based error detection model on edge computing devices,” in *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2023, pp. 1–4. [Online]. Available: https://doi.org/10.1109/ETFA54631.2023.10275725

[15] T. Fabarisov, A. Morozov, I. Mamaev, and K. Janschek, “Deep learning-based error mitigation for assistive exoskeleton with computational-resource-limited platform and edge tensor processing unit,” 11 2021.

[16] Y. Chae, N. V. Katenka, and L. C. DiPippo, “An adaptive threshold method for anomaly-based intrusion detection systems,” *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, pp. 1–4, 2019. [Online]. Available: https://doi.org/10.1109/NCA.2019.8935045

[17] M. Koren, O. Koren, and O. Peretz, “A procedure for anomaly detection and analysis,” *Engineering Applications of Artificial Intelligence*, vol. 117, 10 2022.

[18] Z. Zohrevand and U. Glässer, “Should i raise the red flag? a comprehensive survey of anomaly scoring methods toward mitigating false alarms,” *arXiv preprint arXiv:1904.06646*, 2019.

[19] M.-C. Dani, F.-X. Jollois, M. Nadif, and C. Freixo, “Adaptive threshold for anomaly detection using time series segmentation,” in *Neural Information Processing*. Cham: Springer International Publishing, 2015, pp. 82–89. [Online]. Available: https://doi.org/10.1007/978-3-319-26555-1_10

[20] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, “Long short term memory networks for anomaly detection in time series,” in *Esann*, vol. 2015, 2015, p. 89.

[21] D. A. Reynolds, “Gaussian mixture models,” in *Encyclopedia of Biometrics*, 2018. [Online]. Available: https://doi.org/10.1007/978-0-387-73003-5_196

[22] Q. xuan Jia, C. xu Chen, X. Gao, X. peng Li, B. Yan, G. qun Ai, J. liang Li, and J. hang Xu, “Anomaly detection method using center offset measurement based on leverage principle,” *Knowledge-Based Systems*, vol. 190, p. 105191, 2020. [Online]. Available: https://doi.org/10.1016/j.knosys.2019.105191

[23] K. Hundman, V. Constantinou, C. Laporte, I. Colwell, and T. Soderstrom, “Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding,” in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2018, pp. 387–395.

[24] Q. Li, K. Li, X. Gao, J. Fu, and L. Zhang, “Anomaly detection based on temporal attention network with adaptive threshold adjustment for electrical submersible pump,” *IEEE Transactions on Instrumentation and Measurement*, 2024. [Online]. Available: https://doi.org/10.1109/TIM.2024.3436113

[25] J. Jayaprakash, J. Pemeena Priyadarsini, B. D. Parameshachari, H. Karimi, and S. Gurumurthy, “Deep q-network with reinforcement learning for fault detection in cyber-physical systems,” *Journal of Circuits, Systems and Computers*, vol. 31, 2022.

[26] X. Yang, E. Howley, and M. Schukat, “Adt: Agent-based dynamic thresholding for anomaly detection,” *arXiv:2312.01488*, 2023.

[27] T. Fabarisov, V. G. Naik, A. A. Attar, and A. Morozov, “Remedy: Automated design and deployment of hybrid deep learning-based error detectors,” in *IECON 2023 - 49th Annual Conference of the IEEE Industrial Electronics Society*, 2023, pp. 1–8.

[28] N. Müller, K. Bao, and K. Heussen, “Cyber–physical event reasoning for distributed energy resources,” *Sustainable Energy, Grids and Networks*, vol. 39, 2024.

[29] D. Powers and Ailab, “Evaluation: From precision, recall and f-measure to roc, informedness, markedness & correlation,” *J. Mach. Learn. Technol*, vol. 2, pp. 2229–3981, 2011.