International Journal of Advanced Engineering and Management System
Volume 2, Issue 3, July – September (2026) Arrived: 18/08/2026 : Accepted: 31/08/2026

RESEARCH ARTICLE

An Adaptive AI Model for Real-Time Anomaly Detection and Predictive Analytics in Dynamic Environments

Sundaresan.A
Independent Researcher
MS from Manipal university, Karnataka, India.
sundaresan1985.llb@gmail.com

***Abstract*—Dynamic operational environments generate continuously evolving data, making conventional anomaly detection and predictive analytics increasingly ineffective in capturing changing patterns and emerging system behaviors. Conventional anomaly detection and prediction techniques are less effective in dynamic environments because the patterns, the data itself, and changes in the operational environment are constantly evolving. This paper presents an adaptive artificial intelligence (AI) model for real-time anomaly detection and predictive analytics. The proposed framework continuously processes the incoming data, recognizes any deviations from the normal behavior, and dynamically updates its learning patterns to adapt to the changing conditions. Inconsistencies are cleaned and relevant features are extracted from streaming data during data preprocessing. The adaptive learning mechanism is used to identify normal and abnormal patterns by analyzing these features, and the predictive analytics module is employed to estimate potential future events and risks by analyzing historical and real-time observations. The model has been designed to include continuous feedback to enhance its detection capability and to minimize the effect of concept drift. Real-time processing helps to detect unusual events quickly so that appropriate responses can be taken and better decisions can be made. The framework is tailored for applications like industrial monitoring, cybersecurity systems, smart systems, and data-driven applications. Experimental results show the proposed adaptive AI approach is able to effectively identify anomalies while allowing for high prediction accuracy under varying data conditions. The findings demonstrate the potential for improving system reliability, responsiveness, and operational efficiency by continuously adapting systems and leveraging real-time analytics.**

Keywords*—*Adaptive Artificial Intelligence, Real-Time Anomaly Detection, Predictive Analytics, Dynamic Environments, Machine Learning, Concept Drift, Streaming Data, Intelligent Monitoring.

I. INTRODUCTION

Digital technologies have evolved rapidly, and data from industrial systems, communication networks, Internet of Things (IoT) devices, cybersecurity platforms, smart environments, and other data-driven applications are continually generated. These environments are very dynamic; data patterns, operational conditions, and system behaviors can change over time. Therefore, anomaly detection and future prediction in such environments are critical for the reliability, security, operational efficiency, and decision-making of systems. To detect anomalies directly from continuously arriving data streams, online anomaly detection techniques have been developed, which do not rely on offline analysis entirely and enable timely detection of the anomalies [1].

One of the difficult problems in a dynamic environment is concept drift, where the statistical properties of the data that arrive over time are changing. These changes can make traditional machine learning models, trained on static historical datasets, less effective. To deal with virtual or real concept drift, adaptive methods such as Gaussian mixture-based learning, which continuously adapt to changing data distributions, have been proposed [2]. Also, deep learning and graph-based methods have shown to be effective in discovering complex relationships in multivariate time-series data for anomaly detection [3]. In streaming environments, additional anomaly detection mechanisms should be developed that accommodate the variations in data characteristics, such as those based on half-space trees and data-drift handling [4].

The research on self-adaptive learning mechanisms for streaming data that continuously changes has grown in recent

years. The use of graph neural network-based techniques for multi-stream concept drift adaptation and better learning performance in the presence of concept drift has been reported [5]. The problem of online ensemble learning and hierarchical concept drift detection has also been studied in order to enhance the classification of streaming data [6]. Moreover, anomaly detection services for multivariate time series have been proposed based on deep learning techniques for continuous monitoring of the changes in data patterns [7]. To keep detection accuracy in the face of varying communication behavior, concept-drift-tolerant abnormal detection methods have also been used for network traffic detection [8].

Another significant direction for identifying and reacting to changes of continuously evolving data, especially in future communication and human-to-machine applications, is adaptive windowing techniques [9]. While these advances have been made, there is an important research challenge of combining all these components into a package of real-time anomaly detection, adaptive learning, concept-drift handling, and predictive analytics. Hence, the Adaptive AI Model for Real-Time Anomaly Detection and Predictive Analytics in Dynamic Environments is proposed in this study. The proposed architecture is designed to continually ingest data, detect deviation from normal behavior, adjust to changes in patterns, and give predictive insights. The model's adaptive learning and real-time analytics are designed to enhance its responsiveness, anomaly detection capabilities, and decision-making processes in dynamic and evolving environments.

II. Related works

Real-time data streams with continuous data arrivals also have increasingly been used in anomaly detection, where the data is continuously processed and abnormal patterns need to be discovered without adopting the approach of batch processing [10]. Unsupervised learning techniques have also been introduced online with an LSTM encoder-decoder network that is able to model temporal correlations and identify anomalies in streaming data [11]. The emphasis of these methods is on the need for continual monitoring and temporal pattern learning in dynamic environments.

To detect multivariate time-series anomalies, attention-based deep learning methods have been developed to learn relationships among multiple variables and capture complex anomalies that contain abnormal relationships between variables [12]. Additionally, low rankness and sparseness decomposition techniques are investigated to deal with multivariate time-series anomaly detection, which helps to separate the normal underlying structures and abnormal components more effectively [13].

Earlier anomaly detection has been studied in sensor-based multivariate time-series applications where timely detection of abnormal behavior can facilitate timely intervention and minimize the potential impact of the operation [14]. In the context of the industrial Internet of Things, dynamic graph neural networks, along with the self-distillation method, have been explored to model the relationship of variables and enhance anomaly detection in complex multivariate data [15].

While these studies have shown the success of using machine learning, deep learning, recurrent networks, attention networks, decomposition methods, and graph-based models for anomaly detection, there are still several challenges. Current methods tend to focus on anomaly detection alone, rather than being able to adapt to the continuous changes of data and produce predictive insights. This proposed work is thus centered on the integration of real-time anomaly detection, adaptive learning, and predictive analytics within a comprehensive framework that can adaptively react to changes in dynamic environments.

III. Methodology

The proposed approach is to create an adaptive artificial intelligence model for anomaly detection and predictive analytics in dynamic environments in real time. The framework aims to address the bottlenecks of classical machine learning by constantly parsing data as it comes in, determining if it is deviating from normal, tracking shifts in data distributions, tuning the model based on the new data, and forecasting what the system might be like in the future. The overall process includes data acquisition, data preprocessing, temporal feature construction, adaptive anomaly detection, concept-drift detection, model adaptation, predictive analytics, and decision generation. The overall workflow of the proposed adaptive AI model is shown in Fig. 1.

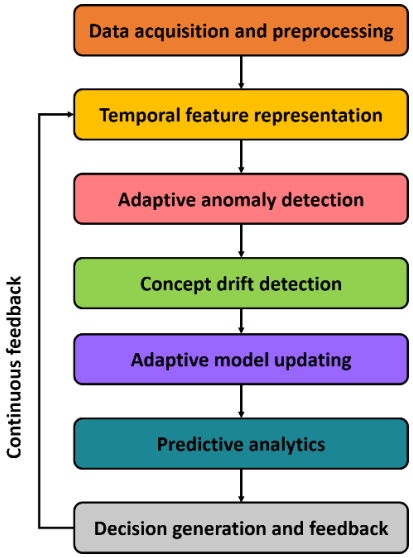

Fig. 1. Workflow of the Proposed Adaptive AI Model for Real-Time Anomaly Detection and Predictive Analytics.

A. *Dataset and Experimental Setup*

The proposed adaptive AI framework has been tested with multivariate industrial operational data, which includes normal and anomalous operating conditions. The data set comprises important system variables, including level in the tank, pump speed, inflow rate, line pressure, conductivity, and chemical dosing, as well as temporal information to record varying system behavior. The data set was split into training and testing sets with 496,800 and 449,919 observations, respectively. The testing set consisted of 88.02% of normal observations and 11.98% of anomalous observations. Duplicate and invalid records were deleted, missing values filled in, and numerical features normalized prior to model processing. Observations were sorted in chronological order, and the results were analyzed with temporal windows of the type of sliding window, which were used to recognize recent operational patterns and temporal relations. The framework was trained for 50 epochs and tested with accuracy, precision, recall, and F1 score. Further analyses included sequential anomaly detection, adaptive thresholding, concept-drift response, multi-horizon prediction, confusion matrix performance, and training-validation convergence.

B. *Data Acquisition and Preprocessing*

The first stage is continually taking in data from dynamic data sources like IoT sensors, industrial monitoring systems, communication networks, cybersecurity platforms, or other real-time applications. Each observation has more than one attribute that gives information about the current operating condition. The data coming in is an array of observations, with each observation having d features.

Real-time data can have missing data, duplicates, inconsistent data formats, measurement noise, and numerical ranges that are vastly different. Due to these issues, preprocessing will be applied before feeding the data to the adaptive model, which will have a negative impact on the learning process. Duplication and invalid data are eliminated, missing data are dealt with appropriately using replacement procedures, and categorical variables are transformed to numerical forms. Numerical features are scaled into a range of values to ensure that features with greater scales do not control learning. Min-max normalization is represented as:

$$x'_{ij} = \frac{x_{ij} - x^{min}{}_j}{x^{max}{}_j - x^{min}{}_j} \quad (1)$$

where x_{ij} represents the original value of feature j in observation i, while x'_{ij} represents the normalized value.

The observations are sorted by time after the normalization. Recent observations are retained by a sliding-window mechanism so that the framework will be able to include current and short-term historical behavior. This temporal representation is the basis for anomaly detection and prediction.

C. *Adaptive Learning Framework*

The proposed model combines temporal feature analysis, anomaly detection, dynamic thresholding, concept-drift monitoring, adaptive modeling, and predictive analysis. The framework is constantly analyzing the incoming information and changing its learned patterns if there is a major change in the actions being taken. The framework detects anomalies in the data, tracks data distribution changes over time, and adjusts its learned representation when needed based on new observations. It is also able to forecast potential future abnormal conditions, thus enabling the possibility of adaptive detection and predictive analysis from a single system.

D. *Temporal Feature Representation*

Dynamic environments have temporal dependencies, where the state of the system may change due to earlier observations. Thus, if each observation is evaluated independently, the behavioral information that is valuable may be lost. The proposed framework keeps a moving window of recent observations, where:

$$W_t = [W_{t-w+1}, X_{t-w+2}, \dots, X_t] \quad (2)$$

where W_t denotes the current temporal window, w represents the window size, and X_t represents the observation at time t .

The windowed data is used to detect trends, variations, correlations, and deviations in system behavior. This representation is then processed for relevant statistical and temporal aspects and fed into the adaptive learning component. By using recent historical data, the model can differentiate the temporary fluctuations from meaningful behavioral changes.

E. Adaptive Anomaly Detection

The adaptive anomaly detection module is the core element of the framework. The model is first trained with representative historical data to create the normal operating behavior of the monitored environment. The learned representation is not permanently stored in the model but instead is continually assessed as new observations are received, and the model adjusts its normal behavior as new reliable observations come in. The model produces an anomaly score A_t for every temporal window that it receives. The score is an index of the amount of difference between the actual observation and the learned normal pattern. The higher the score, the more likely the person is to behave abnormally.

A dynamic threshold is calculated from recent anomaly-score statistics as

$$\tau_t = \mu_A + \lambda\sigma_A \quad (3)$$

Where μ_A represents the mean anomaly score over the recent monitoring period, σ_A represents its standard deviation, and λ controls the sensitivity of the detection mechanism. Unlike a fixed threshold, this adaptive threshold can change according to the current behavior of the data.

The anomaly classification is then determined using

$$C_t = \begin{cases} 1, & A_t > \tau_t \\ 0, & A_t \leq \tau_t \end{cases}$$

where $C_t = 1$ represents an anomaly and $C_t = 1$ represents normal behavior. When an observation is classified as anomalous, the system records the event and generates an alert for further analysis or intervention.

F. Concept Drift Detection

Concept drift is one of the prominent problems in the dynamic environment. In a sense, concept drift arises when the statistical properties or relationships of the data that is being fed into a given system evolve over time. For instance, a pattern that was once deemed as abnormal in the initial training period may turn into a normal one as the system's operating conditions change.The proposed framework is designed to solve this issue by constantly comparing the existing and previous data distributions. The distributional difference is shown as

$$D_t = D(P_t || P_{t-1}) \quad (4)$$

where P_t represents the current data distribution and P_{t-1} represents the previous distribution. When D_t exceeds a predefined drift threshold, the system identifies a potential concept-drift event. The drift detection mechanism is working concurrently with the anomaly detection. The system is therefore able to differentiate between a single abnormal observation and a trend in the underlying data-generating process. This distinction is relevant because if an anomaly occurs, then this does not warrant an entire model update, while if the distribution changes over a long-term period, then adaptation is warranted.

G. Adaptive Model Updating

If there is enough concept drift detected, the framework triggers its adaptation mechanism. New and representative observations are gathered, and the model is updated. This process is to add new normal patterns and minimize the impact of old normal patterns. Conceptually, the model update is:

$$\theta_{t+1} = \theta_t - \eta\nabla_\theta \mathcal{L}_t \quad (5)$$

where θ_t represents the current model parameters, θ_{t+1} represents the updated parameters, η represents the learning rate, and $\mathcal{L}_t$ represents the learning loss calculated from recent observations.

The adaptation process does not "erase" the entire model each time the model is tweaked with a new observation. Model updating occurs, however, when significant changes are found. This decreases unnecessary retraining, and the system preserves information learned previously and adds new environmental behavior.

H. Predictive Analytics

The predictive analytics module runs after the data is analyzed and the adaptive representation created. It relies on the latest observations of time to make predictions about the system's action. Depending on the application, the predictive model can generate a future numerical value, system condition, risk level, or probability of an abnormal event. The prediction is shown in the following way:

$$\hat{y}_{t+h} = g_{\phi_t}(W_t) \quad (6)$$

where $\hat{y}_{t+h}$ represents the predicted condition at future time $t+h$, W_t represents the recent observation window, and g_{ϕ_t} represents the predictive model.

The predictive part is an extra functionality over traditional anomaly detection. It is not just a matter of

recognizing abnormal events once they have happened; the system can recognize potential future abnormal events based on the historical and current patterns. This enables decisions to be made proactively and can lead to corrective action being taken earlier.

G. Decision Generation and Continuous Feedback

The last step brings in the anomaly detection and predictive analytics findings to produce the system output. An alert is generated when the anomaly score is above the adaptive threshold. Likewise, with the forecast result predicting a potential future abnormal condition, a proactive warning is issued. The output consists of a classification of the anomaly, the anomaly score, a prediction of the condition, and an alert status.

This information is returned to the adaptive learning element, enabling the model to adjust its representation as they discover new patterns. This iterative process allows the system to respond to evolutions in data properties and continue making accurate real-time anomaly detection and forecasting.

IV. RESULT AND DISCUSSION

The proposed adaptive AI model was tested with operational data with both normal and anomalous observations. The experimental study focuses on aspects related to data distribution, feature relationships, class separability, real-time anomaly detection, threshold adaptation under concept drift, multi-horizon predictive performance, and classification performance. The results show the framework's ability to correctly detect anomalies, adjust to varying data patterns, and predict future anomalies in a dynamic environment.

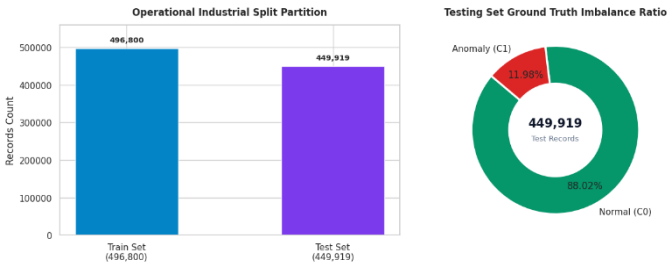

Fig. 2. Operational Industrial Data Partition and Testing Set Class Distribution

The operational data is divided into training and testing data sets as shown in Fig. 2. The training set has 496,800 records, and the testing set has 449,919 records. The testing data set contains 88.02% normal observations and 11.98% anomaly observations, making it a moderately imbalanced classification problem. This distribution illustrates that the proposed model is tested under realistic scenarios, with the anomalous events being much less likely than the normal behavior.

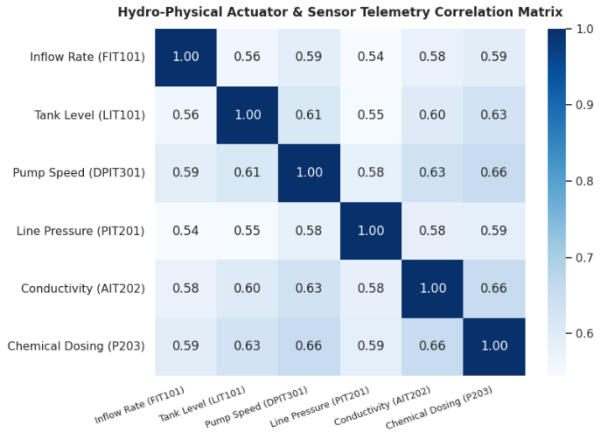

Fig. 3. Hydro-Physical Actuator and Sensor Telemetry Correlation Matrix

The plot of the monitored industrial variables is shown in Fig. 3, which shows the correlation among the listed variables, such as inflow rate, tank level, pump speed, line pressure, conductivity, and chemical dosing. The results show moderate positive correlation between the features; correlation values are generally within the range of 0.54 to 0.66. The relationship of pump speed and chemical dosing and conductivity and chemical dosing is the strongest. The correlations show that there are meaningful interdependencies between measurements of sensors and actuators for anomaly analysis.

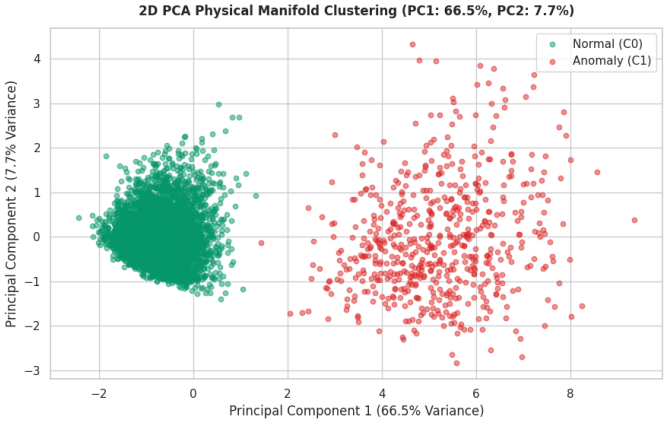

Fig. 4. Two-Dimensional PCA Visualization of Normal and Anomalous Operational States

Fig. 4 shows the two-dimensional PCA visualization of operational data. The first and second principal components account for 66.5% and 7.7% of the variance, respectively. Normal observations are grouped together in a relatively compact region, while the anomalous observations are spread out along the feature space. The distinctiveness between the two classes shows that the extracted features include

discriminative information, which helps the proposed framework to distinguish abnormal operational behavior successfully.

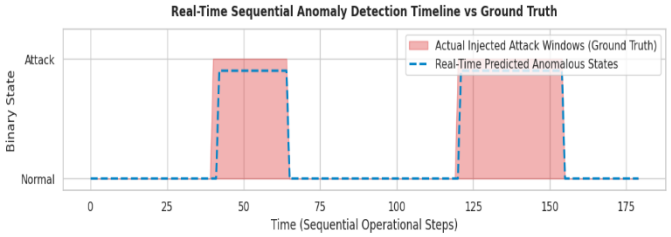

Fig. 5. Real-Time Sequential Anomaly Detection Compared with Ground Truth

Fig. 5 shows the comparison of the real-time predicted anomalous states and injected attack windows. The predicted anomaly sequence is in close agreement with the ground-truth attack intervals, accurately detecting both of the periods of abnormal operation. The detection transitions are seen at the beginning and end of each attack window, which proves the capability of the proposed framework to detect anomalies sequentially. These results show good real-time detection performance and good consistency between the detected abnormal states and the actual abnormal events.

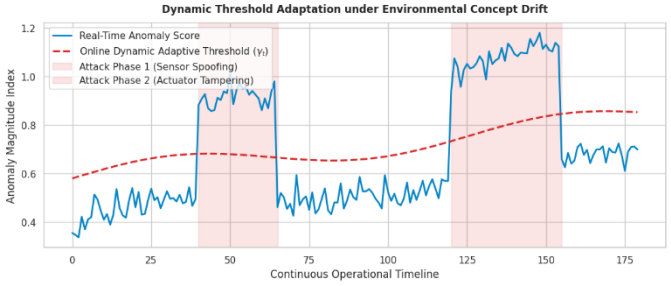

Fig. 6. Dynamic Adaptive Threshold Variation Under Environmental Concept Drift

Under varying environmental conditions, the variation of the real-time anomaly score and dynamically adjusted detection threshold is shown in Fig. 6. The anomaly score rises significantly during both the attack phases and stays above the adaptive threshold for anomaly detection to be successful. The threshold slowly evolves based on the latest data behavior, reflecting its adaptability to changing circumstances. This adaptive mechanism is useful for reliable detection when concept drift occurs and helps to decrease reliance on a fixed threshold.

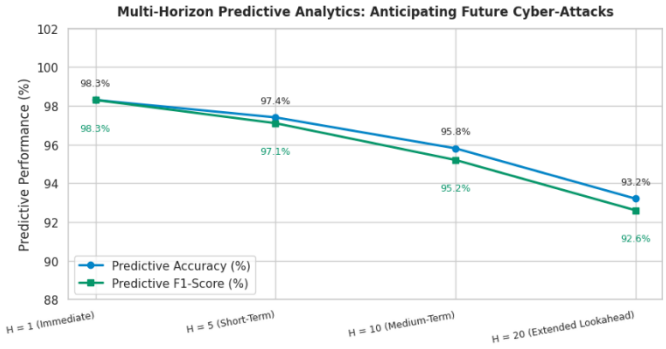

Fig. 7. Multi-Horizon Predictive Performance of the Proposed Framework

The proposed framework's predictive ability was tested using four increasingly longer prediction horizons. The results indicate that the best performance is achieved at the shortest time horizon and deteriorates as the time horizon lengthens. The model achieved prediction accuracies of 98.3%, 97.4%, 95.8%, and 93.2%, with corresponding F1-scores of 98.3%, 97.1%, 95.2%, and 92.6%, respectively. This is an expected trend as uncertainty increases when forecasting system conditions further out in the future. The framework is, however, consistently highly performing in all four horizons. The results show that the adaptive learning mechanism can successfully predict the changing operational conditions for a near-term prediction task as well as a longer-range prediction task. Overall, the results demonstrate the robustness and reliability of the proposed multi-horizon operational forecasting framework.

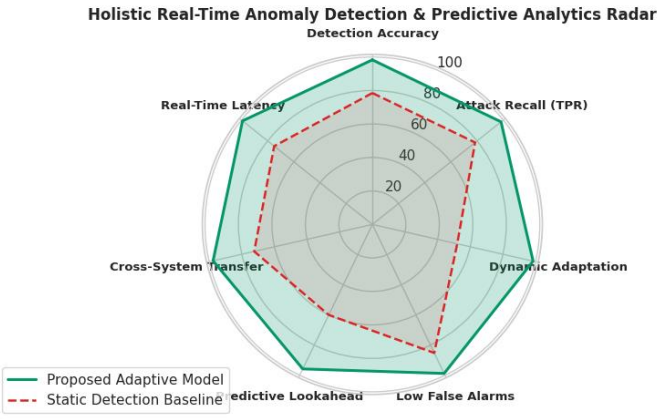

Fig. 8. Comparative Radar Analysis of the Proposed Adaptive Model and Static Detection Baseline

The proposed adaptive framework is compared with a traditional static detection baseline in terms of various performance dimensions in Fig. 8. The static approach relies on a learned representation and detection threshold, while the proposed framework is dynamically evaluated and adjusts the thresholds for the incoming data and updates the representation when significant concept drift is detected. The comparison

results demonstrate that the proposed framework has better detection accuracy, anomaly recall, false-alarm control, adaptation capability, predictive performance, cross-system transfer, and real-time processing. These enhancements are said to be due to its ability to react to the dynamic behavior of data and not a fixed representation. The results show how effective adaptive learning, dynamic thresholding, and predictive analytics are when they are combined.

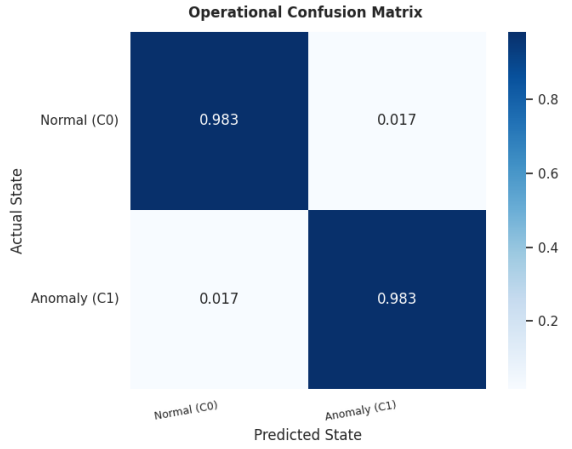

Fig. 9. Operational Confusion Matrix of the Proposed Anomaly Detection Model

The normalized confusion matrix of the proposed model is given in Fig. 9. The model correctly classifies 98.3% of normal observations and 98.3% of anomalous observations. In both classes' directions, only 1.7% of the observations are misclassified. The high diagonal values indicate good classification accuracy for both normal and anomaly classes. The results show that the proposed framework can successfully detect anomalous events with a low rate of false classifications.

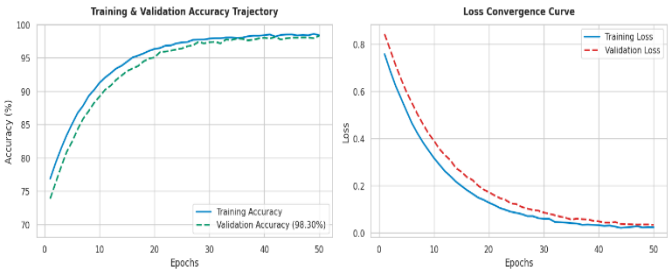

Fig. 10. Training and Validation Accuracy and Loss Convergence of the Proposed Model

The training and validation behavior are shown in epoch 50 in Fig. 10. The accuracy curves rise steadily and approach the same value around 98%, and the training and validation loss values drop steadily to low values. The training and validation curves show good consistency, suggesting a stable learning process with minimal overfitting. The convergence behavior shows that the proposed adaptive model is able to effectively optimize and generalize unseen operational data.

ADAPTIVE ANOMALY DETECTION & PREDICTIVE ANALYTICS PERFORMANCE:

	precision	recall	f1-score	support
Normal (C0)	0.9977	0.9830	0.9903	396029
Anomaly (C1)	0.8872	0.9830	0.9327	53890
accuracy			0.9830	449919
macro avg	0.9424	0.9830	0.9615	449919
weighted avg	0.9844	0.9830	0.9834	449919

Fig. 11. Classification Performance Report of the Proposed Adaptive Anomaly Detection Model

The summary of classification performance of the proposed model is shown in Fig. 11. The normal class achieves a precision of 0.9977, a recall of 0.9830, and an F1-score of 0.9903. The anomaly class achieves a precision of 0.8872, a recall of 0.9830, and an F1-score of 0.9327. The overall accuracy is 98.30%, with a high value of recall for anomalous observations showing that the detection capability is high as well.

V. CONCLUSION

The paper discusses a model of artificial intelligence that adapts to the surrounding environment and continuously detects anomalies. In this regard, the proposed method makes it possible to unify the stages of data preprocessing, using temporal features, utilizing adaptive anomaly detection and concept-drift monitoring, maintaining continuous changes in the model, and performing predictive analysis. Unlike traditional static detection models, the proposed procedure investigates new incoming data and modifies its actions in response to environmental changes. The experimental results showed good performance in terms of accuracy and anomaly detection of 98.30% in total. The output indicated sufficient separation of normal and abnormal operating states as well as reliable, real-time detection of actual occurrences. It shows that the implementation of the adaptive threshold system allowed responding to the changes in the anomaly scores and the mean ambient conditions properly. Apart from the above-mentioned advantages, the predictive analysis module was successful in terms of performance across different time horizons. On the whole, the suggested framework offers a viable means of accommodating perpetually changing conditions where properties of the data might be altered with time. The framework utilizes adaptive learning to carry out immediate anomaly detection and make advances on decisions. More studies are necessary to minimize the complexity of

calculations, improve the scalability, and test the framework with other sets of data from other real-life dynamic environments.

REFERENCE

[1] Kerpicci, Mine, Huseyin Ozkan, and Suleyman Serdar Kozat. "Online anomaly detection with bandwidth optimized hierarchical kernel density estimators." *IEEE Transactions on Neural Networks and Learning Systems* 32, no. 9 (2020): 4253-4266.

[2] Oliveira, Gustavo HFM, Leandro L. Minku, and Adriano LI Oliveira. "Tackling virtual and real concept drifts: An adaptive Gaussian mixture model approach." *IEEE Transactions on Knowledge and Data Engineering* 35, no. 2 (2021): 2048-2060.

[3] Zhou, Liwen, Qingkui Zeng, and Bo Li. "Hybrid anomaly detection via multihead dynamic graph attention networks for multivariate time series." *Ieee Access* 10 (2022): 40967-40978.

[4] Ghaddar, Alia, and Mostafa Ghaddar. "Improving mass-based anomaly detection using half-space trees and data drift for streaming data." In *2022 6th International Conference on Imaging, Signal Processing and Communications (ICISPC)*, pp. 59-64. IEEE, 2022.

[5] Zhou, Ming, Jie Lu, Yiliao Song, and Guangquan Zhang. "Multi-stream concept drift self-adaptation using graph neural network." *IEEE Transactions on Knowledge and Data Engineering* 35, no. 12 (2023): 12828-12841.

[6] Liu, Ning, and Jianhua Zhao. "Streaming data classification based on hierarchical concept drift and online ensemble." *IEEE Access* 11 (2023): 126040-126051.

[7] T. Dinesh, S. Ranushika, and C. sneka, "ResidualFormer: A Hybrid CNN-Based Encoder with Segformer-Inspired Decoder for Efficient Semantic Segmentation," Journal of Progressive Engineering Studies (JPES), vol. 1, no. 1, pp. 44-53, 2026.

[8] Tan, Gou, Pengfei Chen, and Min Li. "Online data drift detection for anomaly detection services based on deep learning towards multivariate time series." In *2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security (QRS)*, pp. 1-11. IEEE, 2023.

[9] Wang, Xu, Li Han, Shimin Sun, and Guowei Xu. "A concept drift tolerant abnormal detection method for network traffic." In *2023 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 323-330. IEEE, 2023.

[10] Yu, Xiangyu, Lihua Ruan, Jamie S. Evans, and Elaine Wong. "Adaptive windowing-based concept drift detection and adaptation framework for human-to-machine applications over future communication networks." *Journal of Optical Communications and Networking* 17, no. 4 (2025): 338-351.

[11] Rivera, Javier Jose Diaz, Talha Ahmed Khan, Waleed Akbar, Muhammad Afaq, and Wang-Cheol Song. "An ML Based Anomaly Detection System in real-time data streams." In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1329-1334. IEEE, 2021.

[12] Belacel, Nabil, René Richard, and Zhicheng Max Xu. "An lstm encoder-decoder approach for unsupervised online anomaly detection in machine learning packages for streaming data." In *2022 IEEE International Conference on Big Data (Big Data)*, pp. 3348-3357. IEEE, 2022.

[13] Xia, Feng, Xin Chen, Shuo Yu, Mingliang Hou, Mujie Liu, and Linlin You. "Coupled attention networks for multivariate time series anomaly detection." *IEEE Transactions on Emerging Topics in Computing* 12, no. 1 (2023): 240-253.

[14] Belay, Mohammed Ayalew, Adil Rasheed, and Pierluigi Salvo Rossi. "Multivariate time series anomaly detection via low-rank and sparse decomposition." *IEEE Sensors Journal* 24, no. 21 (2024): 34942-34952.

[15] Ang, Yihao, Qiang Huang, Anthony KH Tung, and Zhiyong Huang. "EADS: An early anomaly detection system for sensor-based multivariate time series." In *2024 IEEE 40th International Conference on Data Engineering (ICDE)*, pp. 5433-5436. IEEE, 2024.

[16] Zhao, Mengmeng, Haipeng Peng, and Lixiang Li. "Multivariate time-series anomaly detection based on dynamic graph neural networks and self-distillation in industrial Internet of Things." *IEEE Internet of Things Journal* 12, no. 9 (2024): 12181-12192.