International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ENHANCING SECURITY RESILIENCE: DYNAMIC DRIFT DETECTION IN CLOUD-BASED INTRUSION DETECTION USING THE HYBRID MODEL

Aditya Kumar Shukla [1] , Ashish Sharma [2]

[1] Department of Computer Engineering and Applications
GLA University, NH2, Delhi Mathura Highway
Post Ajhai, Mathura (UP) India
e-mail: uraditya@gmail.com

[2] Department of Computer Engineering and Applications
GLA University, NH2, Delhi Mathura Highway
e-mail: ashishs.sharma@gla.ac.in

September 5, 2025

Abstract

Security and trust are seriously challenged by intrusion in cloud computing. The unpredictability of data patterns is a significant barrier that makes it challenging for current machine learning (ML) models to reliably identify and categorize intrusion attacks over an extended period of time. To assess the efficacy of a hybrid model for real-time anomaly detection and adaptive learning, this study combines the XGBoost classifier with the Adaptive Windowing Detection of Drift (AWDD) model. The goal of the hybrid model is to locate drift in streams of continuous data. We evaluate its performance by means of an extensive analysis including diverse metrics and visualizations. According to our research, the XGBoost and AWDD model working together minimizes false negatives while accurately identifying positive cases. The model exhibits strong recall and precision, with an F1-score of 99.6 percent and a precision rate of 99.3 percent. Despite a few false positives, the model continues to function well. The model's remarkable AUC (area under the curve) value of 0.94 on the ROC curve indicates how accurate it is at making predictions. Additionally, the accuracy trend plot shows a steady rising trend, indicating the adaptability of the hybrid model to shifting data distributions. These findings highlight the hybrid model's value as a reliable resource for anomaly identification in real time across a range of industries and applications.

Keywords: Adaptive Windowing Drift Detection(AWDD), AI-ML, Cloud Security, Intrusion detection, Cloud Computing.

Received: July 20, 2025

1 Introduction

Over the evolution of computer networking, Intrusion Detection Systems (IDS) have played a critical role in network security. Originally, IDSs safeguarded IT infrastructures from cyber threats, with many organizations relying on dedicated hardware implementations to protect their assets [1,2,3]. However, due to the rapidly evolving nature of technology, small and medium-sized businesses (SMBs) are finding it more difficult to implement traditional strategies. Instead, they are turning to remote access to platforms and software as needed in order to cut costs and improve flexibility. In [4].

This shift toward cloud-based solutions presents challenges, particularly in the realm of network security. Virtual machines (VMs) are commonly used for IDS deployment, but their varying levels of protection can pose security risks. Furthermore, the advantages of cloud services are compromised by the traditional installations' slow response times to breaches, which have an effect on system security as a whole [5]. Network vulnerabilities may be increased by deploying a distributed Intrusion Detection System (IDS) online, hence IDS systems must function independently and remain hidden within server-hosted systems [6]. IDSs encounter unique difficulties in spite of their significance; notion drift is one of the main issues. Concept drift is the term used to describe how attack patterns change over time and make existing intrusion detection systems useless against new assault techniques [7]. Concept drift in streaming data analytics is characterized by temporal fluctuations in the statistical features of the data distribution that can be divided into two categories: rapid changes and gradual changes [8,9]. It is imperative to tackle these issues, particularly in dynamic environments such as Internet of Things devices, where traditional machine learning models find it difficult to adjust to sudden variations [10].

Enter the Adaptive Windowing Drift Detection (AWDD) framework, which has emerged as a solution to these challenges. AWDD offers real-time detection and adaptation to concept drift in data streams, providing a robust solution to the evolving threat landscape.

Organization of the paper: Here is a summary of the rest of the paper: Section II provides a literature review on the detection and adaptation of concept drifts. The third section outlines the methodology, while Part four describes the exploratory results and discusses the key discoveries. Finally, Section V presents the conclusion, summarizing the paper, discussing its limitations, and suggesting future avenues for research.

2 Related Work

P. Mishra et al. [15] investigated intrusion detection methods specific to cloud computing, with a focus on detecting and mitigating attacks using Virtual Machine Introspection (VMI) and Hypervisor Introspection (HVI) techniques. The author provides a systematic analysis of cloud threat models and attack taxonomies, aiming to classify intrusion detection system (IDS) methodologies and pinpoint research gaps for future exploration, thereby enhancing cloud intrusion detection.

Received: July 20, 2025

D. K. Talapula et al. [16] developed dynamic streaming data analytics by combining deep learning and hybrid models, refining the One-Class Kernel Wavelet (OKW) technique to address duration and memory constraints. The integration of deep Long Short-Term Memory (LSTM) networks and Recurrent Neural Networks (RNN) improves the combined deep learning (DL) and hybrid classifier's ability to identify concept drifts in real-time data. Enhanced drift detection accuracy is achieved through optimal parameter tuning using the proposed intelligent predatory method. The experiment utilizes benchmark datasets including Apache, Hadoop, Linux, Spark, and Cloud monitoring.

H. Mehmood et al. [17] introduced a design for an information system tailored for smart cities in Emerging and Developing Countries (EMDCs), facilitating AI workload deployment over a hybrid cloud-edge continuum. Using a feedback-driven approach, the author addresses notion drift with techniques such as LSTM, Adaptive Windowing (ADWIN), Kolmogorov-Smirnov Windowing (KSWIN), and Page-Hinkley Test (PHT). Data streams from the University of Oulu Smart Campus help predict environmental conditions, with performance assessed using metrics like Mean Absolute Error (MAE), Mean Absolute Percentage Error (MAPE), and Root Mean Square Error (RMSE). The study also evaluates the effectiveness of the proposed solutions.

P. B. Dongre et al. [18] presented a comparative analysis of single classifier and ensemble mining methods for detecting concept drift in data streams. Techniques evaluated include sliding-window methodologies, instance selection methods, and classifier ensembles, aiming to identify the most effective approaches for managing concept drift in data streams.

Q. Zhu et al. [19] introduced DWCDS, a system for detecting drift in data streams using a two-pane technique. By leveraging random decision trees, DWCDS identifies potential concept drifts through analysis of changes in sliding window data distribution. Experimental results demonstrate that DWCDS outperforms single-viewing area-based approaches in detecting concept drifts.

S. Seth et al. [20] proposed a stream-oriented learning strategy for online intrusion detection, capable of adapting to drift in real-world scenarios. This method eliminates the need for periodic model retraining by using an adaptive random forest model with an ADWIN change detector to identify real-time data drift. Evaluation with the CIC-IDS 2018 dataset shows high reliability and recall rates for this approach.

L. Yang et al. [21] introduced PWPAE, a framework for adaptive IoT drift detection of anomalies using advanced change management techniques. PWPAE's adaptability to concept drift enables effective detection of IoT threats, surpassing alternative methods in accuracy based on evaluations using the IoTID20 and CICIDS2017 datasets.

3 Methodology

The The AWDD algorithm is a framework for adjusting window size and updating a model in response to observed data drifts. It comprises crucial methods such as initialization, partial fit and fit, prediction, drift detection, and window size change. The notation W_t indicates the

Received: July 20, 2025

current window size at time t, whereas X_t represents the data stream observed at time t. The adaptive windowing method dynamically modifies W_t in response to identified drift. The goal of this technique is to maximize the sensitivity to idea drift while decreasing the amount of false alarms. According to AWDD, the update rule for W_t may be represented in the following manner:

$$W_t = \begin{cases} 2X\, W_{t-1} & \text{if drift detected} \\ W_t & \text{otherwise} \end{cases}$$

Where,

- W_{t-1} is the previous window size.
- If drift is realized, the size of the window is doubled to increase sensitivity to changes in the information distribution.
- If no detects a shift, window size remains unchanged to maintain stability.

The choice to detect drift is based on statistical testing of the data within the window. These tests examine if the observed changes in data distribution are statistically significant and represent idea drift.. This paper provides a full analysis of the AWDD framework, including its implementation details, design concepts, and empirical assessments using real-world IoT information. We demonstrate the effectiveness and resilience of the AWDD framework in detecting concept drift and maintaining model performance in dynamic Internet of Things scenarios. The XGBoost classifier is the basic classifier, using a gradient boosting ensemble learning method to handle complex data interactions while avoiding overfitting. The AWDD framework is integrated with the XGBoost classifier to build a hybrid model that can learn adaptively and identify drift. The initialization step includes initializing the XGBoost classifier and AWDD settings, setting the base classifier as DecisionTreeClassifier, and defining parameters such as the minimum and maximum window sizes.

Received: July 20, 2025

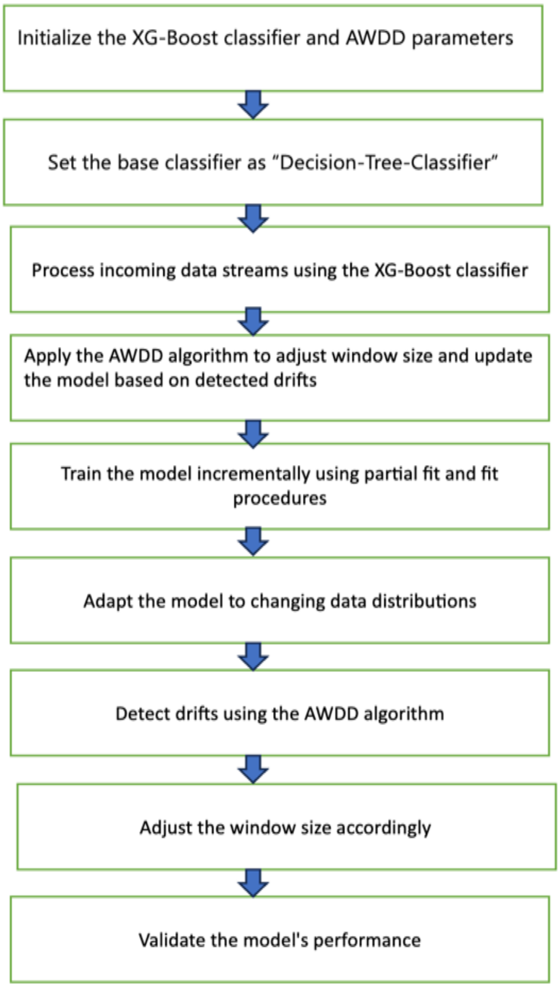
Initialize the XG-Boost classifier and AWDD parameters
Set the base classifier as "Decision-Tree-Classifier"
Process incoming data streams using the XG-Boost classifier
Apply the AWDD algorithm to adjust window size and update the model based on detected drifts
Train the model incrementally using partial fit and fit procedures
Adapt the model to changing data distributions
Detect drifts using the AWDD algorithm
Adjust the window size accordingly
Validate the model's performance

Figure-1 Hybrid AWDD Model for Drift detection

4 Result and Discussion

In this section, we provide a detailed review of the performance of our proposed Hybrid model, Adaptive Windowing Drift Detection (AWDD), in detecting drift events in continuous data streams. We undertake a thorough analysis of AWDD's capabilities and effectiveness in real-time anomaly detection and adaptive learning, employing a variety of assessment metrics and visualizations such as confusion matrices, ROC curves, and accuracy trend charts. These findings provide crucial information into the model's F1 score, recall, accuracy, and capacity to differentiate between drift and non-drift cases, demonstrating its potential for major advances in numerous applications and sectors.

Received: July 20, 2025

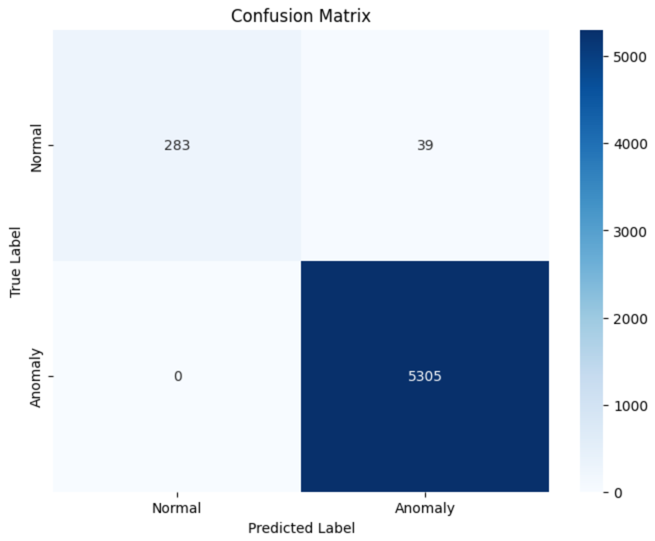

Figure-2 AWDD Confusion Matrix

Our suggested model, Hybrid Adaptive Windowing Drift Detection (AWDD), accurately recognized 283 examples out of 5627 as true positives (TP) based on the presented confusion matrix [Figure-3], demonstrating its capacity to detect the positive class when present. Nonetheless, there were cases of incorrect categorization. 39 cases were mistakenly classified as false positives (FP), meaning that they were positively identified when they were actually negative. Interestingly, the model did not generate any false negatives (FN), meaning that there were no instances of positive samples being missed. Furthermore, the model's ability to identify negative scenarios is demonstrated by the fact that the majority of examples (5305) were correctly classified as true negatives (TN). Overall, even though our AWDD model did a good job of recognizing real positives and true negatives, there is still space for development in terms of lowering false positives to increase overall accuracy.

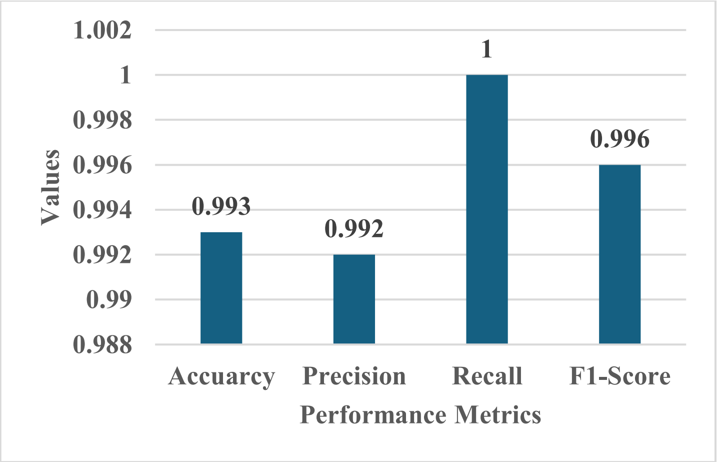

Figure-3 Performance data of Hybrid Model

Received: July 20, 2025

Hybrid Adaptive Windowing Drift Detection (AWDD), outperforms other models in a variety of critical measures [Figure-4]. With an accuracy percentage of 99.3%, AWDD excels at distinguishing drift from non-drift circumstances. The model's high 99.2% accuracy score demonstrates its ability to recognize drift events accurately while reducing false alarms.

Furthermore, achieving a flawless recall score of 100% demonstrates AWDD's capacity to detect all instances of drift, ensuring thorough detection without missing any potential anomalies. The F1-score of 99.6% represents the model's balanced performance in terms of accuracy and recall, demonstrating its durability in the face of varying drift situations. These astonishing results highlight AWDD's usefulness as a trustworthy solution for real-time anomaly detection and adaptive learning, enabling major gains in diverse applications and sectors.

Our study in real-time anomaly detection and adaptive learning has given us priceless insights into the hybrid Adaptive Windowing Drift Detection (AWDD) model's performance and capabilities. An in-depth investigation of the confusion matrix revealed a remarkable lack of false negatives, demonstrating AWDD's robustness in recognizing positive cases without disregarding them. This emphasizes the model's efficacy in discriminating between instances of drift and those without. However, the presence of false positives indicates room for improvement to minimize incorrect classifications. The impressive precision of 99.3%, accuracy of 99.2%, recall of 100%, and F1-score of 99.6% highlight AWDD's exceptional accuracy and ability to fully identify drift events. The ROC curve further emphasizes its outstanding predictive ability, with an impressive AUC value of 0.94, signifying strong discriminatory power.

5 Conclusion

In summary, our study revealed the efficacy and potential value of the combined XGBoost and Adaptive Windowing Drift Detection (AWDD) model in the essential task of real-time anomaly detection and adaptive learning. Through rigorous analysis and evaluation, we have uncovered AWDD's capacity to accurately discriminate drift and non-drift scenarios inside continuous data streams.

The investigation of multiple performance parameters, such as F1-score, recall, and precision, demonstrated AWDD's robustness and dependability in detecting drift events while limiting false alarms. Furthermore, the outstanding Area Under the Curve (AUC) value in the ROC curve analysis confirms AWDD's predictive and discriminatory abilities, establishing it as a versatile tool for a wide range of applications. The accuracy trend plot shows a constant rising slope, suggesting AWDD's adaptability and proficiency in recognizing shifts in data distribution over time. This adaptability is vital in dynamic contexts with constantly developing data patterns. Our discoveries have far-reaching consequences, including possible applications in cybersecurity, financial surveillance, industrial process control, and other areas. Further research and development in this area holds potential for enhancing AWDD's capabilities and

Received: July 20, 2025

unlocking new prospects in the ever-changing landscape of data analytics and decision-making technology.

Future Scope

The hybrid AWDD model's promising performance in real-time anomaly identification paves the way for future study and applications. One potential option is to investigate advanced machine learning algorithms for improving the model's accuracy and resilience in recognizing complex drift patterns. Integrating AWDD with sensor networks and IoT devices may enable real-time monitoring and detection of anomalies across numerous sectors, including manufacturing, banking, and healthcare.

References

[1] A. K. Shukla and A. Sharma, “Cloud Data Security by Hybrid Machine Learning and Cryptosystem Approach”, Int J Intell Syst Appl Eng, vol. 12, no. 2s, pp. 01–14, Oct. 2023.

[2] A. K. Shukla and A. Sharma, "Cloud Base Intrusion Detection System using Convolutional and Supervised Machine Learning," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10112007.

[3] A. K. Shukla and A. Sharma, "Classification and Mitigation of DDOS attacks Based on Self-Organizing Map and Support Vector Machine," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10111988.

[4] W. Yassin, N. I. Udzir, Z. Muda, A. Abdullah and M. T. Abdullah, "A Cloud-based Intrusion Detection Service framework," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 2012, pp. 213-218, doi: 10.1109/CyberSec.2012.6246098.

[5] W. Elmasry, A. Akbulut, and A. H. Zaim, “A Design of an Integrated Cloud-based Intrusion Detection System with Third Party Cloud Service,” Open Comput. Sci., vol. 11, no. 1, pp. 365–379, 2021, doi: 10.1515/comp-2020-0214.

[6] D. Chou and M. Jiang, “A Survey on Data-driven Network Intrusion Detection,” ACM Comput. Surv., vol. 54, no. 9, 2022, doi: 10.1145/3472753.

[7] I. Chouchen and F. Jemili, “Intrusion Detection based on Incremental Learning,” Proc. - 2023 Int. Conf. Cyberworlds, CW 2023, pp. 448–455, 2023, doi: 10.1109/CW58918.2023.00075.

[8] Y. Sun, Z. Wang, H. Liu, C. Du, and J. Yuan, “Online Ensemble Using Adaptive Windowing for Data Streams with Concept Drift,” Int. J. Distrib. Sens. Networks, vol. 2016, 2016, doi: 10.1155/2016/4218973.

[9] A. K. Shukla and A. Sharma, "Distributed Attacks Classification Based on Radical Basis Function and Particle Swarm Optimization In Hypervisor Layer," 2023 6th International

Received: July 20, 2025

Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-4, doi: 10.1109/ISCON57294.2023.10112162.

[10] A. K. Shukla and A. Sharma, "Reduce false intrusion alerts by using PSO feature selection in NSL-KDD dataset," 8th International Conference on Computing in Engineering and Technology (ICCET 2023), Hybrid Conference, Patna, India, 2023, pp. 226-231, doi: 10.1049/icp.2023.1495.

[11] L. Yang and A. Shami, "A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams," IEEE Internet Things Mag., vol. 4, no. 2, pp. 96–101, 2021, doi: 10.1109/iotm.0001.2100012

[12] M. Hassani, "Concept drift detection of event streams using an adaptive window," Proc. - Eur. Counc. Model. Simulation, ECMS, vol. 33, no. 1, pp. 230–239, 2019, doi: 10.7148/2019-0230.

[13] Z. E. Aydin and Z. K. Ozturk, "Performance Analysis of XGBoost Classifier with Missing Data," 1st Int. Conf. Comput. Mach. Intell., no. February, 2021, [Online]. Available: https://www.researchgate.net/publication/350135431

[14] R. Chu, P. Jin, H. Qiao, and Q. Feng, "Intrusion detection in the IoT data streams using concept drift localization," AIMS Math., vol. 9, no. 1, pp. 1535–1561, 2024, doi: 10.3934/math.2024076

[15] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," J. Netw. Comput. Appl., vol. 77, no. October 2016, pp. 18–47, 2017, doi: 10.1016/j.jnca.2016.10.015.

[16] D. K. Talapula, A. Kumar, K. K. Ravulakollu, and M. Kumar, "A hybrid deep learning classifier and Optimized Key Windowing approach for drift detection and adaption," Decis. Anal. J., vol. 6, no. October 2022, p. 100178, 2023, doi: 10.1016/j.dajour.2023.100178.

[17] H. Mehmood, A. Khalid, P. Kostakos, E. Gilman, and S. Pirttikangas, "A novel Edge architecture and solution for detecting concept drift in smart environments," Futur. Gener. Comput. Syst., vol. 150, no. 2024, pp. 127–143, 2024, doi: 10.1016/j.future.2023.08.023.

[18] P. B. Dongre and L. G. Malik, "A review on real time data stream classification and adapting to various concept drift scenarios," Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014, pp. 533–537, 2014, doi: 10.1109/IAdCC.2014.6779381.

[19] Q. Zhu, X. Hu, Y. Zhang, P. Li, and X. Wu, "A double-window-based classification algorithm for concept drifting data streams," Proc. - 2010 IEEE Int. Conf. Granul. Comput. GrC 2010, pp. 639–644, 2010, doi: 10.1109/GrC.2010.125.

[20] S. Seth, G. Singh, and K. K. Chahal, "Drift-based approach for evolving data stream classification in Intrusion detection system," CEUR Workshop Proc., vol. 2889, pp. 23–30, 2021.

[21] L. Yang, D. M. Manias, and A. Shami, "PWPAE: An Ensemble Framework for Concept Drift Adaptation in IoT Data Streams," Proc. - IEEE Glob. Commun. Conf. GLOBECOM, pp. 1–6, 2021, doi: 10.1109/GLOBECOM46510.2021.9685338.

Received: July 20, 2025