O‘ZBEKISTON RESPUBLIKASI
RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARIUNIVERSITETI
SAMARQAND FILIALI

“RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKT: MUOMMOLAR, YUTUQLAR VA RIVOJLANISH ISTIQBOLLARI”

MAVZUSIDAGI XALQARO
ILMIY-AMALIY ANJUMANI MA’RUZALAR TO‘PLAMI
2025 yil 24-25 oktabr

II TOM

СБОРНИК ДОКЛАДОВ
Международная научно-практической конференции

“ ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ, ДОСТИЖЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ”

октябрь 24-25, 2025

O‘ZBEKISTON RESPUBLIKASI
RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI SAMARQAND FILIALI

“RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKT: MUOMMOLAR, YUTUQLAR VA RIVOJLANISH ISTIQBOLLARI” MAVZUSIDAGI XALQARO ILMIY-AMALIY ANJUMANI MA’RUZALAR TO‘PLAMI

24-25- oktabr 2025-yil

II TOM

СБОРНИК ДОКЛАДОВ МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ “ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ, ДОСТИЖЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ”

24-25- октября 2025 года

SAMARQAND 2025

KONFERENSIYA TASHKILIY QO‘MITASINING
T A R K I B I:

Z. A. Karshiyev	Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali direktori
A.R.Axmedjonov	Ilmiy ishlar va innovatsiyalar bo‘yicha direktor o‘rinbosari
O.M.Rajabov	Yoshlar masalalari va ma’naviy-ma’rifiy ishlar bo’yicha direktorning birinchi o’rinbosari
D.K. Yakubjanova	O‘quv ishlari bo‘yicha direktor o‘rinbosari
Sh.Y.Isroilov	Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlarni tayyorlash bo‘limi boshlig‘i
U.X. Narzullayev	Telekommunikatsiya texnologiyalari va kasb ta’limi fakulteti dekani
B.A. Nazarov	Kompyuter injiniringi fakulteti dekani
A.S.Kurbaniyazov	O‘quv-uslubi boshqarma boshlig‘i

DASTURIY QO‘MITA TARKIBI:

R.Sh. Indiaminov	Tabiiy fanlar kafedrasi professori
A.B. Qarshiyev	Dasturiy injiniring kafedrasi professori
M.U.Yaxshiboyev	Tabiiy fanlar kafedrasi mudiri
X.A. Primova	Axborot texnologiyalari kafedrasi professori
N.I. Abdullayeva	Kompyuter tizimlari kafedrasi mudiri
I.M. Boynazarov	Dasturiy injiniring kafedrasi mudiri
I.Sh. Xujayarov	Axborot texnologiyalari kafedrasi mudiri
N.R. Zaynalov	Axborot xavfsizligi kafedrasi mudiri
X.E. Raxmanov	Axborot ta’lim texnologiyalari kafedrasi mudiri
X.B. Mirzokulov	Telekommunikatsiya injiniringgi kafedrasi mudiri
D.F.Toirova	Tillar kafedrasi mudiri
X. Samatov	Ijtimoiy gumanitar fanlar kafedrasi mudiri

To‘plam TATU Samarqand filiali Kengashining 2025-yil 30-sentabrda o‘tkazilgan 2-sonli yig‘ilish qarori bilan chop etishga tavsiya etilgan

5-SHO‘BA

MA’LUMOT UZATISH TARMOQLARI VA AXBOROT XAVFSIZLIGI MUAMMOLARI

DRIFT-AWARE ONLINE LEARNING FOR INTRUSION DETECTION

G. Juraev[1], N. Zaynalov[2], D. Kilichev[3], N. Saydirasulov[4], D. Turimov[4]
[1]National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan
[2]Samarkand branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan
[3]Samarkand branch of Tashkent state university of economics, Uzbekistan
[4]Gachon University, Republic of Korea
dusmurod@gachon.ac.kr

Abstarct. *Intrusion patterns change over time, which makes static models lose accuracy. We present a simple online intrusion detection approach that pairs Adaptive Random Forest (ARF) with the ADWIN drift detector. The system learns one event at a time and refreshes itself automatically when the data distribution shifts. Using the CICEVSE2024 network-traffic dataset, the method delivers strong performance for both binary and multiclass detection and keeps working well during drift events. In our tests, the online model reached about 99.1% accuracy for binary detection and 98.4% for multiclass, while processing each instance in about 0.0037 s, which fits real-time needs.*

Keywords: *Adaptive Random Forest, Concept Drift, Online Machine Learning, Anomaly Detection, Cybersecurity.*

Introduction

The rapid growth of connected systems and digital infrastructures has increased the scale and complexity of cybersecurity threats. Traditional intrusion detection systems (IDSs) rely on models trained with historical data and therefore assume that data distributions remain constant over time. However, in real-world environments, the nature of cyberattacks evolves continuously, leading to concept drift — changes in the statistical properties of data streams that cause models to become outdated and less effective. As a result, static IDS models often fail to detect new or modified attack patterns, which can compromise system reliability and security [1].

To address this challenge, online machine learning has emerged as a promising approach that allows models to learn incrementally from streaming data. Unlike batch learning, online algorithms update their parameters continuously as new data arrives, making them suitable for non-stationary environments. Among these methods, the Adaptive Random Forest (ARF), combined with ADaptive WINdowing (ADWIN) drift detection, provides an efficient and scalable framework for handling evolving data streams. ARF ensembles multiple incremental decision trees, each capable of adapting to changes in data distribution, while ADWIN detects drift by monitoring changes in error rates and dynamically adjusting the training window [2].

This research focuses on developing a drift-aware online learning framework for intrusion detection that can adapt to evolving threats in real time. The proposed approach integrates ARF and ADWIN to automatically identify and respond to concept drift, ensuring continuous model relevance without full retraining. The framework is designed to operate in streaming cybersecurity contexts, where data arrives sequentially, and rapid decision-making is critical [3].

Methods

The proposed method implements a drift-aware online learning framework for real-time intrusion detection in streaming cybersecurity data. The system integrates the Adaptive Random Forest (ARF) classifier with the ADaptive WINdowing (ADWIN) drift detector to identify and adapt to changes in data distribution. The framework continuously updates the learning model as new instances arrive, maintaining accuracy under concept drift while minimizing computational overhead [3].

The approach is evaluated using the CICEVSE2024 dataset, which contains labeled network traffic captured from electric vehicle charging communication protocols, including ISO 15118, OCPP, and OCPI. Each record represents an event characterized by numerical and categorical features extracted from packet-level data such as message type, direction, payload size,

and timing intervals. Before training, the data stream is normalized and transformed into incremental batches suitable for online learning. Features with missing or irrelevant values are removed, and categorical variables are encoded using one-hot encoding. The dataset is then streamed instance-by-instance to the online learner, simulating a real-time intrusion detection environment [4].

The Adaptive Random Forest (ARF) algorithm serves as the core classifier. It consists of an ensemble of incremental decision trees, each trained using online bagging. Leaf nodes employ adaptive Naïve Bayes classifiers to improve prediction accuracy on non-stationary data. Each tree independently learns from incoming data, while the ensemble aggregates predictions through majority voting.
This design enhances robustness by allowing individual trees to specialize in different regions of the data distribution, ensuring resilience against sudden distributional changes.

The ADWIN algorithm monitors the model's prediction error rate over a sliding window. When a statistically significant change in the error rate is detected, ADWIN triggers a drift event, prompting the replacement or retraining of affected trees in the ensemble. This adaptive mechanism ensures that the model dynamically responds to both abrupt and gradual concept drifts without full retraining.
The combined ARF–ADWIN architecture thus supports continuous adaptation, balancing learning stability and reactivity.

Experimental Results

The proposed drift-aware intrusion detection framework was implemented in Python using the *River* online learning library. All experiments were performed on a workstation with an Intel Core i7 processor and 16 GB RAM. The CICEVSE2024 dataset was used to simulate streaming network traffic from electric vehicle charging systems, containing both benign and malicious communication sessions. Data instances were streamed sequentially to mimic real-time operational conditions, and model parameters were updated incrementally after each instance.

For comparison, the performance of the Adaptive Random Forest (ARF) with ADWIN drift detection was benchmarked against static classifiers, including *Random Forest (RF)* and *Support Vector Machine (SVM)* [1].

Authors	Year	Dataset	Model	Learning Method	Class	Accuracy	Precision	Recall	F1-Score
Buedi et al. [46]	2024	CICEVSE2024: Network Traffic	Random Forest	offline	15	0.9374	0.9694	0.9374	0.9478
			Support Vector Machine	offline	15	0.9413	0.9151	0.9413	0.9280
Bozömeroğlu et al. [49]	2024	CICEVSE2024: Network Traffic	Decision Tree	offline	13	0.9999	0.9999	0.9999	0.9999
Purohit et al. [50]	2024	CICEVSE2024: Network Traffic	Federated Learning	federated	2	0.9697	-	-	0.9740
Rahman et al. [51]	2025	CICEVSE2024: Host Data	Deep Learning	offline	3	0.9754	0.9757	0.9754	0.9754
Benfarhat et al. [52]	2025	CICEVSE2024: Host Data	Temporal Convolutional Network	offline	2 5 17	1.0 1.0 0.9300	- - -	- - -	- - -
Our Proposed Model	2025	CICEVSE2024: Network Traffic	Adaptive Random Forest	online	2 15	0.9913 0.9840	0.9999 0.9840	0.9914 0.9840	0.9956 0.9831

Table 1: *Model performance summary*

Table 1 summarizes the results for both classification tasks. The proposed ARF–ADWIN model achieved a binary detection accuracy of 99.13%, with precision of 99.99%, recall of 99.14%, and an F1-score of 99.56%. In the multiclass task, the framework maintained an average accuracy of 98.40%, precision and recall of 98.40%, and an F1-score of 98.31%.

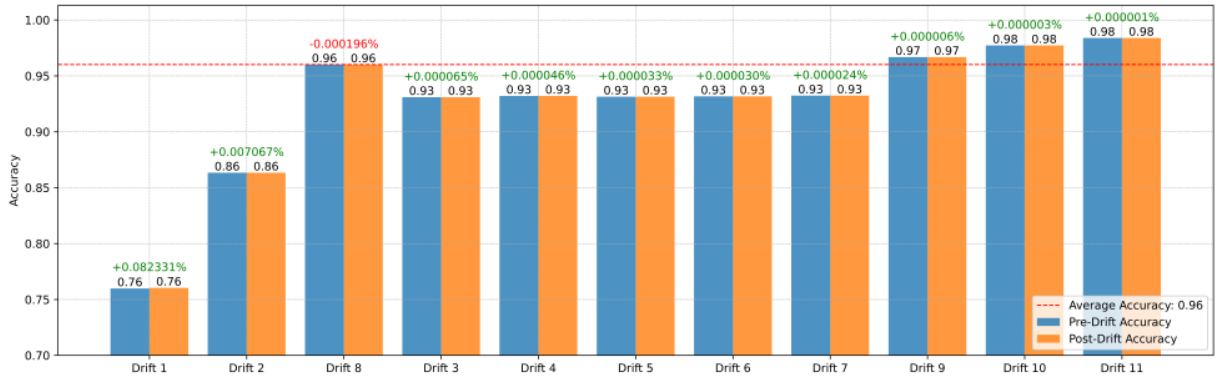

Figure 1: *Accuracy trend under drift*

Importantly, during concept drift events, the system maintained an average accuracy of 99% in binary mode and 96% in multiclass mode, demonstrating effective drift handling. The model processed each data instance in 0.0037 seconds, confirming its suitability for real-time intrusion detection applications.

Compared to baseline models, ARF–ADWIN outperformed RF and SVM by 3–5% in overall accuracy and adapted significantly faster after drift occurrences. Figure 1 illustrates the model's accuracy over time, showing minor fluctuations during drift and rapid recovery afterward [1].

The results confirm that combining adaptive ensemble learning with statistical drift detection provides robust, scalable, and efficient intrusion detection in streaming environments. The ARF–ADWIN framework consistently maintained high accuracy and low latency, even as attack patterns evolved. This demonstrates the potential of online machine learning for real-time cybersecurity, reducing dependence on static retraining and improving system resilience to new or unseen threats.

Conclusions

This study presented a drift-aware online learning framework for intrusion detection in streaming cybersecurity data. By combining the Adaptive Random Forest (ARF) algorithm with the ADaptive WINdowing (ADWIN) drift detector, the proposed system effectively identified and adapted to evolving attack patterns in real time. The framework continuously learned from streaming data, updating its model without the need for full retraining, thus addressing one of the major limitations of traditional, static intrusion detection systems.

- References

1. Makhmudov, F.; Kilichev, D.; Giyosov, U.; Akhmedov, F. Online Machine Learning for Intrusion Detection in Electric Vehicle Charging Systems. *Mathematics* 2025, *13*, 712. https://doi.org/10.3390/math13050712

2. Kilichev, D.; Kim, W. Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO. *Mathematics* 2023, *11*, 3724. https://doi.org/10.3390/math11173724

3. A. Abdusalomov, D. Kilichev, R. Nasimov, I. Rakhmatullayev and Y. Im Cho, "Optimizing Smart Home Intrusion Detection With Harmony-Enhanced Extra Trees," in IEEE Access, vol. 12, pp. 117761-117786, 2024, doi: 10.1109/ACCESS.2024.3422999

4. Kilichev, D.; Turimov, D.; Kim, W. Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models. *Mathematics* 2024, *12*, 571. https://doi.org/10.3390/math12040571

6-SHO‘BA. RAQAMLI MODELLASHTIRISH VA HISOBLASH USULLARI

“RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKT: MUOMMOLAR, YUTUQLAR VA RIVOJLANISH ISTIQBOLLARI” MAVZUSIDAGI XALQARO ILMIY-AMALIY ANJUMANI

MA’RUZALAR TO‘PLAMI

24-25 oktabr 2025-yil

II TOM

“DOKTOR POLIGRAF” MChJ. nashriyot - matbaa ijodiy bo`limi,

Samarqand - 2022.

Tasdiqnona № 12364 (17.03.2015)

Chop etishga ruxsat etildi: 15.10.2025 y.

22.10.2025 yilda chop etildi.

Qog‘oz bichimi A5, 60x84 1/8, Ofset qog‘ozi.

“Times New Roman” garniturasi.

Nashr bosma tabog‘i 48,75

Buyurtma № 005/23A. Adadi 25 nusxa

“DOKTOR POLIGRAF” MChJ.

Nashriyot - matbaa bo‘limida chop etildi.

Tasdiqnona № 12364 (17.03.2015)

Manzil: Samarqand vil. Samarqand sh. Buyuk Ipak Yo`li.