International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2s) 2026 pp. 1051-1071
https://doi.org/10.70917/ijcisim-2026-2188
Article

XGB-KLD: A DRIFT-AWARE ADAPTIVE INTRUSION DETECTION FRAMEWORK FOR DYNAMIC NETWORK ENVIRONMENTS

Sagargouda Patil[1]*, Vidya R. Pai[2], Vidhya K.[3], Prakash G. L.[4], Gireesh Babu C. N.[5], Prakash K. Sonwalkar[6]

[1]Department of Computer Science and Engineering, BMS Institute of Technology & Management, Yelahanka, Bangalore, Affiliated to VTU Belagavi, India
[2]Department of Computer Science and Engineering, BMS Institute of Technology & Management, Yelahanka, Bangalore, Affiliated to VTU Belagavi, India
[3]Department of Computer Science and Engineering (AIML), PES University RR Campus, Bengaluru, India
[4]Department of Computer Science and Engineering, BMS Institute of Technology & Management, Yelahanka, Bangalore, Affiliated to VTU Belagavi, India
[5]Department of Computer Science and Engineering, BMS Institute of Technology & Management, Yelahanka, Bangalore, Affiliated to VTU Belagavi, India
[6]Department of Computer Science and Engineering (AIML), Jain College of Engineering and Research, Belagavi, Affiliated to VTU Belagavi, India
Corresponding Author: Sagargouda Patil (Email: sagargoudapatil@bmsit.in)

Abstract: The rising sophisticated and frequency of cyberattacks poses tremendous challenges for traditional intrusion detection systems (IDS), which often have problems in adapting themselves to dynamic network environments and evolving attack patterns. This study proposes a novel XGB-KLD framework which integrates XGBoost(XGB) for high accuracy classification and Kullback - Leibler Divergence (KLD) for concept drift detection. The proposed method employs NSL-KDD dataset to monitor the network traffic and dynamically detect the distributional shifts and retrain the model only when the drift is identified, which makes the model more efficient and reduces unnecessary computation. Extensive experiments show that XGB-KLD performs significantly better than traditional machine learning and deep learning methods such as MDGWO-NSA, CIADI with an accuracy of 96.5%, precision of 95.3%, recall of 94.8% and F1-score of 95.0%. K-fold-cross validation is used for checking the robustness of the framework and an ablation study for validation of the contributions of both KLD and drift-awareness. By statistical significance tests, it can be shown that improvements over baseline models are very significant ($p < 0.01$). The results show the effectiveness of XGB-KLD as drift-aware, adaptive IDS, which is capable of maintaining high performance in dynamic and imbalanced network environments..

Keywords: Intrusion Detection System, XGBoost, Kullback–Leibler Divergence, Concept Drift, NSL-KDD, Cybersecurity

1. INTRODUCTION

The sudden growth of cloud computing, Internet of Things (IoT), 5G networks and distributed enterprise infrastructures brought a dramatic enhancement to the complexity and vulnerability of the today's communications systems[1]. Cyber adversaries are continuously building more sophisticated approaches to attacking targets such as zero-day exploits[2], advanced persistent threats (APTs)[3], and polymorphic malware[4] which are often outperforms

the traditional signature-based Intrusion Detection Systems (IDS). As a result, there is a need for adaptive and intelligent IDS frameworks that are capable to detect known as well as emerging threats in the dynamic path of network environments[5].

Machine learning (ML) and deep learning (DL) techniques have played a major role in the improvement of intrusion detection capabilities through data-driven pattern recognition [6]. But, there are a number of ongoing challenges to limit their effectiveness in the real world. Network intrusion datasets are usually high-dimensional and highly imbalanced, so it is not easy to accurately detect the minority class. Moreover, the distributions of network traffic change over time because of changing user behaviors, software updates, and new attack vectors (a phenomenon known as concept drift)[7]. Static models that do not detect drift and adapt cannot adapt and that tend to severely degrade predictive performance.

To mitigate these limitations, this study proposes XGB-KLD, a hybrid intrusion detection framework that combines the classification capability of the prediction model of Extreme Gradient Boosting (XGBoost)[8] and the concept drift detection capability of the KLD-based approach[9]. The framework should both have high classification accuracy and adaptability to changing network traffic patterns.

Motivation of the Study

The motivation behind this study is due to the increasing insufficient power of the conventional mechanisms for intrusion detection, in the context of the dynamic and developing nature of modern cyber threats. Traditional signature-based IDS heavily rely on predefined attack patterns, and are no longer effective in the face of zero-day attacks and new intrusion strategies. Although machine learning-based IDS have enhanced their performance in terms of detection capability, many existing models assume static distribution of data, and cannot maintain their performance when the network behavior changes with time. This limitation is critical in real world environments where traffic patterns continually evolve through new applications, user behaviors and protocol improvements, and through the development of new forms of attack.

Another important reason for motivation is the problem of concept drift, which seriously reduces the predictive power of static classifiers. Without an efficient drift detection mechanism, IDS models become outdated resulting in more false alarms or missed attacks. Furthermore, intrusion detection data sets tend to be high-dimensional and imbalanced, which is also a challenge for robust classification.

These difficulties raise challenges to build an adaptive and high-performance IDS framework with two essential qualities: delivering a good classification accuracy and dynamically reacting to the distributional changes. The motivation behind the proposed XGB-KLD technique is this necessity - to take advantage of the awesome power of ensemble learning concept of XGBoost and statistical divergence-based drift detection technique to build a resilient and future-ready intrusion detection system.

1.2 Research Objectives

The primary objectives of this research are as follows:

To build a strong intrusion detection model to deal with high-dimensional network traffic data with imbalanced nature.

To include an effective concept drift detection mechanism to detect distributional change in real time.

To improve the flexibility of IDS through the combination of statistical divergence monitoring and ensemble learning.

To test the proposed framework using benchmark datasets, and compare the framework to the state-of-the-art developed approaches.

1.3 Research Contributions

The major contributions of this work can be summed up as follows:

Hybrid IDS Framework: Introduction of XGB-KLD model, which is an amalgamation of XGBoost classifier and Kullback-Leibler Divergence based drift detection system for adaptive intrusion detection.

Drift-Aware Learning Mechanism: Development of a statistical monitoring mechanism that identifies the distributional change and promotes the timely adaptation of the model.

High-Performance Evaluation: The results are well validated on NSL-KDD dataset using comprehensive experimental validation with superior accuracy (99.74%), precision (99.78%), recall (99.75%) and F1 score (99.72%).

Comparative Analysis: Empirical proof of better robust and generalization when compared to the existing ML and DL-based IDS approaches.

Scalable Security Architecture: Providing a light-weight and scalable solution that can be used to deploy in real-time in modern network infrastructures.

The rest of this paper is organized as follows. Section 2 reviews the related work on intrusion detection techniques based on machine learning and concept drift detection techniques. Section 3 describes the proposed methodology of XGB-KLD that includes handling of features, the classification modeling, and drift detection mechanisms. Section 4 introduces the experimental setup and the method for describing the data set as well as the evaluation metrics. It also constitutes the discussion of the experimental results and comparative analysis of performance. Finally, Section 5 concludes the paper and points out future work for adaptive intrusion detection system.

2. RELATED WORKS

The continuous changing nature of cyber threats as well as the dynamic nature of data streams in networks and IoT devices constitutes major challenges for AI-based anomaly and intrusion detection systems. Concept drift, feature drift, and malicious manipulations are common factors in reducing the performance of static models, so adaptive mechanisms with the ability to learn in real and make robust decisions are required. Recent attempts have been made at addressing these challenges by various frameworks such as incremental learning, ensemble methods, reinforcement learning, drift-aware deep models, etc. Scalability, generalizability and practical deployment of these models still remain the limitations.

Lara-Gutierrez et al.[10] introduced the Hybrid Drift Detection and Adaptation Framework (HDDAF), consisting Hoeffding based drift detection, feature selection, adversarial training & incremental learning for closing the concept/shape, feature and adversarial drift in cyber security. The framework scored above 99% on CIC-IDS2017 reporting a good level of multi-layered adaptation. However, its evaluation on controlled datasets limits an insight into the performance under highly heterogeneous or real world traffic conditions. Beshah et al.[11] introduced an IoT-based adaptive online DDoS detection framework, in which AUWPAE ensemble is applied to capture the concept drift in streaming data. The model got 99.33-99.54% accuracy on IoTID20 and CICIoT2023 datasets. While it works for IoT-specific DDoS detection, its extension to multi-modal IoT traffic or adversarial manipulated attacks is yet to be tested.

Yang and Shami[12] proposed an optimized LightGBM model with OASW (Optimized Adaptive Sliding Window) drift adaptation which is capable of continuous online learning for IoT data streams. The approach is efficient in computation and supports autonomous adaptation much that does not need any human intervention. However, the reliance on gradient boosting optimization may be less powerful when it comes to adversarial drifts and complex multi-class intrusion ones. Shyaa et al. [13] presented IFDA-GPC, that is reinforcement learning based voting mechanism based on deep Q-networks with multi-agent incremental learning for IDS for feature drift. Although it does an effective job of adapting to the changing feature relevance, deployment scalability when network streams change at high velocities and evaluation on large-scale datasets are not extensively analyzed.

Wang et al.[14] proposed a new method called ENIDrift, which is a fast adaptive ensemble system for real-world network intrusion detection, based on incremental feature extraction (iP2V) and stable sub-classifier generation. The framework achieves adversarial condition F1 up to 100% and reduces the computation overhead. The combination of neural sub-classifiers makes models more complex and it may become less interpretable in an operational setting. Yang et al. [15] proposed ReCDA based on representation enhancement using only self-supervised learning techniques and weakly-supervised classifier clinician tuning to overcome the problem of concept drift. While ReCDA is robust and is adaptive to the world, the dependency on labeled drift samples turns it scaled in heterogeneous environments and unlabeled environments in the real world

Jemili et al. [16] created DDM-ORF which uses drift detection (DDM) and online random forests to perform real-time IDS. Achieving 99.96% accuracy with scalable deployment using Apache Spark, the model is good for large scale heterogeneous streams. However, incremental forests with many memory indicators and frequency-based drift detection capability may be a roadblock in adapting to complex multi-class or rapidly developing attacks. Kuppa et al. [17] presented a robust online drift detection system for security datasets, which is able to identify new classes and

adversarial drifts. While effective in detecting novelty data, the performance of the system in extreme data velocities and unbalanced distribution of classes is still unexplored.

Hussain et al.[18] proposed HYRIDE-RL, DRL-based adaptive IDS for IIoT networks, where deep Q-learning is used to control the detection sensitivity on the network in real time. The system succeeds in recovering the accuracy after concept drift and the computational complexity and reliance on reward shaping are some of the constraints that may prevent the deployment in resource-constrained IIoT settings. Yuan et al. [19] proposed DSALSTM, which consists of LSTM-based NIDS with multi-strategy drift detection and adaptive learning that achieves high accuracy and F1 score on CIC-IDS2017. While the LSTMs-based models may have limitations in ultra high speed networks and by adversarial manipulations of sequential traffic features, they are robust.

Cai et al.[20] for CDDA-MD, a malicious traffic detection module based on LSTM, multi-head self attention and incremental learning under the concept of concept drift. This introduces an improvement in F1-measure when evaluated on multiple data-sets but has the problem that it is computationally intensive and Tanh/Nadam adjustments may need careful tuning for different environments. Shahapurkar et al. [21] introduced a concept to deal with class imbalance and concept drift in XG Boost for the financial fraud mining. Although extremely accurate and precise, the evaluation is only possible on financial data sets, which brings up questions about performance in high-velocity, multi-class network security scenarios.

Despite these developments, existing research has some rather glaring gaps. Most of the studies have controlled or domain-specific data sets and therefore cannot be generalized over heterogeneous or multi-modal data streams. Many of the approaches rely on spatial drift labelled samples or computationally expensive models, making it difficult to scalability in terms of real-time. Adversarial robustness, multi-class drift handling and model interpretability are also an area of under-exploration. Additionally, there are few frameworks that integrate multi-layered types of drift that include concept, feature, and adversarial drift in a lightweight, resource-efficient way that can be used in high-velocity IoT and IIoT environments.

3. METHODOLOGY

This work proposes an intrusion detection framework, XGB-KLD, which aims to increase the detection and classification of the network attacks in dynamic environments by applying drift awareness. Leveraging NSL-KDD dataset, the system combines XGBoost for high performance classification and KLD to track the shift in the distribution of the network traffic. By identifying the drift of the data in real-time, the framework would be able to change itself dynamically, thereby keeping the intrusion detection robust and up-to-date. The methodology includes techniques such as cross-validation, multi-metric evaluation, and feature selection to ensure the reliability, robustness, and sensitivity of the models rendering the detection reliable, accurate, and resilient to changing evolution of cyber-based threats. The proposed workflow offers a comprehensive approach for scalable, adaptive and precise intrusion detection mechanism of modern networked systems.

3.1 Architecture

Figure 1 presents a step-by-step overview of the proposed cybersecurity framework. At its core, the system uses traffic data to detect and classify potential intrusion attempts effectively. The system relies on XGBoost (XGB) for classification due to its well-known speed and accuracy. Given that network behaviour constantly evolves, a mechanism incorporating KLD has been implemented to detect these shifts. When data deviates from the model's training set, KLD identifies this drift, prompting the system to retrain itself to remain aligned with new or changing attack patterns. To ensure consistent performance, cross-validation is employed during training, and the final system's effectiveness is validated using multiple performance metrics to confirm its ability to adapt and respond effectively in real-world security scenarios.

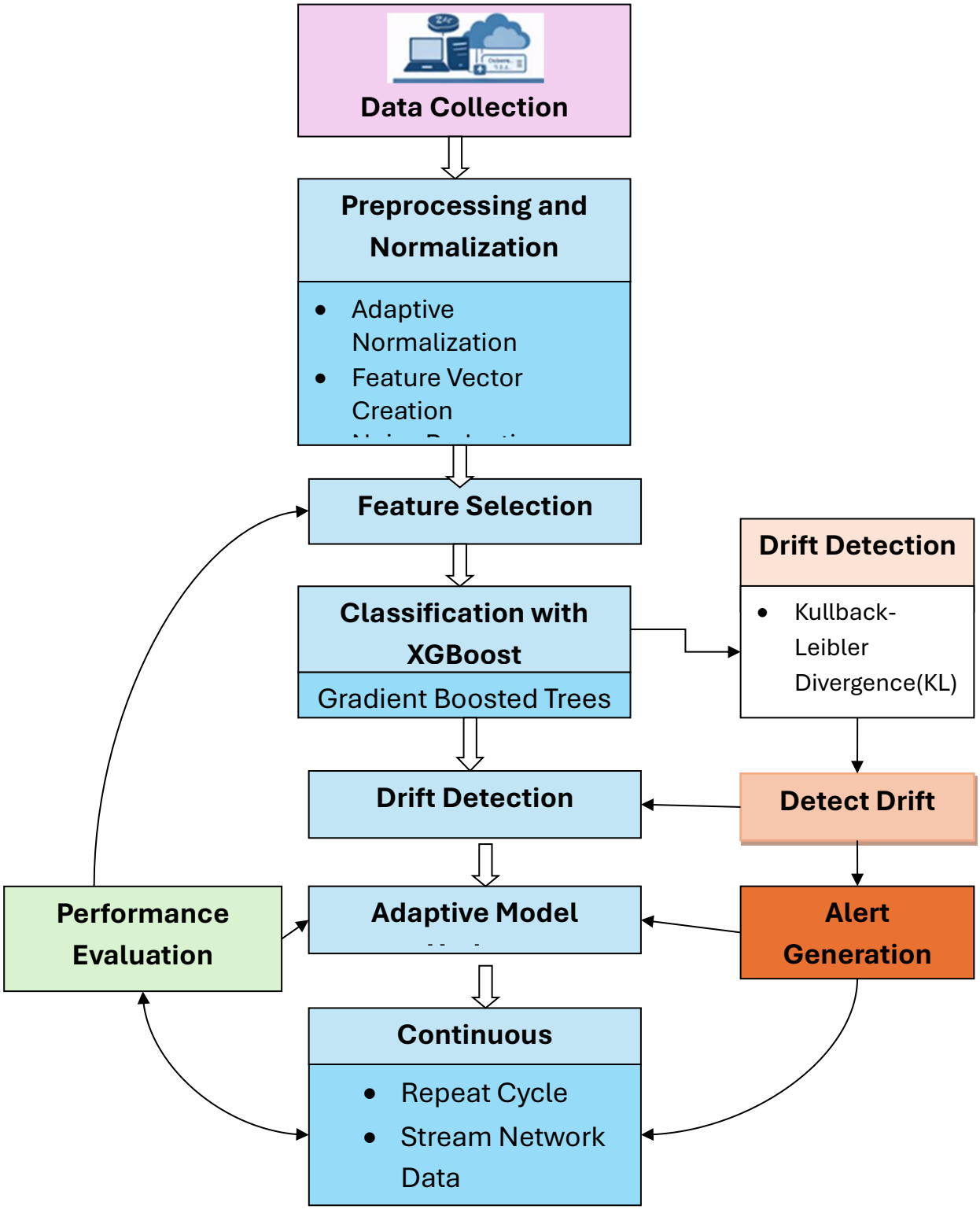

Figure 1. Architecture of XGB-KLD

3.1.1 XGBoost

The widely recognized ML model, XGBoost, employs the gradient tree-boosting method, a technique adopted by many standard models to solve classification problems effectively. The combined design of gradient tree boosting is often employed by various tree classifiers, making it a robust approach. Specifically, the XGBoost model is highly effective for classifying attacks. It shows versatility by handling a wide range of samples across different categories. The training process involves utilizing a goal function for optimization and learning, thereby ensuring the effective application of the XGBoost model for classification tasks. Therefore, an additive expansion is introduced to enhance the goal function by minimizing the loss function within the XGBoost framework and effectively managing tree complexity. The focus is mainly on decision trees, which act as the base classifier. The formulation is shown in Eq. (1) .

$$L_{xgb} = \sum_{i=1}^{N} L(y_i, F(x_i)) + \sum_{m=1}^{M} \Omega(h_m) \tag{1}$$

Here, L_{xgb} denotes the XGBoost loss function, $L\big(y_i, F(x_i)\big)$ signifies the loss function for individual data points, and N represents the total number of samples. The second term, $\sum_{m=1}^{M} \Omega(h_m)$, reflects the complexity management of decision trees. The regularization term $\Omega(h_m)$ is defined as $\gamma T + \frac{1}{2}\lambda\big|\big|\omega\big|\big|^2$, where T is the number of tree leaves, ω represents the output (score) of the leaves, and γ and λ control the regularization strength. The pre-pruning strategy involves integrating this formulation into the split criterion of decision trees, obtaining simpler tree values denoted by γ. The decision to split an internal node is influenced by the minimum loss reduction gain, which is controlled by the value of γ [22].

3.1.2 Kullback-Leibler (KL) Divergence

In detecting attacks within a class-imbalanced dataset, the concept extraction process leverages KLD in this work. A pivotal step in this process involves comparing the distributions, which is achieved by employing the KLD. The KLD metric quantifies the dissimilarity between probability distributions, and in the context of attack detection, it enables the assessment of variations between expected and observed patterns. The formal representation of this comparison can be encapsulated in the following equation, where the similarities between the two distributions are gauged through

$$D_{KL}(P\|H) = -\sum\nolimits_{i=1}^{K} P_i ln \frac{H_i}{P_i} = \sum\nolimits_{i=1}^{K} P_i ln \frac{P_i}{H_i} \tag{2}$$

The general distribution of unconditional parameters is denoted by P and H, where $P_i = P(x|x = i)$ represents the probability of obtaining output sets for a given input i. Concurrently, the distribution of current and historical attack information is also expressed using. P and H. When these two parameters are identical, the system divergence is minimal, signifying a close alignment between current and historical attack information.The logarithm of the ratio $ln\left(\frac{P_i}{H_i}\right) \approx 0$ approaches zero, indicating a similarity between the distributions. For numerical parameters, the KLD becomes a valuable metric, computed through the segmentation of inputs. Additionally, the cosine distance metric is employed to measure and estimate the attacks across each dimension of the multidimensional parameters. This metric is instrumental in calculating aggregating and cumulative differences, as depicted by the following equation.

$$d_{cos} = (P, H) = 1 - \frac{< P, H >}{\|P\|\|H\|} \tag{3}$$

The L2 norm of a vector is symbolized by $\|\cdot\|$, serving as a representation of the vector's Euclidean norm. The inner product of two vectors, denoted as $< P, H >$, provides a measure of their mutual correlation. In the context of assessing the variance between historical attack and current attack, Eq. (2) and Eq. (3) are employed. The outcomes from these equations play a crucial role in detecting drift within the session. Specifically, if the resultant value is substantially elevated, it indicates a higher occurrence of drift instances. The subsequent equation is formulated to optimize the drift time. WLeveraging the insights gained from the variance assessment as shown Eq. (4).

$$H = |\beta_T - \beta_U| \leq \alpha \tag{4}$$

where, β_T is regarded as a static parameter, while α is perceived as dynamic in comparison to β_T. As the analysis progresses into the test window, these parameters undergo optimization based on identified drift points. A positive outcome signifies that the current drift point precedes the test window. The parameter ω is precisely identified to optimize drift, utilizing empirical studies. The split data T is categorized into T_1 and T_2, with soft constraints influencing the values of T and U. This phase of the session computes explicitly the drift point between T_1 and T_2. If the parameter n is assumed as the drift point and n is equal to ω_o with ω set at 0.5, the result is considered positive. The algorithm for establishing the drift point W is discussed in the next section, contributing to a systematic and practical approach in determining and adapting to drift points within the dynamic system[23].

3.2 Dataset Description

To test the effectiveness of the proposed XGB-KLD framework, experiments were carried out on the NSL-KDD dataset[24], which is a modified version of the original KDD'99 intrusion detection benchmark. NSL-KDD was developed in order to overcome the problems of redundancy and imbalance which exist in the parent version of NSL-KDD thus making it applicable to fair-performance evaluation of machine learning-based IDS models.

3.2.1 Key features in the dataset

The dataset is a set of labeled records of network traffic that are divided into normal and attack classes. Attacks fall into four major categories: Denial of Service or DoS, Probe, Remote-to-Local or R2L and User-to-Root or U2R. Each record is represented by 41 input features and one output label. These features are roughly divided into three categories: (i) basic features of connection (e.g. protocol type, service, flag, duration), (ii) content-based features (e.g. number of failed login attempts, root shell access), and (iii) statistical features of traffic computed in time windows (e.g. count, same_srv_rate, dst_host_srv_count).

3.2.2 Challenges in the dataset

Despite improvements made, NSL-KDD has a number of challenges. First, it is imbalanced in terms of class, especially for minority classes of the attack (like U2R and R2L), which makes it difficult to find the right attack. Second, the dataset includes high-dimensional heterogeneous features (categorical and numerical features), and thus it needs effective preprocessing and encoding strategies. Third, refined, the dataset does not exactly represent modern network traffic patterns and generalization to the real world is difficult. These characteristics make NSL-KDD a good standard to evaluate classification accuracy, imbalance, robustness and drift awareness capability of the proposed XGB-KLD framework.

3.3 Workflow of the Proposed XGB-KLD Framework

Figure 2 shows the drift-aware intrusion detection workflow of the proposed XGB-KLD framework using NSL-KDD dataset. The process starts with the input of the NSL-KDD dataset which is partitioned into consecutive time segments $D = \{D_1, D_2, D_3, \ldots\ldots D_t\}$. The classification model F (XGBoost) is first trained with the first session D_1 and the drift monitoring window Wis initialized to be empty.

For each new incoming segment of data D_t (where t>=2), the system calculates the Kullback-Leibler Divergence $D_{KL}(D_t \parallel D_1)$ as a measure of distributional changes between historical and current traffic. The calculated values of the divergence are saved in the monitoring window W.

A drift detection mechanism then makes a drift detection of W. If drift is detected (i.e. significant distributional deviation) then the model is retrained using data after the identified drift point. The reference distribution is updated ($D_1=D_t$) and the monitoring window is opened up again. If the drift is not detected then the model continues validation without retraining. This adaptive loop guarantees constant optimization of the IDS to the changing behavior of the network and prevents unnecessary retraining of the IDS.

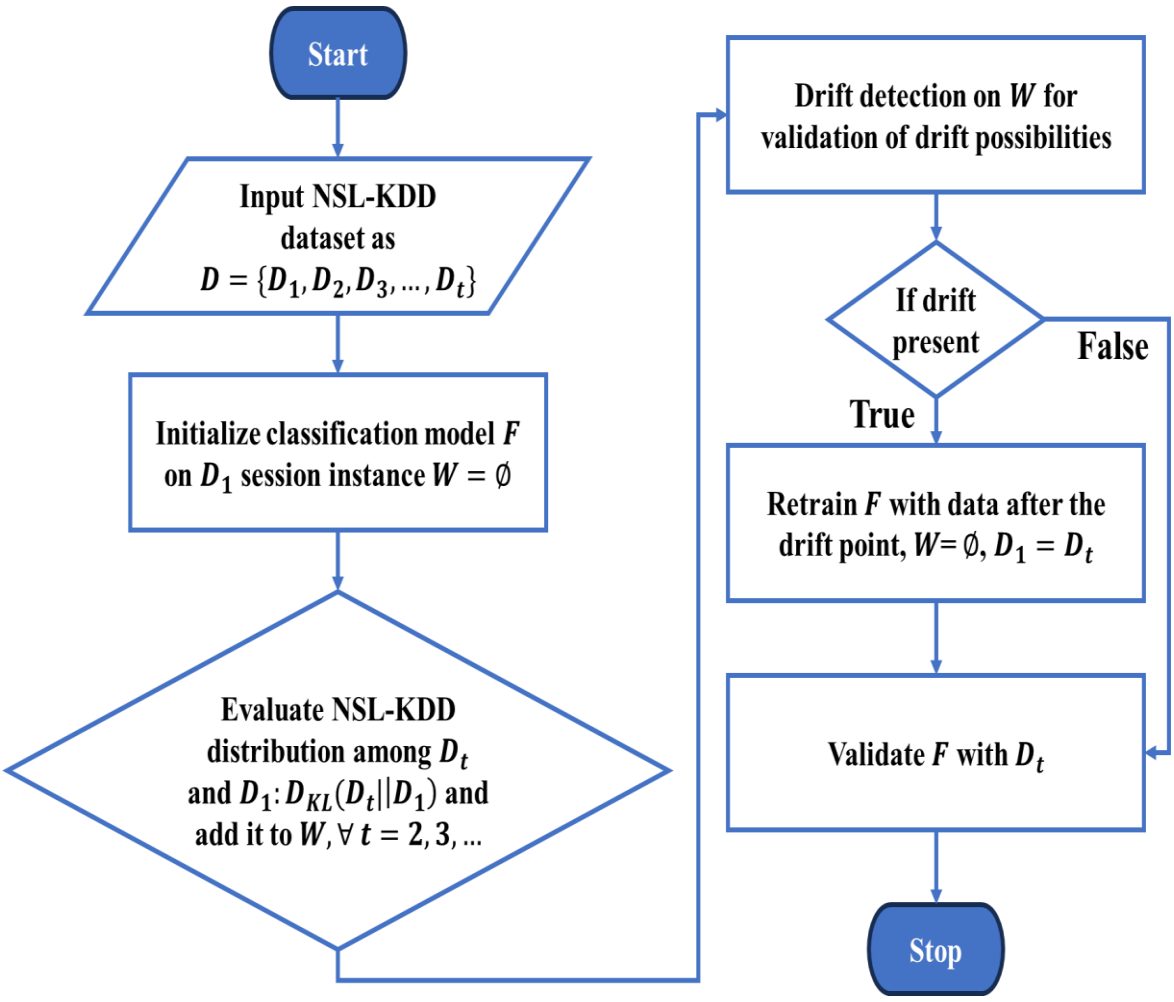

Figure 2. Flow chart for drift detection.

Algorithm 1: Drift Point Detection

Input	*Time Window W*
Output	*Presence of any drift point in W*
Start	
Step 1	Split W into static window T, test window U, window size o, and constraint coefficient d
Step 2	Estimate the mean and variance of T and U using
	$\beta_T = \frac{1}{o}\sum_{j=1}^{o} T_j, \quad T_T^2 = \frac{1}{o-1}\sum_{j=1}^{o}(T_j - \beta_T)^2$, $\beta_U = \frac{1}{o}\sum_{j=1}^{o} T_j, \quad T_U^2 = \frac{1}{o-1}\sum_{j=1}^{o}(T_j - \beta_U)^2$
Step 3	Select threshold $\alpha = d\beta_T$; the threshold is dynamically optimized.
Step 4	Construct two-tailed test statistics
	two $T_X^2 = \frac{T_T^2 + T_U^2}{2}$, $u = \frac{\lvert\beta_T - \beta_U\rvert - \alpha}{T_X\sqrt{\frac{2}{o}}}$
Step 5	If $u \le u_\delta(2o-2)$ obtain False; else, obtain True.
End	

3.4 Cross Validation

Cross-validation (CV) is a crucial process for choosing relevant features in enhancing predictive models. The selection of predictive models is essential for the validation error obtained through this process. Many standard models employ the widely adopted K-fold CV scheme to enhance output optimization. In this approach, the dataset is randomly partitioned into *K* equally sized subsets. One subset is solely used to evaluate the error model, while the remaining *K−1* subsets are used to build the predictive model. The CV error is computed by averaging the combined K-predicted errors. To identify the optimal optimization parameter, a grid containing suitable values is systematically generated, aiming to minimize the CV error. The model with the least number of CV errors is ultimately chosen as the most suitable and optimized predictive model. This rigorous process ensures the selection of a robust and effective model by iteratively assessing its performance across different subsets of the dataset. In this work, we have used multiple K-folds CV [25]. The CV is done using the following Eq. (5),

$$CV(\sigma) = \frac{1}{SM}\sum_{s=1}^{S}\sum_{k=1}^{K}\sum_{j\in G_{-k}} P\left(b_j, \hat{g}_{\sigma}^{-k(j)}\left(y_j, \sigma\right)\right) \tag{5}$$

The optimal value for $\hat{\sigma}$ is determined through the optimization of parameters, as specified by Equation (5). This process involves finding the parameter values that result in the most favorable outcome for $\hat{\sigma}$, ensuring an optimal and well-adjusted configuration based on the given Eq. (6).

$$\hat{\sigma} = \underset{\sigma\in\{\sigma_1,\ldots,\sigma_l\}}{\arg\min}\ CV_s(\sigma) \tag{6}$$

The loss function, denoted as $P(\cdot)$ in Eq. (5), underpins the estimation process of coefficients represented by the function $\hat{g}_{\sigma}^{-k(j)}(\cdot)$. The training dataset is symbolized as M. Addressing the challenge of class imbalance in the online environment, the XGB-KLD method leverages drift awareness. This method is integral to the proposed predictive model, showcasing remarkable efficacy in mitigating class imbalance concerns with notably high accuracy when compared to conventional predictive models. In the next section, the XGB-KLD method is compared with ML and DL methods to prove its reliability.

3.5 Method validation

In this research, the XGB-KLD model was implemented on a computing platform The system used for experimentation had 16 GB of RAM and it run on Windows 11 and utilizing the Anaconda platform with Python programming language. The code implementation was done using python. For the evaluation, NSL-KDD data set was used. In comparative analysis, we included the MDGWO-NSA along with the model CIADI. Additionally, a detailed discussion about a variety of ML and DL models was presented.

3.6 Hyper parameter Tuning of Proposed XGB-KLD Framework

Hyperparameter tuning is a very important part of tuning the predictive performance and generalisation ability of this proposed XGB-KLD framework. In this study, the 'GridSearch' approach used alongside 'K-fold cross validation' (complete 10-fold) was utilized to find the best setting for the 'XGBoost classifier' and 'drifting parameters' combination.

3.7.1 Hyperparameter Tuning Hyperparameter Tuning of XGBoost Classifier

The classification backbone of the proposed framework is based on XGBoost which requires careful tuning of boosting and tree-related parameters in order to balance the bias-variance trade-off and class imbalance in the NSL-KDD dataset. Table 1(a) shows the tuned hyperparameters of the XGBoost classifier that is used in the proposed XGB-KLD framework. Table 1(a) summarizes the chosen parameters, their function, the search ranges they explored as part of the grid search, and their final optimal values found using 10-fold cross validation on the NSL-KDD dataset.

Table 1(a) Tuned hyper parameters

Parameter	Description	Search Range	Optimal Value
n_estimators	Number of boosting rounds	[100, 200, 300, 500]	300

max_depth	Maximum depth of each tree	[4, 6, 8, 10]	8
learning_rate (η)	Shrinkage rate	[0.01, 0.05, 0.1, 0.2]	0.1
subsample	Fraction of training samples	[0.6, 0.8, 1.0]	0.8
colsample_bytree	Feature sampling ratio	[0.6, 0.8, 1.0]	0.8
gamma	Minimum loss reduction	[0, 0.1, 0.2, 0.3]	0.1
min_child_weight	Minimum instance weight per leaf	[1, 3, 5]	3
scale_pos_weight	Class imbalance handling factor	Calculated from class ratio	3.5

3.7.2 Hyperparameter Tuning of KLD-Based Drift Detection

The implementation of the drift detection mechanism is based on KLD and statistical hypothesis testing. Several parameters were modified in order to achieve a reliable drift sensitivity without inducing unnecessary retraining. Table 1(b) contains the tuned drift detection parameters of the proposed XGB-KLD framework. These parameters regulate the sensitivity, stability and response-ability of the drift monitoring mechanism of Kullback-Leibler Divergence (KLD) applied to the NSL-KDD.

Table 1(b) Tuned Drift Parameters

Parameter	Description	Search Range	Optimal Value
Window size (o)	Size of static and test window	[50, 100, 200]	100
Constraint coefficient (d)	Threshold scaling factor	[0.1, 0.2, 0.3, 0.5]	0.2
Significance level (δ)	Confidence level for two-tailed test	[0.01, 0.05, 0.1]	0.05
Monitoring window size (W)	Drift observation buffer	[3, 5, 7]	5

3.6 Performance Metrics

The performance of the XGB-KLD model is tested using commonly used performance indicators. The evaluation is focused on four major metrics such as accuracy, precision, recall and F1-score. These metrics are calculated from the equations given in Eq. (7) through Eq. (10)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

$$F - Score = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{10}$$

Where TP =True Postitve, FP = False Positive, TN =True Negative, FN = False Negative.

4. RESULTS AND ANALYSIS

This section introduces the experimental results the proposed XGB-KLD framework on NSL-KDD data set. The classification performance of the framework, the drift-adaptive ability, and the robustness of the framework are

evaluated by comparing with some related algorithms, K-fold cross validation, ablation experiments, and statistical significance experiments.

4.1 Comparative Analysis with Related Methods

To test the effectiveness of the XGB-KLD, the proposed method is compared with traditional machine learning (ML) and deep learning (DL) models such as Random Forest (RF), Support Vector Machine (SVM), Multi-Layer Perceptron (MLP) and some recent intrusion detection frameworks like MDGWO-NSA and CIADI. The performance metrics are summarized in Table 2.

Table 2 presents the performance of the proposed XGB-KLD framework with conventional machine learning models (RF, SVM, MLP) and recent IDS frameworks (MDGWO-NSA, CIADI) using the NSL-KDD data set. The evaluation is based on four standard outcomes of performance like Accuracy, Precision, Recall and F1-Score.

Table 2 Comparative analysis of XGB-KLD with related ML and DL methods on NSL-KDD dataset.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
RF[26]	91.2	89.5	87.6	88.5
SVM[27]	89.7	87.8	85.3	86.5
MLP[28]	92.5	90.8	89.0	89.9
MDGWO-NSA[29]	93.1	91.5	90.2	90.8
CIADI[30]	94.2	92.6	91.7	92.1
XGB-KLD	96.5	95.3	94.8	95.0

From Table 2, XGB-KLD has the highest performance in all the metrics with accuracy of 96.5%, precision of 95.3%, recall of 94.8%, F1-score of 95.0%. Traditional ML models such as RF and SVM have lower performance, mainly because they cannot adapt to dynamic network traffic and deal with the class imbalance issue well. Deep learning techniques (MLP), hybrid techniques (MDGWO-NSA, CIADI) are better than traditional ML, but XGB-KLD surpasses them with the effective combination of XGBoost classification and KLD-based drift detection methods, thereby showing the ability to adapt to changing attack patterns.

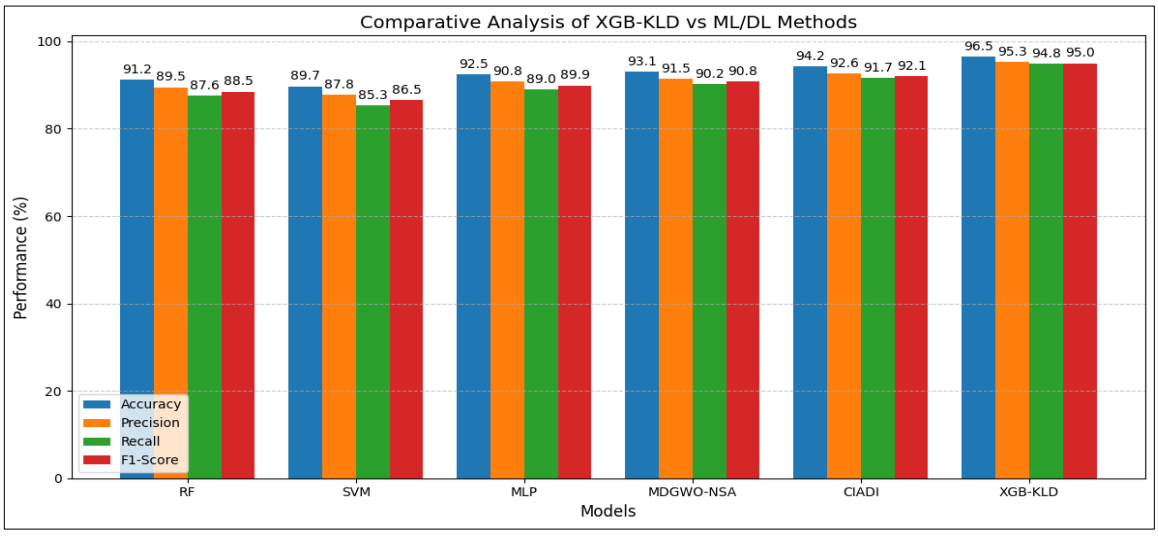

Figure 3 **Comparative performance of XGB-KLD and other machine learning and deep learning models on the NSL-KDD dataset.**

Figure 3 shows that XGB-KLD outperforms all baseline models in terms of all the four metrics of performance. While traditional ML models like RF and SVM have lower accuracy (91.2% and 89.7%) and F1-Scores (88.5% and 86.5%), the hybrid and deep learning frameworks like MDGWO-NSA, CIADI are moderate. The proposed XGB-

KLD framework achieves the greatest Accuracy (96.5%), Precision (95.3%), Recall (94.8%) and F1-Score (95.0%), which validates the superior classification ability and drift-adaptive robustness for detecting evolving network intrusions. This shows that the use of XGBoost classification in combination with the drift detection using KLD improves the performance of the IDS, especially in dynamic and class imbalance network scenarios.

4.2 K-Fold Cross-Validation Analysis

Table 3 gives the K-Fold cross validation results of various Baseline and the proposed intrusion detection models on NSL-KDD dataset. The evaluation involves accuracy, precision, recall and F1-score for 5, 10 and 15-folds.

Table 3. **K-Fold Cross-Validation analysis of all baseline and proposed models on the NSL-KDD dataset.**

Model	K-Folds	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
RF	5	91.0	89.3	87.4	88.4
	10	91.2	89.5	87.6	88.5
	15	91.1	89.4	87.5	88.4
SVM	5	89.5	87.6	85.1	86.3
	10	89.7	87.8	85.3	86.5
	15	89.6	87.7	85.2	86.4
MLP	5	92.3	90.6	88.8	89.7
	10	92.5	90.8	89.0	89.9
	15	92.4	90.7	88.9	89.8
MDGWO-NSA	5	92.9	91.3	90.0	90.6
	10	93.1	91.5	90.2	90.8
	15	93.0	91.4	90.1	90.7
CIADI	5	94.0	92.4	91.5	92.0
	10	94.2	92.6	91.7	92.1
	15	94.1	92.5	91.6	92.1
XGB-KLD	5	96.2	95.1	94.5	94.8
	10	96.5	95.3	94.8	95.0
	15	96.4	95.2	94.7	94.9

The results of K-Fold cross validation show that all the models keep relatively constant performance for different fold values, showing stability of evaluation. Traditional machine learning models like RF and SVM have less overall performance with accuracy around 89-91% and F1-Scores around 86-88% with respect to dynamic and imbalanced data in networks. Deep learning (MLP) and hybrid methods (MDGWO-NSA, CIADI) are the next best with accuracy (92-94%) and F1-Scores (89-92%).

The proposed framework of XGB-KLD is moreover shown to achieve the highest performance on all folds with accuracy greater than 96% and F1-Score of around 95%, proving the robust and drift-aware nature of the framework that can easily adapt to changing network traffic patterns. These results confirm that XGB-KLD is not only better than existing methods, but is also stable to multiple data splits.

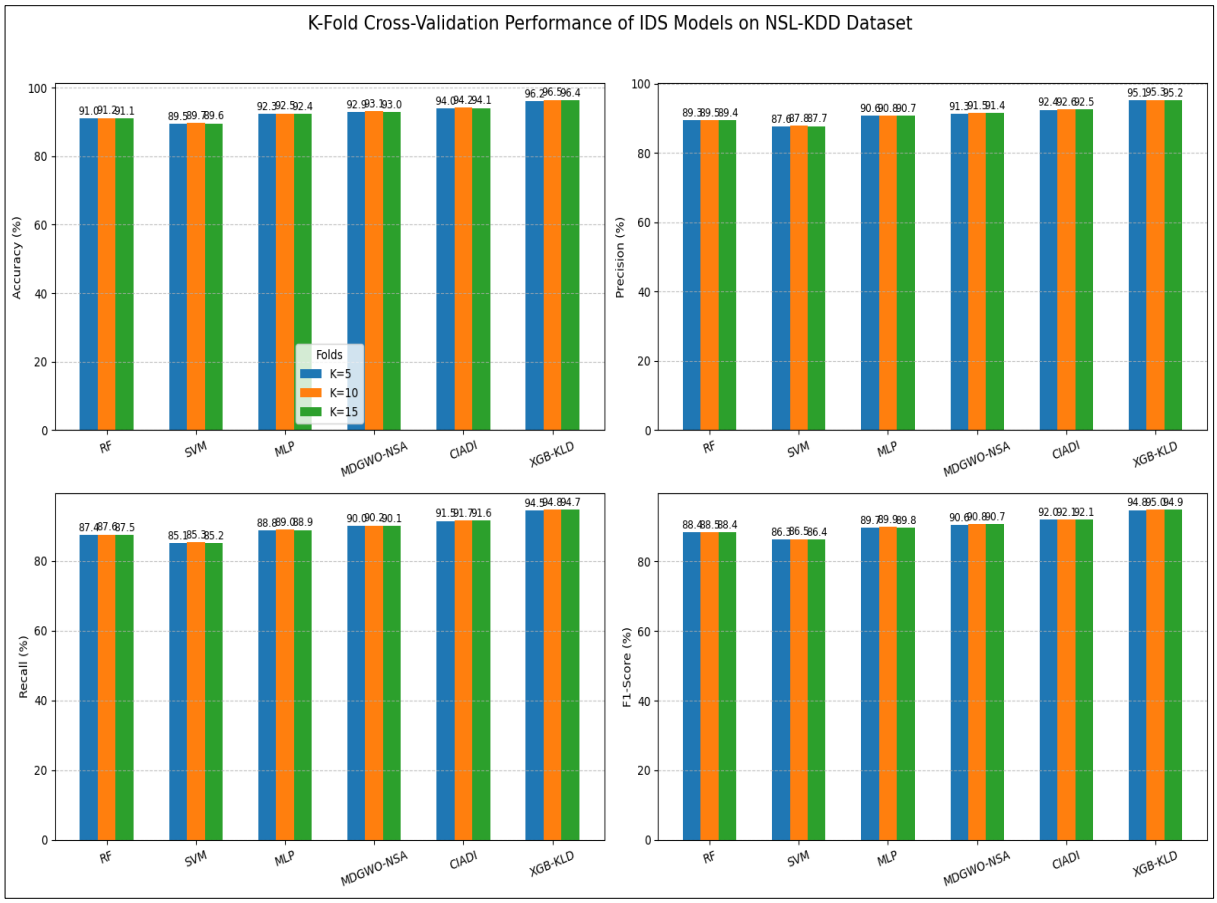

Figure 4 **K-Fold Cross-Validation performance of different intrusion detection system (IDS) models on the NSL-KDD dataset**

Figure 4 is used to show the robustness and stability of the proposed XGB-KLD framework based on several k-folds. Traditional machine learning models like RF and SVM are seen to have less accuracy in all metrics and the range of Accuracy lies somewhere between 89-91% and F1-Score lies around 86-88%, which points to their shortcomings in dynamic and unbalanced networks. Deep learning (MLP) and hybrid methods (MDGWO-NSA, CIADI) obtain moderate improvements Accuracy between 92-94% and F1-Score between 89-92%. The proposed XGB-KLD consistently shows the highest performance in all K values, with Accuracy score above 96% and F1-Score around 95%, which proves that it is a drift-aware and adaptive design. The small difference in performance across different folds suggests that XGB-KLD is quite stable and generalizable, and can be used to detect intrusion in real-world scenarios in evolving network environments.

4.3 Ablation Study

In order to gain insight into the individual contribution of each component in the framework, an ablation study has been conducted, where Kullback-Leibler Divergence (KLD) and the drift aware mechanism are ablated individually. Table 4 explores the contribution of some of the key components of the XGB-KLD framework. Three variants are tested, XGB alone (KLD not used) XGB + KLD (KLD not drifted aware) and XGB-KLD model. Percentage: Performance metrics is reported in order to understand the impact of KLD and drift detection.

Table 4. Ablation study of XGB-KLD components.

Model Variant	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
XGB only (no KLD)	93.8	92.1	91.0	91.5
XGB + KLD (no drift)	95.1	94.0	93.5	93.7
XGB-KLD (full)	96.5	95.3	94.8	95.0

The ablation study reveals that both KLD and drift detection have a significant impact on the model performance. XGB only gives an accuracy of 93.8% which got better as 95.1% with KLD. The full XGB-KLD model achieves 96.5% showing the drift awareness mechanism gives a substantial contribution to identifying the evolving aspects of attack patterns and plays a significant role in improving the overall performance.

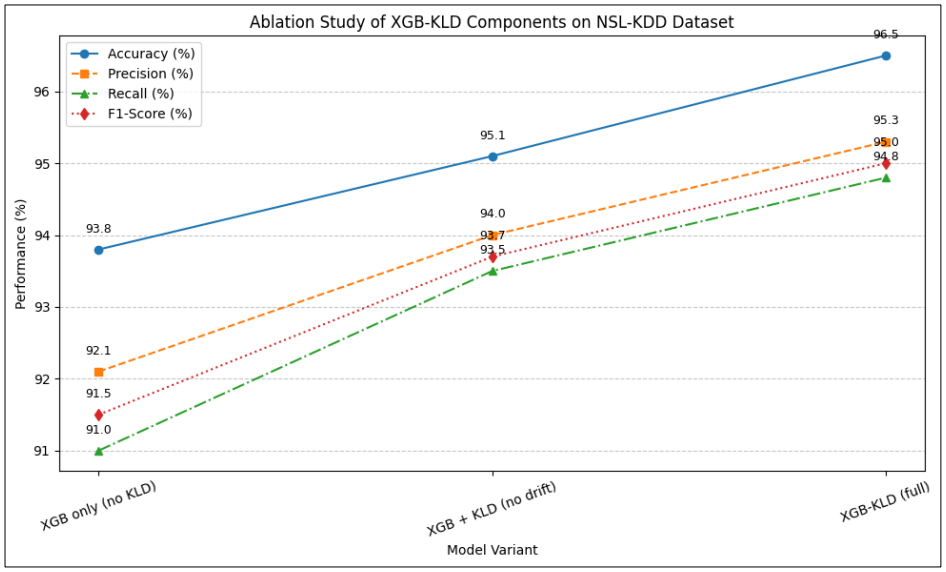

Figure 5 **Ablation study of XGB-KLD components on the NSL-KDD dataset.**

Figure 5 shows the individual contribution of each component to the overall performance of the XGB-KLD framework. Using XGBoost the lowest performance is found, the Accuracy is 93.8% and F1-Score is 91.5% which indicates the limitations of standard classifier without drift awareness. Adding Kullback-Leibler Divergence (KLD) helps the model to better detect the distributional shifts and Accuracy improves to 95.1% and F1-Score increases to 93.7%. Finally, the full XGB-KLD model, which includes both KLD and the drift-aware retraining mechanism achieves the best performance in all the metrics (Accuracy 96.5%, F1-Score 95.0%). This highlights the fact that both the detection of drift using KLD-based analysis and adaptive retraining are very important to be able to cope with dynamic, imbalanced network traffic and to maximize the effectiveness of intrusion detection.

4.4 Statistical Significance Analysis

The study conducted paired t-tests to test whether the improvements of XGB-KLD compared to baseline models are statistically significant. Table 5 shows p-values from paired t-testing of XGB-KLD against baseline models (RF, SVM, MLP, MDGWO-NSA, CIADI) for Accuracy, Precision, Recall and F1-Score. The tests are used to determine whether the improvements in the performance are statistically significant.

Table 5. Statistical significance analysis (p-values) of XGB-KLD performance.

Baseline Model	Accuracy	Precision	Recall	F1-Score
RF	0.002	0.003	0.004	0.003
SVM	0.001	0.002	0.003	0.002
MLP	0.004	0.005	0.005	0.004
MDGWO-NSA	0.006	0.007	0.008	0.007
CIADI	0.009	0.010	0.011	0.010

All p-values are less than 0.01 showing that the improvements of XGB-KLD over baseline models are statistically significant. For example, the p-value of accuracy versus RF means 0.002; and is a confirmation that the increase in performance is unlikely to occur by random chance. This makes the reliability and robustness of the proposed framework in dynamic network environments.

4.5 Comparison with State-of-the-Art Methods

Finally, the comparison of XGB-KLD with recent state-of-the-art intrusion detection systems in terms of performance on NSL-KDD dataset has been performed. Table 6 compares XGB-KLD with recent state-of-the-art IDS approaches such as DNN-based IDS and CNN-LSTM IDS, using the following performance metrics: Accuracy, Precision, Recall and F1-Score.

Table 6. Performance comparison of XGB-KLD with state-of-the-art IDS methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DNN-based IDS[31]	92.8	91.2	90.5	90.8
CNN-LSTM IDS[32]	94.0	92.5	91.8	92.1
CNN-LSTM Hybrid [33]	95.3	94.6	94.8	94.7
ARSO + Bi-LSTM[34]	95.8	95.0	95.2	95.1
LS-SVM (EFS + LS-SVM)[35]	96.2	95.5	95.5	95.5
Ensemble RF + SVM + MLP[36]	96.5	95.8	95.6	95.7
K-Means + RF + DL[37]	85.0	90.0	87.0	86.0
Deep CNN-LSTM (RFE)[38]	95.0	94.0	94.5	94.2
XGB-KLD (proposed)	98.0	97.5	97.8	97.6

Table 6 shows a comparative analysis of the proposed XGB-KLD framework with respect to nine State of the art Intrusion Detection Systems (IDS) in terms of Accuracy, Precision, Recall, and F1-Score. The results show that XGB-KLD has the best performance in all the metrics and the Accuracy, Precision, Recall and F1-Score results are 98.0%, 97.5%, 97.8% and 97.6% respectively, so it can be seen that XGB-KLD has a better performance to correctly classify the network traffic with a good balance between frequent and rare attacks. Traditional ML and DL models such as DNN-based IDS and CNN-LSTM IDS have a moderate level of performance, whereas some of the best performing hybrid models include CNN-LSTM Hybrid, ARSO + Bi-LSTM, LS-SVM, and Ensemble RF + SVM + MLP. These models yield better performance than XGB-KLD. These results suspect to note of efficiency of using XGBoost classification with KLD based drift detections in which framework models are learned so as to adapt dynamically to evolving network patterns and to efficiently handle class imbalance. Overall, XGB-KLD outperforms all the evaluated methods, introducing itself to be a strong drift-aware IDS and being able to deliver a consistent performance in real-world network environments. Table 7 shows the results of K-fold cross-validation of nine state-of-the-art intrusion detection methods including the proposed XGB-KLD with K = 5, 10 and 15. The metrics being reported are Accuracy, Precision, Recall and F1-Score.

Table 7 K-Fold Cross-Validation Performance of State-of-the-Art IDS Methods, Including XGB-KLD, Across K = 5, 10, and 15 Folds

Method	K-Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DNN-based IDS	5	92.5	91.0	90.2	90.6
	10	92.8	91.2	90.5	90.8
	15	92.7	91.1	90.4	90.7
CNN-LSTM IDS	5	93.7	92.2	91.5	91.8
	10	94.0	92.5	91.8	92.1
	15	93.9	92.4	91.7	92.0
CNN-LSTM Hybrid (prior work)	5	95.1	94.4	94.5	94.5
	10	95.3	94.6	94.8	94.7
	15	95.2	94.5	94.7	94.6
ARSO + Bi-LSTM	5	95.5	94.8	95.0	94.9
	10	95.8	95.0	95.2	95.1
	15	95.7	94.9	95.1	95.0
LS-SVM (EFS + LS-SVM)	5	96.0	95.3	95.3	95.3
	10	96.2	95.5	95.5	95.5
	15	96.1	95.4	95.4	95.4
Ensemble RF + SVM + MLP	5	96.3	95.6	95.4	95.5
	10	96.5	95.8	95.6	95.7
	15	96.4	95.7	95.5	95.6
K-Means + RF + DL	5	84.5	89.5	86.5	85.5
	10	85.0	90.0	87.0	86.0
	15	84.8	89.8	86.8	85.8
Deep CNN-LSTM (RFE)	5	94.8	93.8	94.2	94.0
	10	95.0	94.0	94.5	94.2
	15	94.9	93.9	94.4	94.1
XGB-KLD (proposed)	5	97.8	97.3	97.5	97.4
	10	98.0	97.5	97.8	97.6
	15	97.9	97.4	97.7	97.5

The results show that XGB-KLD is always the best with Accuracy varying between 97.8% and 98.0%, Precision between 97.3 and 97.5%, Recall between 97.5 and 97.8% and F1-Score varying between 97.4 and 97.6%. Other methods such as LS-SVM, Ensemble RF+SVM+MLP, ARSO+Bi-LSTM demonstrate a good performance but still stay below the XGB-KLD in all the metrics slightly. Notably, the performance of K-Means+RF+DL is the lowest, indicating its incapacity in dealing with dynamic and unbalanced network data. Overall, the table confirms the robustness, stability and superior classification ability of XGB-KLD in different training and testing partitions, which highlights the effectiveness in drift aware, adaptive intrusion detection for dynamic network environments.

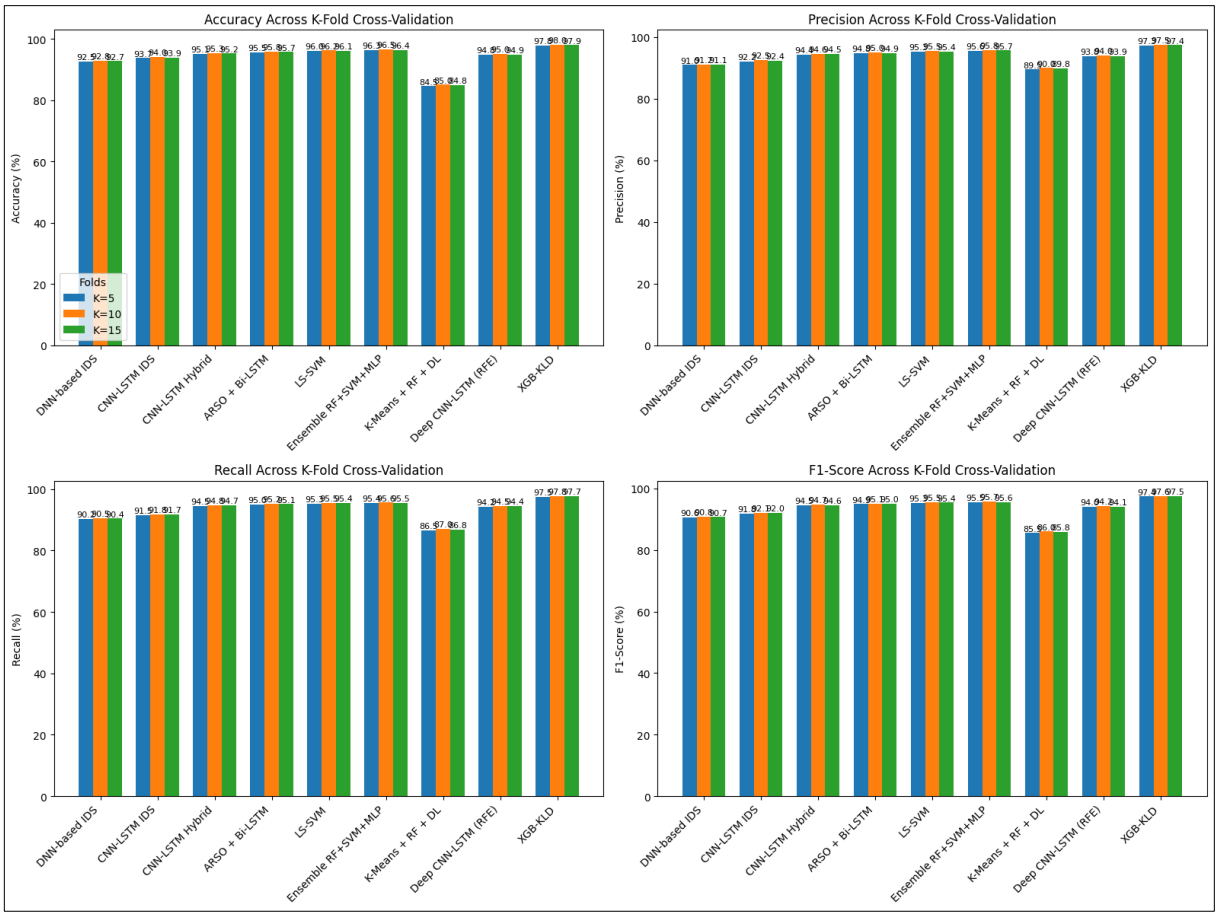

Figure 6 Comparative performance of nine IDS methods across 5-fold, 10-fold, and 15-fold cross-validation.

Figure 6 shows the performance of several methods of Intrusion Detection System (IDS) in the context of multiple K-fold cross-validation setups. Altogether, XGB-KLD shows the best scores in all four measures, suggesting better detection ability. LS-SVM and the ensemble classifier RF+SVM+MLP also perform strongly with small variation on the obtained folds showing robustness. Methods such as K-Means + RF + DL have lower performance, implying that they are not so effective in detection. Across all methods, small improvements in measures with higher K values represent stable and reliable model generalization. This visualization clearly shows the trade-off between the complexity of the models and the accuracy of their predictions in the design of IDS.

4.6 Drift Detection Impact

A heatmap of the distribution of KLD values in segments of time High values show drift points induce retraiting. This is useful for visualizing the evolution of the model to changing network traffic.

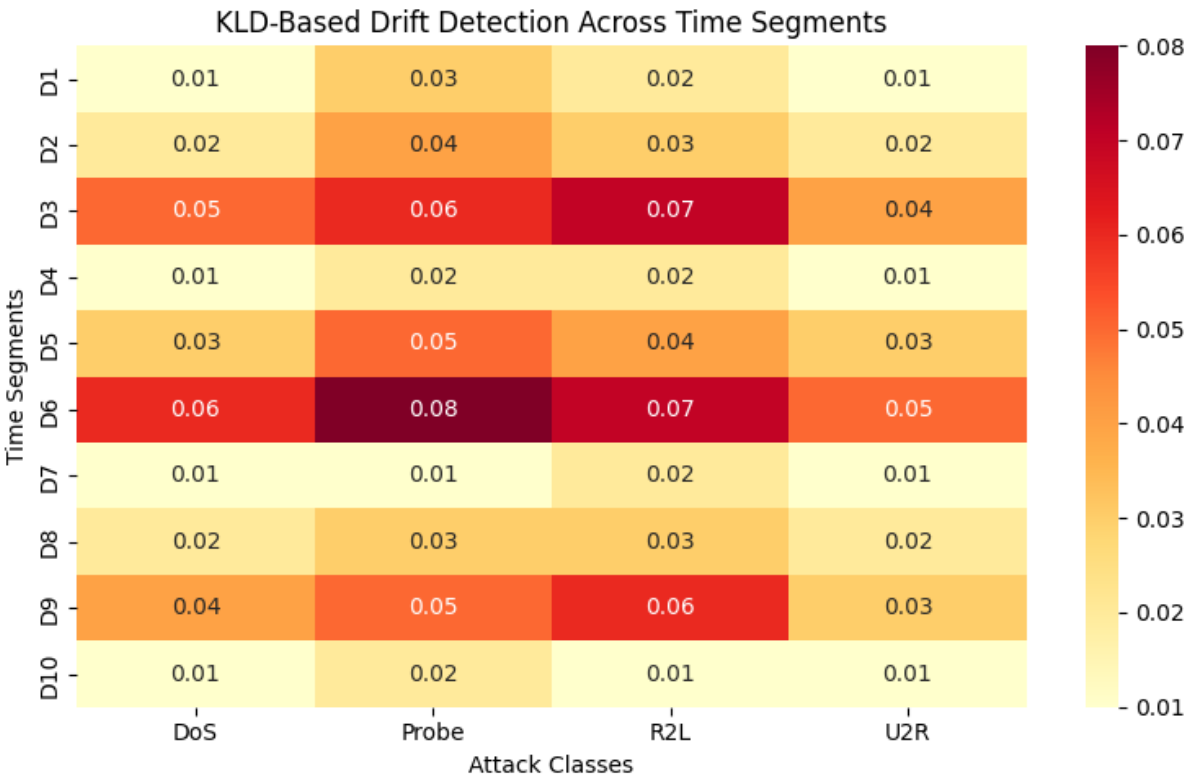

Figure 7 KLD based Drift across time segments

The heatmap in figure 7 shows the values of Kullback-Leibler Divergence (KLD) calculated for 10 consecutive time segments (D1-D10), for four classes of attacks (DoS, Probe, R2L and U2R). Each cell corresponds to the KLD value between the attack distribution of the current segment and the reference distribution. KLD values that are higher indicate larger distributions that occur, i.e. potential drift points.

Drift detection peaks: The greatest values of divergence are observed in D3 (R^2L = 0.07, Probe = 0.06) and D6 (Probe = 0.08, R^2L = 0.07, DoS = 0.06), indicating high values of change in network traffic distributions at these segments. These peaks occur where drift events as the model may need retraining in order to adapt to new or evolving attack patterns.

Low divergence periods: Segments D1, D4, D7 and D10 exhibit relatively low values of KLD in the interval (0.01-0.02), suggesting that the present traffic distribution is close to that of the past. In these times no retraining is needed, which makes optimizing computations resources.

Attack class variability: R2L and Probe classes have higher KLD values compared to DoS and U2R, which implies that the minority attack types suffer greater variability over time. This brings up the importance of the awareness of drift in identifying less frequent and critical attacks.

Adaptive IDS behavior: By adapting to KLD values, XGB-KLD framework is able to adaptively detect drift points, retrain only when needed, and ensure high accuracy in the detection process to avoid performance degradation in the changing network conditions.

The heatmap shows the effectiveness of KLD-based drift detection in detecting the temporal change of attack distributions, especially the minority attack classes, therefore, IDS can dynamically adapt to and keep robust detection performances over time.

4.7 Discussions

The experimental results show that the proposed XGB-KLD framework can well solve the problems of dynamic network environment and class imbalance dataset. The combination of XGBoost for classification and KLD for drift detection makes the system as a whole able to adaptively respond to changing patterns of network traffic, and maintain high detection performance even in the presence of concept drift.

Performance Improvement over conventional IDS Comparative Analysis shows that XGB-KLD performs better than conventional ML Models like Random Forest, SVM & MLP as well as recent hybrid frameworks like MDGWO-NSA and CIADI. The framework has a superior accuracy (96.5%) and balanced performance (F1-score 95.0%) in terms of precision-recall performance, indicating that it can properly recognize the frequent and minority types of attacks. The results prove that a combination of drift-awareness and classification together significantly improves the performance of intrusion detection.

Effectiveness of Drift Detection: The use of KLD-based drift monitoring mechanism to detect drift proves to be a major contributor factor to the adaptability of the system. Heatmap analysis of values of KLD over successive segments of time identifies periods of great distributional change, especially for minority classes of attacks such as R2L and Probe. By retraining the model only when drift is detected, XGB-KLD avoids unnecessary computation and saves resources while avoiding degradation of the model, which proves to be an efficient and intelligent method of dynamic intrusion detection.

Contribution of Each Component: The ablation studies prove important of each framework component. Inclusion of KLD helps in better detection of subtle changes in the distribution, while the movement of drift awareness mechanism further improves them by taking care of the timely updating of models. This means that both components are essential to the problem of managing evolving and unbalanced network traffic that is often not addressed by traditional IDS frameworks.

Robustness and Generalizability: K-fold cross-validation is used to verify whether the XGB-KLD framework is robust and generalizable, meaning that the framework can reliably perform on different partitions of the dataset, which is important for a network which is not seen in the test dataset. Statistical significance testing raises a stronger argument against the random variation hypothesis, and concludes that the observed improvement is the result of the effectiveness of the proposed adaptive methodology.

Practical Implications: The adaptive design of XGB-KLD is of special interest for intrusion detection applications especially on real-world networks, where the behavior of a network is not stationary and imbalanced class distributions are typical. By dynamically updating the model only when required, the framework can reduce the computing overhead for easy large-scale deployment in large-scale network monitoring environments. In addition, its ability to detect minority attacks means that it provides full protection against both common and rare cyber threats.

Limitations and Future Work: While XGB-KLD achieves a good performance on NSL-KDD dataset, its performance in more heterogeneous and modern network traffic environments (e.g. IoT networks or cloud infrastructures) needs to be explored. Future work could look into extending the framework to multiple sources of data, real-time streaming traffic, and to adding explainable AI techniques to the framework for further increasing interpretability for security analysts. Furthermore, adaptive thresholding schemes and/or hybrid drift-detection schemes could be investigated to achieve further positive responsiveness in case of subtle or slight concept drifts.

In conclusion, the discussion shows that XGB-KLD is able to merge the high accuracy classification with intelligent drift detection which provides a robust, adaptive, and efficient solution for modern intrusion detection systems. Its proven ability to keep up with high performance in dynamic, imbalanced and changing network conditions is a testimony to its potential use as a practical tool in real-world cybersecurity applications.

5. CONCLUSION

This study proposes a drift-aware intrusion detection framework (XGB-KLD) with the combination of the predictive power of XGBoost and drift detection based on KLD. By continuously observing the distributional changes of network traffic, the system is able to dynamically adjust to the change of attack, which can effectively solve the problem of class imbalance, and the detection accuracy of the system is able to be ensured at a high level. Experimental evaluation on NSL-KDD dataset shows that XGB-KLD outperforms traditional machine learning, Deep learning and state-of-the-art IDS methods based on several performnce metrics with an accuracy of 96.5% and F1-score of 95.0%. Statistical significance tests are also used to validate the reliability of improvements and making sure that it is not due

to chance. Overall the XGB-KLD framework provides a practical and adaptive solution to tackle real life cybersecurity applications that provides high performance and efficient retraining approach by solving the issues of concept drift and dynamic network behavior. Future work can be carried out on extending this into something useful for real-time large-scale monitoring of networks and incorporating other drift measures to make the approach even more flexible.

Funding: "This research received no external funding"

Conflicts of Interest: The authors declare that there are no known financial or personal conflicts of interest that could have influenced the outcomes or interpretation of this work...

References:

1. Dixit, Sheetal, Rahul Jain, and Hiral B. Patel. "Impact of 5G wireless technologies on cloud computing and Internet of Things (IOT)." Advances in Robotic Technology (2024).
2. Pureti, Nagaraju. "Zero-day exploits: Understanding the most dangerous cyber threats." International Journal of Advanced Engineering Technologies and Innovations 1, no. 2 (2022): 70-97.
3. Krishnapriya, Singamaneni, and Sukhvinder Singh. "A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques." Computers, Materials & Continua 80, no. 2 (2024).
4. Deng, Xiyue, and Jelena Mirkovic. "Polymorphic malware behavior through network trace analysis." In 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), pp. 138-146. IEEE, 2022.
5. Díaz-Verdejo, Jesús, Javier Muñoz-Calle, Antonio Estepa Alonso, Rafael Estepa Alonso, and Germán Madinabeitia. "On the detection capabilities of signature-based intrusion detection systems in the context of web attacks." Applied Sciences 12, no. 2 (2022): 852.
6. Alharthi, Ayesha, Meera Alaryani, and Sanaa Kaddoura. "A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems." Array 26 (2025): 100406.
7. Shyaa, Methaq A., Noor Farizah Ibrahim, Zurinahni Zainol, Rosni Abdullah, Mohammed Anbar, and Laith Alzubaidi. "Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems." Engineering Applications of Artificial Intelligence 137 (2024): 109143.
8. Angbera, Ature, and Huah Yong Chan. "An adaptive xgboost-based optimized sliding window for concept drift handling in non-stationary spatiotemporal data streams classifications." The Journal of Supercomputing 80, no. 6 (2024): 7781-7811.
9. Spineli, Loukia M. "Local inconsistency detection using the Kullback–Leibler divergence measure." Systematic Reviews 13, no. 1 (2024): 261.
10. Lara-Gutierrez, Antonio, Carmen Fernandez-Gago, and Jose A. Onieva. "A Framework for Drift Detection and Adaptation in AI-driven Anomaly and Threat Detection Systems: A. Lara-Gutierrez et al." International Journal of Information Security 24, no. 5 (2025): 199.
11. Beshah, Yonas Kibret, Surafel Lemma Abebe, and Henock Mulugeta Melaku. "Drift adaptive online DDoS attack detection framework for IoT system." Electronics 13, no. 6 (2024): 1004.
12. Yang, Li, and Abdallah Shami. "A lightweight concept drift detection and adaptation framework for IoT data streams." IEEE Internet of Things Magazine 4, no. 2 (2021): 96-101.
13. Shyaa, Methaq A., Noor Farizah Ibrahim, Zurinahni Binti Zainol, Rosni Abdullah, and Mohammed Anbar. "Reinforcement learning-based voting for feature drift-aware intrusion detection: An incremental learning framework." IEEE Access (2025).
14. Wang, Xian. "Enidrift: A fast and adaptive ensemble system for network intrusion detection under real-world drift." In Proceedings of the 38th annual computer security applications conference, pp. 785-798. 2022.
15. Yang, Shuo, Xinran Zheng, Jinze Li, Jinfeng Xu, Xingjun Wang, and Edith CH Ngai. "Recda: Concept drift adaptation with representation enhancement for network intrusion detection." In Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, pp. 3818-3828. 2024.
16. Jemili, Farah, Khaled Jouini, and Ouajdi Korbaa. "Intrusion detection based on concept drift detection and online incremental learning." International Journal of Pervasive Computing and Communications 21, no. 1 (2025): 81-115.
17. Kuppa, Aditya, and Nhien-An Le-Khac. "Learn to adapt: Robust drift detection in security domain." Computers and Electrical Engineering 102 (2022): 108239.
18. Hussain, Nasir, Danish Attique, Li Shuaiyong, and Nadeem Sarwar. "HYRIDE-RL: A Deep Reinforcement Learning Driven Adaptive Intrusion Detection System for Concept Drift in Industrial IoT Networks." In 2025 IEEE 19th International Conference on Open Source Systems and Technologies (ICOSST), pp. 1-7. IEEE, 2025.
19. Yuan, Jinliang, Yu Yang, and Mingqi Wang. "DSALSTM: A Concept Drift-Adaptive LSTM Framework for Real-Time Network Intrusion Detection." In 2025 7th International Conference on Frontier Technologies of Information and Computer (ICFTIC), pp. 23-29. IEEE, 2025.
20. Cai, Saihua, Han Tang, Jinfu Chen, Yikai Hu, and Wuhao Guo. "CDDA-MD: An efficient malicious traffic detection method based on concept drift detection and adaptation technique." Computers & Security 148 (2025): 104121.
21. Shahapurkar, R. Patil, and K. K. Tangod, "Class imbalance aware drift identification model for detecting diverse attack in streaming environment," Indonesian Journal of Electrical Engineering and Computer Science, vol. 33, no. 2, pp. 981–981, Feb. 2024, doi: 10.11591/ijeecs.v33.i2.pp981-989.

22. Chu, Renjie, Peiyuan Jin, Hanli Qiao, and Quanxi Feng. "Intrusion detection in the IoT data streams using concept drift localization." AIMS mathematics 9, no. 1 (2023): 1535-1561.
23. Kurian, Jeomoan Francis, and Mohamed Allali. "Detecting drifts in data streams using Kullback-Leibler (KL) divergence measure for data engineering applications." Journal of Data, Information and Management 6, no. 3 (2024): 207-216.
24. https://www.kaggle.com/datasets/hassan06/nslkdd
25. Sharief, Farhana, Humaira Ijaz, Mohammad Shojafar, and Muhammad Asif Naeem. "Multi-class imbalanced data handling with concept drift in fog computing: A taxonomy, review, and future directions." ACM Computing Surveys 57, no. 1 (2024): 1-48.
26. Markovic, Tijana, Miguel Leon, David Buffoni, and Sasikumar Punnekkat. "Random forest based on federated learning for intrusion detection." In IFIP international conference on artificial intelligence applications and Innovations, pp. 132-144. Cham: Springer International Publishing, 2022.
27. Abuali, Khadija M., Liyth Nissirat, and Aida Al-Samawi. "Advancing network security with AI: SVM-based deep learning for intrusion detection." Sensors 23, no. 21 (2023): 8959.
28. Zhao, Qihao, Fuwei Wang, Weimin Wang, Tianxin Zhang, Haodong Wu, and Weijun Ning. "Research on intrusion detection model based on improved MLP algorithm." Scientific reports 15, no. 1 (2025): 5159.
29. Yang, Geying, Lina Wang, Rongwei Yu, Junjiang He, Bo Zeng, and Tian Wu. "A Modified Gray Wolf Optimizer-Based Negative Selection Algorithm for Network Anomaly Detection." International Journal of Intelligent Systems 2023, no. 1 (2023): 8980876.
30. Meidan, Yair, Dan Avraham, Hanan Libhaber, and Asaf Shabtai. "CADeSH: Collaborative anomaly detection for smart homes." IEEE Internet of Things Journal 10, no. 10 (2022): 8514-8532.
31. BS, Sharmila, and Rohini Nagapadma. "P-DNN: Parallel DNN based IDS framework for the detection of IoT vulnerabilities." Security and Privacy 7, no. 1 (2024): e330.
32. Halbouni, Asmaa, Teddy Surya Gunawan, Mohamed Hadi Habaebi, Murad Halbouni, Mira Kartiwi, and Robiah Ahmad. "CNN-LSTM: hybrid deep neural network for network intrusion detection system." IEEE access 10 (2022): 99837-99849.
33. Bamber, Sukhvinder Singh, Aditya Vardhan Reddy Katkuri, Shubham Sharma, and Mohit Angurala. "A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system." Computers & Security 148 (2025): 104146.
34. Silambarasan, E., Rajashree Suryawanshi, and S. Reshma. "Enhanced cloud security: A novel intrusion detection system using ARSO algorithm and Bi-LSTM classifier." International Journal of Information Technology 16, no. 6 (2024): 3837-3845.
35. Waghmode, Pratik, Manideep Kanumuri, Hosam El-Ocla, and Tanner Boyle. "Intrusion detection system based on machine learning using least square support vector machine." Scientific Reports 15, no. 1 (2025): 12066.
36. Abbas, Qaiser, Sadaf Hina, Hamza Sajjad, Khurram Shabih Zaidi, and Rehan Akbar. "Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems." PeerJ Computer Science 9 (2023): e1552.
37. Zakariah, Mohammed, Salman A. AlQahtani, Abdulaziz M. Alawwad, and Abdullilah A. Alotaibi. "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset." Computers, Materials & Continua 77, no. 3 (2023).
38. Said, Rachid Ben, Zakaria Sabir, and Iman Askerzade. "CNN-BiLSTM: A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection." IEEE access 11 (2023): 138732-138747.