Adaptive Intrusion Detection System with Ensemble Classifiers for Handling Imbalanced Datasets and Dynamic Network Traffic

Moaad Almania [1*], Anazida Zainal [2], Fuad A Ghaleb [3], Ahmad Alnawasrah [4], Mahmoud Al Qerom [5]
[1, 2] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor, 81310, Malaysia
[1] College of Computing and Information Technology, Shaqra University, Shaqra, Kingdom of Saudi Arabia
[3] College of Computing and Digital Technology, Birmingham City University, Birmingham, B47XG, United Kingdom
[4, 5] Department of Information Communication Technology, British University of Bahrain, Bahrain
Email: [1] malmane3@su.edu.sa
*Corresponding Author

***Abstract*—Intrusion Detection Systems (IDS) are crucial for network security, but their effectiveness often diminishes in dynamic environments due to outdated models and imbalanced datasets. This paper presents a novel Adaptive Intrusion Detection System (AIDS) that addresses these challenges by incorporating ensemble classifiers and dynamic retraining. The AIDS model integrates K-Nearest Neighbors (KNN), Fuzzy c-means clustering, and weight mapping to improve detection accuracy and adaptability to evolving network traffic. The system dynamically updates its reference model based on the severity of changes in network traffic, enabling more accurate and timely detection of cyber threats. To mitigate the effects of imbalanced datasets, ensemble classifiers, including Decision Tree (DT) and Random Forest (RF), are employed, resulting in significant performance improvements. Experimental results show that the proposed model achieves an overall accuracy of 97.7% and a false alarm rate (FAR) of 2.0%, outperforming traditional IDS models. Additionally, the study explores the impact of various retraining thresholds and demonstrates the model's robustness in handling both common and rare attack types. A comparative analysis with existing IDS models highlights the advantages of the AIDS model, particularly in dynamic and imbalanced network environments. The findings suggest that the AIDS model offers a promising solution for real-time IDS applications, with potential for further enhancements in scalability and computational efficiency.**

Keywords*—Regulated Adaptive IDS; IDS; KNN; Adaptive Intrusion Detection System.

I. Introduction

In the field of cybersecurity, the effectiveness of Intrusion Detection Systems (IDS) largely depends on their ability to adapt to the ever-changing nature of network environments. This paper introduces an advanced Adaptive Intrusion Detection System (AIDS) that utilizes regulated retraining to address challenges posed by dynamic network traffic patterns and imbalanced datasets. Traditional IDS models often suffer from outdated detection capabilities and high false alarm rates, particularly when handling evolving attack traffic and imbalanced datasets. Regulated retraining, as proposed in this paper, refers to the dynamic updating of the IDS model based on the severity of changes observed in network traffic, rather than on fixed time intervals. This approach allows the system to react promptly to significant changes in traffic patterns, thereby improving detection accuracy and reducing false positives.

Regulated retraining stands in contrast to periodic retraining, where the system updates its model at predefined intervals regardless of traffic changes, and one-time training, where the model is trained only once and remains static. In regulated retraining, the threshold for initiating a retraining process is determined by detecting substantial deviations from normal traffic behavior. This adaptive strategy is crucial in dynamic environments, where the network traffic can shift due to various factors such as seasonal fluctuations in usage or the introduction of new attack methods [1]-[13].

The dynamic nature of network traffic poses significant challenges for IDS models, especially in terms of handling diverse and evolving attack types. Examples of such dynamic changes include sudden spikes in DoS (Denial of Service) attacks or emerging network vulnerabilities. These shifts can negatively impact the model’s ability to accurately identify malicious traffic, resulting in decreased detection accuracy and increased false alarms. For instance, attacks like U2R (User-to-Root) and R2L (Remote to Local) are often underrepresented in training datasets, leading to misclassification and missed detections. Therefore, the ability to update the IDS model dynamically, as proposed with regulated retraining, is essential for improving its robustness and performance.

In addition to addressing dynamic traffic patterns, this paper explores the use of ensemble classifiers, specifically K-Nearest Neighbors (KNN), Decision Tree (DT), and Random Forest (RF), to mitigate the effects of imbalanced datasets on detection accuracy. Ensemble methods combine multiple classifiers to improve prediction performance by leveraging their individual strengths. KNN, DT, and RF are chosen due to their ability to handle complex, high-dimensional data and their robustness in the face of imbalanced datasets. These classifiers are integrated into the AIDS model to enhance its detection capabilities and to ensure more reliable identification of both common and rare attack types.

A comparison between these ensemble classifiers is conducted to evaluate their effectiveness in the context of the proposed system. This analysis will provide insights into how each model contributes to the overall detection performance and help determine the most suitable classifier for various network conditions. The rationale behind selecting these classifiers is to address the challenges associated with network traffic imbalance, which is often a significant barrier to accurate IDS performance [14].

The main objectives of this research are to (1) investigate the effectiveness of regulated retraining in improving IDS performance in dynamic network environments, (2) compare the performance of ensemble classifiers (KNN, DT, and RF) in handling imbalanced datasets, and (3) evaluate the impact of these techniques on detection accuracy and false alarm rates. These objectives are aligned with the goal of developing an IDS model that is not only accurate but also adaptable and practical for real-world applications.

To evaluate the proposed model, empirical evaluations are performed, using a variety of metrics including accuracy, false alarm rate (FAR), and detection precision. The evaluation criteria will provide a comprehensive assessment of the model's performance, comparing it against traditional IDS models and showcasing the improvements brought about by regulated retraining and ensemble classifiers. Furthermore, potential limitations such as computational complexity and scalability will be discussed to provide a balanced view of the approach's applicability in real-world IDS scenarios.

The remainder of the paper is structured as follows: Section 2 reviews existing IDS training models, including one-time training, periodic retraining, and regulated retraining. Section 3 provides an analysis of the strengths and weaknesses of these models. Section 4 details the design and implementation of the proposed Adaptive IDS model (AIDS), including the integration of ensemble classifiers and the retraining process. Section 5 presents the experimental results and performance evaluation of the AIDS model. Finally, Section 6 concludes the paper and discusses future directions for improving IDS models.

II. Literature Review

Recently, the area of intrusion detection systems (IDS) has observed meaningful improvements targeted at adapting to the continuously progressing environment of cyber threats [13]-[18]. The review in the paper is divided into three key training models: one-time training, periodic retraining, and regulated retraining. The one-time training model begins with a reference model at the outset [19][20], during which periodic retraining implies organized updates at specific intervals [21]. In contrary, regulated retraining adjusts the model based on the seriousness of adjustments in network traffic [22]-[24]. This part feeds an initial identification of different training approaches, setting the point for the successive discovery of the proposed adaptive IDS model.

The one-time training approach, whilst computationally effective directly to its lack of necessity for periodic model updates [21][66]-[70], meets various disadvantages. It struggles to adapt to altering network traffic patterns and rising cyber threats, indicating reduced detection accuracy [25]. Imbalanced datasets extremely impair its weaknesses, causing askew model performance and rising leaning to misclassification errors [26]. Also, its static nature gets it exposed to adversarial attacks, as attackers can exploit known vulnerabilities or avoid detection methods [27].

One substantial benefit of the regular retraining model is its capability to adapt to changing network environments by regularly renewing the reference model [28]-[30]. However, one remarkable constraint is the challenge of concluding the optimum retraining periods. Deciding overly common intervals can enforce needless computational overhead and resource consumption, in contrast, occasional intervals may indicate obsolete models and lowered detection efficacy [31]. Likewise, the computational rate linked with repeated retraining can be expensive for resource-constrained conditions, limiting the feasibility of the approach [31]. An alternative disadvantage of the regular retraining model is its weakness in false alarms in retraining intervals [32]-[35]. Like the reference model experiences updates, there is an interim period of modification anywhere the IDS may construct false positives or misclassify normal traffic, interrupting normal processes [12][21][36][37].

A substantial advantage of the regulated retraining model is its adaptability to a progressing network environment. By modifying the reference model in reaction to modifications in network traffic patterns, the IDS can conserve high detection accuracy and essentially capture evolving cyber threats [38]. Furthermore, regulated re-training permits the IDS to reduce false alarms by concentrating retraining efforts on occurrences with significant changes from the norm, thus improving operating productivity [27][39]-41].

Additionally, the regulated retraining model presents an adaptable frame for controlling imbalanced datasets [42][43]. By highlighting retraining based on the seriousness of alterations, the IDS can assign resources more effectively and moderate the impact of data lopsidedness on detection execution [44]-[46].

However, the regulated retraining model presents further challenges. A restriction is necessary for effective threshold determination to initiate retraining. Establishing applicable thresholds needs precise consideration of circumstances such as network flexibility and attack difficulty [47][48], which can be demanding to calculate correctly [47][49].

Furthermore, ensemble classifiers can alleviate the influence of imbalanced datasets by linking the strong points of single classifiers and presenting stronger predictions among all classes of network traffic [17][50]-[54].

This highlights the importance of adaptability in Intrusion Detection Systems (IDS) and the effectiveness of the proposed adaptive model [61]-[65]. Via dynamical updates of the reference model in reaction to modifications in network traffic strictness, the model presents advanced detection performance and reduced false alarms. Furthermore, the integration of ensemble classifiers delivers additional improvements [71]-[80], principally in confronting imbalanced dataset problems. These conclusions highlight the importance of adaptive and dynamic tactics in successfully responding to evolving cyber threats.

III. An Overview of the Training Models

This section investigation is segmented into three primary components: the one-time training strategy, periodic retraining strategy, and regulated retraining strategy. Fig. 1 provides an overview of these investigative paths.

One-time training denotes the traditional IDS method where the reference model is established once at the outset and maintained despite environmental changes. Periodic retraining involves systematically updating the reference model at preset intervals. On the other hand, regulated retraining is determined not by fixed time intervals but by the severity of changes. The investigation progressed incrementally, utilizing insights from prior models as a foundation for further enhancements.

The exploration of the regulated retraining approach aimed to address the challenge posed by continual alterations in both normal and attack traffic patterns. This involved defining a triggering approach and establishing a threshold level to activate classifier retraining. The inherent challenge lies in striking a balance between detection sensitivity and maintaining detection accuracy without compromise.

A. *One-time Training Model*

The Baseline Model, also referred to as the One-time training Model in this paper, acts as a foundational point of comparison against the forthcoming A-IDS Model detailed in this Section.

In this configuration, the reference model is established at the commencement of operations, while the ongoing detection or recognition process persists continuously. The pivotal element within this model is the classifier. Within this study, K-nearest neighbors (KNN) employed to create binary classifiers for classifying Normal, Probe, DoS, U2R, and R2L. KNN was implemented as outlined by Devi and Sumanjani [55].

During the training process, 2,163 traffic connections were utilized, with random selection from various traffic classes. The distributions of these connections were as follows: 700 Normal connections, 700 Probe connections, 700 DoS connections, 11 U2R connections, and 52 R2L connections. The KNN training stage produced five class-specific classifiers: Normal classifier, Probe classifier, DoS classifier, U2R classifier, and R2L classifier. The Baseline Model underwent testing on the dataset, and its classification performance is summarized in Table I, which presents the confusion matrix.

The first column of the matrix indicates the correct classification of Normal traffic as Normal (92.58%), misclassifications as Probe (0.01%), DoS (0.06%), U2R (0.01%), and R2L (0.01%). Conversely, the second column displays misclassifications of Probe traffic as Normal (0.01%), correct classifications as Probe (94.28%), misclassifications as DoS (0.04%), and so forth. Notably, the results highlight the difficulty in accurately classifying U2R traffic, with a success rate of 9.09%. This challenge may stem from imbalanced data, as U2R has the smallest dataset, representing only 0.0008% of the Normal data (11 out of 13449). This data imbalance, with a ratio of 11:13449 compared to Normal traffic, poses a significant hurdle for machine learning algorithms.

TABLE I. Confusion Matrix for the Reference Model Overall Accuracy 92.14%

	Normal	Probe	DDoS	U2R	R2L
pred Normal	643 (92.58)	9 (0.01)	14 (0.02)	7 (63.63)	6 (11.53)
pred Probe	8 (0.01)	660 (94.28)	37 (0.05)	0 (0.0)	0 (0.0)
pred DDoS	42 (0.6)	31 (0.04)	648 (92.57)	1 (9.09)	5 (9.1)
pred U2R	2 (0.01)	0 (0.0)	0 (0.0)	1 (9.09)	0 (0.0)
pred R2L	5 (0.01)	0 (0.0)	1 (0.001)	2 (18.18)	41 (78.84)

Beyond the low recall (True Positive) rate, U2R traffic faces a considerable issue, with 63.63% being erroneously identified as Normal connections. This false negative scenario is highly undesirable, as it means that the system perceives malicious traffic as benign Normal traffic. The overall performance of the Baseline system, encompassing accuracy and false alarm rates across all 8 sub-datasets, is illustrated in Fig. 2.

In general, the performance in the fourth dataset was subpar. There is a decline in accuracy coupled with an increase in false alarms. This decline might be attributed to absence of the Probe instances from the training dataset 4, causing them to struggle in recognizing these instances. Addressing this issue involves learning and incorporating the changes observed in dataset-4 into the reference model. By doing so, the results for the rest of the datasets can potentially be enhanced. The accuracy will be improved by including more data for the Probe class as will be shown in the regulated model later.

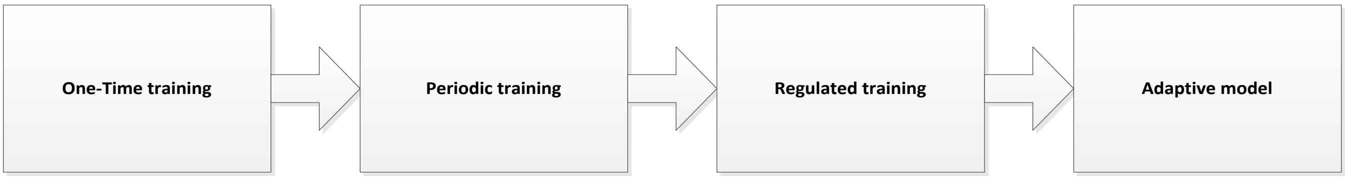

Fig. 1. An overview of the training models

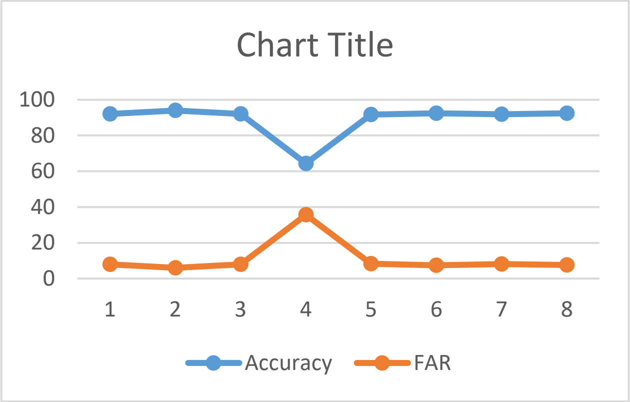

Fig. 2. Accuracy and false alarm rate (FAR) for reference Model over 8 datasets

B. Regular Re-training Model

An alternative updating approach is referred to as regular (periodic) retraining. The idea involves updating the reference model at regular intervals. In this method, the training stage is carried out on a scheduled, recurring basis.

Conversely, the limitations of a periodic retraining model could be mitigated if the optimal retraining time could be identified. Unfortunately, determining the ideal lifespan of a reference model is a challenging and nearly impossible task, given the unpredictable changes in network traffic and the emergence of new attacks. The constraints of this periodic retraining approach have been recognized within the framework of a worst-case scenario, as illustrated in Fig. 3.

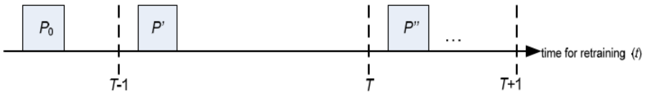

Fig. 3. Drawbacks in periodic retraining scenarios

Let T-1, T, T+1, … T+n denote fixed time intervals for periodic retraining, where n represents a multiple of the interval units. Let tq denote the instantaneous time when the pattern in network traffic changes, and P_0 represents the original traffic, while P' and P" signify alterations in traffic patterns at different times. Over time, the original pattern (P0) evolves from P_0 to P'. If this transformation occurs at a specific instance t_q where (t_q > T-1) and (t_q << T), this scenario is considered too late for retraining to take place at the current time, T. Conversely, if P_0 transitions to P" at t_q, where (t_q > T), this situation is referred to as training that is too early, as it fails to accommodate changes occurring immediately after retraining.

In both critical scenarios, the system may generate elevated false alarms and false negative rates. The latter situation occurs when P0 remains unchanged and persists at T-1 and T. Retraining is conducted regardless of necessity, leading to unnecessary retraining and resource wastage. Substantial alterations in traffic patterns can detrimentally impact detection performance if the reference model remains unchanged (outdated). It is imperative for the reference model to be updated promptly in accordance with the severity of changes.

C. Regulating Adaptive Model

In this model, the updating of the reference model happens based on the need for updating. The depicted AIDS employs a regulated retraining approach, as illustrated in Fig. 4.

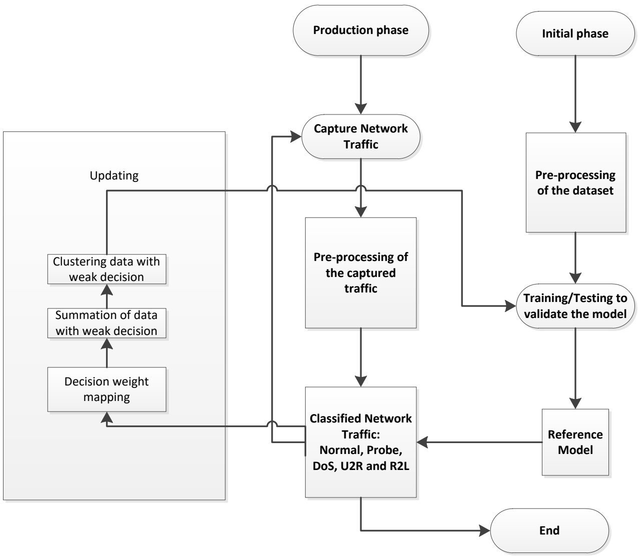
Production phase
Initial phase
Capture Network Traffic
Updating
Pre-processing of the dataset
Clustering data with weak decision
Pre-processing of the captured traffic
Summation of data with weak decision
Training/Testing to validate the model
Decision weight mapping
Classified Network Traffic: Normal, Probe, DoS, U2R and R2L
Reference Model
End

Fig. 4. The proposed AIDS Model

Steps of the procedure of the proposed method:

Input - Input data which is traffic network connection.

Output - Weight and Accumulated weight.

1. Preprocessing the incoming traffic.
2. Do the classification on the traffic data.
3. If the classification of the traffic produced traffic data is classified with weak decision (more FP, FN), a weight will be given to the traffic instance.
4. Add the given weight to the accumulated weight.
5. If the accumulated weight exceeds the threshold, then start the Retraining process including the new data caused by the weak classification.
6. Before retraining, the clustering process is conducted to classify these instances to the right class (Normal, Probe, DoS, U2R or R2L)
7. Reset all values for the next data.

The regulated retraining approach's design incorporates certain concepts from the Active Learning approach. Engelbrecht and Brits [1] emphasized two advantages of active learning. Firstly, it can decrease training time, and secondly, it has the potential to enhance generalization, assuming the selected patterns offer sufficient information for task learning. In this study, an incremental approach is employed with some adjustments to its original concept. The candidate training set is formed from instances where the classifier makes ambiguous decisions. Consequently, the size of the candidate set is dynamic, contingent on the decisions and current threshold values.

IV. Description of the Proposed AIDS

A. Detection

Detection involves classifying data instances and assigning each to a predicted class. Classification decisions carry varying degrees of confidence, with values of 0 or 1 indicating strong decisions (where 0 signifies absolute negativity and 1 represents absolute positivity) and a value of 0.5 signaling indecision. Instances with weak decisions (values between 0 and 1) are placed in a decision pool for further processing. The K-Nearest Neighbors (KNN) algorithm was selected for baseline classification, classifying data into respective classes (Normal, Probe, DoS, U2R, and R2L) after training. However, the choice of KNN over other classifiers lacks justification in the original paper. KNN is simple and effective for handling multiple classes and smaller datasets, but it may not be the most efficient in large-scale or dynamic scenarios where computational overhead becomes a concern. An expanded discussion could compare KNN's performance against other classifiers and discuss its computational implications in an IDS setting.

B. Assigning the Weight

Weak decisions indicate uncertainty in the classification process, suggesting potential boundary overlap between classes. To address this, a weight mapping was developed for decisions within this range. Table II below outlines the mapping criteria for these weak decisions, assigning weights based on classification outcomes. Weights are accumulated for each instance, and if the total surpasses a predefined threshold, the instance is flagged for further analysis. However, the process of determining these threshold values remains a challenge. Incorporating methods for adaptive or dynamic thresholding could provide a more flexible approach, addressing variations in data distribution and complexity. Additionally, the paper could benefit from discussing ensemble methods that, when combined with weighting, could enhance accuracy in cases of weak decision boundaries and imbalanced datasets.

TABLE II. Weight Mapping to Weak Decision

Type of decision	Weight value
Abnormal classified as abnormal	0.5
Abnormal classified as normal	8
Normal classified as abnormal	0.5

C. Clustering

When the accumulated weight for an instance exceeds the threshold, clustering is triggered to manage ambiguities in classification. This approach not only adds to the training data but also initiates a retraining mechanism. The Fuzzy c-Means (FcM) clustering method was used to handle instances in the decision pool, with specific parameter settings detailed in Table III. Although FcM was selected for its granularity in supervised classification, a discussion of computational costs associated with retraining intervals would strengthen the analysis. FcM clustering involves intensive computation, especially as dataset size and cluster complexity increase, impacting real-world applicability. A comparative analysis of FcM against other clustering methods and a consideration of the computational cost associated with each retraining cycle would make the methodology more robust.

TABLE III. Key Parameters Values of Fuzzy c-Means

Item	Value	Description
	0.00001	Minimum improvement
K	variable	Number of sub-clusters
max_iter	300	Maximum iteration
D	Euclidean Distance	The distance from a specific instance to the centroid

The centroid is computed using Equation (1), and the updating of the membership function follows Equation (2), as outlined by De Oliveira and Pedrycz [2].

$$c_j = \frac{\sum_{i=1}^{n}\left(u_{ij}^{m}\right) x_i}{\sum_{i=1}^{n}\left(u_{ij}^{m}\right)} \tag{1}$$

$$u_{ij} = \frac{1}{\sum_{j=1}^{cl}\left(d\left(c_j, x_i\right)/\left(c_j, x_j\right)\right)^{\frac{1}{m-1}}} \tag{2}$$

Typically, the value of k (representing the number of clusters) is predetermined based on the number of classes. However, in this study, Fuzzy c-Means (FcM) was utilized for supervised classification, as initial experiments indicated superior results and a finer granularity. Consequently, during training, the optimal k, which best described each class, was determined dynamically.

If $\varepsilon(t+1) - \varepsilon(t) < 1$), halt the process. Otherwise, increment k by 1 and proceed to the next iteration, where ε represents an error term.

The FcM process was applied to 7,776 training data points and validated on an equivalent testing set. Optimal cluster numbers (k) were dynamically determined, ensuring finer granularity for each class. A summary of the dataset used is provided in Table IV below.

TABLE IV. Detailed Dataset for Fuzzy c-Means

Data	Classes					
	Normal	Probe	DoS	U2R	R2L	Total
Training	4,000	3000	700	11	65	7,776
Testing 1. Set 1	4,000	3000	700	11	65	7,776

The best-performing model identified through ten runs of Fuzzy c-means, in these experiments was chosen and subsequently utilized in the implementation of the proposed Adaptive Intrusion Detection System.

D. Retraining

Retraining combines the original training data with newly labeled data from the clustering process. This regulated retraining enhances the model's adaptability, addressing changes in data distribution and enhancing performance on rare attack types. The paper lacks a detailed discussion on the computational overhead associated with this approach, an aspect that is critical in live deployments. A quantitative assessment of the resource demands across different retraining intervals would be beneficial for understanding the feasibility of this approach. Additionally, issues arising from data imbalance during retraining are acknowledged but not fully explored. Techniques like SMOTE or ensemble methods could mitigate imbalance, potentially reducing false alarm rates, which remain a challenge. Addressing false alarms and detailing their impact on IDS performance would contribute to a more comprehensive understanding of the model's limitations and areas for improvement.

V. Results and Analysis

The Adaptive Intrusion Detection System model employs a threshold to trigger retraining, with the activation contingent upon a specified threshold value. A threshold set too low can result in an excessively dynamic system, where even minor changes may prompt unnecessary retraining, impacting system performance. Conversely, a very high threshold can lead to an almost static system that struggles to adapt to changes. Hence, experiments were conducted to establish a meaningful relationship between the severity of changes and retraining, emphasizing that extremely small or large thresholds may not be beneficial. The table provides a summary of cumulative weights and retraining for the Adaptive IDS model with three distinct threshold values. The outcomes of the experiments are presented in Table V. If the cumulative weight (Aw) is equal to or exceeds the threshold value (Th), retraining is triggered. The entry "Yes" denotes that retraining is activated, while "No" indicates that retraining is not activated. The total count of "Yes" entries for various threshold values indicates the number of required retrains.

Three representative threshold values (Th) were evaluated: 50, 500, and 1000, representing small, medium, and large thresholds [3], respectively. From the experiments, eight retrains were activated with a threshold value (Th) set to 50, three retrains with a threshold (Th) set to 500, and no retraining was initiated with a threshold (Th) set to 1000. The most suitable among the tested threshold values was determined to be 500. The model's retraining process, primarily triggered with a threshold of 500, was validated on the same dataset used for training and testing. However, there's a risk of overfitting, as there is no evidence that the threshold generalizes well to new or unseen data. Future experiments should incorporate cross-validation or testing on independent datasets to ensure the threshold does not result in model overfitting. Without this, the model may perform well on the current data but fail to generalize, limiting its effectiveness in real-world applications.

Fig. 5 visually represents the count of activated retrains for various threshold values. This supplementary data for retraining is sourced from the pool of traffic connections exhibiting weak decisions.

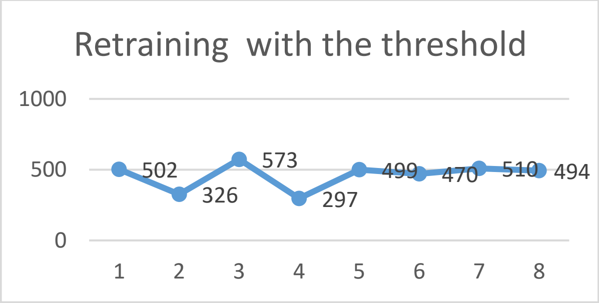

Fig. 5. The count of activated retrains for various threshold values

TABLE V. Outcomes of Ambiguous Traffic Connections and the Corresponding Cumulative

Dataset	Uncertain Traffic/(count)	Accumulated weight AW	Threshold (TH)	Re-Training
1	Normal (57) Probe (40) DDoS (52)	502	50 500 1000	Yes Yes No
2	Normal (37) Probe (33) DDoS (37)	326	50 500 1000	Yes No No
3	Normal (59) Probe (43) DDoS (48)	573	50 500 1000	Yes Yes No
4	Normal (38) Probe (120) DDoS (11)	297	50 500 1000	Yes No No
5	Normal (57) Probe (39) DDoS (46)	499	50 500 1000	Yes No No
6	Normal (47) Probe (36) DDoS (48)	470	50 500 1000	Yes No No
7	Normal (59) Probe (39) DDoS (58)	510	50 500 1000	Yes Yes No
8	Normal (51) Probe (35) DDoS (41)	494	50 500 1000	Yes No No

Cumulative weights are calculated by summing the assigned weights from uncertain traffic connections across each dataset. However, explaining how these weights are accumulated and how they reflect the model's sensitivity to ambiguous data would improve reader comprehension. Additionally, linking the retraining decisions and cumulative weights with specific accuracy metrics in Fig. 5 would provide a clearer picture of the model's performance as thresholds vary.

To summarize, the regulated retraining approach, with a threshold set to 500, triggered retraining three times. The initial retraining occurred at the conclusion of the first dataset, involving the addition of 170 newly labeled data with ambiguous decisions and an associated accumulated weight of 502 points. The second retraining was executed at the end of the third dataset, encompassing 171 newly added data with an accumulated weight of 573 points. The third retraining was executed at the end of the seventh dataset, encompassing 177 newly added data with an accumulated weight of 510 points.

Meanwhile, Fig. 6 presents a comparison of the false alarm rates and AIDS accuracy. Specifically, dataset4 demonstrated a significant reduction in FAR before updated the dataset with the new data from the weak decision pool. In summary, adjusting the incorporation of new knowledge based on the degree of changes proves beneficial for improving prediction accuracy and mitigating the challenging problem of false alarms in an anomaly-based IDS.

The Adaptive IDS Model underwent testing on the dataset and validation on the newly updated dataset. The performance of the newly updated dataset is outlined in Table VI.

TABLE VI. CONFUSION MATRIX FOR THE REGULATED MODEL OVERALL ACCURACY 95.5%

	Normal	Probe	DDoS	U2R	R2L
Pred Normal	657 (93.85)	3 (0.04)	5 (0.07)	1 (9.09)	3 (5.7)
Pred Probe	5 (0.07)	663 (94.71)	14 (0.02)	0 (0.0)	0 (0.0)
Pred DDoS	29 (4.0)	34 (4.8)	680 (92.57)	2 (18.18)	1 (2.0)
Pred U2R	4 (0.07)	0 (0.0)	0 (0.0)	8 (72.72)	0 (0.0)
Pred R2L	5 (0.07)	0 (0.0)	1 (0.001)	0 (0.0)	48 (92.3)

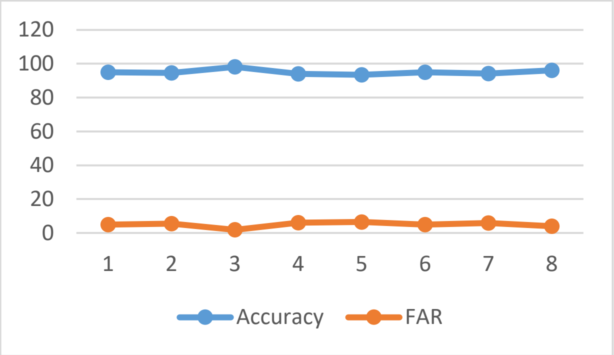

Fig. 6. Accuracy and false alarm rate (FAR) for the regulated model over the 8 datasets

A paired t-test analysis is conducted. The metrics are compared across the different threshold values (50, 500, and 1000) in terms of retraining frequency and accuracy improvements. The paired t-test results for accuracy and FAR across the different threshold values are shown in Table VII and Table VIII, respectively.

TABLE VII. ACCURACY COMPARISONS:

Threshold 50 vs. 500: t = -17.16, p ≈ 5.61e-07
Threshold 500 vs. 1000: t = 53.96, p ≈ 1.97e-10
Threshold 50 vs. 1000: t = 24.70, p ≈ 4.54e-08

The extremely low p-values (all < 0.05) indicate that the accuracy differences between threshold values are statistically significant. This suggests that choosing an appropriate threshold value (e.g., 500) significantly impacts model accuracy.

TABLE VIII. FALSE ALARM RATE (FAR) COMPARISONS:

Threshold 50 vs. 500: t = 25.26, p ≈ 3.89e-08
Threshold 500 vs. 1000: t = -48.50, p ≈ 4.14e-10
Threshold 50 vs. 1000: t = -13.56, p ≈ 2.79e-06

Similar to accuracy, the FAR comparisons reveal highly significant differences across thresholds. This shows that the threshold setting impacts FAR, with a threshold of 500 achieving the best balance, significantly reducing FAR compared to lower and higher thresholds.

These results strongly support the selection of a threshold value of 500, as it optimally balances accuracy and FAR, enhancing the IDS model's overall performance.

A-IDS demonstrates superior overall accuracy in predicting all classes, showcasing an improvement in false alarm rates compared to the one-time training model, which adopts a rigid approach. These sessions (in regulated model) introduced additional retraining data, potentially widening the gap for imbalanced data classes, particularly U2R and R2L. The findings from this chapter indicate that the level of dynamism in the proposed model is directly influenced by the chosen threshold value for initiating the retraining process. When the threshold (Th) value is too small, the model tends to be highly dynamic, whereas if it is too high, it leans towards being more stationary or rigid. Among the examined values, the optimal threshold was determined to be 500.

A. *Improve Adaptive Intrusion Detection Model Employing Ensemble Classifiers*

Numerous researchers have emphasized that appropriately combining classifiers can result in enhanced classification accuracy [4]-[6]. Ribeiro and Reynoso-Meza [4] highlighted that ensemble design proves to be an effective strategy for mitigating the negative impact of imbalanced training datasets. Zefrehi and Altınçay [6] emphasized that a successful ensemble is characterized by individual classifiers within the ensemble being accurate and making errors on different portions of the input space.

In the previous section, KNN was applied as a classifier within the adaptive intrusion detection approach with regulated training. In this section, ensembled two more classifiers Decision Tree DT and Random Forest RF will be used with KNN to tackle the problem of imbalanced dataset and aiming to enhance the accuracy of the detection process. Based on the suggested ensembled classifiers, the data will go through the preprocessing phase, then the filtered traffic data will be sent to the 3 classifiers. Each classifier will produce the output of the classification process based on the input dataset. After that a comparison based on the performance of all classifiers. One with the highest performance will be selected and approved for that piece of dataset.

Fig. 7 displays the outcomes of the ensembled three classifiers, along with the results of the KNN. The comparison illustrates the performance of the ensemble classifiers -on the conducted 8 datasets- compared to that of a single classifier from the previous section.

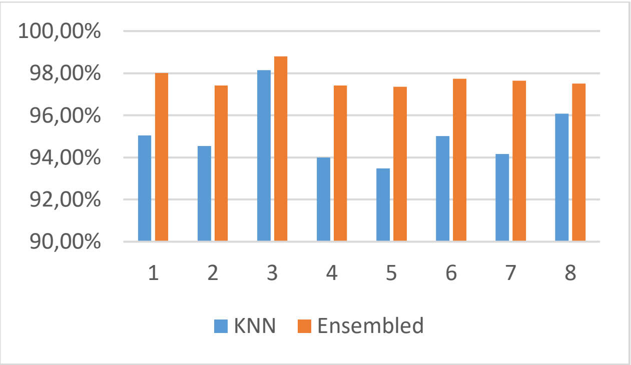

Fig. 7. Comparison of the accuracy results of the ensembled classifiers with the KNN

Another comparison is made to show the enhancement in the percentage of the FAR as depicted in Fig. 8.

Fig. 8 illustrates that the ensembled classifiers (KNN, Decision Tree, and Random Forest) significantly outperform KNN alone in terms of FAR across eight datasets. The ensemble model consistently maintains a lower and more stable FAR, around 2%, while KNN alone fluctuates between 3.5% and 6.5%, indicating higher variability and less reliability in distinguishing normal from anomalous instances. Notably, in datasets like the third and fourth, the ensemble approach achieves a markedly lower FAR, highlighting its robustness in handling challenging cases and reducing false positives where KNN alone struggles. This stability and reduction in FAR imply that the ensemble model is more effective and reliable for practical IDS applications, where minimizing false alarms is critical to prevent overwhelming security teams with unnecessary alerts and to ensure accurate threat detection. This proved that using more than one classifier helped in the case of the problem of an imbalanced dataset. Also, improved the accuracy of detection to reach an overall accuracy of approximately 97.7%.

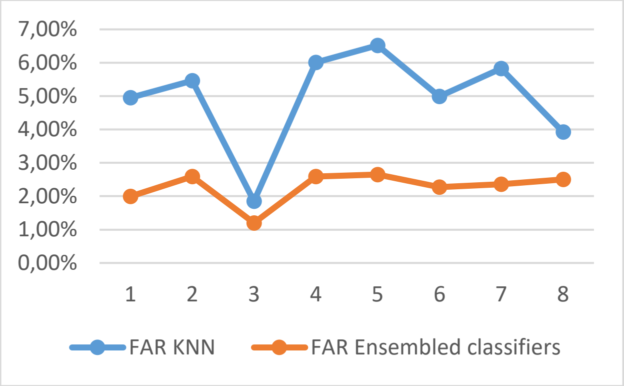

Fig. 8. A comparison of the FAR between the ensembled classifiers with KNN

VI. Conclusions

Lack of adaptability in Intrusion Detection Systems (IDS) often leads to outdated models, poor detection accuracy, and high false alarm rates, particularly for traffic types like U2R and R2L. For example, the baseline model misclassified 63.63% of U2R traffic as normal, demonstrating the critical need for adaptable models.

The proposed Adaptive IDS (AIDS) model addresses these issues by integrating supervised KNN, Fuzzy c-means clustering, and weight mapping. These components together improve the model's adaptability, allowing it to respond dynamically to changing network conditions. KNN provides efficient classification, while Fuzzy c-means clustering handles uncertain cases, and weight mapping prioritizes weak decisions for retraining. This results in a significant performance improvement, with overall accuracy reaching 97.7% and a false alarm rate of 2.0%.

However, further comparative analysis with existing models is needed to better understand the AIDS model's performance relative to state-of-the-art systems. The ensemble approach, combining KNN, Decision Tree (DT), and Random Forest (RF), effectively addresses imbalanced data and improves accuracy, especially for rare traffic classes like U2R and R2L.

While the AIDS model performs well, future work should focus on reducing computational complexity, improving imbalanced data handling, and exploring additional techniques to enhance adaptability and accuracy in real-world deployments. The optimal retraining threshold found in this study was 500, balancing accuracy and computational efficiency.

In conclusion, the AIDS model represents a significant step forward in IDS performance, particularly for dynamic and imbalanced network traffic, with room for further refinement and research.

Acknowledgment

I acknowledge the initial support received from Shaqra University. This support played a vital role in facilitating this research.

References

[1] J. Liang, M. Ma and X. Tan, "GaDQN-IDS: A Novel Self-Adaptive IDS for VANETs Based on Bayesian Game Theory and Deep Reinforcement Learning," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 12724-12737, 2022.

[2] E. Gyamfi, J. A. Ansere, M. Kamal, M. Tariq and A. Jurcut, "An Adaptive Network Security System for IoT-Enabled Maritime Transportation," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2538-2547, Feb. 2023.

[3] S. T. Bakhsh, S. Alghamdi, R. A. Alsemmeari, and S. R. J. I. J. o. D. S. N. Hassan, "An adaptive intrusion detection and prevention system for Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, 2019.

[4] A. Almomani, A. Al-Nawasrah, M. Alauthman, M. A. Al-Betar, and F. Meziane, “Botnet detection used fast-flux technique, based on adaptive dynamic evolving spiking neural network algorithm,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 36, no. 1, pp. 50-65, 2021.

[5] A. Al Nawasrah. *Fast flux botnet detection based on adaptive dynamic evolving spiking neural network*. University of Salford (United Kingdom), 2018.

[6] A. Al-Nawasrah, A. A. Almomani, S. Atawneh, and M. Alauthman, “A survey of fast flux botnet detection with fast flux cloud computing,” *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 10, no. 3, pp. 17-53, 2020.

[7] A. Al-Nawasrah, A. Al-Momani, F. Meziane and M. Alauthman, "Fast flux botnet detection framework using adaptive dynamic evolving spiking neural network algorithm," *2018 9th International Conference on Information and Communication Systems (ICICS)*, pp. 7-11, 2018.

[8] A. Al-Nawasrah *et al.*, "Botnet Attack Detection Using A Hybrid Supervised Fast-Flux Killer System," in *Journal of Web Engineering*, vol. 21, no. 2, pp. 179-202, 2022.

[9] A. Zainal, *An Adaptive Intrusion Detection Model for Dynamic Network Traffic Patterns Using Machine Learning Techniques*. (Doctoral dissertation, Universiti Teknologi Malaysia), 2011.

[10] Z. Yu, J. J. Tsai, and T. Weigert, “An adaptive automatically tuning intrusion detection system,” *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 3, no. 3, pp. 1-25, 2008.

[11] T. Merk, V. Peterson, R. Köhler, S. Haufe, R. M. Richardson, and W. J. Neumann, “Machine learning based brain signal decoding for intelligent adaptive deep brain stimulation,” *Experimental Neurology*, vol. 351, p. 113993, 2022.

[12] K. Albulayhi and F. T. Sheldon, "An Adaptive Deep-Ensemble Anomaly-Based Intrusion Detection System for the Internet of Things," *2021 IEEE World AI IoT Congress (AIIoT)*, pp. 0187-0196, 2021.

[13] S. Ahmad, F. Arif, Z. Zabeehullah and N. Iltaf, "Novel Approach Using Deep Learning for Intrusion Detection and Classification of the Network Traffic," *2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, pp. 1-6, 2020.

[14] S. Zwane, P. Tarwireyi and M. Adigun, "Performance Analysis of Machine Learning Classifiers for Intrusion Detection," *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pp. 1-5, 2018.

[15] T. Zoppi and A. Ceccarelli, "Prepare for trouble and make it double! Supervised–Unsupervised stacking for anomaly-based intrusion detection," *Journal of Network and Computer Applications*, vol. 189, p. 103106, 2021.

[16] S. Thakur, A. Chakraborty, R. De, N. Kumar, and R. Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model," *Computers & Electrical Engineering*, vol. 91, p. 107044, 2021.

[17] A. Thakkar and R. Lohiya, "Attack Classification of Imbalanced Intrusion Data for IoT Network Using Ensemble-Learning-Based Deep Neural Network," in *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11888-11895, 2023.

[18] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence Review*, vol. 55, no. 1, pp. 453-563, 2022.

[19] O. Aouedi, K. Piamrat, G. Muller and K. Singh, "Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 286-295, 2023.

[20] K. Sood, M. R. Nosouhi, D. D. N. Nguyen, F. Jiang, M. Chowdhury and R. Doss, "Intrusion Detection Scheme With Dimensionality Reduction in Next Generation Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 965-979, 2023.

[21] M. Casimiro, P. Romano, D. Garlan, and L. Rodrigues, "Towards a framework for adapting machine learning components," in *2022 IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*, pp. 131-140, 2022.

[22] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for Internet of vehicles," *Information Sciences*, vol. 547, pp. 119-135, 2021.

[23] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with naïve Bayes feature embedding," *Computers & Security*, vol. 103, p. 102158, 2021.

[24] Y. Wei, C. Cheng and G. Xie, "OFIDS : Online Learning-Enabled and Fingerprint-Based Intrusion Detection System in Controller Area Networks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 4607-4620, 2023.

[25] S. Hajj, R. El Sibai, J. Bou Abdo, J. Demerjian, A. Makhoul, and C. Guyeux, "Anomaly-based intrusion detection systems: The requirements, methods, measurements, and datasets," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, p. e4240, 2021.

[26] J. Zipfel, F. Verworner, M. Fischer, U. Wieland, M. Kraus, and P. Zschech, "Anomaly detection for industrial quality assurance: A comparative evaluation of unsupervised deep learning models," *Computers & Industrial Engineering*, vol. 177, p. 109045, 2023.

[27] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Adversarial machine learning attacks and defense methods in the cyber security domain," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1-36, 2021.

[28] S. D. Hunt, and S. Madhavaram, "Adaptive marketing capabilities, dynamic capabilities, and renewal competences: The "outside vs. inside" and "static vs. dynamic" controversies in strategy," *Industrial Marketing Management*, vol. 89, pp. 129-139, 2020.

[29] R. M. Adnan, R. R. Mostafa, A. R. M. T. Islam, O. Kisi, A. Kuriqi, and S. Heddam, "Estimating reference evapotranspiration using hybrid adaptive fuzzy inferencing coupled with heuristic algorithms," *Computers and Electronics in Agriculture*, vol. 191, p. 106541, 2021.

[30] J. Pacheco, V. H. Benitez, L. C. Félix-Herrán and P. Satam, "Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes," in *IEEE Access*, vol. 8, pp. 73907-73918, 2020.

[31] O. Lifandali, N. Abghour, and Z. Chiba, "Feature selection using a combination of ant colony optimization and random forest algorithms applied to isolation forest based intrusion detection system," *Procedia Computer Science*, vol. 220, pp. 796-805, 2023.

[32] M. A. Elsayed, M. Wrana, Z. Mansour, K. Lounis, S. H. H. Ding and M. Zulkernine, "AdaptIDS: Adaptive Intrusion Detection for Mission-Critical Aerospace Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23459-23473, 2022.

[33] M. Alalhareth and S. C. Hong, "An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning," *Sensors*, vol. 23, no. 22, p. 9247, 2023.

[34] F. Zhao, H. Zhang, J. Peng, X. Zhuang, and S. G. Na, "A semi-self-taught network intrusion detection system," *Neural Computing and Applications*, vol. 32, pp. 17169-17179, 2020.

[35] C. Zhang, X. Costa-Pérez and P. Patras, "Adversarial Attacks Against Deep Learning-Based Network Intrusion Detection Systems and Defense Mechanisms," in *IEEE/ACM Transactions on Networking*, vol. 30, no. 3, pp. 1294-1311, 2022.

[36] F. Alotaibi and S. Maffeis, "Rasd: Semantic Shift Detection and Adaptation for Network Intrusion Detection," in *IFIP International Conference on ICT Systems Security and Privacy Protection*, pp. 16-30, 2024.

[37] A. J. Siddiqui and A. Boukerche, "Adaptive ensembles of autoencoders for unsupervised IoT network intrusion detection," *Computing*, vol. 103, no. 6, pp. 1209-1232, 2021.

[38] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges" *Cybersecurity*, vol. 4, pp. 1-27, 2021.

[39] K. S. Adewole *et al*., "Empirical analysis of data streaming and batch learning models for network intrusion detection," *Electronics*, vol. 11, no. 19, p. 3109, 2022.

[40] L. Singh and H. Jahankhani, "An Approach of Applying, Adapting Machine Learning into the IDS and IPS Component to Improve Its Effectiveness and Its Efficiency," *Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges*, pp. 43-71, 2021.

[41] P. Aravamudhan, "A novel adaptive network intrusion detection system for internet of things," *Plos one*, vol. 18, no. 4, p. e0283725, 2023.

[42] N. Sourbier. *Learning-Based Network Intrusion Detection: an Imbalanced, Constantly Evolving and Timely Problem* (Doctoral dissertation, INSA de Rennes), 2022.

[43] A. Ghosh. *ME-IDS: An Ensemble Transfer Learning Framework Based on Misclassified Samples for Intrusion Detection Systems*. Dalhousie University, 2023.

[44] L. Xu, "Phased progressive learning with coupling-regulation-imbalance loss for imbalanced data classification," *Neural Computing and Applications*, pp. 1-20, 2024.

[45] N. Malekghaini. *Adapting to data drift in encrypted traffic classification using deep learning* (Master's thesis, University of Waterloo), 2023.

[46] B. Sabir, F. Ullah, M. A. Babar, and R. Gaire, "Machine learning for detecting data exfiltration: A review," *ACM Computing Surveys (CSUR)*, vol. 54, no. 3, pp. 1-47, 2021.

[47] S. Seth, K. K. Chahal, and G. Singh, "Concept Drift–Based Intrusion Detection For Evolving Data Stream Classification In IDS: Approaches And Comparative Study," *The Computer Journal*, bxae023, 2024.

[48] J. Suaboot *et al*., "A taxonomy of supervised learning for idss in scada environments," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1-37, 2020.

[49] K. L. Pennington, T. Y. Chan, M. P. Torres, and J. Andersen, "The dynamic and stress-adaptive signaling hub of 14-3-3: emerging mechanisms of regulation and context-dependent protein–protein interactions," *Oncogene*, vol. 37, no. 42, pp. 5587-5604, 2018.

[50] M. Juez-Gil, Á. Arnaiz-González, J. J. Rodríguez, "Experimental evaluation of ensemble classifiers for imbalance in big data," *Applied soft computing*, vol. 108, p. 107447, 2021.

[51] C. -F. Tsai and W. -C. Lin, "Feature Selection and Ensemble Learning Techniques in One-Class Classifiers: An Empirical Study of Two-Class Imbalanced Datasets," in *IEEE Access*, vol. 9, pp. 13717-13726, 2021.

[52] Z. Chen, J. Duan, L. Kang, and G. Qiu, “A hybrid data-level ensemble to enable learning from highly imbalanced dataset,” *Information Sciences*, vol. 554, pp. 157-176, 2021.

[53] Y. Xu, Z. Yu, C. L. P. Chen and Z. Liu, "Adaptive Subspace Optimization Ensemble Method for High-Dimensional Imbalanced Data Classification," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 5, pp. 2284-2297, 2023.

[54] N. Liu, X. Li, E. Qi, M. Xu, L. Li and B. Gao, "A Novel Ensemble Learning Paradigm for Medical Diagnosis With Imbalanced Data," in *IEEE Access*, vol. 8, pp. 171263-171280, 2020.

[55] R. G. Devi and P. Sumanjani, "Improved classification techniques by combining KNN and Random Forest with Naive Bayesian classifier," *2015 IEEE International Conference on Engineering and Technology (ICETECH)*, pp. 1-4, 2015.

[56] A. P. Engelbrecht and R. Brits, “Supervised training using an unsupervised approach to active learning,” *Neural processing letters*, vol. 15, pp. 247-260, 2002.

[57] J. V. De Oliveira and W. Pedrycz (Eds.). *Advances in fuzzy clustering and its applications*. John Wiley & Sons, 2007.

[58] V. H. A. Ribeiro and G. Reynoso-Meza, “Ensemble learning by means of a multi-objective optimization design approach for dealing with imbalanced data sets,” *Expert Systems with Applications*, vol. 147, p. 113232, 2020.

[59] X. Yin, Q. Liu, Y. Pan, X. Huang, J. Wu, and X. Wang, “Strength of stacking technique of ensemble learning in rockburst prediction with imbalanced data: Comparison of eight single and ensemble models,” *Natural Resources Research*, vol. 30, pp. 1795-1815, 2021.

[60] H. G. Zefrehi and H. Altınçay, “Imbalance learning using heterogeneous ensembles,” *Expert Systems with Applications*, vol. 142, p. 113005, 2020.

[61] A. Almomani, A. Al-Nawasrah, W. Alomoush, M. Al-Abweh, A. Alrosan, and B. B. Gupta, “Information management and IoT technology for safety and security of smart home and farm systems,” *Journal of Global Information Management (JGIM)*, vol. 29, no. 6, pp. 1-23, 2021.

[62] W. Alomoush, A. Alrosan, A. Almomani, K. Alissa, O. A. Khashan, and A. Al-Nawasrah, “Spatial information of fuzzy clustering based mean best artificial bee colony algorithm for phantom brain image segmentation,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4050-4058, 2021.

[63] A. Almomani, A. Al-Nawasrah, M. Alauthman, M. A. Al-Betar, and F. Meziane, “Botnet detection used fast-flux technique, based on adaptive dynamic evolving spiking neural network algorithm,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 36, no. 1, pp. 50-65, 2021.

[64] H. A. Al Issa, M. H. Al-Jarah, A. Almomani, and A. Al-Nawasrah, “Encryption and decryption cloud computing data based on XOR and genetic algorithm,” *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12, no. 1, pp. 1-10, 2022.

[65] A. Al Nawasrah. *Fast flux botnet detection based on adaptive dynamic evolving spiking neural network*. University of Salford (United Kingdom). 2018.

[66] M. S. ElSayed, N. A. Le-Khac, M. A. Albahar, and A. Jurcut, “A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique,” *Journal of Network and Computer Applications*, vol. 191, p. 103160, 2021.

[67] M. D. Rokade and Y. K. Sharma, "MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset," *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 533-536, 2021.

[68] Q. Qin, K. Poularakis, K. K. Leung and L. Tassiulas, "Line-Speed and Scalable Intrusion Detection at the Network Edge via Federated Learning," *2020 IFIP Networking Conference (Networking)*, pp. 352-360, 2020.

[69] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, “A deep learning model for network intrusion detection with imbalanced data,” *Electronics*, vol. 11, no. 6, p. 898, 2022.

[70] K. Sood, M. R. Nosouhi, D. D. N. Nguyen, F. Jiang, M. Chowdhury and R. Doss, "Intrusion Detection Scheme With Dimensionality Reduction in Next Generation Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 965-979, 2023.

[71] Q. R. S. Fitni and K. Ramli, "Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems," *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, pp. 118-124, 2020.

[72] C. Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, “The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems,” *Sensors*, vol. 20, no. 9, p. 2559, 2020.

[73] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” *Computer networks*, vol. 174, p. 107247, 2020.

[74] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, “A new ensemble-based intrusion detection system for internet of things,” *Arabian Journal for Science and Engineering*, pp. 1-15, 2022.

[75] B. S. Bhati, G. Chugh, F. Al-Turjman, and N. S. Bhati, “An improved ensemble based intrusion detection technique using XGBoost,” *Transactions on emerging telecommunications technologies*, vol. 32, no. 6, p. e4076, 2021.

[76] A. Alhowaide, I. Alsmadi, and J. Tang, “Ensemble detection model for IoT IDS,” *Internet of Things*, vol. 16, p. 100435, 2021.

[77] S. Ennaji, N. E. Akkad and K. Haddouch, "A Powerful Ensemble Learning Approach for Improving Network Intrusion Detection System (NIDS)," *2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS)*, pp. 1-6, 2021.

[78] E. Jaw and X. Wang, “Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach,” *Symmetry*, vol. 13, no. 10, p. 1764, 2021.

[79] D. N. Mhawi, A. Aldallal, and S. Hassan, “Advanced feature-selection-based hybrid ensemble learning algorithms for network intrusion detection systems,” *Symmetry*, vol. 14, no. 7, p. 1461, 2022.

[80] F. Jemili, R. Meddeb, and O. Korbaa, “Intrusion detection based on ensemble learning for big data classification,” *Cluster Computing*, vol. 27, no. 3, pp. 3771-3798, 2024.

[81] Y. Alotaibi and M. Ilyas, “Ensemble-learning framework for intrusion detection to enhance internet of things’ devices security,” *Sensors*, vol. 23, no. 12, p. 5568, 2023.