International Journal of Multidisciplinary Research and Growth Evaluation.

Explainable Hybrid Intelligence for Adaptive Cyber Defense in Distributed Environments

Mr. Jayesh Sendre [1*], **Dr. Piyush Choudhary** [2]
[1-2] Department of Computer Science & Engineering, Prestige Institute of Engineering Management & Research Indore, India

* Corresponding Author: **Mr. Jayesh Sendre**

Article Info

ISSN (Online): 2582-7138
Impact Factor (RSIF): 8.04
Volume: 07
Issue: 01
Received: 24-11-2025
Accepted: 28-12-2025
Published: 31-01-2026
Page No: 670-675

Abstract

Cloud and IoT distributed computing environments are now being attacked by many new types of cyber threats and older rule-based intrusion detection systems (IDS) can only detect attacks they know about. Machine learning based IDS have shown better ability to detect attacks but the black box nature of these models limits the ability to understand and be trusted in security critical environments.

This research proposes an explanation-driven hybrid intrusion detection system that uses both rules and an XGBoost classification algorithm for an adaptive cyber defense against evolving network behaviors and changes in network characteristics over time. The SHapley Additive exPlanations (SHAP) method will be used to enable interpretation of the reasoning behind each detection decision at an individual instance level. Additionally, this system has an incremental learning module which allows the model to evolve with changing network behavior and concept drift as it learns from data on the network. The proposed framework was tested using a balanced sample of the CICIDS2017 data set, showing an average of 95.61% accuracy across all validation folds. These results show the effectiveness of the proposed approach to balance detection accuracy with the need for interpretability and adaptability in distributed network security.

Keywords: Adaptive Learning, Explainable AI, Hybrid Intelligence, Intrusion Detection System, Network Security, SHAP, XGBoost.

1. Introduction

Modern distributed computing environments, including cloud platforms, Internet of Things (IoT) networks, and large-scale enterprise systems, have significantly increased system scalability and connectivity. However,

this expansion has also widened the attack surface, making networks more vulnerable to sophisticated and evolving cyber threats [6], [12]. Attackers increasingly employ adaptive techniques that can bypass conventional security mechanisms, posing serious challenges for reliable network protection.

Intrusion Detection Systems (IDS) are widely used to monitor network traffic and identify malicious activities. Traditional IDS primarily rely on rule-based or signature-driven approaches, which are effective for detecting known attacks but perform poorly against zero- day and evolving threats due to their static nature [7]. To overcome these limitations, machine learning–based IDS have been extensively studied, as they can automatically learn complex patterns from large volumes of network traffic data [8], [9].

Although IDS using machine learning are getting better at identifying intrusions, they are generally functioning as a "black box, " providing little information about why an IDS makes a particular decision. Due to the limitations of transparency in these IDS, analysts do not have confidence in the results provided by these systems; therefore, they can be difficult to deploy in real-world security settings. As a result, analysts require explanations for the IDS-generated alarms to validate them and to support incident responses [10, 11]. Therefore, researchers have turned to Explainable Artificial Intelligence (XAI) to improve the interpretability of IDS-generated alarms [3, 20]. However, most of the current IDS using Explainable Artificial Intelligence (XAI) are based on data alone, and thus typically ignore rule-based domain knowledge that is commonly utilized by cybersecurity professionals.

Another significant problem in intrusion detection is adaptability. The behavior of networks and the tactics employed by attackers are continually changing; therefore, static models will degrade over time, resulting in concept drift [18, 19]. Although researchers have suggested approaches for incrementally updating IDS so they are adaptable, there are few studies that examine combining adaptive and incremental learning with explainable and hybrid IDS.

To address these challenges, this paper proposes an explainable hybrid intrusion detection framework that integrates rule-based intelligence with an XGBoost- based machine learning model for adaptive cyber defense [2], [17]. The framework leverages SHapley Additive exPlanations (SHAP) to provide transparent, instance-level explanations of detection decisions [3], while an incremental learning mechanism enables continuous adaptation to evolving network traffic patterns. By jointly addressing accuracy, interpretability, and adaptability, the proposed approach aims to provide a practical and trustworthy intrusion detection solution for modern distributed network environments.

Contributions of this paper are as follows:

1. A unified hybrid intrusion detection framework integrating rule-based intelligence with XGBoost learning.
2. Seamless integration of SHAP-based explainability for both global and instance-level interpretation.
3. An incremental adaptive learning mechanism to handle evolving attack patterns without full retraining.
4. Extensive evaluation on CICIDS2017 with cross-validation and comparative baselines.

2. Related Work

Research in intrusion detection has primarily used rule- based and signature-based systems that utilize pre- defined rules to recognize established attacks [7, 16]. While these methods are highly interpretable and require very little computation time; they cannot recognize zero day or evolving threats as a result of being static. The increase in network complexity and increasing threat sophistication led to an increased interest in data driven approaches for intrusion detection.

Machine Learning (ML)-based Intrusion Detection Systems (IDS) have been extensively investigated to address the limitations of static rule-based systems. By using classical ML algorithms such as Logistic Regression, Support Vector Machines and Random Forests; researchers have found a higher level of detection accuracy using these algorithms to learn the relationship between network traffic data and attacks [8, 9]. Additionally, researchers have used ensemble and gradient boosting techniques, including XGBoost, which have shown to be effective and scalable on structured intrusion detection datasets (CICIDS2017 and UNSW-NB15) [2, 17]. However, while these algorithms have shown to be successful; many of them are considered to be "black box" models. This limits both the transparency of the decision making and the practicality of implementing IDS models in security critical environments.

The use of Explainable Artificial Intelligence (XAI) techniques in intrusion detection has addressed some of the issues related to the lack of transparency in machine learning based IDS models. Techniques such as SHapley Additive exPlanations (SHAP), can provide post-hoc explanations regarding how each feature contributes to the overall prediction made by a model [3, 20]. Researchers have also studied the application of SHAP to enhance the trustworthiness and analyst's understanding of IDS decisions [12]. However, most XAI-based IDS approaches rely entirely on providing explanation after prediction and do not include any form of domain specific rule-based knowledge in the detection process.

Another major limitation recognized by researchers today is the lack of ability to adapt to changing network behavior. Machine learning models that are trained statically will often degrade over time as a result of changes in network behavior and/or changing attack strategies [18, 19]. While there are adaptive and incremental learning techniques that have been developed to help mitigate this problem; integrating these with XAI-based and hybrid IDS frameworks is still limited.

In contrast to existing studies, the proposed work integrates rule-based detection, XGBoost-based learning, SHAP-driven explainability, and incremental adaptive learning within a unified intrusion detection framework. By combining deterministic security rules with explainable machine learning and continuous adaptation, the proposed approach addresses key gaps in prior research related to transparency, robustness, and long-term effectiveness in dynamic distributed network environments.

3. Dataset Description

In this study, the proposed IDS framework has been tested for its effectiveness on the CIC IDS 2017 dataset, which can be freely downloaded on the Kaggle platform as the “Network Intrusion Dataset” offered by Chethan H N [1], [13]. In reality, CIC IDS 2017 has been extensively employed in the area of intrusion detection as it represents realistic network traffic patterns, including both normal network activities as well as various threat scenarios created on a testbed network.

In CICIDS2017, network traffic is represented as flow records. The records are extracted using CICFlowMeter, and each record represents flows using time and packet- based, as well as statistical parameters based on communication [13]. This dataset has various types of attacks involving Brute Force, Botnet, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks, Port Scanning, Web-Based attacks, and normal traffic.

To address this problem, a fair sample subset of 35, 000 flow recordings was developed for this research. The sample subset was designed to provide a just and fair assessment for all traffic categories. The creation of a fair sample subset is a challenge for intrusion detection data, as identified in [14]. The sample subset contains a total of seven categories, which are Normal Traffic, Brute Force, Botnet, DoS, DDoS, Port Scanning, and Web Attacks, with 5, 000 samples for each.

Before the commencement of model training, non- numeric and identifier columns like IP addresses, port numbers, and timestamps were eliminated to prevent bias and improve generalization. Missing and infinity values were dealt with during the preprocessing steps following general data preprocessing techniques to maintain data reliability [15]. The preprocessed data was split into the training and test sets in proportion of 70:30 data for model evaluation as further discussed in the experimental design.

While multi-dataset evaluation might assist in further improving the generalization process, the focus, in this case, remains upon the CICIDS2017 for its realism, variety, and acceptance that are widely seen in the literature related to the intrusion detection system. The extension towards other evaluation datasets like UNSW- NB15 and NSL-KDD remains a matter for the future.

As the data is publicly available and does not hold any personal identifiers, no approval or consent is required for the conduct of this research.

4. Methodology

The proposed intrusion detection system follows an explainable hybrid intelligence architecture that integrates rule-based detection, machine learning–based classification, explainability, and adaptive learning. The overall workflow of the proposed framework is illustrated in Fig. 1, which shows the sequential processing of network traffic from preprocessing to adaptive model updating.

4.1. Data Preprocessing

Network traffic data typically contains non-numeric attributes, missing values, and redundant features that can degrade model performance. Therefore, non- numeric and identifier attributes such as IP addresses, port numbers, and timestamps were removed to avoid bias and improve generalization. Missing and infinite values were handled using column-wise median imputation, which is suitable for skewed network traffic distributions [15]. Feature scaling was applied to normalize numerical attributes, and class labels were encoded numerically to ensure compatibility with machine learning algorithms.

4.2. Hybrid Rule–Based and Machine Learning Framework

As described in Fig. 1, the incoming network stream is first processed by a rule-based detection component that leverages domain expertise and security knowledge to effectively detect well-known and high-confidence attacks. The purpose of this component is a front-end decision tool that rapidly detects well-known intrusions.

The rule-based detection logic is designed to identify typical attack behaviors that involve excessively large transmission rates of packets, unusually large durations of flows, unusual distributions of the length of packets, and connection attempts. These behaviors are typically observed in attacks such as port scan attacks, brute force intrusion, and DoS and DDoS attacks [7], [16]. Typical examples of the rule-based detection logics used in the proposed system are given in Table I.

If traffic flows meet the conditions of the predefined rules, they are automatically identified as malicious. Otherwise, they will be checked by the machine learning-based detection phase.

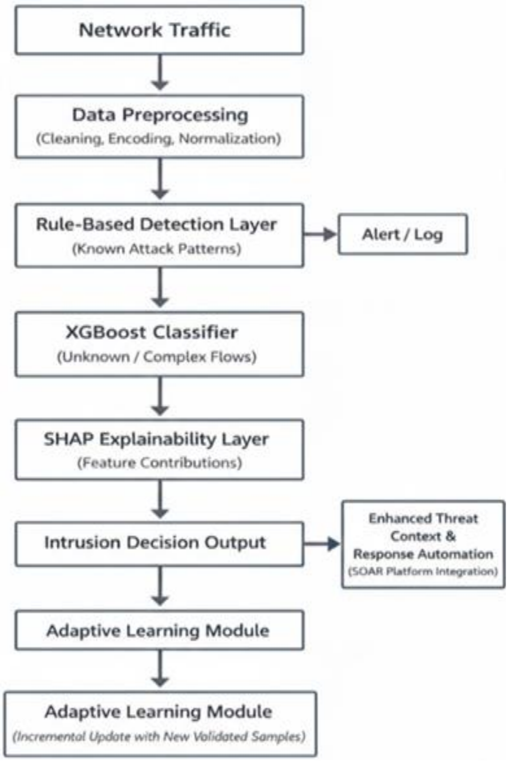

Network Traffic
Data Preprocessing
(Cleaning, Encoding, Normalization)
Rule-Based Detection Layer
(Known Attack Patterns)
Alert / Log
XGBoost Classifier
(Unknown / Complex Flows)
SHAP Explainability Layer
(Feature Contributions)
Intrusion Decision Output
Enhanced Threat Context & Response Automation
(SOAR Platform Integration)
Adaptive Learning Module
Adaptive Learning Module
(Incremental Update with New Validated Samples)

Fig 1: Flow diagram of the proposed explainable hybrid intrusion detection framework with adaptive learning.

Representative examples of the rule-based detection logic employed in the proposed framework are summarized in Table I.

Table 1. Examples of rule-based detection logic used in the proposed hybrid IDS

Rule Indicator	Threshold Condition	Likely Attack Type
High packet rate	Packet rate > 1000 packets/sec within a single flow	DoS / DDoS
Flow duration	Flow duration > 300 packets /sec with continuous traffic	DoS
Packet length pattern	Backward packet length mean < 50 bytes	Port Scanning
Connection attempts	> 20 connection attempts to different ports within 10 sec	Brute Force

4.2. XGBoost-Based Detection Model

The learning part of the framework uses an XGBoost classifier because of its robustness, scalability, and power to capture non-linear interaction among features, which are present in the structured network traffic data [2, 17]. Thus, the hybrid framework gets to leverage the efficiency and flexibility that result from the combination of deterministic rule-based intrusion filtering and the data-driven machine learning model.

4.3. Adaptive Learning Mechanism

In practical environments, the behavior and techniques for attacks in the network traffic continue to drift over time, resulting in the concept drift and decreased performance of the static models [18], [19]. For this purpose, an incremental adaptive learning method is incorporated into the proposed system as shown in Fig. 1.

In the first instance, the XGBoost classifier model is trained on the baseline dataset. Once the model has been implemented, the new network traffic observations are acquired periodically. These observations are then preprocessed for analysis. Once the observations are validated by the confidence level and rules, the dataset can then be used to update the model without the need for retraining.

The incremental learning mechanism in the proposed framework follows a controlled warm-starting strategy. Instead of modifying existing tree structures, the model is periodically updated by appending new trees trained on recent validated traffic samples while retaining previously learned trees. This approach leverages XGBoost's ability to continue training from an existing booster model, enabling adaptation to concept drift without complete retraining. This strategy ensures stability of prior knowledge while allowing the model to evolve with changing network behavior.

4.5. Explainability using SHAP

To improve explainability and gain trust from analysts, a novel framework is proposed that uses SHapley Additive exPlanations (SHAP) to explain detection outcomes [3]. These values can measure how each individual feature contributes to a particular result and offer a global approach to understanding how a model works as well as an instance-wise approach to traffic patterns [20].

SHAP addresses the black-box limitation by computing the marginal contribution of each feature to a model's prediction based on cooperative game theory, enabling both global and instance-level interpretability of complex ensemble models.

5. Experimental Setup

5.1. Implementation Environment

All the above-mentioned experiments were carried out using the Python programming language and popular machine learning libraries like Scikit-Learn, XGBoost, and SHAP. In the experimental evaluation setup, the environment was a system integrated with an Intel i7 processor operating at 3.6 GHz, with 16 GB RAM, running Windows 11 OS. This configuration was sufficient to facilitate model training, evaluation, and explanation of the proposed framework.

5.2. Data Preparation Methods for Machine Learning

The preprocessed data was first split into training and testing sets with a 70:30 ratio, and it was ensured that nothing from the test set was seen during training. Further to improve the reliability and accuracy of model performance and mitigate the randomness associated with data splitting for model selection, 5-fold cross- validation was used only on the training data. The model selection performance was determined by taking the average of the five folds, and testing set evaluation performance was used to evaluate models.

This validation approach helps achieve proper model parameter adjustment and also helps prevent biased model performance evaluation.

5.3. Model Configuration and Hyperparameter Tuning

The XGBoost classifier was chosen for the learning- based detection approach because of its effectiveness even with structured network traffic data [2], [17]. The parameters of the XGBoost classifier can be optimized using cross-validation during training. The main parameters that need optimization in this case are the number of trees, learning rate, and tree depth, as well as the subsampling ratio.

The baseline classification algorithms, such as Logistic Regression and Random Forest, were trained using identical train-test splits. This allowed for comparison of their performance.

The optimized hyperparameter settings for the XGBoost classifier, obtained using 5-fold cross-validation on the training set to balance detection performance and overfitting., are summarized in Table II.

Table 2: XGBoost Hyperparameter Settings

Parameter	Value
Number of Trees	200
Learning Rate	0.1
Maximum Tree Depth	6
Subsample Ratio	0.8
Column Sample Ratio	0.8
Objective Function	multi:softprob

5.4. Evaluation Metrics

The standard metrics for intrusion detection- performance, accuracy, precision, recall, F1-score, and Receiver Operating Characteristic-Area Under the Curve-were used to evaluate model performance. These are extensively used in intrusion detection research and comprehensively judge classification performance over different classes of traffic[21].

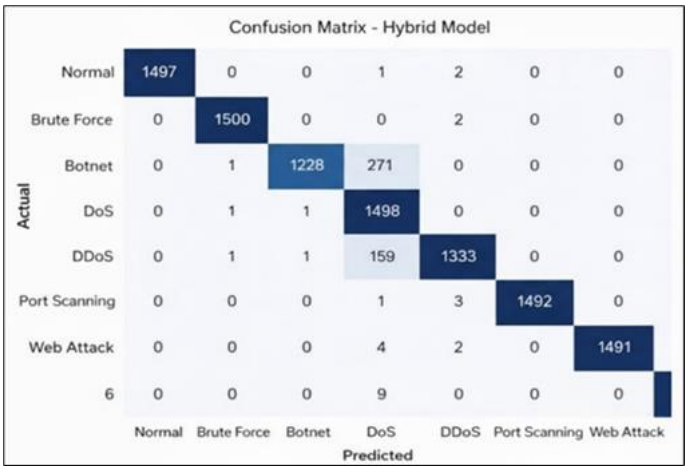
5.5. Comparative Evaluation

To evaluate the performance of the proposed hybrid framework, the performance was matched with those of the Logistic Regression and Random Forest classifiers. All models were identically exposed to experimental conditions while partitioning the dataset, choosing a validation strategy, and performing on similar metrics.

6. Results and Discussion

The proposed hybrid intrusion detection system demonstrated a test accuracy of 95.61% with a weighted F1-score of 0.9571, which is indicative of excellent overall detection capability. Furthermore, this model achieved a ROC–AUC score of 0.9999, demonstrating great class separation capability for the dataset under evaluation. The performance was compared to that of baseline classifiers, and the proposed framework outperformed Logistic Regression and Random Forest by about 3–7% in terms of both accuracy and F1-score, ensuring the adequacy of the novel concept of hybrid rule-guided learning.

Therefore, the proposed framework is designed for architectural robustness rather than optimization specific to particular datasets. It indicates its usefulness across a series of different network environments.



	Normal	Brute Force	Botnet	DoS	DDoS	Port Scanning	Web Attack
Normal	1497	0	0	1	2	0	0
Brute Force	0	1500	0	0	2	0	0
Botnet	0	1	1228	271	0	0	0
DoS	0	1	1	1498	0	0	0
DDoS	0	1	1	159	1333	0	0
Port Scanning	0	0	0	1	3	1492	0
Web Attack	0	0	0	4	2	0	1491
6	0	0	0	9	0	0	0

Fig 2: Confusion matrix of the proposed hybrid intrusion detection system across seven traffic classes.

For class-wise performance analysis, the prediction results are visualized using a confusion matrix in Fig. 2. The obtained confusion matrix demonstrates strong diagonal dominance, indicating that a large portion of instances belonging to various network traffic classes are predicted correctly. The detection of normal traffic and Brute Force attacks is almost perfect, while Bot, Port

Scanning, and Web Attacks also show very high detection accuracy. A minor amount of misclassification is experienced between the DoS and DDoS class; this is understandable as their respective classes also overlap in characteristics, such as high packet rates and long flow duration [22]. However, the overall misclassification rate is low.

The proposed system therefore has an accuracy of 95.61% ± 0.42% average across five-fold cross- validation, showing stability and consistency in performance across different splits of the data. Statistical confirmation of this performance gain was achieved by performing a paired t-test for both the proposed system and a number of benchmark systems. The statistical significance of the performance gain demonstrated by the proposed system is confirmed through a p-value of < .05 at a 95% confidence level; therefore, the reported performance gains are considered reliable based upon the statistical analysis. Misclassification between DoS and DDoS traffic is primarily due to overlap in traffic characteristics (i.e., high packet rates, long flow durations). To address this issue, the hybrid system incorporates two new features: source IP entropy and packet distribution rules. Low source IP entropy combined with high packet rates indicates DoS traffic, while high source IP entropy across multiple concurrent flows indicates DDoS traffic. These rule-based indicators assist the learning model in distinguishing single-source and multi-source flooding behaviors more effectively. A feature importance analysis further reveals that such attributes as the PSH Flag Count, Active Minimum Time, and Backward Packet Length Mean are of great importance in making the detection decisions. These results are thus consistent with established principles of network security and hence show that the model indeed learns meaningful behavior instead of noise from the dataset [23]. Moreover, after adaptive retraining with newly observed traffic samples, the framework continued to yield stable performance; therefore, the incremental learning mechanism works well in practice against evolving attack patterns.

7. Conclusion

In this paper, an explainable and adaptive hybrid model for intrusion detection is proposed, catering to the needs of the current distributed network environment. The proposed model is a combination of rule-based systems, XGBoost classification, SHAP explanation techniques, and adaptive learning, making it highly accurate and transparent.

Experimentation results show that the hybrid method has been able to address the limitations of traditional IDS systems by maintaining intelligence, speed, and interpretability. In the future, the aim is to apply deep learning models for the analysis of attacks in time, as well as implementing the model in a distributed environment.

8. Future Work

The future research will be based upon extension of the suggested model using deep learning algorithms for the discovery of a time-dependent nature of the network traffic (i.e., the ability of the algorithm to discover a pattern that has developed over time) as well as for the recognition of multi-step cyber-attacks. Deployment of the system within a real-time environment (i.e., within a network) will provide an opportunity to evaluate the scalability, latency, and real-world robustness of the system. In addition, the evaluation of the system's performance with other existing benchmark datasets, including those containing traffic imbalance, will help to determine the system's cross-dataset generalizability as well as its feasibility for use in real-world applications.

9. Acknowledgment

The authors sincerely thank Dr. Manoj Kumar Deshpande, Senior Director, and Dr. Piyush Choudhary, Head of the Department of Computer Science, for their guidance and support during this research.

10. References

10. Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP); 2018 Jan; Funchal, Portugal. 2018. p. 108-16.
11. Chen T, Guestrin C. XGBoost: a scalable tree boosting system. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; 2016 Aug; San Francisco, CA. New York: ACM; 2016. p. 785-94. doi:10.1145/2939672.2939785.
12. Lundberg SM, Lee SI. A unified approach to interpreting model predictions. In: Advances in Neural Information Processing Systems (NeurIPS); 2017 Dec; Long Beach, CA; 2017. p. 4765-74.
13. Bishop CM. Pattern recognition and machine learning. New York: Springer; 2006.
14. Javaid A, Niyaz Q, Sun W, Alam M. A deep learning approach for network intrusion detection system. In: Proceedings of the IEEE International Conference on Big Data; 2016 Dec; Washington, DC. Piscataway: IEEE; 2016. p. 1906-13. doi:10.1109/BigData.2016.7840811.
15. Sommer R, Paxson V. Outside the closed world: on using machine learning for network intrusion detection. In: Proceedings of the IEEE Symposium on Security and Privacy; 2010 May; Oakland, CA. Los Alamitos: IEEE Computer Society; 2010. p. 305-16. doi:10.1109/SP.2010.25.
16. Denning DE. An intrusion-detection model. IEEE Trans Softw Eng. 1987;SE-13(2):222-32. doi:10.1109/TSE.1987.232894.
17. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In: Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA); 2009 Jul; Ottawa, ON, Canada. Piscataway: IEEE; 2009. p. 1-6.
18. Lee W, Stolfo SJ. Data mining approaches for intrusion detection. In: Proceedings of the 7th USENIX Security Symposium; 1998 Jan; San Antonio, TX. Berkeley: USENIX Association; 1998. p. 79-93.
19. Adadi A, Berrada M. Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). IEEE Access. 2018;6:52138-60. doi:10.1109/ACCESS.2018.2870052.
20. Doshi-Velez F, Kim B. Towards a rigorous science of interpretable machine learning. arXiv. 2017. Available from: https://arxiv.org/abs/1702.08608.
21. Zhang Y, Chen R, Li J, Zhang X. Explainable artificial intelligence in cybersecurity: a survey. IEEE Secur Priv. 2021;19(5):72-83. doi:10.1109/MSEC.2021.3082954.
22. Lashkari AH, Draper-Gil G, Mamun MSI, Ghorbani AA. Characterization of CICIDS2017 dataset. In: Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP); 2018 Jan; Funchal, Portugal; 2018. p. 1-10.
23. He H, Garcia EA. Learning from imbalanced data. IEEE Trans Knowl Data Eng. 2009;21(9):1263-84. doi:10.1109/TKDE.2008.239.
24. Han J, Kamber M, Pei J. Data mining: concepts and techniques. 3rd ed. Waltham: Morgan Kaufmann; 2011.
25. Axelsson S. Intrusion detection systems: a survey. Göteborg: Chalmers University of Technology, Department of Computer Engineering; 2000.
26. Friedman JH. Greedy function approximation: a gradient boosting machine. Ann Stat. 2001;29(5):1189-232. doi:10.1214/aos/1013203451.
27. Ditzler G, Roveri M, Alippi C, Polikar R. Learning in nonstationary environments: a survey. IEEE Comput Intell Mag. 2015;10(4):12-25. doi:10.1109/MCI.2015.2471196.
28. Tsymbal A. The problem of concept drift: definitions and related work. Dublin: Trinity College Dublin, Department of Computer Science; 2004.
29. Guidotti R, Monreale A, Ruggieri S, Turini F, Giannotti F, Pedreschi D. A survey of methods for explaining black box models. ACM Comput Surv. 2019;51(5):93. doi:10.1145/3236009.
30. Davis J, Goadrich M. The relationship between precision-recall and ROC curves. In: Proceedings of the 23rd International Conference on Machine Learning (ICML); 2006 Jun; Pittsburgh, PA. New York: ACM; 2006. p. 233-40.
31. Kasongo SM, Sun Y. A deep learning method with feature engineering for wireless intrusion detection. IEEE Access. 2020;8:135324-34. doi:10.1109/ACCESS.2020.3010545.
32. Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS). Gaithersburg: National Institute of Standards and Technology; 2007. NIST Special Publication 800-94.
33. Chiba Z, Abghour N, Moussaid K, Rida M. Machine learning based intrusion detection system for cloud environments. Comput Secur. 2019;83:153-65.
34. Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems. In: Proceedings of the IEEE Military Communications and Information Systems Conference (MilCIS); 2015 Nov; Canberra, Australia. Piscataway: IEEE; 2015. p. 1-6.
35. N CH. Network Intrusion Dataset (CICIDS2017). Kaggle; 2017. Available from: https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset.

How to Cite This Article

Sendre MJ, Choudhary P. Explainable hybrid intelligence for adaptive cyber defense in distributed environments. Int J Multidiscip Res Growth Eval. 2026;7(1):670–675.

Creative Commons (CC) License