I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

Adaptive Machine Learning Framework for Robust Network Intrusion Detection

Umar Yahaya Namahe [1*], Amit Jain [2], Ronak Duggar [3]
[1-3] School of Computer Science & Engineering, Geeta University, Panipat, India

Corresponding Author: *Umar Yahaya Namahe

DOI: https://doi.org/10.5281/zenodo.19706329

Abstract

The rapid growth of computer networks, cloud computing, and Internet of Things (IoT) environments has significantly increased the complexity and frequency of cyber threats. Traditional signature-based intrusion detection systems are effective for known attacks but fail to detect emerging and evolving threats. To address these limitations, this paper proposes an adaptive machine learning framework for network intrusion detection.

The proposed framework integrates data preprocessing, class imbalance handling, multi-model learning, and a feedback-driven adaptive learning mechanism to enable continuous model improvement in dynamic network environments. The system incorporates both machine learning and deep learning models, including Random Forest, Support Vector Machine, Convolutional Neural Networks, and Long Short-Term Memory networks.

Experimental evaluation is conducted on benchmark datasets such as NSL-KDD, CICIDS, and UNSW-NB15 using standard performance metrics including accuracy, precision, recall, F1-score, and ROC-AUC. The results demonstrate that deep learning models achieve superior detection performance, while the adaptive framework enhances robustness and adaptability under changing network conditions.

The study highlights the importance of adaptive learning in modern intrusion detection systems and provides a scalable and effective solution for real-world cybersecurity applications.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 16-04-2026
- **Accepted:** 17-04-2026
- **Published:** 23-04-2026
- **IJCRM:**5(2); 2026: 785-791

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Namahe U Y, Jain A, Duggar R. Adaptive Machine Learning Framework for Robust Network Intrusion Detection. Int J Contemp Res Multidiscip. 2026;5(2):785-791.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Network Intrusion Detection System, Machine Learning, Deep Learning, Cybersecurity, Adaptive Intrusion Detection, Concept Drift Detection

1. INTRODUCTION

The development of digital communication infrastructures, cloud computing, and Internet of Things (IoT) technologies has grown rapidly, which has also made addressing the issue of cybersecurity particularly tricky. In modern networks, the large volumes of heterogeneous data are exchanged and thus it is prone to cyber-attacks like distributed denial-of-service (DDoS), malware propagation, as well as unauthorized access. Consequently, securing network infrastructures has emerged a major issue to organizations and researchers. NIDS are imperative in use as they monitor the traffic and detect anomalous activities that may indicate malicious behavior.

The conventional intrusion detection systems are mainly based on signature recognition, with the incoming traffic compared with the already identified attack signatures. Although it is good in relation to familiar attacks, these systems cannot detect new or new mutating attacks like zero-day attacks and advanced persistent threats. Also, their scalability in dynamic environments is limited by the necessity to constantly update their signature, which prompts the move toward the implementation of the machine learning and artificial intelligence-driven solutions.

Machine learning methods have generated strong performance in detecting intrusion based on learning patterns on network traffic data. Decision Trees, Random Forest, and Support Vector Machines (SVM) are popular algorithms that are used in the classification and detection of anomalies [1], [2]. State-of-the-art intrusion detection is further improved with Deep learning models, such as Convolutional Neural Networks (CNN) and Long Short-Memory (LSTM) networks, which identify the spatial-temporal patterns of the high-dimensional data [3], [4].

Although all these have been made, there are still several challenges. Imbalance in the class, where normal traffic significantly exceeds attack instances, causes a lower detection accuracy of the minority classes [5]. There is also poor generalization of models to other datasets and are susceptible to concept drift where changing traffic patterns deteriorate the performance of the models over time [6]. Also, deep learning models can be opaque and thus can be less interpretable and therefore less trusted in critical applications. Explainable AI methods like SHAP and LIME have been presented to enhance transparency and insight model decisions [7].

In order to overcome these issues, in this work, the adaptive machine learning is going to be proposed as a network intrusion detection framework. The architecture combines the pre-processing of data, class imbalance, multi-model learning and concept drift management to enhance performance during dynamic conditions. It also uses explainability mechanisms to attain more transparency. Several machine learning and deep learning models are tested on benchmark datasets and the performance is evaluated through accuracy, precision, recall, F1-score, false positive rate and ROC-AUC.

The key contributions of this research are as follows:

1. A novel adaptive intrusion detection framework that integrates machine learning and deep learning models within a unified architecture.
2. A feedback-driven learning mechanism that continuously monitors model performance and dynamically updates the model in response to concept drift in network traffic.
3. A layered system design that enables scalable and real-time intrusion detection in dynamic environments.
4. Integration of class imbalance handling and explainable AI techniques to improve detection accuracy and model transparency.
5. Comprehensive evaluation on benchmark datasets demonstrating the effectiveness of the proposed adaptive framework compared to static intrusion detection models.

Unlike existing intrusion detection systems that rely on static training, this study proposes a feedback-driven adaptive framework capable of continuous learning in evolving network environments.

2. LITERATURE REVIEW

Network intrusion detection has emerged as a significant topic because the level of cyber threats in existing networks has been escalating. The traditional system of intrusion detection relies on signature-based detection techniques where known attack patterns are used, but this does not detect newer or emerging threats. To address these shortcomings, machine learning and deep learning approaches are dynamically explored and generalized to provide superior functionality in the mode of detection accuracy and adaptability.

Several research works have been carried out on conventional machine learning algorithms in intrusion detection. The literature reviews by Liu and Lang [1] and Halbouni et al. [2] were comprehensive and highlight the applicability of machine learning in anomaly detection. Typical examples of such models are Decision Trees and Random Forest due to their high classification performance with low computational cost. Hybrid approaches have also been suggested as being useful in improving accuracy of detection. That being said, the NBS were used alongside the SVM by Wisanwanichthan and Thammawichai [8], the clustering in conjunction with the Random Forest and the deep learning in Liu et al. [9]. Similarly, Seth et. al [10] also determined that patterns of resiliency were improved when ensemble model was used in intrusion detection systems.

Deep learning techniques have also enhanced intrusion detection ability as it automatically discloses complex features to identify intruders in the network traffic data. The deep learning models have been found to be superior to the classical machine learning model in many configurations in the study done by Lansky et al. [3]. The CNN and LSTM architectures are the most popular in that they have the capacity to acquire both the spatial and temporal patterns. The above statements are in the agreement that the foundations of Farhan et al. [4] state that the models improve the degree of attack detection significantly.

As such, there are some challenges that remain despite these developments. One of them is a class imbalance in which a larger percentage of the attack examples is normal traffic because of which the detection rates of smaller classes are reduced [5]. Incidentally, it is also the case that the network environments are dynamic, and therefore concept drift where

the performance of unchanging models is eroded. They recommended to address this issue using adaptive strategies, including, the strategy of Villegas-Ch et al. [6] and Okutan Kara et al. [12] who demonstrated the efficiency of adaptive and reinforcement learning-based intrusions detection systems.

The other significant matter is that machine learning models cannot be interpreted. Majority of deep learning systems are black boxes thus limiting their potential usage. Mohale and Obagbuwa [7] have gone into as far as elucidating explainable artificial intelligence such as SHAP and LIME to enhance transparency. Further, the intrusion detection has been applied to certain environments such as in the case of IoT and industrial system. Yu et al. [13] and Sharma and Bairwa [14] have highlighted the usefulness of the adaptative mechanisms of security in the distributed environment.

Further more latest studies have been done on model enhancement and optimization. The systematic reviews have been demonstrated by Arnob et al. [15] and Abdulkareem et al. [16] to identify the prevailing trends in research. The optimized features fusion methods have been proposed by Li et al. [17], and the AutoML features optimization is the one that Bisen et al. [18] tested. According to Benka et al. [19], the machine learning efficacy was found in the industrial control system.

Studies on security challenges have also been made such as adversarial attacks. The weaknesses of machine learning-based intrusion detection system have been reviewed by Ennaji et al. [20] and approaches to operating hybrid ensembles have been recommended by Ababneh et al. [21] to show continuous detection of dynamic environment.

Despite these contributions, most of the available techniques focus on the need to improve classification accuracy as well as limited consideration of adaptability, interpretability, and robustness. Therefore, there is a need for a comprehensive intrusion detection system with adaptive learning, realistic classification and interpretable decision-making systems.

3. PROPOSED METHODOLOGY

The given research paper presents a dynamic machine learning approach to the construction of an effective network intrusion detection framework that is expected to deliver high-performance network intrusion detection alongside flexibility and understanding of network conditions. The architecture is made up of data preprocessing, feature engineering, class imbalance handling, multi-model learning, concept drift detection and interpretable artificial intelligence techniques.

The overall structure of the proposed model includes a sequence of data flow from data acquisition to performance evaluation.

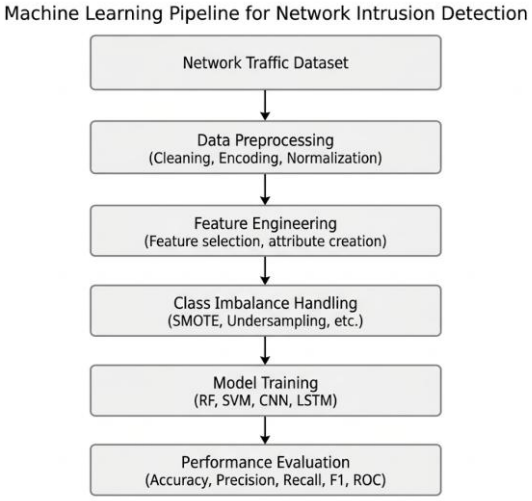

Figure 1. Proposed Adaptive Framework Architecture for Network Intrusion Detection

3.1 Layered Architecture of the Proposed Framework

The proposed adaptive intrusion detection system is designed using a layered architecture to ensure scalability, flexibility, and real-time adaptability in dynamic network environments.

The architecture consists of the following layers:

1. Data Acquisition Layer

This layer captures real-time network traffic data from various sources and converts it into a structured format for processing.

2. Preprocessing Layer

This layer performs data cleaning, normalization, encoding of categorical features, and removal of redundant records to improve data quality.

3. Feature Engineering Layer

Relevant features are selected and transformed to reduce dimensionality and improve model efficiency and accuracy.

4. Model Learning Layer

This layer applies machine learning and deep learning models such as Random Forest (RF), Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) for intrusion detection.

5. Drift Detection Layer

This layer continuously monitors model performance and detects changes in data distribution (concept drift).

6. Adaptive Feedback Layer
This is the core layer of the system, where model parameters are updated dynamically based on feedback from performance evaluation.

7. Decision Layer
This layer generates the final classification results and triggers alerts for detected intrusions.
This layered design transforms the system from a static detection pipeline into a dynamic and adaptive intrusion detection framework suitable for real-world cybersecurity environments.
The input data can be given in the following form:

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

$D = \{ (x_i, y_i) \}_{i=1}^{N}$
x_i denotes feature vectors and $y_i \in \{0,1\}$is the data of the label of a normal or attack. Preprocessing is applied to raw network traffic data and it entails eliminating redundant records, handling missing values, encoding categorical attributes, and normalization. In order to use feature scaling, the following formula is used:

$$x' = \frac{x - \mu}{\sigma}$$

where $\mu$and σ equals the mean and the standard deviation respectively. The transformation makes the model training stable and enhances the convergence.
Then, feature engineering mechanisms are performed to minimize the dimensions and discard nonrelevant characteristics after allowing preprocessing. This is with the aim of choosing the best set of features:

$$X_{opt} \subseteq X$$

which enhances the performance of classification as well as minimizing the complexity of the computational algorithm [20].
One of the biggest issues when it comes to intrusion detection is the issue of class imbalance, where normal traffic is significantly higher than attack samples

$$P(y = 0) \gg P(y = 1)$$

To overcome this, resampling approaches are used to come up with a balanced data:

$$D_{balanced} = f(D)$$

where $f(\cdot)$denotes the imbalance defense procedures like oversampling or SMOTE, enhancing the minority classes of attack detection [21].
The framework uses the multi-model learning approach as it compares multiple machine learning and deep learning models, such as the Random Forest (RF), the Support Vector Machine (SVM), the Convolutional Neural Networks (CNN), and the Long Short-Term Memory (LSTM) networks. The process of classification cannot be defined as:

$$\hat{y} = f(x)$$

where f represents the learnt model. The conventional models are effective at classification, and deep learning models are able to recognize complex spatial and temporal patterns of data on network traffic.
The framework integrates a concept drift detection mechanism so that it becomes flexible. The distribution of the data can vary with time in dynamic environment:

$$P_t(X) \neq P_{t+1}(X)$$

In case drift is identified the model is re-estimated as: $Model_{new} = Update(Model_{old})$
This will allow the system to perform in changing network conditions [6].

3.2 Adaptive Feedback Learning Mechanism
To enhance adaptability, the proposed framework introduces a feedback-driven learning mechanism that continuously updates the model based on incoming network traffic.
Let the incoming data stream be defined as:
$S = \{x_1, x_2, x_3, \ldots, x_t\}$
A sliding window approach is applied:
$W_t = \{x_{t-n+1}, \ldots, x_t\}$
The prediction model is defined as:
$\hat{y}_t = f\theta_t(X_t)$
Model performance is evaluated using a loss function:
$L(W_t, \theta_t) = (1 / |W_t|) \Sigma\ \ell(y_i, f\theta_t(x_i))$
Concept drift is detected when:
$L(W_t, \theta_t) > \delta$
When drift is detected, the model is updated as:
$\theta_{t+1} = \theta_t + \eta\ \nabla L(W_t, \theta_t)$
This process creates a closed-loop adaptive system:
Prediction → Evaluation → Drift Detection → Model Update → Deployment
The proposed mechanism enables continuous learning, improves robustness, and ensures that the intrusion detection system adapts effectively to evolving network traffic patterns.
Explainable artificial intelligence methods as SHAP and LIME are incorporated into the framework as a way of enhancing interpretability. These are techniques of estimating feature significance:

$$Importance(x_j)$$

enabling the analysts to know the value that each feature has towards the model prediction hence boosting openness and trust [7].
At last, the efficiency of the proposed framework is measured by conventional classification indications. These parameters include accuracy, precision, recall and F1-score which are calculated as:

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

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

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

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

These metrics give an in-depth analysis of the performance of the model in tracking malicious traffic with minimal false positive.
All in all, the proposed framework offers a strong, dynamic, and readable intrusion detection system that can be efficiently used in dynamic cyber security setting.

4. EXPERIMENTAL SETUP AND DATASET
To assess the suggested adaptive intrusion detection framework, experiments are carried out with a benchmark data, including

NSL-KDD, CICIDS, and UNSW-NB15. These datasets have gained popularity in the literature due to their variety of attack categories and realistic traffic distribution that can be effectively compared with current literature [22], [23].

The data is preprocessed before training in order to enhance quality and consistency of the data. Duplicated and redundant records are eliminated, missing values are processed and nominal features are coded to numbers. The feature normalization is used to size the data and improve the model performance.

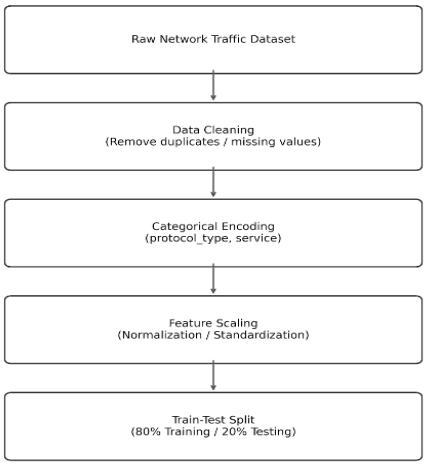

Figure 2. Data Preprocessing Pipeline for Intrusion Detection Dataset

An 80:20 split is then used to give out the dataset to training and the testing sets. Stratified sampling is used to maintain distribution across the classes so as to carry out correct assessment of the minority attack detection.

The framework considers several models, such as, Random Forest (RF), Support Vector Machine (SVM), Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks among others, as it is known to be effective when performing intrusion detection tasks [3], [4].

All the experiments are carried out under Python with the help of Scikit-learn, TensorFlow and Keras libraries. Preprocessing of data is done with the help of Pandas and NumPy, and visualization is done with the help of Matplotlib.

Standard measures are used to assess the model performance, among which are accuracy, precision, recall, F1-score, the false positive rate (FPR) and ROC-AUC. The metrics offer a full measure of detection and minimization of false alarms [24].

Besides, concept drift monitoring is also included to measure the performance in a dynamic network environment. The framework can be kept to detect models using the updated models as major changes are detected, thus staying effective with time [6].

Altogether, this experimental environment allows performing the objective analysis of machine learning and deep learning systems to detect intrusions in the real environment.

5. RESULTS AND DISCUSSION

This part analyses the selected adaptive machine learning model of network intrusion detection with the use of the Random Forest (RF), Support Vector Machine (SVM), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) libraries. Performance also is evaluated with standard classification metrics, such as accuracy, precision, recall, and F1-score, to determine general correctness, false alarm reduction, intrusion detection capacity, and a possibility to balance precision and recall.

The results of the experiment performed with the instituted models are summarized in Table 1.

Table 1. Intrusion Detection Model Comparisons on Performance.

Model	Accuracy	Precision	Recall	F1Score
Random Forest	0.762	0.966	0.603	0.743
Support Vector Machine	0.783	0.978	0.633	0.769
Convolutional Neural Network	0.801	0.975	0.668	0.793
Long ShortTerm Memory	**0.812**	0.972	**0.689**	**0.807**

The results of the evaluated models are given in Table 1. The accuracy of the Random Forest classifier was 76.2 percent and there was high precision (96.6%) and lower recall (60.3%), thus making it effective in reducing the false positives and therefore not identifying all attack cases. The Support Vector Machine (SVM) performed better, with an accuracy of 78.3% and higher recall (63.3%) and a much better precision at 97.8% indicating that it was more effective in distinguishing between normal and malicious traffic.

Performance on detection was also enhanced by the deep learning models. The Convolutional Neural Network (CNN) was able to identify complex relationships between features and its results were as follows: it achieved an accuracy of 80.1% and improved recall (66.8%). All other models gave lower results, with the Long Short-Term Memory (LSTM) model being the most accurate (81.2%) and achieving the highest recall (68.9%), having its F1-score at 80.7. This can be explained by its ability to learn the temporal dependencies of data that make up the network traffic.

results indicate that the Receiver Operating Characteristic (ROC) curve analysis shows that the models with larger Area Under the Curve (AUC) values are more successful in the separation of normal and malicious traffic.

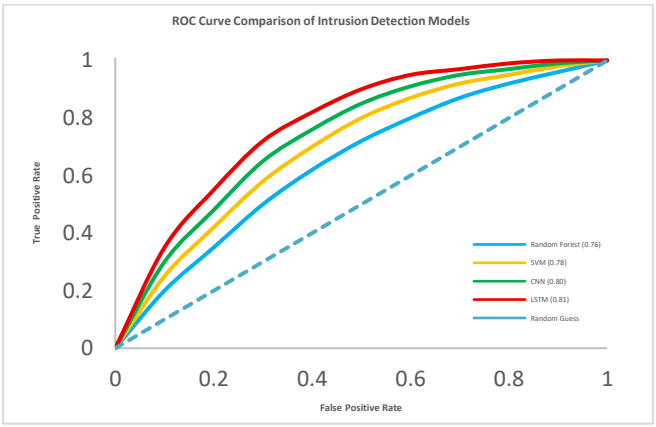

Figure 3. ROC Curve Comparison of Intrusion Detection Models with AUC Values

The ROC curve comparison shows that all the considered models demonstrate good classification performance in terms of network intrusion detection. It is worth mentioning that deep learning models is that the improve the separation between normal and attack traffic, which leads to better performance metrics on their evaluation.

Besides ROC analysis, the Precision-Recall (PR) curve was also analyzed to give more information about the performance of the models in case of class imbalance. As normal traffic samples are significantly higher than the number of attack instances in intrusion detection datasets, the PR curve is a better evaluation metric than evaluating only the minority (attack) class.

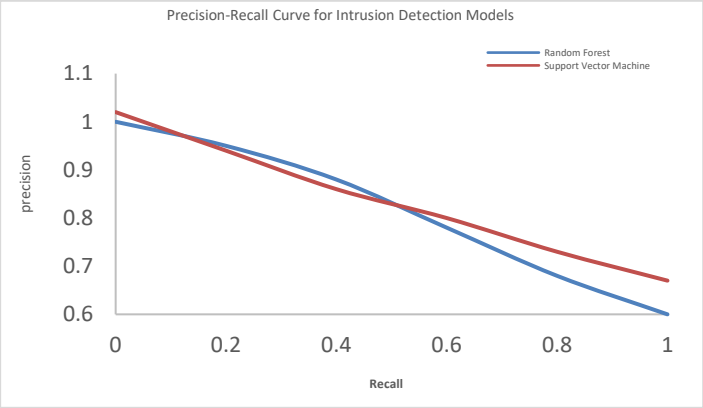

Figure 4. Precision–Recall Curve for Random Forest and Support Vector Machine Models

The Precision-Recall (PR) curve analysis indicates that the precision of standard Random Forest and the Support Vector Machine (SVM) remains high at higher recall values. This means that these models can accurately detect the malicious network traffic and false positive rates are low. Additionally, the performance of the Random Forest model is relatively steady at higher recall values, which implies a greater ability to identify larger percentages of attack examples.

Overall, the experimental outcomes are revealing that deep learning techniques are more effective compared to the traditional machine learning techniques for network intrusion detection. Whereas the Random Forest and the SVM models have high precision and stable results in classification, the Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) models have achieve better recall and F1-scores, as they are more effective in identifying malicious traffic patterns. The LSTM network is the most successful among all the evaluated models in terms of a compromise between the accuracy of detection and the rate of false alarms.

These results show that the proposed adaptive machine learning framework is efficient in the network intrusion detection. The robust and reliable performance of the framework in dynamic network settings is achieved by incorporating the data preprocessing, various learning models, and adaptive detection mechanisms.

In comparison with recent studies in the literature, the performance of the proposed framework demonstrates competitive results while offering additional advantages in adaptability and robustness. Unlike traditional static models, the proposed system incorporates a feedback-driven adaptive mechanism, enabling continuous performance improvement in dynamic environments.

Although the accuracy values are moderate compared to some state-of-the-art models, the framework provides a balance between detection capability, interpretability, and adaptability, which are critical for real-world deployment. The results highlight that adaptability is as important as accuracy in modern intrusion detection systems.

6. CONCLUSION AND FUTURE WORK

In conclusion, this study presents a robust and adaptive machine learning framework for network intrusion detection that addresses the limitations of traditional static models. By integrating multi-model learning, concept drift detection, and a feedback-driven adaptive mechanism, the proposed system demonstrates improved robustness and adaptability in dynamic network environments.

The experimental results confirm that deep learning models, particularly LSTM, provide superior detection capability, while the adaptive framework ensures sustained performance under evolving network conditions. The proposed approach contributes to the development of intelligent and scalable intrusion detection systems suitable for real-world cybersecurity applications.

Future work will focus on integrating advanced adaptive learning techniques, real-time deployment in live network environments, and enhancing model interpretability using explainable artificial intelligence methods.

REFERENCES

1. Liu H, Lang B. Machine learning and deep learning methods for intrusion detection systems: a survey. Appl Sci. 2019;9(20):4396. doi:10.3390/app9204396.
2. Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R. Machine learning and deep learning approaches for cybersecurity: a review. IEEE Access. 2022;10:19572–19585. doi:10.1109/ACCESS.2022.3151248.
3. Lansky J, Ali S, Mohammadi M, Majeed MK, Karim SHT, Rashidi S, et al. Deep learning-based intrusion detection systems: a systematic review. IEEE Access. 2021;9:101574–101599. doi:10.1109/ACCESS.2021.3097247.
4. Farhan M, Waheed Ud Din H, Ullah S, Hussain MS, Khan MA, Mazhar T, et al. Network-based intrusion detection using deep learning technique. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-08770-0.
5. Mirsadeghi SMH, Bahsi H, Vaarandi R, Inoubli W. Learning from few cyber-attacks: addressing the class imbalance problem in machine learning-based intrusion detection in software-defined networking. IEEE Access. 2023;11:140428–140442. doi:10.1109/ACCESS.2023.3341755.
6. Villegas-Ch W, Govea J, Gutierrez R, Maldonado Navarro A, Mera-Navarrete A. Effectiveness of an adaptive deep learning-based intrusion detection system. IEEE Access.

2024;12:184010–184027. doi:10.1109/ACCESS.2024.3512363.
7. Mohale VZ, Obagbuwa IC. Evaluating machine learning-based intrusion detection systems with explainable AI: enhancing transparency and interpretability. Front Comput Sci. 2025;7. doi:10.3389/fcomp.2025.1520741.
8. Wisanwanichthan T, Thammawichai M. A double-layered hybrid approach for network intrusion detection system using combined naive Bayes and SVM. IEEE Access. 2021;9:138432–138450. doi:10.1109/ACCESS.2021.3118573.
9. Liu C, Gu Z, Wang J. A hybrid intrusion detection system based on scalable K-means + random forest and deep learning. IEEE Access. 2021;9:75729–75740. doi:10.1109/ACCESS.2021.3082147.
10. Seth S, Chahal KK, Singh G. A novel ensemble framework for an intelligent intrusion detection system. IEEE Access. 2021;9:138451–138467. doi:10.1109/ACCESS.2021.3116219.
11. Okutan Kara A, Kara M, Boyaci A. A comparative analysis of machine learning and deep reinforcement learning approaches for adaptive intrusion detection. IEEE Access. 2025;13:189833–189849. doi:10.1109/ACCESS.2025.3627098.
12. Yu J, Shvetsov AV, Alsamhi SH. Leveraging machine learning for cybersecurity resilience in Industry 4.0: challenges and future directions. IEEE Access. 2024;12:159579–159596. doi:10.1109/ACCESS.2024.3482987.
13. Sharma SB, Bairwa AK. Leveraging AI for intrusion detection in IoT ecosystems: a comprehensive study. IEEE Access. 2025;13:66290–66317. doi:10.1109/ACCESS.2025.3550392.
14. Arnob AKB, Chowdhury RR, Chaiti NA, Saha S, Roy A. A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions. J Edge Comput. 2025;4(1):73–104. doi:10.55056/jec.885.
15. Abdulkareem SA, Heng Foh C, Shojafar M, Carrez F, Moessner K. Network intrusion detection: an IoT and non-IoT-related survey. IEEE Access. 2024;12:147167–147191. doi:10.1109/ACCESS.2024.3473289.
16. Li Y, Zhang J, Yan Y, Lei Y, Yin C. Enhancing network intrusion detection through the application of the dung beetle optimized fusion-model. IEEE Access. 2024;12:9483–9496. doi:10.1109/ACCESS.2024.3353488.
17. Bisen D, Ghanghoria A, Saurabh P, Rohith D, Singh U. Optimizing intrusion detection in software-defined networks through automated machine learning and intelligent feature engineering. IEEE Access. 2025;13:194097–194114. doi:10.1109/ACCESS.2025.3632116.
18. Benka D, Horváth D, Špendla L, Gašpar G, Strémy M. Machine learning-based detection of anomalies, intrusions, and threats in industrial control systems. IEEE Access. 2025;13:12502–12514. doi:10.1109/ACCESS.2025.3530902.
19. Ennaji S, de Gaspari F, Hitaj D, Kbidi A, Mancini LV. Adversarial challenges in network intrusion detection systems: research insights and future prospects. IEEE Access. 2025;13:148613–148645. doi:10.1109/ACCESS.2025.3600984.
20. Ababneh J, Al-Nsour EYA, Al-Shaikh A, Al-Mousa MR, Al-Zabin A, Asassfeh M, et al. Enhancing DevOps continuous monitoring phase: hybrid intrusion detection and ensemble learning system (HIDELS). IEEE Access. 2026;14:4733–4755. doi:10.1109/ACCESS.2026.3650793.
21. Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems. In: Military Communications and Information Systems Conference; 2015.
22. Tavallaee M, et al. A detailed analysis of the KDD Cup 99 dataset. In: IEEE Symposium on Computational Intelligence for Security and Defense Applications; 2009.
23. Le Jeune L, Goedeme T, Mentens N. Machine learning for misuse-based network intrusion detection: overview, unified evaluation and feature choice comparison framework. IEEE Access. 2021;9:63995–64015.

About the corresponding author

Umar Yahaya Namahe is affiliated with the School of Computer Science and Engineering at Geeta University, Panipat, India. His academic interests include cybersecurity, machine learning, and network intrusion detection systems. He is actively engaged in research focusing on intelligent systems and advanced computing technologies for improving digital security and performance.