Scientiarum: A Multidisciplinary Journal
Volume 2, Issue 4, August 2026, pp. 1–8
DOI: 10.54646/SAPARS.2026.35

SAPAR SERVICES LLP
Scholarly Articles Publication And Repository Services

ORIGINAL RESEARCH

Detection of distributed denial of service attacks in NFV environments using machine learning-based anomaly detection

Sai Vineela Gali[1,2*]

[1]Department of Computer Science, University of Dayton, Dayton, OH, United States
[2]Artex Risk Solutions, Fairlawn, OH, United States

***Correspondence:**
Sai Vineela Gali,
Saivineelagali@gmail.com

Received: 11 June 2026; **Accepted:** 07 July 2026; **Published:** 31 July 2026

Objectives: The rise of Network Function Virtualization (NFV) has created a scalable, flexible alternative to traditional hardware-based networking infrastructures. However, due to the nature of NFV, there is a potential for an increased occurrence of Distributed Denial of Service (DDoS) attacks in a dynamic NFV environment and the need for adaptive security mechanisms capable of identifying DDoS attacks with high levels of accuracy. Through this research, the author intends to develop a machine learning (ML)-based anomaly detection framework that uses ML techniques to detect DDoS attacks accurately within an NFV environment.

Methodology: A ML model with the use of CICDDoS2019 (2020): Data (a dataset) includes data preprocessing, feature scaling, and principal component analysis (PCA), which are techniques for reducing the dimensions of the dataset and maintaining important features for analysis of traffic on the network in this article. Five ML models were developed from the training dataset: Isolation Forest, Autoencoder, One-Class Support Vector Machine (SVM), Random Forest (RF) and XGBoost (XG). An ensemble approach was also created to improve detection performance by combining three or more of these (or other) ML techniques. Findings from this research demonstrate that PCA can facilitate a reduction in dimensionality from 29 unique features to 24 unique principal components while preserving almost 95% of the variability in the original feature set. In addition, RF and XG were identified as the two highest-performing modeling algorithms, with each scoring a perfect “100” on all measures of performance (including accuracy, precision, recall, and F1) calculated. One-Class Support Vector Machine (OSVM) scored an average of 96%, and the composite of all three models (ensemble model) averaged 93% with a very limited ability to detect each of the different types of DDoS attacks with the same degree of confidence. Therefore, the results of this study support the use of the developed system for detection purposes for both previously known and unknown forms of DDoS attacks as well as increasing the overall level of reliability and resiliency against attacks targeting NFV infrastructure.

Novelty: This research presents a novel hybrid framework for anomaly detection in NFV by integrating supervised, unsupervised, and semi-supervised ML methods within a single NFV security architecture. In addition, the proposed method employs PCA for dimensionality reduction and ensemble learning to improve detection accuracy, adaptation to evolving attack patterns, and computational efficiency of detected anomalies, thereby providing a more effective means of defeating DDoS attacks within virtualized network environments.

Keywords: network function virtualization, distributed denial-of-service, anomaly detection, machine learning, principal component analysis, random forest, XGBoost, ensemble learning

The author is the Claims Data Science Specialist in Artex Risk Solutions, United States

CC BY

Introduction

Network Function Virtualization (NFV) has changed the way we manage networks today; it has taken away the need for dedicated hardware devices to create a new standard use of commodity computing in order to run virtual cloud-based network functions (1, 2). With this change, we have increased scalability and flexibility and reduced operational costs to meet the increasing demands from Cloud Computing, the Internet of Things (IoT) and 5G networks (1, 2). By decoupling all of the Network Services from the physical hardware platforms, organizations can easily and quickly deploy, modify, and manage Network Functions, such as Firewalls, Load Balancers, and Intrusion Detection Systems (IDS), to improve the use of resources and reduce operating expenses (1).

While NFV provides numerous benefits, it also has a number of significant security challenges related to the fact that NFV is a virtualized/distributed system (2, 3). Features like dynamic resource allocation, multi-tenancy, virtualization layers, and software-defined orchestration pose increased attack surfaces that can expose NFV infrastructures to multiple cyber threats (2, 3). Distributed Denial of Service (DDoS) attacks are one of the most significant types of cyber threats to NFV environments today (4, 5). DDoS attacks target specific services and overwhelm them with large amounts of malicious traffic in an effort to exhaust the computational and network resources of those services, causing those services to be unavailable (4, 5). When an DDoS attack occurs against an NFV environment, the number of services impacted by the attack is amplified, since many Virtual Network Functions share the same physical resources (2, 5).

Recently, researchers have begun to investigate DDoS detection through machine learning (ML) methods in both cloud-based and NFV scenarios (6–9). A variety of supervised learning techniques (e.g., Random Forest (RF), Support Vector Machines (SVM), and XGBoost (XG)) have generally provided high accuracy rates with respect to already known DDoS attack patterns (6, 7). Unsupervised models that attempt to identify anomalies (e.g., Isolation Forest and Autoencoders) have also been tested as methods of detecting attacks in changing network environments (8, 9). However, most of these existing studies examine only a particular type of learning, and they typically suffer from limitations in detecting previously unobserved attack patterns; adapting to emerging threat vectors; or retaining performance across different types of networks (7–10). Additionally, a lack of research integrates supervised, unsupervised, and semi-supervised approaches to develop a unified framework for detecting and mitigating DDoS attacks using NFV technologies (9, 10).

This study proposes to develop a hybrid model-based anomaly detection framework for detecting DDoS attacks inside NFV architectures using the CICDDoS2019 dataset (11). The proposed framework employs PCA to reduce the dimensionality of features and integrates multiple ML models (e.g., Isolation Forest, Autoencoder, One-Class SVM, RF, and XG) designed around differing DDoS attack characteristics (6–10). The goal of integrating multiple methods into a commonly implemented framework is to improve the accuracy, robustness, and adaptability of the intended model for detecting and mitigating both previously observed and unobserved DDoS attacks occurring across virtualized environments (4, 5, 9, 10).

Methodology

The Canadian Institute for Cybersecurity (CIC) has created a new benchmark dataset, called the CICDDoS2019, to test the efficacy of IDS and Anomaly Detection Systems (ADS) (11). The dataset contains real-world network traffic examples, including good traffic examples and network DDoS attacks (11). There is sufficient flow feature data for both types of systems (11). Each flow provides a variety of features, including the total duration (seconds) of the flow, ingress rate into the flow (packets per second), egress rate from the flow (packets per second), size (bytes) of the TCP/IP header of each flow, average size (bytes) of each packet in the flow, and the average time between two packets in the flow (11). These flow features allow for the creation and testing of ML-based DDoS detection models designed for use in NFV environments (1, 11).

Data preprocessing

Data preprocessing has two purposes: first, improve the quality of data through removing bad data, missing values, and duplicate records to be reliable and valid; second, normalize the scales of the traffic features so that all numeric traffic features have a mean of 0 and a standard deviation of 1 so that they won't skew the results of the model training by being larger than the smaller numeric traffic features. As an example, we would use StandardScaler to standardize all numerical traffic features (12).

When we prepared the data for the anomaly detection task, we created a two-class, binary representation of the categorical traffic labels (0 = benign traffic, 1 = DDoS attack traffic). This makes it easier to have a definite decision to make as to whether a sample of traffic is normal or malicious (6, 7).

The final dataset was split into training and testing datasets with an 80:20 split. The training dataset will be used to create and train a ML model, and the testing dataset will be used to assess the performance of the ML model after it has been trained (12).

EDA

Exploratory Data Analysis (EDA) was carried out to identify the characteristics of network traffic and discover clues for DDoS attack-associated patterns (11). Throughout this analysis, a variety of statistical techniques were utilized, including graphs, to study how each of the features within DDoS protocol families and at the packet level, as well as which class of packets, was being transmitted over the network and how they are distributed.

In addition to using statistical methods, visual analysis was also performed, indicating that a class imbalance exists and that there are statistically significant differences in benign and malicious patterns of traffic, which provides evidence of using ML to detect possible DDoS attacks from network traffic data (6–10).

In order to reduce multidimensionality, PCA is typically used to reduce the quantity of features within a dataset that have many features or a number of variables measuring the same characteristic (12). Using more than one type of measure to create an accurate model from a dataset creates a time-consuming and potentially inaccurate use of computational resources (12).

By applying PCA, the collection of original features was transformed into new (orthogonal) features that retain approximately 95.25% of the original information (from analyzing the variance within the dataset from the first 24 principal components) (12). The new (orthogonal) features were then used to create changers and test changers and produced good computational efficiencies and retained the fundamental characteristics present within the original dataset that would allow for effective DDoS detection (12).

Machine learning models

To evaluate the various techniques available to learn to identify anomalies, we used five different ML models based on the methodologies of supervised, unsupervised, and semi-supervised learning (6–10).

Isolation forest

The isolation forest was used as an unsupervised model to find anomalies from data by making use of tree structures that recursively split the data into groups of observations by dividing by half until there are only the observations that require the fewest number of divisions remaining (being isolated) (8). The isolation forest is a quick and efficient way to find anomalies throughout large high-dimensional networks and traffic flow (8).

The Deep Learning-based Autoencoder is a neural network architecture for identifying anomalies (9). The Autoencoder is composed of two neural networks, the encoder, which produces a reduced representation of normal network activity, and the decoder, which tries to reconstruct the original input of the given network (9). If the reconstruction error of any sample from the input set is above a predetermined value, then this could signal a possible DDoS attack or some other type of unknown malicious act (9).

The One-Class SVM (often called One-Class SVM) is a semi-supervised anomaly detection method that has also been used in many applications (10). One-Class SVM is trained using a set of training samples that contain only the normal traffic of the network (10). These normal training samples are used by the One-Class SVM to create a boundary between the normal and abnormal behavior of the traffic (10). Any traffic sample falling outside of this boundary will be classified as an anomaly and could indicate a potentially malicious act (10).

Random forest

RF is a supervised learning technique implemented as a classification algorithm (6). Depending on bootstrap sampling and randomly chosen variables, many decision trees are constructed by a RF (6). As a direct result, RF produces a better level of confidence due to superior generalization, less overfitting, and a higher level of confidence than using only the classification accuracy of a decision tree classifier alone (6). The ultimate classification will be determined by a popular vote of all of the created trees (6).

XGBoost

XG is a more advanced supervised learning technique that is based upon gradient boosting (7). A tree is built one at a time, with each tree being built in such a way that it improves upon the prediction of the prior classifier by optimizing and thus better regulating the nature of the classifier's predictions on the training data (7). XG has demonstrated its capacity to produce very high levels of accuracy with respect to large datasets, thus, making it very useful in ML (7).

Hybrid ensemble method for detecting anomalies

Three approaches (Classification of an Attack – Anomaly Detected) of anomaly detection, Isolation Forests, Autoencoders, and One-Class SVM, were used in the ensemble of this framework to identify an anomaly in the data (8–10). An ensemble voting system was created to classify an instance of data as an attack if two or more

of the three models classified the sample as anomalous traffic (8–10).

The purpose of using the Hybrid Ensemble Method of multiple anomaly detection models was to improve the reliability of the classification of an attack and improve detection methods (8–10). The intent was to combine different learning paradigms, which would provide lower numbers of false positives and provide better identification of unknown DDoS attack patterns (8–10).

Evaluation metrics for performance

We evaluated performance on the classification task using standard metrics of accuracy, precision, recall, and F1-score for all three models (as well as the entire framework) (12). These performance metrics evaluate the model's ability to classify benign (normal) versus malicious (DDoS) traffic in real-time (12).

Receiver operating characteristic (ROC) curves and AUC values were also used to evaluate how well each model performed at classifying normal and DDoS traffic (12). Each metric provides an evaluation of the detection capability of the models, as well as an indication of overall performance when detecting DDoS attacks in an NFV environment (4, 5).

Results and discussion

Principal component analysis to reduce dimensionality

Principal Component Analysis (PCA) was utilized to reduce the dimensionality of the CICDDoS2019 dataset as well as to provide more efficient computational processing. The cumulative explained variance analysis determined that 24 of the principal components retained approximately 95.25% of the total variance of the original feature set. Therefore, PCA can provide a significant amount of dimensionality reduction (i.e., remove redundant or highly correlated features) while retaining much of the information necessary for accurate DDoS detection.

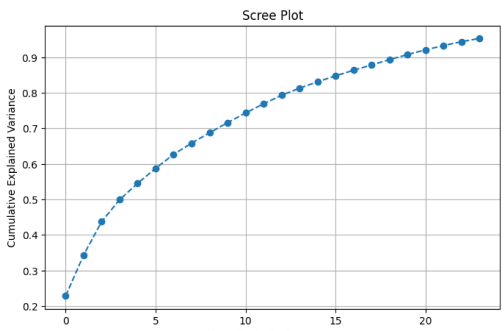

FIGURE 1 | PCA scree plot.

Isolation Forest Report:

	precision	recall	f1-score	support
0	0.20	0.84	0.32	97831
1	0.26	0.02	0.03	333540
accuracy			0.20	431371
macro avg	0.23	0.43	0.18	431371
weighted avg	0.25	0.20	0.10	431371

FIGURE 2 | Isolation forest performance report.

Figure 1 shows the PCA scree plot that illustrates the cumulative variance retained by the selected principal components. PCA reduced the computational complexity of model training and minimized the chances of overfitting through the elimination of redundant and highly correlated features. The result is that PCA became an effective feature extraction method for subsequent ML analysis.

Performance of individual machine learning models

To determine the effectiveness of different learning paradigms for DDoS detection within NFV environments, five ML models were implemented and tested against the preprocessed dataset; these included Isolation Forest, Autoencoder, One-Class SVM, RF, and XG.

Isolation forest

Isolation Forest was assessed as an unsupervised anomaly detection model that has the ability through recursive data partitioning to detect traffic anomalies. The model is computationally efficient, making it well suited for large-scale network monitoring applications. This model, however, achieved a relatively low classification accuracy at 20%, precision of 0.26, a recall of 0.02, F1 score of 0.03. While Isolation Forest may be capable of detecting high-level anomalies, it is not capable of discerning subtle differences in both normal traffic and attack traffic in complex NFV environments. **Figure 2** presents the performance report of the Isolation Forest model.

Autoencoder

The Autoencoder is an approach to detecting anomalies using deep learning. By creating compressed representations of normal network traffic and reconstructing those compressed packets back into the original data packet, the Autoencoder will identify potential anomalies based on the amount of error between the reconstructed data and its original form. The confusion matrix and ROC analysis were used to show the ability of this architecture

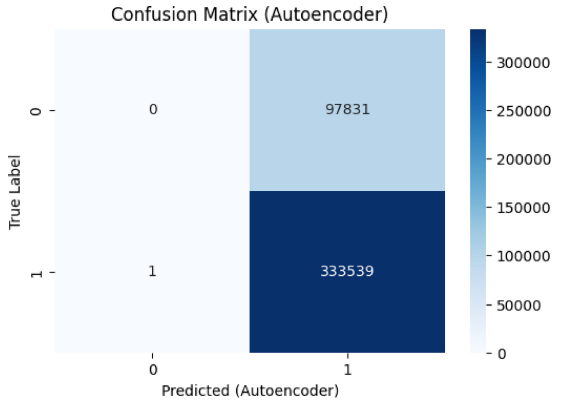

FIGURE 3 | Autoencoder confusion matrix.

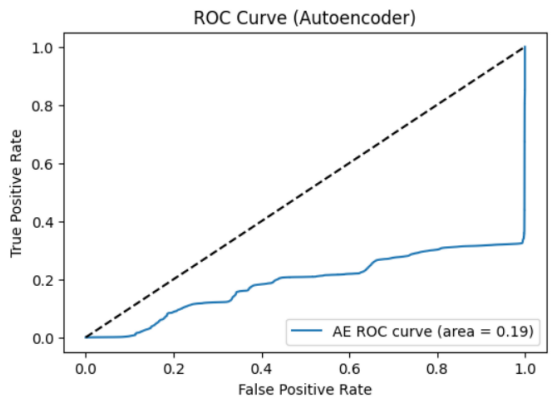

FIGURE 4 | Autoencoder ROC curve.

to distinguish between benign and malicious network traffic; however, the overall classification performance was limited, with an accuracy of 22%, precision of 0.39, recall of 0.03, and an F1-score of 0.05. Therefore, while reconstruction-based anomaly detection methods detected abnormal behavior, the methods' effectiveness was determined by the attacking patterns present in the training dataset when implementing this type of model for the purpose of Network Intrusion Detection. **Figure 3** shows the Autoencoder confusion matrix. **Figure 4** presents the ROC curve of the Autoencoder model.

One-Class SVM

Training was performed on benign traffic samples using the One-Class SVM model, which utilized an radial basis function (RBF) kernel to form a boundary defining the expected behavior of normal traffic on the network. Any sample that fell outside this boundary was determined to be an anomaly. The One-Class SVM model produced an accuracy of 96%, a precision of 0.98, a recall of 0.96, and an F1 score of 0.97 indicating that this model is

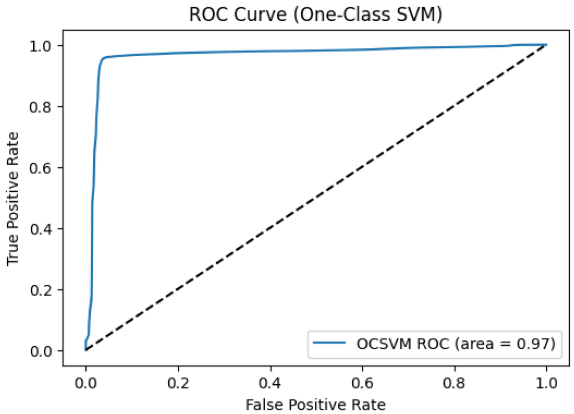

FIGURE 5 | One-Class SVM ROC curve.

One-Class SVM Report:

	precision	recall	f1-score	support
0	0.87	0.95	0.91	97831
1	0.98	0.96	0.97	333540
accuracy			0.96	431371
macro avg	0.93	0.95	0.94	431371
weighted avg	0.96	0.96	0.96	431371

FIGURE 6 | One-Class SVM performance report.

very effective at identifying attack traffic since it has a high recall value; therefore, it is a viable semi-supervised methodology for detecting previously unknown attacks. However, because the performance of the model depends upon its parameters, they need to be well tuned in order to achieve optimal performance. **Figure 5** illustrates the ROC curve of the One-Class SVM model. **Figure 6** presents the performance report of the One-Class SVM model.

Random forest

RF performed exceptionally well in classifying and was found to be one of the best models assessed in the research. This model achieved a perfect score on all metrics: 100% for accuracy, precision, recall, and F1-score. The RF's multiple decision tree architecture effectively modeled the relationships between network traffic features while minimizing overfitting of the classifier. The features analysis indicates that flow duration, packet statistics, and attributes related to the protocol were strong contributors to the classification of attack traffic. This means that the characteristics of network traffic flow will be highly useful in detecting whether an attack against a DDoS has occurred. **Figure 7** shows the performance report of the Random Forest model. **Figure 8** illustrates the feature importance obtained using the Random Forest model.

```
=== Random Forest ===
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     19619
           1       1.00      1.00      1.00     66656

    accuracy                           1.00     86275
   macro avg       1.00      1.00      1.00     86275
weighted avg       1.00      1.00      1.00     86275
```

FIGURE 7 | Random forest (RF) performance report.

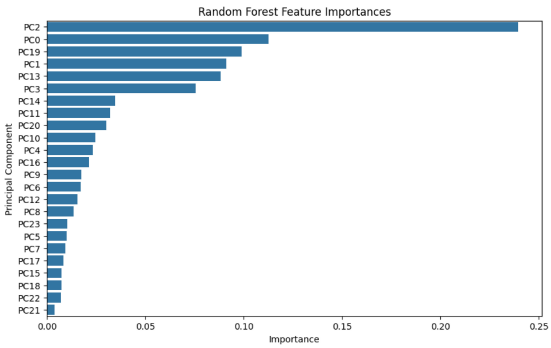

FIGURE 8 | RF feature importance.

```
=== XGBoost ===
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     19619
           1       1.00      1.00      1.00     66656

    accuracy                           1.00     86275
   macro avg       1.00      1.00      1.00     86275
weighted avg       1.00      1.00      1.00     86275
```

FIGURE 9 | XGBoost (XG) performance report.

XGBoost

XG was the best-performing model across all models tested. Similar to RF, XG had a perfect score for each of the metrics: 100% for accuracy, precision, recall, and F1-score. The use of gradient boosting by XG allowed the model to perform well in learning the complex interactions between features resulting in fewer classification errors. The feature importance analysis of XG confirmed the importance of the network flow characteristics when distinguishing between benign traffic and malicious traffic. Furthermore, XG produced the lowest false positive rates of all the models tested; therefore, it would be very appropriate for use in an operational environment where the generation of accurate alerts is critical. **Figure 9** presents the performance report of the XGBoost model. **Figure 10** illustrates the feature importance generated by the XGBoost model. **Figure 11** compares the ROC curves of the Random Forest and XGBoost models.

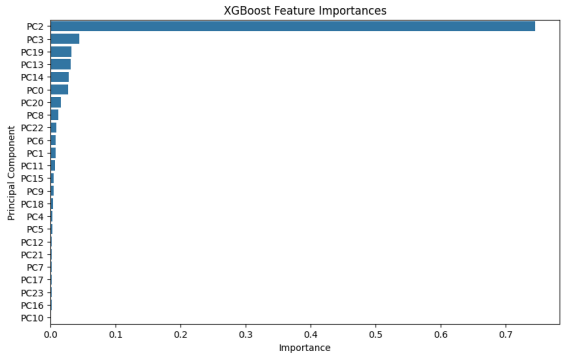

FIGURE 10 | XG feature importance.

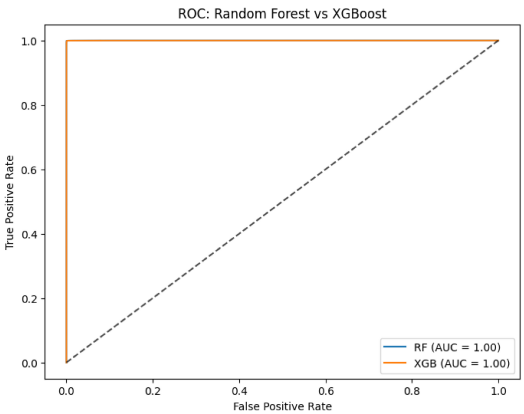

FIGURE 11 | RF vs. XG ROC comparison.

TABLE 1 | Models' performance comparison.

Model	Precision	Recall	F1-score	Accuracy
Isolation Forest	0.26	0.02	0.03	0.2
Autoencoder	0.39	0.03	0.05	0.22
One-Class SVM	0.98	0.96	0.97	0.96
Ensemble	0.95	0.96	0.96	0.93
RF	1.00	1.00	1.00	1.00
XG	1.00	1.00	1.00	1.00

Comparative model evaluation

A comparative analysis was conducted to assess the performance of all evaluated models. The results are presented in **Table 1**.

The comparative results show that supervised learning techniques are much more effective than any of the unsupervised anomaly detection methods. Furthermore, RF as well as XG reached perfect classification accuracy, showing their ability to identify discriminative patterns of attacks from labeled data during training. On the other hand, One-Class SVM achieved strong classification results, even though it learned to classify the attacks on the basis of benign traffic alone.

```
Ensemble Model Report:
              precision    recall  f1-score   support

           0       0.86      0.83      0.84     97831
           1       0.95      0.96      0.96    333540

    accuracy                           0.93    431371
   macro avg       0.90      0.90      0.90    431371
weighted avg       0.93      0.93      0.93    431371
```

FIGURE 12 | Ensemble model performance report.

When the ROC curves were created, they confirmed the above analysis, as RF and XG distinguished between benign and malicious traffic nearly perfectly. XG had slightly better overall classification confidence than RF and also had a lower false-positive classification rate.

Performance of the hybrid ensemble model

The hybrid anomaly detection framework comprised Isolation Forest, Autoencoder and One-Class SVM and used a majority voting system to enable classifying any anomalies detected in the network traffic sample as malicious if any 2 out of the 3 models classified that sample as anomalous.

When comparing the hybrid ensemble model to the supervised models, the hybrid ensemble demonstrated an overall lower accuracy (93%) but was significantly more robust than each individual model, using the individual models together to provide a lower false positive rate and greater consistency across different attack types by combining the results of the separate models to provide classification. **Figure 12** presents the performance report of the proposed hybrid ensemble model.

Suitability for NFV deployment

Suitability for deployment in NFV environments will consider the practical operational suitability of the various models. There are practical issues in choosing the proper operation model, such as the fact that the supervised models have demonstrated a practical maximum accuracy in classifying attacks; however, they will require large amounts of labeled data for training and will not work well against attacks that are completely new and different. On the other hand, the unsupervised and semi-supervised models have the greatest flexibility to develop and utilize detection methods to identify and locate new threat patterns; however, they have exhibited lower classification accuracies.

The hybrid ensemble will provide the appropriate approach for combining the adaptability of detection capability with a reliable detection accuracy within an NFV environment. The ability for a model to adjust to variations in computational resources, virtualization technologies, and rapidly evolving behaviors of threat actors (attack patterns) requires security mechanisms that can continue to perform effectively in an ever-changing and evolving environment in an NFV solution. **Table 2** compares the evaluated machine learning techniques based on real-time capability, accuracy, scalability, label requirements, and adaptability for deployment in NFV environments.

Conclusion

Anomaly detection in DDoS attacks on NFV environments was examined in this study through the use of a hybrid machine-learning anomaly detection framework utilizing the CICDDoS2019 dataset. The framework incorporated PCA with supervised, unsupervised, and semi-supervised machine-learning approaches; these included RF, XG, Isolation Forest, Autoencoder, and One-Class SVM.

Results obtained experimentally showed that PCA could reduce the dimensionality of the feature space down to 24 principal components while retaining approximately 95.25% of the variance of the original data and, at the same time, improving computational efficiency without a loss of information. RF and XG provided outstanding performances, with both having perfect accuracies (100%), precision (100%), recall (100%), and F1-scores (100%). One-Class SVC had an accuracy of 96% and an F1-score of 97%, while the hybrid ensemble framework proposed herein had an accuracy of 93% and an F1-score of 96%. Therefore, results demonstrated that machine-learning techniques are

TABLE 2 | Comparison of techniques and suitability for network function virtualization (NFV) deployment.

Technique	Real-time	Accuracy	Scalability	Requires labels	Adaptability
Isolation Forest	✓	✗	✓	✗	✓
Autoencoder	✗	✗	✓	✗	✓
One-Class SVM	✓	✓	✓	Only benign	✓
RF	✗	✓	✓	✓	✗
XG	✗	✓	✓	✓	✓
Ensemble	✓	✓	✗	Partial	✓

very effective in detecting all forms of DDoS attack types that may either already be known or not previously known within the NFV environment.

Data availability statement

The CICDDoS2019 dataset used in this study is publicly available from the Canadian Institute for Cybersecurity (CIC). The dataset can be accessed through the official CIC dataset repository for research purposes.

Ethics statement

This study did not involve human participants, animals, or clinical data. Therefore, ethical approval was not required.

Funding

The author declares that financial support was not received for this work and/or its publication.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Novaes MP, Carvalho LF, Lloret J, Proença ML. Adversarial deep learning approach for detection and defense against DDoS attacks in software-defined networks. *Fut Generat Comput Syst*. (2021) 125:156–67. doi: 10.1016/j.future.2021.06.017
2. Sayed MSE, Le-Khac NA, Azer MA, Jurcut AD. A flow-based anomaly detection approach with feature selection against DDoS attacks in software-defined networks. *IEEE Transac Cognit Commun Netw*. (2022) 8(4):1862–80. doi: 10.1109/TCCN.2022.3185819
3. Elubeyd H, Yiltas-Kaplan D. Hybrid deep learning approach for automatic DoS and DDoS attack detection in software-defined networks. *Appl Sci*. (2023) 13(6):3828. doi: 10.3390/app13063828
4. Al-Dunainawi Y, Al-Kaseem BR, Al-Raweshidy HS. Optimized artificial intelligence model for DDoS detection in software-defined network environments. *IEEE Access*. (2023) 11:106733–48. doi: 10.1109/ACCESS.2023.3319214
5. Zhou H, Zheng Y, Jia X, Shu J. Collaborative prediction and detection of DDoS attacks in edge computing using deep learning and distributed SDN. *Comput Netw*. (2023) 225:109642. doi: 10.1016/j.comnet.2023.109642
6. Ahuja N, Mukhopadhyay D, Singal G. DDoS attack traffic classification in software-defined networking using deep learning. *Person Ubiquit Comput*. (2024) 28(2):417–29. doi: 10.1007/s00779-023-01785-2
7. Han D, Li H, Fu X, Zhou S. Traffic feature selection and distributed denial of service attack detection in software-defined networks based on machine learning. *Sensors*. (2024) 24(13):4344. doi: 10.3390/s24134344
8. Tymoshchuk D, Yasniy O, Mytnyk M. *Detection and Classification of DDoS Flooding Attacks Using Machine Learning Methods*. arXiv (2024). Available online at: https://arxiv.org/abs/2412.18990
9. Abiramasundari S, Ramaswamy V. Distributed denial-of-service attack detection using supervised machine learning algorithms. *Sci Rep*. (2025) 15:13098. doi: 10.1038/s41598-024-84879-y
10. Batool S, Ahmed M, Rehman A. A comprehensive review of DDoS detection and mitigation using machine learning and deep learning in software-defined networking. *Electronics*. (2025) 14(21):4222. Available online at: https://www.mdpi.com/journal/electronics
11. Kalambe D, Sharma D, Kadam P, Surati S. A comprehensive plane-wise review of DDoS attacks in software-defined networking using machine learning and deep learning. *J Netw Comput Appl*. (2025) 235:104081. doi: 10.1016/j.jnca.2025.104081
12. Rahman MA. *Detection of Distributed Denial of Service Attacks Based on Machine Learning Algorithms*. arXiv (2025). Available online at: https://arxiv.org/abs/2502.00975