International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Behaviour-Based Machine Learning Framework for Detecting Anomalous Network Activities

1. Sejal Sharad Shirole
2. Dyaneshwar Balu Lokhande (Assistant Professor)
Department of Master of Computer Application,
JCEI's Jaihind Institute of Management and Research, Vadgaon Sahani
Email: sejalshirole5@gmail.com

Abstract - The increasing complexity of cyber threats has created a need for intelligent network security systems capable of identifying malicious activities that evade traditional signature-based detection mechanisms. Conventional intrusion detection systems primarily depend on predefined rules and known attack signatures, limiting their effectiveness against previously unseen threats and evolving attack behaviours. This paper proposes a behaviour-based machine learning framework for detecting anomalous network activities through the analysis of network traffic patterns and communication characteristics. The proposed framework combines statistical traffic feature extraction, behavioural profiling, unsupervised anomaly detection, and supervised classification to identify suspicious network activities. Isolation Forest and Autoencoder models are considered for detecting deviations from normal traffic behaviour, while Random Forest is used to classify identified activities when labelled data are available. The framework incorporates adaptive anomaly thresholds and interpretable feature-based explanations to improve detection reliability and operational usability. The proposed approach is designed for evaluation using benchmark datasets such as UNSW-NB15 and CICIDS2017. Performance will be assessed using precision, recall, F1-score, false positive rate, and detection latency. The framework aims to support proactive network security by identifying unusual communication patterns, reducing dependence on known attack signatures, and enabling timely investigation of potential threats.

Key Words: Network Security, Machine Learning, Behaviour-Based Detection, Anomaly Detection, Intrusion Detection System, Isolation Forest, Autoencoder, Random Forest.

1. INTRODUCTION

Computer networks have become essential infrastructure for communication, education, business operations, cloud computing, and digital services. As network usage increases, cyber threats such as denial-of-service attacks, scanning, data exfiltration, credential misuse, and botnet communication continue to challenge conventional security mechanisms.

Traditional intrusion detection systems (IDS) commonly rely on signature-based detection. These systems compare observed traffic against known attack patterns and generate alerts when a match is found. Although effective for previously identified threats, signature-based methods may fail to detect zero-day attacks, modified attack techniques, and unusual activities that do not match existing signatures.

Machine learning provides an alternative by learning patterns from network traffic and identifying deviations from expected behaviour. Behaviour-based detection focuses on characteristics such as connection frequency, packet size, communication duration, protocol distribution, and data transfer volume. By learning these characteristics, an intelligent IDS can identify potentially malicious activities even when their exact signatures are unknown.

This research proposes a behaviour-based machine learning framework that combines unsupervised and supervised learning techniques to improve the detection of anomalous network activities.

1.1 Problem Statement

Existing network intrusion detection systems face challenges in detecting previously unseen attacks, adapting to changing traffic patterns, and maintaining a low false positive rate. Many machine learning-based systems also depend heavily on labelled attack datasets, which may not represent emerging threats.

The research problem is to develop a behaviour-based framework that learns normal network activity, detects significant deviations, and supports reliable classification and interpretation of suspicious traffic..

1.2 Objectives

1. Identify important behavioural features that characterize normal and anomalous network activities.
2. Develop a machine learning framework combining unsupervised anomaly detection and supervised classification.
3. Evaluate Isolation Forest, Autoencoder, and Random Forest models for network anomaly detection.
4. Investigate adaptive thresholding to reduce false alarms under changing traffic conditions.
5. Assess the framework using benchmark network traffic datasets and established performance metrics.

2. LITERATURE REVIEW

Machine learning has become an important approach to network anomaly detection because it can learn complex traffic patterns and identify deviations from normal activity.

2.1 Signature-Based and Behaviour-Based Detection

Signature-based IDSs identify attacks using known patterns, making them effective for recognized threats but less adaptable to novel attacks. Behaviour-based detection instead identifies deviations from a learned baseline, offering the potential to detect previously unseen malicious activities.

A review of machine learning approaches to malicious network behaviour detection highlights the importance of extracting meaningful flow-level, statistical, and temporal features from network traffic [1].

2.2 Unsupervised Anomaly Detection

Unsupervised learning is particularly useful when labelled attack data are limited. Isolation Forest identifies anomalies by isolating observations using random partitioning. Autoencoders learn compact representations of normal traffic and use reconstruction error to identify unusual observations.

Recent work on flow-level behavioural fingerprinting has investigated Isolation Forest, One-Class SVM, Local Outlier Factor, K-Nearest Neighbours, and Autoencoder models using normal-only training data [2]. This supports the use of unsupervised models in environments where attack labels are unavailable.

2.3 Deep Learning for Network Anomaly Detection

Deep learning models can learn complex relationships in network traffic. Convolutional neural networks can identify local feature patterns, while recurrent models such as LSTMs can capture temporal dependencies. Autoencoders are useful when the objective is to learn a representation of normal traffic and identify deviations.

A recent survey of network anomaly detection discusses the strengths and limitations of CNNs, LSTMs, and generative models across commonly used benchmark datasets [3].

2.4 Research Gap

Despite progress in machine learning-based intrusion detection, several challenges remain:

- Dependence on labelled datasets containing known attacks.
- High false positive rates when legitimate traffic changes.
- Limited adaptability to evolving network behaviour.
- Difficulty explaining why a particular connection is considered anomalous.
- Inconsistent evaluation across datasets and experimental settings.

This research addresses these challenges through a modular framework combining behavioural profiling, unsupervised anomaly detection, adaptive thresholds, and interpretable classification.

3. METHODOLOGY

The research will follow an experimental design involving dataset preparation, feature engineering, model development, evaluation, and comparative analysis.

3.1 Research Framework

The proposed system consists of six major stages:

1. Network traffic data collection
2. Data preprocessing and feature extraction
3. Normal behavioural profile learning
4. Anomaly detection using machine learning
5. Classification and explanation of suspicious activities
6. Performance evaluation and alert generation

3.2 Dataset Selection

The framework will be evaluated using publicly available network intrusion datasets.

Dataset	Description	Purpose
UNSW-NB15	Modern network traffic containing normal and attack activities	Primary evaluation
CICIDS2017	Network flows representing benign traffic and multiple attack types	Cross-dataset validation
NSL-KDD	Benchmark dataset for intrusion detection	Optional baseline comparison

Using multiple datasets will help assess whether the framework generalizes beyond a single traffic environment.

3.3 Data Preprocessing

The following preprocessing operations will be performed:

- Remove duplicate records and handle missing values.
- Encode categorical features such as protocol and service.
- Normalize numerical features using training data statistics.
- Identify and remove redundant or highly correlated features where appropriate.
- Separate training, validation, and testing data to prevent data leakage.
- Address class imbalance using suitable training-only techniques where required.

3.4 Behavioural Feature Extraction

The framework will extract features describing network communication behaviour.

Feature category	Example features
Traffic volume	Bytes sent, bytes received, packet count
Connection behaviour	Connection duration, connection frequency
Packet statistics	Average packet size, packet size variation
Protocol behaviour	TCP, UDP, ICMP distribution
Temporal behaviour	Inter-arrival time, activity rate
Communication patterns	Destination diversity, failed connection rate

These features will be used to construct a behavioural representation of each network flow or observation window.

3.5 Machine Learning Models

A. Isolation Forest

Isolation Forest will be used as the primary unsupervised anomaly detection model. It identifies observations that can be isolated more quickly than typical observations.

Advantages:

- Suitable for high-dimensional data.

- Does not require labelled attack examples during training.
- Relatively efficient for large datasets.

B. Autoencoder

An Autoencoder neural network will be trained to reconstruct normal network traffic. The reconstruction error will be used as an anomaly score:

A higher reconstruction error indicates that the observed traffic differs from the learned normal behaviour.

C. Random Forest

Random Forest will be used as a supervised classifier when labelled training data are available. It will classify traffic into normal and anomalous categories and, where supported by the dataset, identify attack classes.

3.6 Hybrid Detection Strategy

The proposed hybrid strategy combines the strengths of unsupervised and supervised learning:

- Isolation Forest identifies unusual traffic patterns.
- Autoencoder provides a complementary reconstruction-based anomaly score.
- Random Forest classifies suspicious observations using labelled examples.
- An adaptive threshold determines whether an observation should generate an alert.

3.7 Adaptive Thresholding

Network behaviour may change over time because of new applications, users, or workload patterns. A fixed threshold may therefore produce excessive false alarms.

The framework will investigate adaptive thresholding based on recent benign traffic statistics. Threshold updates will be restricted to validated traffic to reduce the risk of malicious data contaminating the normal behavioural profile.

3.8 Explainability

To improve interpretability, the system will report the features contributing most strongly to an anomaly score or classification.

For supervised predictions, feature importance or SHAP-based explanations may be used. For unsupervised models, the system will provide feature-level deviations from the learned normal profile.

Each alert may include:

- Anomaly score and threshold.
- Relevant traffic features.
- Predicted category, when available.
- Explanation of the principal behavioural deviations.

4. EXPERIMENTAL DESIGN

4.1 Experimental Setup

The models will be implemented using Python and machine learning libraries such as Scikit-learn and TensorFlow or PyTorch. Experiments will be conducted on a system with sufficient memory and processing capacity for the selected datasets.

The dataset will be divided into training, validation, and testing partitions. Where possible, time-aware or scenario-aware splitting will be used to reduce leakage and provide a more realistic assessment of generalization.

4.2 Baseline Models

The proposed framework will be compared against:

- Isolation Forest
- Autoencoder
- Random Forest
- One-Class SVM

The comparison will assess both individual models and the proposed hybrid strategy.

4.3 Evaluation Metrics

Metric	Purpose
Accuracy	Overall proportion of correctly classified observations
Precision	Proportion of detected anomalies that are actual anomalies
Recall	Proportion of actual anomalies successfully detected
F1-score	Balance between precision and recall
False Positive Rate	Proportion of normal traffic incorrectly flagged
ROC-AUC	Ability to distinguish normal and anomalous traffic
Detection latency	Time required to process traffic and generate an alert

Because network datasets are often imbalanced, precision, recall, F1-score, and false positive rate will be emphasized over accuracy alone.

5. EXPECTED RESULTS & CONTRIBUTIONS

The research is expected to produce:

1. A behaviour-based network anomaly detection framework combining unsupervised and supervised machine learning.

2. An evaluation of complementary anomaly detection models on public benchmark datasets.
3. An analysis of adaptive thresholding for reducing false alarms.
4. An interpretable alert mechanism that provides useful information about anomalous traffic.
5. A reproducible experimental pipeline that can support further research in network security.

These are expected contributions and hypotheses, not experimentally verified findings. Actual performance values will be reported after implementation and testing.

6. DISCUSSIONS

The proposed framework is intended to improve detection of suspicious network activities that may not match known attack signatures. Unsupervised learning can reduce dependence on labelled attack examples, while supervised classification can improve categorization when reliable labels are available.

However, the framework may face challenges related to class imbalance, concept drift, encrypted traffic, computational overhead, and false positives. Benchmark datasets may also fail to represent the full diversity of real-world network environments.

The study will therefore evaluate generalization across datasets and examine the trade-off between detection performance and computational cost.

7. CONCLUSION

This paper proposes a behaviour-based machine learning framework for detecting anomalous network activities. By combining behavioural feature extraction, Isolation Forest, Autoencoder, Random Forest, adaptive thresholding, and interpretable alerts, the framework aims to address limitations of conventional signature-based intrusion detection systems.

The proposed research will evaluate the framework using established network intrusion datasets and standard performance metrics. The findings are expected to contribute to the development of more adaptive, interpretable, and effective network anomaly detection systems.

REFERENCES

[1] M. A. A. K. A. et al., “A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies,” *[Journal article]*, 2021. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC8145138/

[2] “Flow-Level Statistical Fingerprinting for Unsupervised Network Intrusion Detection,” *Lusófona University Research Repository*. [Online]. Available: https://research.ulusofona.pt/en/publications/flow-level-statistical-fingerprinting-for-unsupervised-network-in/

[3] S. Choi, S. Kim, and J. Ryu, “A Survey of Deep Learning-Based Network Anomaly Detection: Benchmarking on NSL-KDD, UNSW-NB15, and CICIDS2017,” *IEIE Transactions on Smart Processing and Computing*, vol. 15, no. 3, pp. 410–425, 2026, doi: 10.5573/IEIESPC.2026.15.3.410.

[4] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015.

[5] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “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, pp. 108–116.