Machine Learning Based Network Traffic Forensics for Cyber Crime Investigation

Dr. Avinash Kumar[1], *Bhawna Anand[2], Akanchha Rani[3], Shashank Pandey[4]

[1]Associate Professor, Department of Computer Science and Engineering, Sarala Birla University, Ranchi, India

[2,3,4]Department of Computer Science and Engineering, Sarala Birla University, Ranchi, India

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2026.110400063

Received: 11 April 2026; Accepted: 16 April 2026; Published: 04 May 2026

ABSTRACT

The growing reliance on internet-based technologies, cloud infrastructures, and interconnected digital systems has resulted in a significant rise in the incidents of cyber crimes and sophistication of the attack. Many modern cyber threats such as distributed denial-of-service (DDoS) attacks, dissemination of malware, and unauthorized access, as well as the large-scale data breaches, take place through network communication channels. These activities create a large volumes of network traffic that can be used as important digital evidence during cybercrime investigations. Network traffic forensics concentrates on analyzing such traffic to gain understanding of the attack behavior and help reconstruct security incidents so as to support the analysis of investigative nature. However, traditional forensic methods based on manual inspection or predefined rules are often not able to handle the volume and complexity of traffic generated on modern high speed networks.

Recent developments in machine learning (ML) have provided automated methods that are capable of detecting the hidden pattern and anomalies within massive amounts of network traffic data. This paper gives an organized review of machine learning-based approaches for network traffic forensic analysis with special focus on researches based on the UNSW-NB15 benchmark dataset. The paper deals with commonly used supervised learning algorithms, i.e. Decision Tree (DT), Random Forest (RF), and Support Vector Machine (SVM), and analyses how these methods are used in traffic classification and forensic interpretation. In addition, commonly used evaluation metrics including accuracy, precision, recall, and F1-score are discussed to understand the evaluation of model performance in different studies.

Through the analysis of existing research, several limitations are identified, such as insufficient consideration of the interpretability of models, too heavy reliance on accuracy as a fundamental measurement of interest, and the lack of standardization of analytical frameworks for forensic purposes. Addressing these limitations, this paper focuses on the need for balanced evaluation practices and interpretability in machine learning models in order to achieve reliable cybercrime investigations. The presented insights in this review to help support future research in order to develop more effective machine learning-driven network traffic forensics solutions using the UNSW-NB15 dataset. The experimental setup adheres to the tradition of preprocessing and evaluation steps applying the UNSW-NB15 dataset to guarantee the reproducibility and consistency with the current literature.

Keywords: Network Forensics, Machine Learning, Cyber Crime Investigation, UNSW-NB15 Dataset, Intrusion Detection System

Abbreviations: DT - Decision Tree, RF - Random Forest, SVM - Support Vector Machine, ML - Machine Learning, IDS - Intrusion Detection System, IPS - Intrusion Prevention System, DoS - Denial of Service, DDoS - Distributed Denial of Service, IoT - Internet of Things, CNN - Convolutional Neural Network, LSTM - Long Short-Term Memory, TPR - True Positive Rate, FPR - False Positive Rate, F1 - F1-Score

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

INTRODUCTION

Advancements in information and communication technologies have caused a dramatic transformation on how the exchange of digital communication and data between individuals, enterprises and government systems takes place. The adoption of cloud computing platform, mobile technologies, Internet of Things (IoT) devices and high-speed networking infrastructure has led to unprecedented growth in network traffic. While these technologies offer many benefits in terms of connectivity and operational efficiency, they also create new security risks and underpin new cybercriminal acts. As a result, cyber threats such as unauthorized system access, the distribution of malware, phishing campaigns, ransomware attacks, data breaches and distributed denial-of-service (DDoS) attacks have become increasingly common and sophisticated.

Most cyber attacks of today tend to make extensive use of network communication during various phases of an attack lifecycle, such as reconnaissance, exploitation, payload transmissions, and data exfiltration . Consequently, the network traffic produced during the conduct of such activities tends to include traces of these activities that may be entered into as digital evidence in cybercrime investigations. Network forensics is therefore concerned with the capture, preservation and the analysis of network traffic in order to reconstruct the events of an attack and identify malicious activities within the digital environment . Unlike traditional digital forensics which is focused on static artifacts like storage medium or system logs, network forensics comes in contact with dynamic or high volume stream of network traffic analysis that needs to be analyzed quickly and efficiently.

Conventional approaches to network forensic investigation are normally based on the analysis, manual procedure, of packet captures, firewall logs, or monitoring software such as Wireshark and tcpdump. Although these tools are useful to inspect the activity on the network, manual investigation becomes increasingly difficult when dealing with large-scale and high-speed network environments. The sheer volume of traffic generated in association with time constraints and dependency on humans is one of the factors that limit the practicality of purely manual forensic techniques. In addition, the attackers often use encryption and obfuscation techniques that make the inspection of traffic by the traditional rule-based methods more difficult .

To tackle those difficulties, automation security mechanisms such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which aim to identify malicious activities, were introduced in network environments. However, many traditional IDS solutions use signature-based detection mechanisms that can only detect known attack patterns by previous. Such systems tend to have problems detecting emerging threats or zero day attacks that do not correspond to existing signatures. These limitations have favoured the use of machine learning techniques which are capable of learning patterns directly from data and detecting in previously unseen attack behaviours .

Supervised Machine learning algorithms such as Decision Tree, Random Forest and SVM have been widely applied in network traffic classification and intrusion detection problems. These techniques have proven to show promising performance in the detection of malicious traffic patterns in large datasets. Nevertheless, a large part of the existing research mainly focuses on real-time intrusion detection and does not contribute to post-incident forensic investigations. For forensic applications, further considerations such as interpretability, reliability and reproducibility of the results are crucial in order to ensure that the results of the analytics can support investigative and legal processes.

Another crucial element of network traffic analysis that relies on machine learning models is access to appropriate benchmark datasets. Earlier datasets like KDD-99 and NSL-KDD have been widely exploited in the field of intrusion detection, however, they are outdated with attack patterns and unrealistic traffic distributions that are not an accurate representation of modern network environments. To overcome these limitations, the UNSW-NB15 dataset was developed with realistic network traffic and a wide diverse set of modern attack scenarios. Because of these features, UNSW-NB15 has been one of the most popular datasets in recent network security and forensic research.

Several papers based on the use of the UNSW-NB15 dataset report the good and balanced classification performance of ensemble-based learning techniques, especially Random Forest models . Support Vector Machine models might produce good level of detection sensitivity but can also cause a greater number of false

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

positive detections, which could have a negative impact on the reliability of forensic models. Therefore, when analyzing network traffic in forensic settings, the evaluation of machine learning models by several metrics such as precision, recall and F1-score needs to be conducted.

Motivated by these observations, in this study a review based analysis of machine learning techniques for network traffic forensic investigation is presented, which is focused on the research made using the UNSW-NB15 dataset. The aim of this work is to identify important and prominent methodological trends and also to identify the limitations in the current research practices and to gain insights that can be used to inform future researches for machine learning driven network traffic forensics analysis.

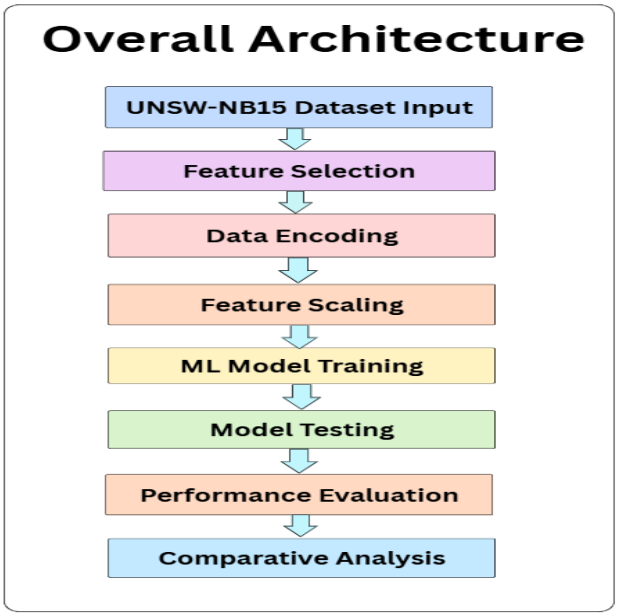

Figure 1. Overall Architecture

BACKGROUND AND MOTIVATION

The explosion of digital connectivity using cloud computing services, mobile communication technologies, Internet of Things (IoT) and high-speed networking infrastructure has dramatically changed the modern computing environment. These advancements in technology make it possible to exchange information efficiently, while digital resources can be made more accessible as well. However, they also create new security loopholes which are exploitable by malicious individuals. As a consequence, the rise of cyber attacks such as distributed denial-of-service (DDoS), ransomware campaigns, malware propagation, unauthorized access, phishing and data exfiltration is becoming more and more prevalent in today's networks.

Many cyber attacks use network communication channels to facilitate the various stages of malicious activity such as reconnaissance, command-and-control communications, payload delivery, and extraction of sensitive information. Due to this dependency in network traffic created during these operations can give valuable evidence about getting to know attack patters and reconstruct security incidents. Network forensics is, therefore, an important discipline within the field of digital forensics focusing on the collection, preservation, and examination of network traffic in order to understand how cyber attacks occur, and how they propagate through the network environments.

Unlike traditional digital forensic investigations where the main source of information is static data (storage devices, memory images, etc.), in network forensic analysis, the data sources are continuous streams, i.e., those generated in real time through network drives. Investigators are typically implied to analyze packet captures, network flow records, and protocol traces for abnormal behaviors, identify the origin of attacks; and establish timelines of occurrences of malicious events which may subsequently be used in the course of some investigation or legal proceedings.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Traditional methods for network traffic analysis are frequently based on manual inspection methods using various tools such as Wireshark tool, tcpdump tool, and rule-based intrusion detection systems (IDS). While such tools are valuable for analyzing individual traffic occurrences, they prove less useful in large-scale environments, where the network traffic volumes are extremely high. The growing adoption of encryption technologies and sophisticated evasion strategies, employed by the attackers, adds further complexities to the manual analysis and reduces the effectiveness of traditional forensics methods.

In response to these challenges, automated methods for detecting anomalies in network traffic were developed, including Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) which can monitor network traffic and detect suspicious activity. However, many of these systems rely on signature-based detection methods which are only able to detect attacks that match previously known attack patterns. As a result, such systems are frequently not able to identify emerging behaviors as well as unattended behaviors of attacks.

Machine learning methods have become potential solutions to overcome these limitations. By learning patterns in large amounts of data, machine learning models are able to automatically identify complex relationships in network traffic and detect anomalous behavior that might indicate cyber attacks. Algorithms like Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM) and k-Nearest Neighbors (k-NN) have been very well studied for network intrusion detection and classification of network traffic. Among the listed approaches, ensemble learning approaches, and more specifically Random forest approach, has shown strong performance among the various categories of attacks, thanks to its robustness and its ability to work with noisy data or high dimension data.

Despite such developments, much of the research that has already been conducted is more focused on detecting real-time intrusions than it is on investigating a crime after it has occurred. Intrusion detection focuses instead on identifying and reacting (as fast as possible) to active attacks, while forensic analysis must consist of a reliable and reproducible generation of evidences, explainable decision processes and outcomes that can be used in the course of an investigation. These additional requirements call for machine learning models that are not only highly accurate in detection, but also interpretable by producing outputs that can be used for forensic analysis.

The use of the right benchmark datasets is also crucial in testing machine learning models for network security research. Early datasets like KDD Cup 1999 and NSL-KDD have been popular; however, the datasets are already outdated because of unrealistic traffic patterns and outdated attack scenarios. In order to overcome such limitations, the UNSW-NB15 dataset was proposed by Moustafa and Slay, which offers realistic network traffic with various modern attack categories generated using a hybrid testbed environment.

Due to its realistic structure and various attack representation, the UNSW-NB15 data set has been extensively used as benchmark data sets for the evaluation of machine learning-based network intrusion detection and forensic analysis systems. Its availability enables researchers to carry out consistent performances from one machine learning model to another and, more importantly, being able to perform research to see how different algorithms seem to fare at detecting modern cyber threats.

The motivation of such a research is thus threefold :

1. to systematically explore the machine learning based works making use of the UNSW-NB15 dataset, and
2. to analyze the common methodologies and evaluation practices in use, and
3. to determine research gap based on the view of network forensic investigation.

By specifically discussing research efforts based on UNSW-NB15, in this paper, we aim to give a coherent picture of current research efforts and bring attention to future efforts for the field of machine learning-based network traffic forensic analysis.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

LITERATURE REVIEW

This section reviews the existing study related to machine learning-based network traffic analysis with a particular emphasis on research that utilises the UNSW-NB15 data set. The literature is categorized into various themes, such as benchmark datasets used in network security researches, classical machine learning techniques, feature selection and hybrid models, ensemble learning methodologies, deep learning approaches, and evaluation practices that are related to forensic investigations.

Network Traffic Data and Benchmarking

Early studies on machine learning-based intrusion detection usually involved the use of benchmark datasets such as KDD Cup 1999 dataset and an improved version of it, NSL-KDD. Although these datasets played an important role in the development of intrusion detection techniques, they are associated with several limitations. Researchers have found problems including redundant entries, unrealistic network traffic distributions and outdated categories of attacks that no longer reflect modern cyber threats.

Researchers have not yet learned to generalize models effectively to real-world network environments Due to these shortcomings, models trained on these datasets often do not generalize well to real-world network environments. To overcome these challenges, Moustafa and Slay presented the UNSW-NB15 dataset which was developed using a hybrid testbed environment that captures both real life network traffic as well as the simulated attack scenarios. This data set contains various modern types of attacks such as denial of service (DoS), exploits, fuzzer, reconnaissance, worms, and shellcode attack which suit to test the modern intrusion detection and forensic analysis system. Subsequent research has verified that UNSW-NB15 serves as a realistic and reliable criterion for network security research based on machine learning.

Supervised Machine Learning Convention and Methods in Classical Approach

Numerous research works have used traditional supervised machine learning algorithms to network traffic classification tasks using the UNSW-NB15 dataset. Decision Tree classifiers are often applied due to their simplicity and interpretability. The rule-based structure that is created by Decision Trees makes it possible for the investigator to understand how the classification decisions are being made, which can be helpful in interpreting results in forensic investigations. However, single models of Decision Trees face a possible overfitting problem when applied to complex high dimensional network data sets.

Support Vector Machine (SVM) is another popular algorithm in network intrusion detection research literature owing to its sound theoretical background and its ability to work well in high-dimensional feature space. SVM models can be highly accurate in detection, especially if an appropriate use of the kernel functions and parameters is made. However, training the SVM models for large sized datasets can lead to computational challenges and inappropriate parameter selection can hinder the classification performance.

Random Forest is another ensemble learning algorithm that makes use of several decision trees that have been greatly shown to perform well on network traffic classification tasks. Through the combination of the predictions of several trees, Random Forest models mitigate the overfitting problem and provide better generalization for various attack classes. These are the characteristics that make Random Forest a common baseline model of many UNSW-NB15-based studies.

Feature Selection and Hybrid Models

Feature selection plays an important role in improving the machine learning performance for network traffic analysis. Network datasets frequently have a great number of features and several of them may be redundant or irrelevant to the classification task. The choice of the features that are most informative can enhance the accuracy of classification while diminishing the amount of computation.

Several papers have used optimization-based feature selection methods to determine the discriminative attributes for network traffic dataset. For example, Gharaee et al. applied feature selection using genetic algorithm in

conjunction with Support Vector Machine classifiers and achieved higher detection performance results on the UNSW-NB15 dataset.

Hybrid methods of absorbing latest feature selection methods and ensemble learning algorithms have also been explored. Aljawarneh et al. showed that combining feature selection methods and ensemble classifiers can be used to increase detection performance by eliminating features that are irrelevant to the problem and increasing model flexibility. However, the use of hybrid approaches may add complexity to the models and decrease their interpretability, which can be a limitation when these techniques are applied in the context of forensic investigations.

Ensemble and Survey Based Results

Survey studies that investigate the use of machine learning techniques in network security have consistently reported that ensemble learning techniques tend to be highly effective in comparison to individual classifiers in complex network environments. Ensemble techniques use a combination of the predictions from different models, however, the result is to have a more stable and reliable classification performance.

Ferrag et al. presented the analysis of security mechanisms in large-scale and IoT-enabled networks and presented the effectiveness of ensemble learning techniques used to detect cyber attacks with varying network conditions. Their results warrant the adoption of models built from ensembles to handle analysis of complex network traffic datasets such as UNSW-NB15.

Approaches Based on Deep Learning

Recent attempts have been made in the context of network traffic analysis by using deep learning architectures. Models like Convolutional Neural Networks (CNN) and Long Short Term Memory (LSTM) networks have the power to extract spatial and temporal patterns from the network traffic data. These types of models have shown promising performance in the detection of complex attack behaviors.

Despite their advantages, deep learning models tend to be computationally expensive and require large training datasets. Additionally, the decision processes of deep learning models can often be difficult to interpret, which might restrict their use in forensic investigations where the models' explanations are important.

Evaluation Measures and Forensic Perspective

Another, key issue highlighted in literature is the use of evaluation metrics to rate the model performance. Many researches are written using accuracy as the main performance index; however, using accuracy alone may be misleading in dealing with those datasets with dataset imbalance, such as network traffic data.

Researchers stress the need for further evaluation factors such as precision, recall, F1-score, and false alarm rate. These metrics give a more comprehensive understanding on model performance, especially to examine the reliability of detected attacks. High recall values without equivalent precision may produce more false positives than are appropriate to the results of forensic investigations.

Identified Research Gaps

Based on the reviewed literature, we can identify a number of research gaps:

1. **Limited special attention to forensic analysis:** Many of the studies focus on intrusion detection performance as opposed to post incident forensic investigation.

2. **Lack of interpretability:** Some high-performance models have results that cannot be interpreted easily, limits them in their usefulness whether in an investigative or legal context**.**

3. **Imbalanced evaluation practices:** Several studies emphasize on accuracy while giving limited attention to the evaluations on the metrics on false positives and forensic reliability.

4. **Incomplete analytical pipeline:** limited research reports complete end-to-end forensic workflows, which interface results of machine learning analysis, preservation of evidence, and procedures of research.

These gaps indicate that a need exists for research focusing on interpretability, balanced evaluations, as well as forensic usability to support machine learning-based network traffic analysis.

Although the current literature illustrates excellent detection performance, little focus has been given on the aspects of reproducibility and forensic interpretability which the presented study will tackle.

METHODOLOGY

This section explains the methodology followed in this research work which is review oriented in the field of machine learning based Network Traffic Forensics using UNSW-NB15 dataset. Since this work is listed as a review work with experimental validation, methodology is an amalgamation of practices that were widely adopted in previous studies and put them in the same context as the experimental setup of the comparison work. The methodology consists of choice of dataset, feature selection and preprocessing strategies, types of machine learning models that have been used in literature along with evaluation metrics in the performance evaluation.

Dataset Description

The UNSW-NB15 dataset is used as the main benchmark dataset in this study, as this is the most commonly used modern dataset for network intrusion detection and forensic research. The dataset was created with a hybrid testbed environment, where real normal network traffic and synthetically generated attack traffic is combined, so that the generated cyber attack scenarios of the present day can be represented realistically.

UNSW-NB15 is a set of network flow records which have been extracted from the raw packet captures and contains both normal and malicious traffic instances. The dataset spans across several types of attacks including Denial of Service (DoS), Exploits, Fuzzers, Reconnaissance, Worms, Shellcode and Generic attacks making it apt for evaluating machine learning techniques in intrusion detection analysis as well as the forensic analysis.

One of the main features of the UNSW-NB15, which has been repeatedly highlighted in the literature, is the presence of pre-defined training and testing subsets. The total number of records in the training dataset is 175,341 and the total records in the testing dataset is 82,332. Many previous works have these predefined splits in order to prevent bias and ensure reproducibility of results. Following this standard practice, the current study also uses the full training and testing datasets without sampling so that full evaluation can be performed as per real forensic scenarios.

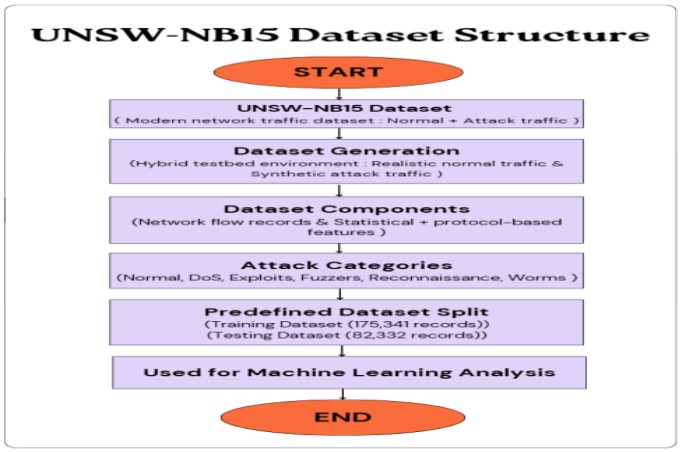

Figure 2. UNSW-NB15 Dataset Structure

Figure 2 depicts the structural composition of the UNSW-NB15 dataset; the generation process of the dataset, composition of features, categories of attacks, and predefined partitioning of the dataset as usually cited by the previous research.

The data training (175,341 records) and the testing (82,332 records) splits were used without modification to guarantee the reproducibility of the training and testing.

Feature Selection and Preprocessing

Feature selection and preprocessing are very important stages in the process of machine learning-based network traffic analysis, especially because of the high dimensionality and heterogeneity of network flow data. In the literature, a subset of relevant features is selected to improve the performance of classification, reduce the computational complexity, and improve the interpretability of the model.

In this paper a subset of often used network flow features reported across UNSW-NB15-based research is considered. These include connection duration, protocol type, number of packets from source and destination and the total bytes exchanged between communicating entities. Such features are often chosen in the previous work because they are very relevant to the forensic analysis, since they reflect the behavior of traffic, communication intensity, and protocol usage patterns related to cyber attacks.

Categorical features, for instance protocol type, are converted into numerical feature values by label encoding, a popular method in the reviewed literature. Numerical features are normalized with the help of standard scale, so that the features contribute equally while training the model. Feature normalization is especially useful in margin-based classifiers like Support Vector Machine, because it enhances the convergence and stability.

These preprocessing specifically represent best practices that have been discovered in existing studies and ensure that training and testing data sets are consistent which is important for forensics in reliability and reproducibility.

The chosen group of features consists of dur (duration), proto (protocol type), spkts (source packets), dpkts (destination packets), sbytes (source bytes), and dbytes (destination bytes), popular attributes in the analysis of the network traffic behavior.

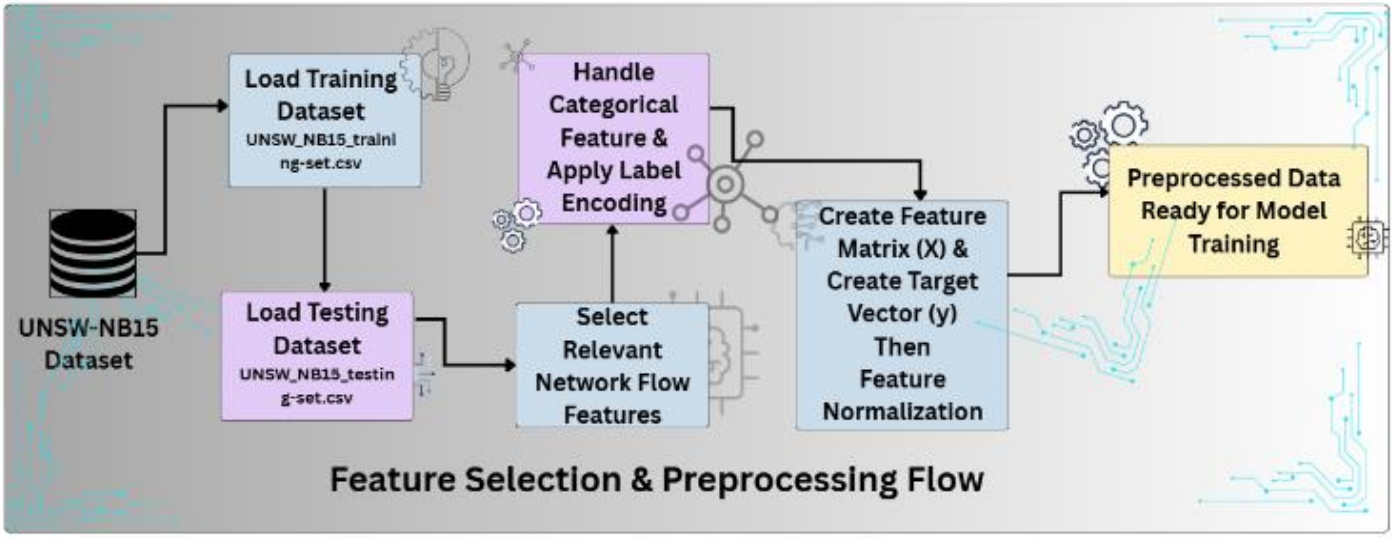

Figure 3. Feature Selection & Preprocessing Flow

Figure 3 illustrates the typical preprocessing pipeline that is played out in UNSW-NB15-based studies including data set loading, categorical encoding, feature selectivity, normalization, generation of the feature matrix. This workflow represents the prevailing preprocessing strategy that is used to help ready forensic-ready data for supervised learning models.

Encoding

Label Encoding was used as the means of encoding nominal feature proto. It was applied to the categorical feature "proto" using a combined dataset of training and testing data to ensure consistency across both sets.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Scaling

StandardScaler was used to normalize numerical features to make each feature equally contribute to the model and enhance its convergence.

Machine Learning Models

Based on the survey of the existing literature, in order to tackle this question, the aim of the present study is to focus on three supervised machine learning models widely applied to the UNSW-NB15 data set offered and to provide competive performance.

Decision Tree (DT)

Decision Tree classifiers are popularly followed in network traffic analysis because of their simplicity, low computational cost, and also high interpretability. Decision Trees are used to create rules-based decision paths used to explain how classification decisions are made in a comprehensible way and this is especially useful in forensic investigations where explainability and traceability of evidence are crucial. However, previous works also indicate that standalone Decision Trees are likely to overfit when decision trees are applied to high-dimensional network traffic data.

Random Forest (RF)

Random Forest is also an ensemble learning algorithm that builds several decision trees equivalents based on random sets of data and features. The last prediction will be derived by majority of the individual trees. Numerous studies report that Random Forest performs better than single classifiers consistently on UNSW-NB15 because of its robustness, resistance to overfitting and ability to deal with noisy data. It is these properties that make Random Forest especially suitable for network traffic forensic analysis.

Support Vector Machine (Linear SVM)

Support Vector machine is a supervised learning algorithm which finds an optimal separating hyperplane between classes. In the case of UNSW-NB15-based studies, SVM is often employed because it has a solid theoretical basis and excellent ability to work in high dimensions. Linear SVM variants are frequently used in large-scale data sets in order to minimize the computation complexity, even though previous researches have reported sensitivity to parameter choice and the possibility of false positiveness.

The Scikit-learn was used to implement the models. Decision tree was set up with random state=42, random forest set up with 100 estimators and random state=42 and linear SVM (LinearSVC) was set up with max-iter=5000. Default parameters were used for other settings.

Figure 4 illustrates the shelves of the standard supervised learning pipeline for UNSW-NB15 studies containing the processes of data splitting, model training, prediction and evaluation of performances. This is the typical architecture that lies between the most commonly stated architecture of experiments to be performed in intrusion detection and forensic-oriented research.

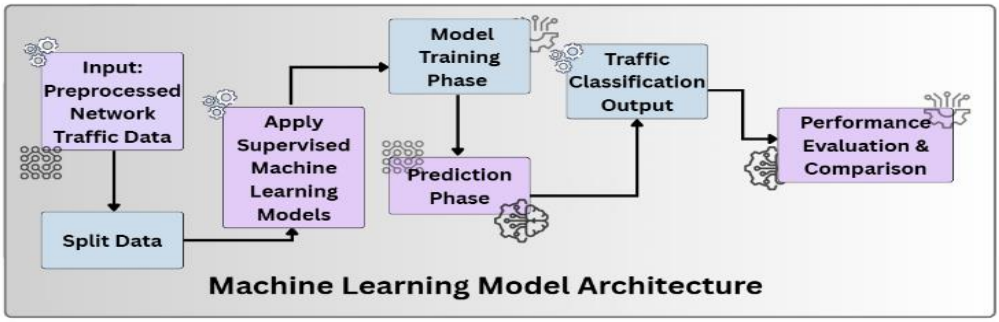

Figure 4. Model Architecture of Machine Learning Models

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Evaluation Metrics

In line with the previous work, there are several evaluation metrics that are applied to measure the model performance. Accuracy gives an over-all measure of correct classification. Precision expresses the reliability of detected malicious traffic by detecting the ratio of the correctly identified malicious traffic among all predicted positives. Recall assesses the capacity of a model to capture actual attacks which is so critical in forensic investigation in order not to miss any malicious events. The F1-score being a harmonic mean of precision and recall provides a balanced assessment of the evaluation results especially in case of imbalanced data sets such as UNSW-NB15.

The reviewed literature refers to the fact that it is misleading to base decisions on a simple assessment of accuracy only in forensic contexts where the consequences of a false positive and a false negative are highly significant from an investigative perspective. Therefore, the use of multiple metrics brings the methodology closer to the requirements of forensic reliability that is emphasized in existing studies.

Performance metrics (accuracy, precision, recall, F1-score) were calculated with the help of regular Scikit-learn evaluation functions.

EXPERIMENTAL RESULTS

This section showcases the experimental results obtained from the application of the commonly used supervised machine learning models to the UNSW-NB15 dataset. The defined training subset is used to train the models and the standard testing subset is used to test the models, as these evaluation practices are widely reported for existing UNSW-NB15-based studies.

All the experiments were conducted in Python environment with the help of Pandas, NumPy and Scikit-learn libraries.

The goal of this experimental analysis is not to present a new algorithm, but to validate trends that are consistently seen in the literature and to contextualize them under the viewpoint of network forensic, in terms of reliability, interpretability and balanced performance metrics.

Table 1. Model Performance on UNSW-NB15

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	90.24%	96.82%	88.56%	92.51%
Random Forest	90.83%	97.36%	88.94%	92.96%
Linear SVM	76.83%	77.32%	93.33%	84.57%

The results show that Random Forest has the most balanced performance, and this performance is shown by the highest accuracy and F1-score. Decision Tree also showcases its competitive outcomes especially in the form of high precision and interpretability. Linear SVM has the best recall which means it is sensitive to attack traffic but has low precision which indicates it has a high false positive rate which decreases the reliability of the forensics application.

MODEL PERFORMANCE

	Model	Accuracy	Precision	Recall	F1-Score
0	Decision Tree	0.902379	0.968239	0.885622	0.925089
1	Random Forest	0.908327	0.973593	0.889434	0.929613
2	SVM	0.768280	0.773198	0.933317	0.845746

Figure 5. Model Performance

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

As you can see in Figure 5, there is the individual performance of the Decision tree, Random forest and Linear SVM models on the UNSW-NB15 dataset. The figure shows how the ensemble-based models were comparably strong at achieving balanced classification performance, as is consistent with previous studies.

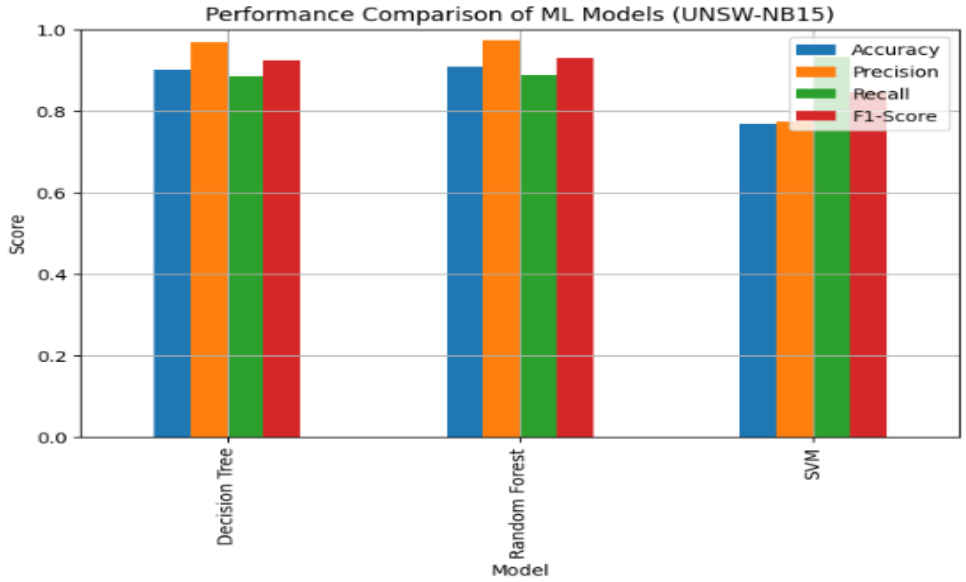

Figure 6. Performance Comparison

Figure 6 shows a comparative study of accuracy, precision, recall, and F1-score of the various models tested. This comparison highlights the trade-off between the sensitivity to detect and the false positive reduction which is crucial in network forensic investigations.

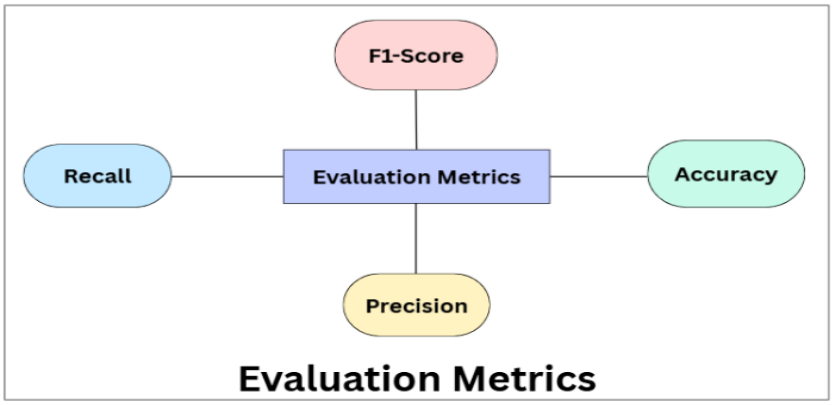

Figure 7. Model Evaluation Metrics

Figure 7 summarizes the evaluation metrics that are commonly used when conducting UNSW-NB15 prototypes-based research, which include accuracy, precision, recall and F1-score. These metrics overall give a complete measure of the level of forensic reliability especially in unbalanced network traffic datasets.

In a forensic context, these findings imply that Random Forest is more balanced in terms of detection and Decision Tree is more conducive to visualization and SVM is more conducive to detecting attacks. These outputs may help the investigators to determine any suspicious traffic pattern and revisit past cyber activity.

COMPARATIVE ANALYSIS WITH EXISTING STUDIES

Comparative analysis is necessary in review-type research in order to place findings of experiments into the larger context of research. Numerous research works have been conducted to assess machine learning methods on UNSW-NB15; however, direct numerical comparison is still difficult because of the differences in feature selection, preprocessing strategies and experimental setups.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Moustafa and Slay proposed the UNSW-NB15 for overcoming the limitations of old datasets such as KDD-99 and NSL-KDD with the focus on realistic traffic generation and contemporary attack scenarios. Subsequent researches approved its suitability for machine learning-based intrusion detection and forensic researches.

Gharaee et al. used genetic algorithm-based SVM classifiers to predict accurate detection results and also reported high accuracy using optimization-based hybrid algorithms. However, such approaches bring about extra computational complexity and reduced interpretability, which might be limiting the usage in forensic contexts.

Aljawarneh et al. proposed hybrid intrusion detection models based on feature selection and ensemble learning that have better detection performance on UNSW-NB15.While they work, these approaches are more focused on the accuracy of detection and less so on forensic analysis of incidents after they have occurred.

Ferrag et al. have already done an extensive survey on security mechanisms for large scale and IoT-enabled networks and reported in their paper that ensemble-based classifiers like Random Forest, are always better than the individual classifiers for diverse attack scenarios.

Ahmad et al. and Sarhan et al. separately showed that ensemble learning methods offer better robustness and generalization capabilities by applying them to UNSW-NB15. Such findings are in strong accordance with the obtained experimental trends for this study.

Unlike most of the surveyed works that focus on the real-time detection of intrusion, the current research considers these results under the perspective of network forensic, with a special focus on balanced metrics, interpretability, and as false-positive control in post-incident investigation and evidence analysis.

Table 2. Survey Based Comparison to related Research

Reference	**Dataset**	**ML Approach**	**Key Observation**
Moustafa & Slay (2015)	UNSW-NB15	LR, NB, EM	Introduced UNSW-NB15 dataset and demonstrated applicability of ML techniques
Gharaee et al. (2017)	UNSW-NB15	GA-optimized SVM	High detection performance achieved through genetic algorithm-based feature optimization
Aljawarneh et al. (2018)	UNSW-NB15	Hybrid ML	Improved detection accuracy using feature selection and hybrid modeling
Ferrag et al. (2020)	Survey (UNSW-NB15 discussed)	Ensemble & ML methods	Survey reports ensemble-based methods as robust across diverse attack scenarios
Ahmad et al. (2021)	UNSW-NB15	Decision Tree, RF, SVM	Highlighted interpretability and efficiency of supervised ML for IoT intrusion detection
Sarhan et al. (2022)	UNSW-NB15	Ensemble learning	Ensemble models outperform single classifiers in intrusion detection tasks
Proposed Work	UNSW-NB15	DT, RF, Linear SVM	Balanced performance with focus on forensic reliability and interpretability

DISCUSSION

The experimental and comparative results confirm the fact that ensemble-based machine learning models and in this case Random Forest provide the best guarantee in terms of network traffic forensic analysis performance. Their capacity of uniforming overfitting, noisy features and still remaining stable for various metrics makes them suitable for forensic applications.

Decision Tree models offer high interpretability to trace back the deduction process and support for the forensic conclusions. This characteristic is particularly useful in the legal and procedural fields where explainability is prescribed.

Linear SVM shows high recall percent which is good for ensuring that any malicious activities are not overlooked. However, its only relatively lower degree of accuracy points to a possible limitation to forensic workflows as too many false positives make the workload on investigators too high and make them less confident in automated tools.

Overall, this study serves to highlight the importance of accuracy, but that in itself is not enough for forensic applications. Balanced evaluation in terms of precision, recall, and F1-score are indispensable to guarantee detection's effectiveness as well as factual evidence's reliability.

CONCLUSION AND FUTURE WORK

This is a study performed based on a review of the machine learning methods for network traffic forensics which is using the UNSW-NB15 dataset. By combining and synthesizing experiment findings and the existing literature, results showed that classical supervised learning models are still highly effective to be used in forensic analysis if using balanced evaluation metrics.

Random Forest was the most reliable model thanks to its ability to do ensemble learning while Decision Trees were helpful in providing useful interpretability. The findings validate that machine learning can significantly improve the scalability and efficiency of the network forensic investigations.

Future research should focus on combining explainable AI techniques and hybrid forensic frameworks with real world traffic datasets to make forensics more reliable. Exploring and anomaly detection as well as semi-supervised learning may additionally improve the finding of unknown and zero day attacks strengthening the forensic readiness in dynamic threat environment.

Another finding that was emphasized in the study is the significance of reproducibility and interpretability when using machine learning to perform network forensic analysis.

Ethical Considerations

This study does not involve human or animal subjects. Therefore, ethical approval was not required.

Conflict Of Interest

The authors declare no conflict of interest.

Data Availability

The dataset used in this study (UNSW-NB15) is publicly available.

REFERENCES

1. S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Tech. Rep., Chalmers Univ., 2000.
2. Z. Ahmad et al., “Network intrusion detection using machine learning techniques,” Future Generation Computer Systems, vol. 117, pp. 20-30, 2021.
3. M. Ahmad et al., “Intrusion detection in IoT using supervised ML based on UNSW-NB15,” EURASIP J. Wireless Commun. Netw., 2021.
4. I. Aljawarneh, M. Aldwairi, and M. Yassein, “Anomaly-based intrusion detection system through feature selection,” J. Comput. Sci., vol. 25, pp. 152-160, 2018.
5. A. Behl and K. Behl, Cyberwar: The Next Threat to National Security. Oxford, U.K.: Oxford Univ. Press, 2017.
6. L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5-32, 2001.

7. J. Brownlee, Machine Learning Mastery with Python. Melbourne, Australia, 2018.
8. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153-1176, 2016.
9. M. Bhuyan, D. Bhattacharyya, and J. Kalita, "Network anomaly detection: Methods, systems and tools," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 303-336, 2014.
10. E. Casey, Digital Evidence and Computer Crime, 3rd ed. Burlington, MA, USA: Academic Press, 2011.
11. C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning, vol. 20, no. 3, pp. 273-297, 1995.
12. G. Creech and J. Hu, "A semantic approach to host-based intrusion detection," Proc. RAID, 2013.
13. M. A. Ferrag et al., "Security for 5G and IoT networks: A survey," IEEE Network, vol. 34, no. 6, pp. 144-152, 2020.
14. A. Gharaee and H. Hosseinvand, "A new feature selection IDS based on GA and SVM," Proc. ICEE, 2017.
15. H. Hindy et al., "A taxonomy of network threats and machine learning," IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2511-2545, 2020.
16. H. Hindy et al., "Machine learning based cyber threat detection," IEEE Commun. Surveys, 2020.
17. M. Hodo et al., "Threat analysis of IoT networks using artificial neural networks," IEEE Access, vol. 4, pp. 681-695, 2016.
18. S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for intrusion detection," Computers & Security, vol. 92, 2020.
19. S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems," IEEE Access, vol. 8, pp. 59351-59363, 2020.
20. G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Syst. Appl., vol. 41, no. 4, pp. 1690-1699, 2014.
21. N. Koroniotis et al., "Design of network forensic systems for cyber crime investigations," Computers & Security, vol. 80, pp. 129-147, 2019.
22. Y. Li, J. Xia, S. Zhang, and X. Yan, "Network intrusion detection based on improved random forest," Proc. ICMLC, 2019.
23. H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection," Applied Sciences, vol. 9, no. 20, 2019.
24. S. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," Advances in NIPS, 2017.
25. J. McHugh, "Testing intrusion detection systems: A critique of the DARPA IDS evaluations," ACM TISSEC, vol. 3, no. 4, pp. 262-294, 2000.
26. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," Proc. MilCIS, 2015.
27. T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," IEEE Commun. Surveys Tuts., vol. 10, no. 4, pp. 56-76, 2008.
28. A. Patcha and J. Park, "An overview of anomaly detection techniques," IEEE Commun. Surveys & Tutorials, vol. 9, no. 4, pp. 1-15, 2007.
29. M. Ring et al., "A survey of network-based intrusion detection datasets," Computers & Security, vol. 86, pp. 147-167, 2019.
30. M. Ring et al., "Flow-based benchmark data sets for intrusion detection," Proc. AIMS, pp. 361-378, 2019.
31. M. Ring et al., "Flow-based intrusion detection using machine learning," IEEE Access, vol. 7, pp. 179179–179193, 2019.
32. M. Ring et al., "Flow-based network traffic generation using realistic intrusion scenarios," IEEE Access, vol. 7, pp. 19112-19127, 2019.
33. Y. Sarhan et al., "Ensemble learning for network intrusion detection," Computers & Security, vol. 112, 2022.
34. Y. Sarhan et al., "Multiclass network intrusion detection using ensemble learning," Computers & Security, vol. 113, 2022.
35. K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST SP 800-94, 2007.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

36. J. Shone et al., “A deep learning approach to network intrusion detection,” IEEE Trans. Emerging Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.
37. M. Samek et al., “Explainable AI for forensic analysis,” arXiv, 2019.
38. M. Samek, W. Samek, and K.-R. Müller, “Explainable artificial intelligence,” arXiv:1708.08296, 2017.
39. R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” Proc. IEEE Symp. Security and Privacy, pp. 305-316, 2010.
40. M. Tavallaee et al., “A detailed analysis of the KDD CUP 99 data set,” Proc. IEEE CISDA, 2009.
41. A. Verma and V. Ranga, “Statistical analysis of UNSW-NB15 dataset,” Proc. ICCT, 2018.
42. W. Wang et al., “HAST-IDS: Learning hierarchical spatial-temporal features for intrusion detection,” IEEE Access, vol. 6, pp. 1792-1806, 2018.
43. Y. Xin et al., “Machine learning and deep learning methods for cybersecurity,” IEEE Access, vol. 6, pp. 35365-35381, 2018.
44. J. Zhang, M. Zulkernine, and A. Haque, “Random forest-based intrusion detection,” IEEE Trans. SMC-C, 2008.