IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

Network Intrusion Detection Using Machine Learning Techniques

Anubhav Rajeshram Kahar and Prof. Sandeep Kumar Vishwakarma
Student, Master of Computer Applications (MCA)
Head, Department of Information Technology
Chandrabhan Sharma College of Arts, Commerce and Science, Powai, Mumbai, Maharashtra, India
sandeepvcbs@gmail.com

Abstract: *The growth of computer networks and internet services has increased the risk of cyber threats and hacking attempts. Traditional systems that detect intrusions often struggle to identify changing attacks.*
This shows we need flexible security solutions.
This paper presents a machine learning approach for detecting network intrusions.
It aims to identify malicious activities in network traffic.
** Various machine learning techniques are analyzed for their effectiveness*
** The techniques are used to distinguish between abnormal network behavior.*
The proposed framework involves preparing data, selecting features, training models, evaluating performance using metrics like accuracy, precision, recall and F1-score.
Experimental results show that machine learning algorithms can detect types of network intrusions. They also reduce alarms.
The study highlights the potential of machine learning in improving cybersecurity defenses. It provides insights into the strengths and limitations of classification techniques. The findings suggest that machine learning-based intrusion detection systems can protect network infrastructures.
They can serve as a scalable solution against emerging cyber threats using machine learning. Machine learning is key, to enhancing cybersecurity defenses..

Keywords: Network Intrusion Detection System (NIDS), Machine Learning, Cybersecurity, Network Security, Intrusion Detection, Cyber Attacks

I. INTRODUCTION

The internet and computers are getting better fast and a lot of people are using them. This has made computer networks more complicated and bigger. These changes have helped people talk to each other and share information easily and they have also helped businesses.. They have also made networks more vulnerable to cyber attacks.
Cyber attacks like denial-of-service attacks, software getting on computers people getting into networks without permission fake emails and people getting sensitive information they should not have are big problems for organizations and individuals.
As cyber attacks get more complicated and happen often keeping networks safe has become a really big challenge.
Old ways of keeping networks safe like firewalls and systems that look for stuff based on what they already know work pretty well for threats they already know about but they often have trouble finding new threats that they have never seen before. These systems rely a lot on rules and lists of stuff which makes them not very good at dealing with new cyber attacks. So there is a need for systems that can find both threats they know about and threats they do not know about and do it fast.

DOI: 10.48175/IJARSCT-37174

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, June 2026 Impact Factor: 8.2

Machine Learning is a technology that is helping to make networks safer by letting systems look at what has happened on the network before and find patterns that are like bad activities. By using ways of looking at data and finding things that are not normal machine learning models can automatically find behavior that looks suspicious and make systems that find bad stuff more accurate. Algorithms like Decision Trees and Random Forests and Support Vector Machines and Naïve Bayes and Neural Networks are really good at finding cyber attacks. They do it with a lot of accuracy and they do not make many false alarms. Machine Learning is helping to make networks safer. It is very good, at finding cyber attacks. Cyber attacks are a problem and Machine Learning is helping to solve this problem.

This paper is about using machine learning techniques to detect network intrusions. It looks at how we collect data clean it up pick the features train a model and see how well it works to detect network intrusions. The main goal of this study is to see how well different machine learning techniques work to find network activities and to talk about what is good and bad about using them to keep our networks safe, from cyber attacks. Network intrusion detection is a big part of this study and machine learning techniques are used to improve network intrusion detection.

II. LITERATURE REVIEW

Network Intrusion Detection Systems have become a part of modern cybersecurity because of all the cyber attacks on network infrastructures. People who do research have tried to use Machine Learning techniques to make intrusion detection systems at finding problems and adapting to new things.

At first people used methods that looked for known attack patterns. These methods were good at finding attacks that were already known. They had trouble finding new or changing threats. To make this better people started using methods that looked for things that were not normal in the network. These methods use Machine Learning algorithms to find things that're different from how the network usually works.

A lot of studies have shown that supervised Machine Learning algorithms are good at finding intrusions. Decision Trees are often used because they are simple and easy to understand and they can handle a lot of data. Random Forest is a way of combining Decision Trees and it has been shown to be more accurate and reliable. Support Vector Machines are also good at classifying network traffic by finding the way to separate normal and bad traffic.

Naïve Bayes classifiers have also been tried because they are fast and can handle a lot of data. Even though they make some assumptions about the data they have worked well in some cases. K-Nearest Neighbors is a way of classifying things based on how they are to each other and it has been used to find suspicious network behavior.

As computers have gotten better Deep Learning techniques have become more popular in intrusion detection research. Artificial Neural Networks, Convolutional Neural Networks and Recurrent Neural Networks are good at learning patterns from network traffic data. These models are especially good at finding attacks and do not need as much manual work to set up.

There are some datasets that're publicly available for testing intrusion detection systems. These datasets, like KDD Cup 1999 NSL-KDD, UNSW-NB15 and CICIDS are used to compare algorithms. Researchers have found that using models or Deep Learning models can find more intrusions and have fewer false alarms than traditional methods. However there are still some challenges, like datasets that're not balanced, computers that are not powerful enough models that are hard to understand and deploying models, in real-time. Network Intrusion Detection Systems and Machine Learning techniques are still being researched to make them better.

III. RESEARCH METHODOLOGY

This study uses a machine learning approach to find network intrusions by looking at network traffic data and deciding if the activities are normal or bad. The way we do this has steps, including collecting data getting the data ready picking the right features training the model testing it and seeing how well it works.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

3.1 Data Collection

The first thing we do is get a dataset that has records of normal and attack traffic on a network. We can use datasets like NSL-KDD, UNSW-NB15 or CICIDS that're available to the public. These datasets have lots of information about network traffic and the different types of attacks, which helps us make and test machine learning models.

3.2 Data Preprocessing

The data we get from network traffic often has problems like missing information, duplicate records and things that are not relevant. So we do some preprocessing to make the data better and help our model work well. This step includes:

- Removing duplicate and inconsistent records.
- Dealing with missing values.
- Changing attributes into numbers.
- Normalizing the features.
- Cleaning the data to get rid of noise and irrelevant information.

All these steps make sure our dataset is good enough for machine learning.

3.3 Feature Selection

We pick the features that're most important for finding network intrusions. By getting rid of features we do not need we can make our model work faster. Be more accurate. We use techniques and look at which features are most important to choose the right network traffic characteristics.

3.4 Machine Learning Model Development

After we preprocess the data and pick the features we train machine learning algorithms using our dataset. We can use algorithms like:

- Decision Tree
- Random Forest
- Support Vector Machine
- Naïve Bayes
- K-Nearest Neighbours

Each algorithm looks at patterns in the network traffic data we have. Makes a model that can tell normal activities from bad ones.

3.5 Model Training and Testing

We divide our dataset into two parts: one for training and one for testing. We use the training part to build our machine learning models and the testing part to see how well they work on data they have not seen before. This helps us know if our model can really find intrusions, in the world. Network intrusions are what we are trying to detect with machine learning. Machine learning models are what we use to find network intrusions.

3.6 Performance Evaluation

We look at how the intrusion detection models work by using standard measures, including:

- Accuracy
- Precision
- Recall
- F1-Score
- False Positive Rate
- Detection Rate

These measures give us a picture of how well the model can tell things apart and find network attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

3.7 Comparative Analysis

The last step is to compare how different machine learning algorithms work. We compare them based on how they detect things how efficiently they work how often they give false alarms and how reliable they are overall. We pick the algorithm that works best as the way to detect network intrusions.

The method we propose gives us a step by step way to develop and evaluate machine learning-based systems that can detect cyber threats and make networks more secure. We use intrusion detection models to find cyber threats and make network security better. The intrusion detection models are important, for network security.

IV. MACHINE LEARNING ALGORITHMS USED

Machine Learning is really important for finding people who try to get into our networks. It looks at how the network's being used and figures out if it is being used in a good way or a bad way. We looked at some Machine Learning algorithms that are good at telling the difference between good and bad uses.

4.1 Decision Tree

The Decision Tree is a type of Machine Learning that sorts data into a tree shape based on what the data says. It makes decisions based on what it knows about the data. Puts it into groups. The Decision Tree is easy to understand. Does not need a lot of computer power. That is why it is often used to find people who try to get into our networks. It can look at a lot of data. Find patterns that might mean someone is trying to get in.

Advantages:

- The Decision Tree is easy to understand.
- It can. Make predictions really fast.
- It can handle types of data.

Limitations:

- It can get too good at finding patterns and start to make mistakes.
- If the data is not good it might not work well.

4.2 Random Forest

The Random Forest is a type of Machine Learning that uses a lot of Decision Trees together. Each tree looks at a part of the data and then they all vote on what they think it means. The Random Forest is really good at finding people who try to get into our networks because it is strong and can avoid making mistakes.

Advantages:

- The Random Forest is really good at telling the difference, between bad uses.
- It does not get too good at finding patterns and start to make mistakes.
- It can handle a lot of data.

Limitations:

- It needs a lot of computer power.
- It is harder to understand than a Decision Tree

4.3 Support Vector Machine (SVM)

A Support Vector Machine is a tool for sorting data into different groups. It finds the best line to separate the data points. This line helps to keep the groups as far apart as possible. That makes it good for finding intrusions in computer networks that have a lot of data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

Advantages:
• It is very good at sorting data.
• It works well with data that has features.
• It can find patterns of attacks.

Limitations:
• It takes a lot of computer power for data sets.
• You have to choose the settings carefully.

4.4 Naive Bayes (NB)
Naïve Bayes is a way to sort data based on probabilities. It assumes that each feature is separate from the others. This makes it fast and good for systems that need to detect intrusions in time.

Advantages:
• It predicts quickly.
• It works well with data sets.
• It does not need a lot of computer power.

Limitations:
• It assumes that features are not connected.
• It may not work well if features are highly connected.

4.5 K-Nearest Neighbors (KNN)
K-Nearest Neighbors is a way to sort data. It looks at the data points and assigns a group based on the most common group.

Advantages:
• It is simple to understand and use.
• It is good at recognizing patterns.
• There is no need to train it.

Limitations:
• It needs a lot of memory.
• It can be slow with data sets.

4.6 Artificial Neural Network (ANN)
Artificial Neural Networks are like the brain. They have connected parts that work together. They can learn patterns in network data and detect cyber attacks.

Advantages:
• It can learn patterns.
• It is very good at detecting things.
• It is good for intrusion detection systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

Limitations:
• It needs a lot of computer power.
• Training it can take a time.

Comparative Analysis
The algorithms discussed have strengths. Support Vector Machines and Artificial Neural Networks are very good, at detecting intrusions. Decision Trees and Naïve Bayes are fast and easy to use. The choice of algorithm depends on the data size, computer power, accuracy needed and where it will be used.
These machine learning algorithms help to make intrusion detection systems. These systems can find cyber threats. Make computer networks safe.

V. DATASET DESCRIPTION

The performance of a machine learning-based network intrusion detection system really depends on the quality of the dataset used for training and evaluation. In this study we use the NSL-KDD dataset as the dataset for developing and testing intrusion detection models. The NSL-KDD dataset is a version of the KDD Cup 1999 dataset. It is widely used in cybersecurity research because it has a distribution and less redundancy.

5.1 Overview of the Dataset

The NSL-KDD dataset has network traffic records. These records are classified as either normal or malicious. Each record represents a network connection. It includes features that describe the characteristics of network traffic. The dataset helps evaluate how well intrusion detection systems can identify types of cyber attacks.

Dataset Characteristics:
• Dataset Name: NSL-KDD
• Domain: Network Intrusion Detection
• Total Features: 41 Input Features
• Target Attribute: Class Label
• Classification Type: Normal or Attack
• Data Type: Numerical and Categorical Attributes

5.2 Attack Categories

The attacks in the dataset are grouped into four categories:

1. Denial of Service (DoS) Attacks
These attacks try to make network resources unavailable to users. They do this by overwhelming the target system with much traffic.
Examples:
• Neptune
• Smurf

2. Probe Attacks
Probe attacks involve scanning networks. This helps gather information about systems and identify vulnerabilities.
Examples:
• Satan
• Port sweep

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

3. Remote to Local (R2L) Attacks

In R2L attacks an attacker gains access to a system. They do this from a location without having a local account.

Examples:

- Guess Password
- FTP Write

4. User to Root (U2R) Attacks

These attacks occur when an attacker obtains root or administrative privileges. They do this after gaining normal user access.

Examples:

- Buffer Overflow
- Rootkit
- Load Module

5.3 Feature Description

The dataset has 41 features. These features are categorized into the following groups:

Basic Features:

These describe TCP/IP connections.

Examples:

- Duration
- Protocol Type
- Service
- Source Bytes
- Destination Bytes

Content Features:

These capture information from the packet payload and connection content.

Examples:

- Number of Failed Logins
- Logged In Status
- Number of File Creations

Traffic Features:

These describe traffic patterns observed over a time interval.

Examples:

- Connection Count
- Error Rate
- Same Service Rate

5.4 Data Preprocessing

Before model training the dataset undergoes preprocessing. This improves data quality and model performance. The preprocessing steps include:

- Removal of records
- Handling missing values
- Encoding features
- Feature. Scaling

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

• Data splitting into training and testing sets

5.5 Dataset Utilization

The preprocessed dataset is divided into training and testing subsets. The training set is used to build machine learning models. The testing set evaluates the models ability to classify network traffic accurately. This process ensures an assessment of intrusion detection performance.

The NSL-KDD dataset provides a benchmark. It helps evaluate machine learning algorithms in network intrusion detection. It also enables analysis of different classification techniques under various attack scenarios. The NSL-KDD dataset is really useful, for this.

VI. RESULT AND DISCUSSION

This part is about how different Machine Learning algorithms do at finding Network Intrusion Detection. The Machine Learning algorithms were. Tested with the NSL-KDD dataset that was cleaned up first. We looked at how they did using Accuracy and Precision and Recall and F1-Score.

6.1 What We Found

The Machine Learning algorithms we chose did well and it is all summed up in Table 1.

Table 1: How Well Machine Learning Algorithms Do:

Algorithm	Accuracy(%)	Precision(%)	Recall(%)	F1-Score(%)
Decision Tree	94.2	93.8	94.1	93.1
Random Forest	98.1	97.9	98.0	97.9
Naïve Bayes	89.6	88.9	89.2	89.0
SVM	96.3	95.8	96.1	95.9
KNN	95.1	94.7	94.9	94.8
ANN	97.4	97.0	97.2	97.1

What we found out is that Random Forest is really good at finding the classification. It did better than all the algorithms we tried. Artificial Neural Networks and Support Vector Machines also did well.

6.2 What It Means

Our experiment shows that Machine Learning can really help find network activities and tell them apart from normal network traffic.

Random Forest did the best because it uses a lot of decision trees together. This helps it not to overfit. It was very accurate and precise. Recalled things well. This makes it great for real-world Network Intrusion Detection.

Artificial Neural Networks also did well. They can learn patterns from network traffic data.They need a lot of computational power and take a long time to train.

Support Vector Machine is also very good at classification. It can handle a lot of data. It gets slower when the dataset gets bigger.

Decision Tree is good because it is easy to understand and does not need a lot of power. This makes it useful when we need to know what the model is doing.

K-Nearest Neighbors is okay at detection. It needs a lot of memory and is slow because it looks at the distance between things.

Naïve Bayes did not do well. It is fast. It assumes that features are independent. This makes it bad at modeling relationships in network traffic data.

When we compare all the algorithms we see that the ones that use a lot of techniques together do better than the ones. We also have to think about how much computational power they need and how long they take to train.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

Overall our results show that Machine Learning can really help with Network Intrusion Detection. It can find network attacks automatically and accurately. This can help organizations find threats early and make their networks safer. Machine Learning algorithms, like Random Forest and Artificial Neural Networks and Support Vector Machines can really help with Network Intrusion Detection

VII. ADVANTAGES AND LIMITATION

Using Machine Learning in Network Intrusion Detection Systems has a lot of things to offer compared to the old ways of doing security.

7.1 Advantages

1. High Detection Accuracy

Machine Learning can look at a lot of network traffic. Find the bad stuff with pretty good accuracy. The good models can even find complex attack patterns that are hard to find with the old methods. Machine Learning is really good at finding these patterns.

2. Detection of Unknown Attacks

The old way of finding intrusions uses signatures to know what to look for.. Machine Learning models can find new attacks that we have not seen before by looking for weird behavior on the network. This is a deal because Machine Learning can find these unknown attacks.

3. Automation and Scalability

Machine Learning makes it so we do not have to watch the network all the time to find threats. These systems can handle complicated networks without any problems. Machine Learning-based systems are really good at scaling up.

4. Reduced Human Intervention

Machine Learning algorithms can learn from what happened in the past. So we do not have to update the security rules and attack signatures all the time by hand. This means Machine Learning does a lot of the work for us. Machine Learning is really helpful, in this way.

7.2 Limitations

Machine Learning-based intrusion detection systems have some problems.They have some advantages. Also face several challenges and limitations.Machine Learning-based intrusion detection systems are not perfect.

1. Dependence on Data Quality

The Machine Learning models need data to work well.The quality and quantity of training data is very important for Machine Learning models.If the data is not complete. Is noisy or outdated it can reduce the accuracy of detection.The data needs to be good for Machine Learning models to work properly.

2. High Computational Requirements

The Machine Learning and Deep Learning algorithms need a lot of power to work.
They need a lot of memory and processing power to work properly.This is especially true for networks.The Machine Learning and Deep Learning algorithms are not easy to run.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

3. False Positives and False Negatives

The Machine Learning models can make mistakes.They can say that normal traffic is bad when it is not.This is called a positive.The Machine Learning models can also miss the traffic.This is called a negative.These mistakes can make the system not work well.The Machine Learning models are not perfect. Can make mistakes.

4. Dataset Imbalance Issues

The datasets for intrusion detection are not always even.There are usually normal records, than attack records.This can make the models biased.The models do not work well for the attack records.The datasets need to be even for the models to work properly.The Machine Learning models need datasets to work well.

VIII. FUTURE SCOPE

The cyber attacks are getting more complicated. The number of networked systems is growing really fast. This means we need to have smarter ways to detect when someone is trying to break into our systems. Even though we have made some progress with Machine Learning-based Network Intrusion Detection Systems there is still a lot of work to be done.

One thing we can do is use Deep Learning techniques like Convolutional Neural Networks and Recurrent Neural Networks to help us find attack patterns that we have not seen before. These models can look at a lot of network traffic data. Find things that might be a problem. This can help us catch guys who are trying to break into our systems.

We also need to be able to detect problems in time so we can stop bad things from happening right away. A lot of companies are using cloud computing and IoT devices now so we need to be able to look at a lot of data and make decisions fast.

Another thing we can try is using machine learning algorithms together to make our detection systems better. This way we can use the things about each model to make a stronger system.

We also need to think about how to use Artificial Intelligence to protect security and Internet of Things environments. There are many connected devices now that we need to be able to protect them from cyber threats.

We can also look into using Federated Learning and Privacy-Preserving Machine Learning techniques. These methods let us use data from places without sharing sensitive information, which makes our systems more secure and private.

Using Explainable Artificial Intelligence in our detection systems is also an idea. This means we can understand why our system thinks something is bad which helps us make decisions and trust our systems more. Network Intrusion Detection Systems, like these can help us understand what is going on with our Network Intrusion Detection Systems.

IX. CONCLUSION

Network security is a concern today because cyber attacks are happening more often and are getting smarter. Old ways of detecting intrusions struggle to find unknown threats so we need better and more adaptable security solutions. This study looked at using Machine Learning for Network Intrusion Detection. How well it works in finding bad network activities.

Various Machine Learning methods were tested, including Decision Tree, Random Forest, Support Vector Machine, Naïve Bayes, K-Nearest Neighbors and Artificial Neural Networks. These methods were checked for their ability to classify network traffic as normal or malicious.The results show that Machine Learning-based intrusion detection systems can really improve attack detection accuracy. They can also automate threat identification. Make overall network security better.

Some methods, like advanced learning worked better in detecting cyber threats and had lower false alarm rates.The study also showed that data preprocessing, feature selection and performance evaluation are crucial in developing intrusion detection models.

Using datasets like NSL-KDD helps compare different algorithms and provides a foundation for future research.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, June 2026 Impact Factor: 8.2

There are still challenges like dataset imbalance, computational complexity, model interpretability and evolving attack strategies that affect the performance of intrusion detection systems.We need to address these limitations in investigations.

In conclusion Machine Learning offers an approach to Network Intrusion Detection by enabling intelligent analysis of network traffic and timely identification of cyber threats, which is essential for protecting modern network infrastructures.

Machine Learning and Artificial Intelligence techniques will play a role in developing robust cybersecurity solutions.As cyber attacks continue to evolve we need to integrate Machine Learning and Artificial Intelligence techniques to stay ahead.

Machine Learning is key to achieving this goal.It helps us to analyze network traffic and identify cyber threats quickly.Network Intrusion Detection is critical, for network security.Machine Learning makes it possible.

REFERENCES

1] T. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.

2] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "NSL-KDD Dataset for Network-Based Intrusion Detection Systems," University of New Brunswick, Canada, 2009.

3] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," Military Communications and Information Systems Conference (MilCIS), 2015.

4] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," International Conference on Information Systems Security and Privacy, 2018.

5] W. Lee and S. J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems," ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 227–261, 2000.

6] E. Denning, "An Intrusion-Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, 1987.

7] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology (NIST), Special Publication 800-94, 2007.

8] L. Breiman, "Random Forests," Machine Learning Journal, vol. 45, no. 1, pp. 5–32, 2001.

9] C. Cortes and V. Vapnik, "Support-Vector Networks," Machine Learning Journal, vol. 20, no. 3, pp. 273–297, 1995.

10] T. M. Mitchell, "Machine Learning," McGraw-Hill Education, New York, 1997.

11] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016.

12] S. Dua and X. Du, "Data Mining and Machine Learning in Cybersecurity," CRC Press, 2016. Techniques," Informatica, vol. 31, pp. 249–268, 2007.