International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

An Intelligent Machine Learning Framework for Real-Time Cyber Threat Detection in Network Traffic

Jeevaa S R [1], Dr. B. Leelavathi [2]

Student [1], Professor [2]

Department Of Computer Technology Dr. N.G.P. Arts and Science College, Coimbatore

https://doi.org/10.55041/ijsmt.v2i3.053

Cite this Article: R, J. S. (2026). An Intelligent Machine Learning Framework for Real-Time Cyber Threat Detection in Network Traffic. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.053

Abstract

There has been a drastic increase in the cyber threats associated with using digital technologies across many areas of our daily lives. Many of us rely heavily on the Internet for things like communicating (chatting/emailing), storing data, etc., so as a result, everyone (big businesses and individuals alike) is subjected to increased risk. Many cybercriminals have become very sophisticated in their methods of invading networks. They have developed different types of malware that can bypass traditional security measures (i.e., firewalls and antivirus software). Therefore, many intrusion detection systems (IDS) do not provide adequate response capabilities against novel or evolving cyberattacks; rather, due to their limited detection methodology, most IDS only recognize established "attack signatures".

An approach to resolving this challenge is to implement a machine learning-based cyberthreat prediction and detection system that monitors network activities in real time. This prediction/detection mechanism will provide system administrators with early notifications of possible threats based on previous patterns. As the system processes live information and confirms suspicious activity, it will convert disorganized/unstructured data into structured forms (e.g., visual displays (charts)).

The visual trends will allow system administrators to quickly find out about significant deviations in normal network activity, thereby enabling them to quickly identify any uncharacteristic network behavior as a result of potential security compromises.

Keywords

Cybersecurity, Machine Learning, Network Traffic Analysis, Real-Time Threat Detection, Intrusion Detection System, Anomaly Detection, Traffic Visualization, Predictive Security.

1.Introduction

With the rapid rise and expansion of the digital network and online services, internet traffic is more complex and overwhelming all the time. Therefore, keeping your data secure from cybercrime has become a major concern for both companies and individuals alike. As companies rely more on these networks to perform everything from communication to document storage, they expose themselves to many different types of cyber threat—such as DDoS attacks, ransomware, phishing and unauthorized access.

The conventional security systems to protect against cybercriminals primarily rely on identifying well known attack patterns. Thus, these systems provide limited protection against unknown or "zero-day" attacks and, therefore, are not effective in protecting against anything new. In addition, manually monitoring traffic on a network that has such large volume of traffic is simply

not viable. This is where Machine Learning (ML) plays a crucial role; it uses historical traffic information to determine whether or not a new piece of incoming network traffic is secure or malicious. By analyzing multiple different factors such as the size of a packet, what type of protocol it is using, how long it takes to complete the connection, and how often the traffic is occurring, ML models are able to identify any abnormal passenger behaviour that occur on the network. This helps increase the accuracy of detection and decrease the number of false positives.

The goal of this project is to develop a real-time system for predicting cyber threats that will capture the current network traffic and show the traffic behaviour with dynamic charts, as well as provide optional ML training capabilities so that predictions can be completed based on future traffic behaviour. Once the system is in place and running, the ML training model can be developed and the results will demonstrate that continual monitoring of new network traffic, using the ML training model, will provide the most accurate and consistent identification of potential cyber threats.

2.Literature Review

Cybersecurity professionals have investigated Intrusion Detection Systems (IDS) extensively as an important technology to protect computer networks from cyber crime. Two types of IDS are commonly used today: Signature-Based and Anomaly-Based Systems. Signature-based IDS relies on knowing and storing the previous signatures of attacks in order to identify them in real time (i.e. by comparing incoming traffic against known signatures). Therefore, if the signature for a new attack does not already exist (i.e. if it is a 'zero-day' or if the attack is evolving), then the signature-based IDS will be unable to identify the attack. Anomaly-based IDS, on the other hand, detects new attacks by identifying deviations from established normal network behaviours. However, the presence of changing network patterns (i.e. traffic) creates problems for anomaly detection-based IDS due to their tendency to produce many false positives. [1] Researchers have actively utilized machine learning (ML) for IDS to provide additional benefit. ML can provide an intelligent decision-supporting framework to enhance decision-making processes. Recent studies, such as [4], have looked extensively at the various approaches of ML-based intrusion detection for all aspects of this area: IDS designs, datasets, network threats, etc. and have demonstrated an obvious shift from traditional IDS designs to more intelligent ML-based IDS designs. Many ML-based algorithms (including supervised learning methods such as Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbour (KNN), and Artificial Neural Networks (ANN)) have been shown to perform very well when classifying normal versus malicious traffic as well as comparing various comparison techniques to identify which methods (e.g., delivered via ensemble method or tree-based) provide the highest accuracy or performance. . Additionally, B Leelavathi et al. [9] proposed a system for detecting network worms by analysing multiple, distinct features of executables to identify malicious behaviour, aiming for a high detection rate with low false positives.

3.Problem Statement

Nowadays, monitoring a computer network is becoming increasingly difficult. A massive volume of data moves through an organization's network, making it challenging to identify potential cyber threats. Most conventional intrusion detection and prevention systems are based on predefined attack patterns. While they are able to detect attacks against known vulnerabilities, they are not capable of detecting new, sophisticated, or stealthy attacks, including advanced hacking activity. Additionally, many legacy rule-based systems cannot keep up with today's rapidly changing network environments. As a result, many organizations will not realize that there has been an incident until it is too late to take any action.

Another concern is that many older security products lack appropriate real-time visibility or do not provide an adequate means of forecasting the future successfully. As such, network administrators must frequently utilize spot-checking methods or utilize multiple disparate security tools, which can create a tremendous amount of frustration for the administrator, despite not providing an adequate solution. The lack of interoperability and collaboration between these tools increases administrative confusion and creates too many false positives. All of these factors contribute to the burnout of security professionals.

4. Objectives

The objectives of this project focus on developing an intelligent and efficient system for real-time cyber threat detection using machine learning techniques. The system is designed to enhance proactive network security by integrating traffic monitoring, visualization, predictive analysis, and automated alert mechanisms within a unified framework.

4.1 Real-Time Network Traffic Monitoring

The main goal of this project is to create a smart and efficient system that can spot cyber threats in real time using machine learning. We're aiming to boost network security by bringing together tools for monitoring traffic, visualizing data, predicting potential issues, and sending out alerts—all in one easy-to-use system.

4.2 Traffic Visualization and Analysis

The system monitors real-time network traffic constantly, giving us insight into how packets occur on a network. This allows us to visualize traffic almost immediately by collecting packet-level information at the same time. This is very valuable for identifying potential threats.

4.3 Machine Learning Model Development

In this initiative, we want to identify regular and abnormal Network Traffic utilizing machine learning and leverage Data in the Traffic Analysis system to develop a tool that learns from collected traffic data and can respond to an evolving cyber threat landscape.

4.4 Real-Time Threat Prediction

One of our primary objectives is to have a machine-learning system that can classify network traffic instantaneously in real-time. In other words, we want a system that can look at a flow of incoming traffic and analyse that traffic quickly. This means we need to be able to accurately analyse this data, and we need to do so very quickly.

Think of data flowing in and out of our system as a freeway that is continually under construction and is constantly experiencing traffic delays. As data comes in, our model acts as a traffic cop by providing us with early warning signs of any potential threats or abnormal behaviour. The faster we can identify these types ofevents, the quicker we can take action to ensure that our overall system remains safe and functioning correctly.

In order to accomplish this goal, we will first perform a model refinement phase where we train our system to recognize traffic patterns from an ongoing series of incoming data. Specifically, we will present it with many different types of examples relating to both normal and unsafe traffic so that it can determine the differences between these two types of traffic patterns. Once we are satisfied that our system is sufficiently well-trained, we will move forward with implementing it in a production environment. Because this will be an important transition for our model, we will need to closely track its performance during this period of time until we determine whether or not it is producing accurate results.

4.5 Alert Generation and Logging

We are looking for a feasible and efficient solution to develop an automated approach for predicting the likelihood of a problem (or "issue") occurring with regards to the net traffic network. In order to identify the problem as early on in the process as possible, we want to come up with a method of monitoring incoming data in order to fix/mitigate any issues that arise as quickly as possible. By having the ability to provide rapid and reliable detection of the incoming packets when they enter the network we can prevent the problem from becoming any worse; furthermore, if we develop a reliable detection process we can greatly reduce the amount of false alarms generated. Ultimately, the goal is to create and maintain a secure and functioning network infrastructure. In light of the ever-changing world we live in, it is essential to create a proactive solution for ensuring that the network remains secure.

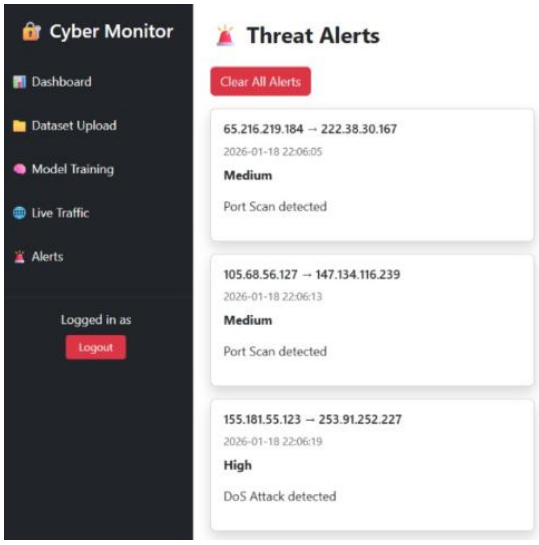

Fig 1:Cyber Monitor & Threat Alerts

5. Methodology

Searching for threats in real-time is carried out by systematically reviewing network logs in order to predict future cyber threats. There are multiple steps taken to collect, process, and sort through network traffic flow as well as predicting f

uture threats from what you find in the logs. Each of the components (e.g., the steps and processes) has been built with speed and scalability in mind so that you can detect all threats successfully and respond to them as quickly as possible. You combine all of the components together (network monitoring, processing data, visualizing data, and performing predictive analytics) to have a solid solution that provides a greater level of accuracy for detecting cyber threats while not negatively impacting your ability to respond in a timely manner to suspicious types of activity.

5.1 Data Collection

The data collection process refers to the collection of some basic information (IP address, protocol, timestamp and severity of incident) associated with network traffic via our monitoring system. The data collected is useful for identifying possible suspicious behaviour and also provides information useful for further investigating, cleaning up the collected data and using machine learning to positively identify possible threats.

Attribute Name	Description
timestamp	Time when the suspicious traffic event was detected
source_ip	Originating IP address of the request
destination_ip	Target IP address receiving the traffic
protocol	Network protocol used (HTTP, HTTPS, TCP, UDP, ICMP, etc.)
severity	Threat level assigned (Low, Medium, High)
description	Summary of the detected suspicious traffic

Table.1 Dataset Description

5.2 Network Traffic Acquisition and Preprocessing

The very first step of the overall processes is collecting live network traffic from actual host systems/network interfaces. We're collecting source & destination IP, port numbers, protocols used, size of packets, timestamps, how long a connection lasts, etc. All collected data can be collected 24 hours a day, 7 days a week; the problem is, this raw network traffic data is extremely unorganized and has a lot of unnecessary or incomplete information in them, thus, we need to clean it up before we can truly utilize it.

Now during the data 'clean up' process we will remove duplicate packets; fill in any missing values; and convert things such as protocol type into numeric values so they can be used with the machine learning algorithms. We will also unify all of the data so that data will be on the same scale by normalizing/scaling the numerical features. After that, we will extract some major pieces of information regarding the frequency of the traffic, packet rates, and duration of the various connections. These data points are essential for determining what is considered to be normal network activity versus something that may be more suspicious.

5.2 Machine Learning-Based Threat Prediction Framework

We clean all of our data and then use our data to build and train machine learning models that will allow us to classify traffic flows. The type of machine learning we use is called 'supervised learning', which means we have previously labelled our data to show examples of 'normal' traffic vs 'bad' traffic patterns. We then create separate training and testing datasets, so that we can evaluate how the model is performing, using different metrics (precision, recall, F1 score, accuracy, etc.) to evaluate the model.

Once validated as performing well, the model is then put into a state where it is able to predict traffic in real time. When new traffic flows into our system, we convert that new traffic into feature vectors and feed them into our model for classification. When the model detects any signs of malicious activity, it sends out an alert immediately, as well as logging that event for future postmortem analysis. This gives us the capability of early detection of threats to our systems, as well as significantly increasing the speed of our response to cyber attacks.

6. Results and DiscussionModel Performance Evaluation

We evaluated the success of our machine learning model by evaluating four primary metrics, which include accuracy, precision, recall, and F1-score. In each of these four evaluations, it was determined that the machine learning model accurately identified differences between regular network traffic and harmful network traffic; thus validating the reliability of the machine learning model.

Reduction in False Positives

Accuracy is improved significantly under the new system, thus reducing the number of false alarms when compared to older rule-based intrusion detection systems. Users can have more confidence that it will work properly and everything runs much more smoothly.

Real-Time Detection Capability

Accuracy is improved significantly under the new system, thus reducing the number of false alarms when compared to older rule-based intrusion detection systems. Users can have more confidence that it will work properly and everything runs much more smoothly.

Effectiveness of Traffic Visualization

Admin Dashboard allowed admins to see different traffic patterns and any unusual spikes in activity. Admins could easily get a quick visual view of what was happening at that moment. If there were any irregularities, admins could also quickly trace those back to traffic changes and take immediate action to fix the problem. This provided a much faster view for the Admin to get an understanding of what the situation was, which in turn made their job much less difficult. The ability to see visually allows admins the ability to respond quickly to any unusual activity. All in all, Admin Dashboard is a fantastic tool to help keep everything safe and operational.

Adaptability to Evolving Threats

Machine-learning models are not restricted by signatures; instead, they analyse historical information to understand how a computer system functions in order to identify what constitutes as ‘normal’ behaviour and identify patterns that do not conform to ‘normal’ behavioural standards. Machine-learning models are particularly effective against new and unfamiliar cyber threats as they can take into account an attacker’s previous actions and adaptively learn from abnormal activity and/or abnormal behavioural patterns over time. Traditional security systems tend not to keep up with evolving hacking techniques and will not be able to identify new hacks on their own. Therefore, using machine-learning made models provides the user with an intelligent and adaptable level of protection from numerous forms of cyber threats to the protection of computer networks from such threats.

System Reliability and Practical Applicability

Through research regarding monitoring, predicting, and sending alerts, the ability of the combined system to meet these needs has been demonstrated. The results substantiate the claim of increasing proactive cyber security defenses within a real-time network environment by using this method.

7. Conclusion

By utilizing machine learning models for the Analysis of Network Traffic, the Cyber Threat Prediction System utilizes Real-Time Data to Evaluate Cyber Threats. The cyber threat prediction system uses an integrated architecture to Monitor Traffic, Preprocess Data, Extract Features, and Classify Traffic Using Machine Learning and Provide Automated Alerts Using a Unified Architecture. By monitoring live network traffic, the cyber threat prediction system converts network traffic to Structured Features for Intelligent Classifying and Analysis of Network Traffic. Network Traffic Classified as Malicious will have no false positives compared to malicious network traffic versus traditional rule-based network traffic classifications, resulting in Less False Positive Rate.

The Cyber Threat Prediction System is designed to Provide Real-Time Threat Prediction and Alerts To Respond to Potential Cyber Threats as Soon As They Occur, Reducing Cyber Detection Latency, and Decreasing System Vulnerability Due to Detected Cyber Threats. By including a feature to assist administrators in determining the source of Network Activity and Quantum of Anomalies in Network Traffic Behavior, The Cyber Threat Prediction System Provides A Visual Representation of Network Activity That Will Assist Administrators In Understanding Network Activity.

The cyber threat prediction system is an overall scalable, efficient, and Pro-Active Network Threat Detection System, By Providing Intelligent, Adaptive Threat etection Systems to Strengthen the Security of Networks.

8. Future Scope

Advanced algorithms, such as Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN), for machine learning allow for more precise identification of complex traffic flow patterns than conventional algorithms. Through automatic retraining of the model(s), the system will not only increase the accuracy of the model but will also continue to learn from all historical training data.

Cloud computing is likely an area to be explored in the near future. Moving to the cloud will provide improved performance for extensive, geographically located, multi-site networks. Integrating this technology into firewall solutions, along with automation of responses to potential threats, will greatly increase the time it takes to detect and respond to these threats.

Future research will be focused on developing techniques to identify / recognize abnormal encrypted traffic and Advanced Persistent Threats (APT). The previously described improvements to this system will help to strengthen the capabilities of this system, which is vital to maintaining a strong, secure cybersecurity posture.

9. References

[1] A. Farhan, *et al*., "Network-based intrusion detection using deep learning integrating DNN and Extra Tree Classifier," *Scientific Reports*, vol. 15, 08770, pp. 1–12, 2025.

[2] M. Cantone, C. Marrocco, and A. Bria, "Machine learning in network intrusion detection: A cross-dataset generalization study," *IEEE Access*, vol. 12, pp. 3472–3485, 2024.

[3] M. Al Lail, *et al*., "A comparative study on machine learning-based network intrusion detection," *Future Internet*, vol. 15, no. 7, pp. 243, 2023.

[4] P. Kumar and R. Singh, "Real-time network traffic analysis using ML models: A survey," *Journal of Network and Computer Applications*, vol. 190, pp. 103–425, 2022.

[5] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy and survey of intrusion detection system design techniques, network threats, and datasets," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1–35, 2021.

[6] M. A. Ferrag, L. Maglaras, A. Ahmim, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," *Future Internet*, vol. 9, no. 3, pp. 1–16, 2017.

[7] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns," *IEEE Transactions on Computers*, vol. 63, no. 4, pp. 807–819, 2014.

[8] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 305–316.

[9] B. Leelavathi, "An Efficient Worm Detection System Using Multi Feature Analysis and Classification Techniques," *Springer Nature Link,* vol. pp 1054–1064, 2019