AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(1) (2026)
www.ajmimc.com

MACHINE LEARNING TECHNIQUES FOR CYBER ATTACKS DETECTION

Mr.P.Murali Krishna[1], Yanumula Srinivasa Rao[2] Boddu Koteswara Rao[3]
Komma bhavana[4], Dammalapati Pawan kalyan[5]

[1]*Assistant Professor, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.*

[2,3,4,5] *UG Scholar, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.*

ABSTRACT

Cyber attacks have become increasingly sophisticated, making traditional security methods less effective at identifying malicious activities. Machine learning (ML) techniques offer powerful solutions for detecting and preventing these attacks by automatically analyzing large amounts of network and system data. This paper reviews various ML approaches—including supervised, unsupervised, and reinforcement learning—for identifying threats such as malware, intrusion attempts, phishing, and anomalous behavior. It highlights how ML models can learn patterns of normal and abnormal activities, improve detection accuracy, and reduce false alarms. Challenges such as data quality, model interpretability, and evolving attack strategies are also discussed. Overall, machine learning provides an adaptive and efficient framework for strengthening cybersecurity systems.

Keywords:

Machine Learning, Cybersecurity, Intrusion Detection, Anomaly Detection, Malware Detection, Network Security, Artificial Intelligence.

Introduction

The rapid growth of internet technologies and connected devices has created new opportunities for cybercriminals to exploit system vulnerabilities. Cyber attacks can lead to data theft, financial loss, privacy breaches, service disruption, and damage to organizational reputation. Common cyber attacks include phishing, ransomware, SQL injection, botnet attacks, Distributed Denial of Service attacks, and insider threats.

Traditional security solutions rely mainly on rule-based systems and predefined signatures to identify threats. Although these methods can detect known attacks, they are ineffective against new and unknown attack patterns. Modern cyber attacks are dynamic and continuously evolve, making it difficult for static systems to keep up.

Machine learning provides an intelligent solution by analyzing large volumes of data and identifying hidden patterns associated with malicious behavior. It enables cybersecurity systems to learn from past attack data and adapt to new threats automatically. Machine learning models can process data from network packets, server logs, user activity records, email traffic, and file systems.

The use of machine learning in cyber attack detection has increased significantly because it provides high accuracy, scalability, adaptability, and faster response times. Organizations can use these systems to detect suspicious activities in real time and prevent severe damage.

Existing System

Existing cyber attack detection systems mainly depend on signature-based and rule-based methods. Signature-based systems maintain a database of known attack patterns and compare incoming traffic against those signatures. If a match is found, the system raises an alert. Rule-based systems use manually defined conditions to identify suspicious behavior.

Although these methods are useful for detecting known threats, they have several limitations. They cannot detect zero-day attacks, unknown malware, or new phishing techniques because such attacks do not match existing signatures. Another problem is that traditional systems require frequent updates to remain effective.

Rule-based systems also produce high false positive rates because they may classify normal behavior as malicious. In large-scale networks, the

volume of traffic is very high, making it difficult for traditional systems to process all data efficiently.

Existing System	Limitation
Signature-Based Detection	Cannot detect unknown attacks
Rule-Based Systems	Requires manual updates
Traditional Firewalls	Limited intelligent analysis
Antivirus Software	Fails against advanced malware
Static Monitoring	Poor adaptability

Proposed System

The proposed system uses machine learning algorithms to analyze network traffic and detect cyber attacks in real time. The system collects data from network packets, logs, user activities, emails, and connected devices. The collected data is preprocessed to remove noise, duplicates, and irrelevant information.

After preprocessing, important features such as source IP address, destination IP address, packet size, protocol type, session duration, login attempts, and unusual behavior patterns are extracted. These features are then provided to machine learning models for training and classification.

Algorithms such as Decision Tree, Random Forest, Naive Bayes, Logistic Regression, Support Vector Machine, and K-Nearest Neighbor are used for attack detection. Deep learning techniques such as Convolutional Neural Networks and Recurrent Neural Networks can further improve accuracy by identifying complex patterns.

The proposed system classifies activities into normal and malicious categories. If suspicious activity is detected, the system generates an alert for the administrator.

Proposed Module	Function
Data Collection	Gathers logs and network traffic
Preprocessing	Cleans and normalizes data
Feature Extraction	Selects important attack indicators
ML Classification	Detects cyber attacks
Alert Generation	Sends warning notifications
Dashboard Monitoring	Displays attack statistics

Machine Learning Techniques Used

Different machine learning techniques are used in cyber attack detection depending on the type of data and attack patterns.

Decision Tree is a supervised learning algorithm that creates a tree-like structure for classification. It is easy to understand and works well for detecting suspicious network activities.

Random Forest is an ensemble learning method that combines multiple decision trees to improve accuracy and reduce overfitting. It is one of the most commonly used algorithms in cybersecurity.

Support Vector Machine is used for binary classification and is effective in distinguishing malicious and normal traffic. Naive Bayes is a probabilistic classifier that works well with large datasets and email spam detection.

K-Nearest Neighbor classifies data based on similarity with neighboring records. Logistic Regression predicts the probability of a cyber attack based on feature values.

Deep learning models such as Artificial Neural Networks, Convolutional Neural Networks, and Recurrent Neural Networks can detect advanced threats by learning hidden patterns in large datasets.

Algorithm	Application
Decision Tree	Intrusion detection
Random Forest	Malware detection
Support Vector Machine	Traffic classification
Naive Bayes	Spam and phishing detection
K-Nearest Neighbor	Behavioral analysis
Deep Learning	Advanced threat detection

Advantages

Machine learning-based cyber attack detection systems provide several advantages over traditional methods. They can identify both known and unknown attacks with high accuracy. These systems can analyze large amounts of data quickly and generate alerts in real time.

Machine learning models also reduce false positives and improve detection efficiency. They are scalable and suitable for large enterprise networks, cloud environments, IoT devices, and industrial systems.

Another important advantage is adaptability. Machine learning systems can be retrained using new attack data, allowing them to recognize evolving threats.

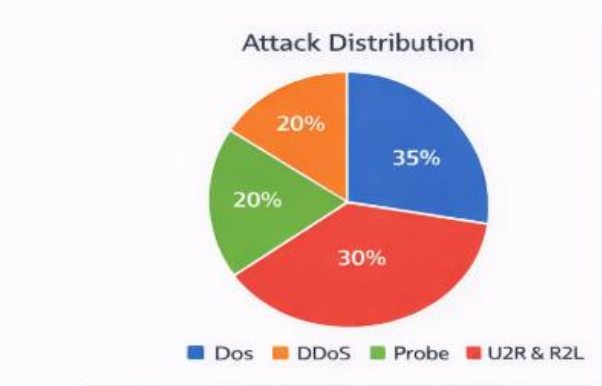
Advantage	Benefit
High Accuracy	Improves attack detection
Real-Time Monitoring	Faster response to threats
Scalability	Supports large networks
Adaptive Learning	Detects new attack patterns
Low False Positives	Reduces unnecessary alerts

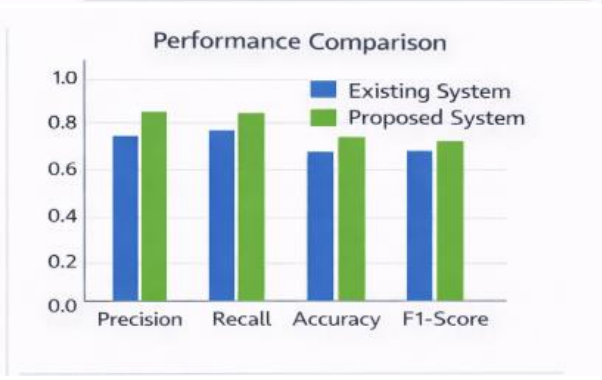
Applications

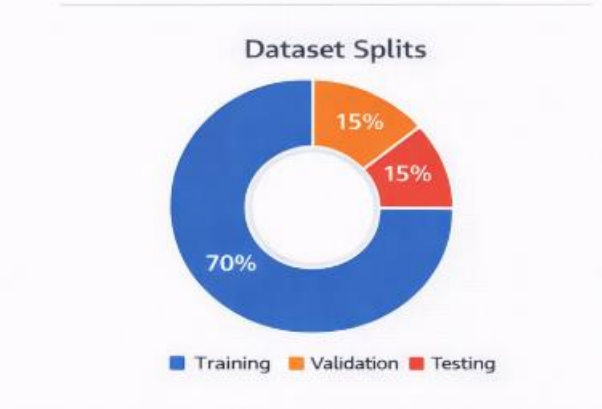
Machine learning techniques for cyber attack detection are used in many fields. In banking systems, they help identify fraudulent transactions and phishing attempts. In healthcare systems, they protect patient data from ransomware and unauthorized access.

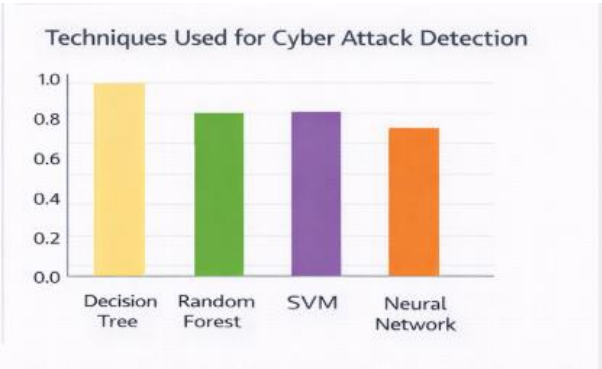
In cloud computing, machine learning models detect suspicious login attempts and malware activities. In IoT environments, they secure smart devices from botnet attacks and network intrusions. Enterprises use these systems to monitor employee activities, detect insider threats, and secure sensitive data.

Application Area	Security Purpose
Banking	Fraud detection
Healthcare	Patient data protection
Cloud Computing	Malware detection
IoT Networks	Intrusion prevention
Enterprise Systems	Insider threat monitoring









RESULTS AND DISCUSSIONS

CONCLUSION

Machine learning techniques have become essential for detecting cyber attacks in modern digital environments. Traditional security systems are no longer sufficient because they cannot handle

rapidly evolving attack patterns. Machine learning algorithms provide intelligent, adaptive, and real-time detection capabilities that improve cybersecurity.

By analyzing network traffic, user behavior, and system logs, machine learning systems can identify suspicious activities accurately and reduce the impact of cyber attacks. Techniques such as Random Forest, Support Vector Machine, Decision Tree, and Deep Learning play a major role in improving detection performance.

In the future, cyber attack detection systems can be enhanced further by integrating blockchain, cloud computing, and edge computing technologies. The combination of machine learning and advanced cybersecurity techniques will provide stronger protection against modern threats.

REFERENCE

1. K. K. . Kommineni and A. . Prasad, “A Review on Privacy and Security Improvement Mechanisms in MANETs”, Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.
2. Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w
3. Machine Learning and Security: Protecting Systems with Data and Algorithms by Clarence Chio and David Freeman
4. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
5. Machine Learning for Cybersecurity by Sumeet Dua and Xian Du
6. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
7. Artificial Intelligence for Cybersecurity by Leslie F. Sikos
8. IEEE research papers on machine learning-based cyber attack detection
9. Springer journal publications on intrusion detection and cybersecurity analytics
10. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
11. Elsevier articles related to malware detection, phishing detection, and network intrusion analysis
12. Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782
13. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.
14.
15. Poojari, R. (2024). Assessing Clinical Natural Language Processing (NLP) Models for Interpreting Electronic Health Records (EHR): Focus on Accuracy, Bias, and Generalizability.
16. Cyril, H. P., & Kumara, S. Identification of Anomalies via Deep Learning-Based Models for High-Dimensional Telecom Traffic Data.
17. Kaggle cybersecurity datasets such as NSL-KDD, CICIDS2017, UNSW-NB15, and phishing datasets
18. Dayal, P. S., Chandra, B. R., Keerthi, M., Sruthi, M., Venkatesh, K., Appalaraju, G., & Eswari, G. (2013). Design of Pyramidal Horn Antenna at 10GHz Using WIPL-D Optimizer. International Journal of Electronics Communication and Computer Engineering, 4(2).
19. Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering and Management Research, 10(10), 49–56.
20. Reddy, S. K. R. (2024). Designing Blockchain Architecture to Transform Loyalty Rewards into Cryptocurrency Investments.
21. Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.
22. Cisco annual cybersecurity reports and threat intelligence studies

23. IBM security intelligence reports on AI and machine learning in cybersecurity