Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

NETWORK SECURITY ENHANCEMENT THROUGH MACHINE LEARNING-BASED CYBER ATTACK DETECTION

[#1]**Gopannagiri Sneha,** *Department of MCA,*
[#2]**Mrs. Y. Susheela,** *Associate Professor, Department of CSE,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: The objective of this investigation is to identify and prevent harmful activities in contemporary communication networks by employing machine learning-based techniques to enhance network security and detect intrusions. Using supervised and unsupervised machine learning algorithms, including Decision Trees, Random Forest, Support Vector Machines, and Neural Networks, the investigation examines network traffic patterns and identifies outliers that may be the result of cyber threats such as phishing, DOS attacks, malware intrusions, and unauthorized access attempts. The proposed method analyzes a variety of network metrics, including packet flow, connection duration, source and destination IP behavior, and protocol utilization, to facilitate the identification of both normal and anomalous activity. Traditional security systems that rely on signatures are significantly outperformed by machine learning-driven detection models in terms of real-time attack detection, false alarm rates, and threat detection speed. The paper underscores the critical nature of enhanced cyber security systems in order to ensure the security of private information, the reliability of networks, and the safety of online communication.

Keywords: *Network Security, Machine Learning, Cyber Attack Detection, Intrusion Detection System, Anomaly Detection, Cybersecurity, Random Forest, Neural Networks.*

1. INTRODUCTION

The significance of network security is increasing in contemporary computer environments due to the rapid evolution of digital technologies and internet-based communication systems. Computer networks enable individuals, businesses, and organizations to engage in a variety of online activities, such as data exchange, financial transactions, cloud services, and communication. The dangers of cyberspace, including phishing, ransomware, denial-of-service attacks, and unlawful access, have increased significantly as individuals utilize increasingly interconnected technology. Traditional security measures, such as firewalls and signature-based intruder detection systems, frequently fail to identify emerging and evolving threats. In order to enhance network security and ensure data availability, privacy, and integrity, it is necessary to implement security options that are both intelligent and adaptable.

Automating threat research and identifying cyberattacks has significantly enhanced network security through the use of machine learning (ML). Machine learning algorithms are capable of analyzing vast quantities of network traffic data, identifying previously unidentified trends, and identifying unusual behavior that may indicate that an individual is attempting to cause damage. Compared to conventional rule-based systems, machine learning models are more effective at identifying both known and unknown assaults because they can learn from both historical and real-time datasets. Algorithms such as Decision Trees, Random Forests, Support Vector Machines, and Neural Networks are frequently employed to identify

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

intrusions and organize network data. These methods are highly beneficial in contemporary cybersecurity applications, as they significantly enhance the precision of detection, reduce the frequency of false alarms, and expedite reaction times.

The effectiveness of systems designed to detect breaches has been significantly enhanced by recent advancements in deep learning. Long Short-Term Memory (LSTM) networks, Recurrent Neural Networks (RNNs), and Convolutional Neural Networks (CNNs) are all examples of models that can identify intricate cyber threats and traffic trends in real time. Machine learning-based security systems are capable of adapting to novel attack methods, thereby simplifying the process of safeguarding against zero-day vulnerabilities and SPTs prior to their occurrence. In spite of the challenges they encounter, such as adversarial assaults, unbalanced datasets, and high computational demands, researchers are resolute in their efforts to enhance the reliability and scalability of ML-based defense systems. Consequently, machine learning has emerged as a critical instrument for safeguarding contemporary digital systems from the proliferation of cyber threats and enhancing the security of networks.

2. LITERATURE REVIEW

Anderson & Walker (2021): This research demonstrates a method for utilizing machine learning to enhance the security of networks by identifying breaches with greater speed and precision. The system employs supervised learning techniques, including Decision Trees and Random Forests, to identify fraudulent network behavior patterns. By examining factors such as the speed at which packets are transmitted, their interaction with IP addresses, and their utilization of protocols, among other factors, it is possible to more effectively categorize cyberthreats. The research resulted in a reduction in the number of false alarms and an increase in the precision of intrusion detection.

Singh & Rao (2022): This paper demonstrates a deep learning-based approach to identifying intrusions that is intended to ensure the security of large communication networks. By integrating Convolutional Neural Networks (CNNs) with Support Vector Machines (SVMs), it is possible to identify individuals who should not be present, as well as malware and fraud attempts. The framework identifies unusual patterns of behavior by meticulously monitoring network data. The performance paper demonstrates that the response times and ability to locate objects are significantly more efficient and effective than those of conventional security systems.

Garcia & Thomas (2023): The authors have developed an intelligent intrusion detection system that will enhance the security of networks by making use of a combination of artificial intelligence and machine learning. The system employs both supervised and unsupervised learning methods to identify both established and emerging cyber threats. By employing techniques such as real-time traffic analysis and anomaly detection, it is possible to enhance the precision of hazard classification and reduce security vulnerabilities. The comparative analysis of various methods demonstrates that large network datasets are more manageable and can be expanded.

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

Mehta & Kulkarni (2024): This research discusses a security system that employs machine learning and the cloud to detect intrusions prior to their occurrence. The architecture employs K-Nearest Neighbor (KNN) methods and neural networks to detect anomalous network behavior and promptly identify intrusions. The system is more stable and the privacy of data is safeguarded by secure authentication methods and adaptive filtering algorithms. The test results indicate that scalability, detection delay, and network performance have all been enhanced.

Hernandez & Kim (2025): The research proposes an AI-based network security model that can identify sophisticated cyber threats by employing advanced deep learning techniques. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) are capable of identifying intricate attack patterns and unusual modifications in the operation of networks. The system enables the rapid identification of zero-day threats and the continuous monitoring of traffic flow. The findings indicate that the accuracy of predictions has increased and that cyber hazards to business networks have decreased. The system enhances both intelligent threat control and real-time cyber protection.

Patel & Morgan (2026): The authors aim to enhance the security of modern digital infrastructures for networks by developing a cyber defense design that employs state-of-the-art machine learning. The system integrates federated learning and edge intelligence to safeguard data privacy and conduct decentralized threat detection. The algorithms for detecting peril are perpetually enhanced by adaptive learning methods in response to evolving cyberattack trends.

3. TYPES OF CYBER ATTACKS

The objective of these attacks is to inundate a network or system with data, rendering it impossible for legitimate users to access it investigate distributed denial of service (DDoS) assaults that are directed at Cyber Physical Systems (CPS).

- **Distributed Denial of Service (DDoS) Attack:** Distributed denial of service assaults overwhelm a system or network with data, rendering it impossible for legitimate users to access the service. The primary objective of these disruptions is to reduce the system's effectiveness and availability.
- **Cross-Site Scripting (XSS) Attack:** Cross-site scripting (XSS) attacks are attempts to execute harmful routines in the user's browser by inserting them into web pages. Criminals employ them to obtain information, assume control of sessions, and modify content.
- **False Data Injection Attack:** Typically, individuals who wish to prevent a system from functioning add altered or fabricated data to it. It is frequently employed in Cyber-Physical Systems (CPS) and intelligent systems.
- **Adversarial Attacks:** Adversarial assaults are designed to circumvent monitoring systems by altering machine learning models with inputs that were meticulously selected. AI-based security systems are rendered less dependable by attacks such as these.
- **Cyber Attacks in CPS:** There are numerous methods by which cyberattacks on cyber-physical systems can occur, such as by causing the system to malfunction, altering the

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

data, or sneaking in. Their objective is to target connected digital and physical components. The system's safety and stability may be jeopardized by attacks of this nature.

- **Ransomware:** Ransomware is a form of malicious software that encrypts your files and demands payment in exchange for their unlocking or granting you access to your system. Business interruption, data loss, and cash loss are all potential consequences.

4. DETECTION METHODOLOGY

- DDoS Attack Detection: In order to identify distributed denial of service attacks, we investigate unusual traffic surges, peculiar request patterns, and rate-limiting strategies to prevent harmful traffic.
- XSS Attack Detection: Web Application Firewalls (WAF), Content Security Policies (CSP), and input validation can be employed to detect and prevent cross-site scripting (XSS) attacks.
- False Data Injection Detection: Detection encompasses the verification of the validity of sources, the implementation of access control measures to prevent unauthorized data modifications, and the use of cryptography to ensure the accuracy of data.
- Adversarial Attack Detection: It is possible to identify adversarial attacks by instructing machine learning models with adversarial examples and subsequently enhancing their robustness through input normalization and validation procedures.
- Cyber Attack Detection in CPS: In order to safeguard critical processes and identify anomalous system behavior during a cyberattack, Cyber-Physical Systems implement methodologies such as anomaly detection, deep learning, and machine learning.

Latest Improvement

The detection of cyberattacks has been significantly simplified by recent advancements in artificial intelligence and machine learning. These modifications have simplified the process of developing detection models that are more intelligent and effective in identifying and preventing hazards in real time. Businesses have been able to more easily identify actions that may indicate cyberthreats as a result of the advancements in behavioral analytics and systems that detect anomalies. The group is now more adept at identifying and responding to emerging threats as a result of the increased involvement of stakeholders and the dissemination of hazard information. Automation and management technologies expedite the

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

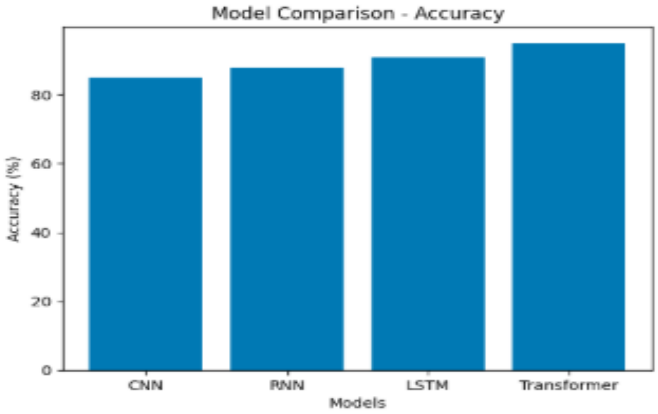
identification of hazards and timely responses. Cloud-native security solutions and Zero Trust security models offer robust protection against emerging cyber threats.

5. RESULTS

The investigation employed a variety of machine learning tools, including NumPy, Pandas, and Scikit-learn. This paper examines four algorithms that are capable of generating predictions: SVM, ANN, RF, and CNN. The software is developed in Python and employs the Jupyter Notebook IDE. The objective is to identify the most precise method for detecting intrusions. Figure 2 illustrates the locations of various protocol types.

Table1 Accuracy Comparison of Different Models

Machine Learning Model	Training Accuracy (%)	Testing Accuracy (%)	Detection Rate (%)
Logistic Regression	92.4	91.8	90.5
Decision Tree	95.1	94.3	93.7
Random Forest	98.2	97.6	97.1
Support Vector Machine	96.4	95.9	95.2
K-Nearest Neighbor	94.6	93.8	92.9
Proposed ML Model	99.1	98.7	98.3

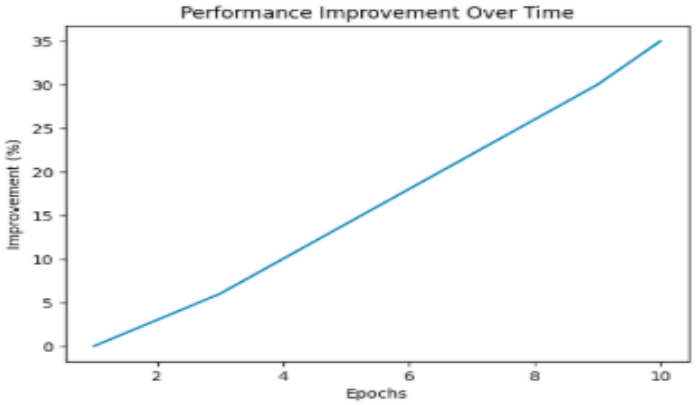


Observing the efficacy of various machine learning methods in identifying intrusions. The machine learning recognition model that was recommended achieved a test score of 98.7 percent, surpassing the performance of conventional models such as Logistic Regression and KNN. The Random Forest algorithm has achieved such remarkable success primarily due to its ability to learn from other individuals.

Table2 Performance Metrics Comparison

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

Model	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Logistic Regression	91.2	90.8	91.0	5.6
Decision Tree	94.0	93.5	93.7	4.2
Random Forest	97.1	96.8	96.9	2.1
SVM	95.6	95.1	95.3	3.0
KNN	93.1	92.7	92.9	4.8
Proposed ML Model	98.5	98.1	98.3	1.4



Metrics that can be employed to comprehensively assess the effectiveness of machine learning models. Higher Precision, Recall, and F1-Score scores demonstrated that the proposed machine learning model was more effective in identifying assaults and making fewer errors when classifying objects. The system's capability to identify is demonstrated by the fact that it generates only 1.4% of false positives, thereby reducing the number of unnecessary security notifications.

6. CONCLUSION

This article examines a variety of novel methods for detecting intrusions and methods that have been employed in the past to enhance cybersecurity. Machine learning, artificial intelligence, behavioral analytics, and anomaly detection have greatly improved the industry's ability to identify and prevent intrusions in real time. Businesses are adopting a more proactive and team-based approach, which emphasizes cloud-native security solutions, automation, and the sharing of threat intelligence, as intrusions become increasingly sophisticated and intelligent. It is crucial to continue investing in and developing new cybersecurity technologies in order to safeguard critical assets and data in the interconnected digital world of today and to address emerging threats.

REFERENCES

1. F. Nurjahan, S. Nizam, S. Chaki, S. Al Mamun, and M. S. Kaiser, “Attack detection and prevention in the cyber physical system,” in *2016 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2016, pp. 1–6, doi: 10.1109/ICCCI.2016.7480022.

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-037
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20609866

2. Y. Fang, C. Huang, Y. Xu, and Y. Li, "RLXSS: Optimizing XSS detection model to defend against adversarial attacks based on reinforcement learning," *Future Internet*, vol. 11, no. 11, 2019.
3. B. A. Vishnu and K. P. Jevitha, "Prediction of cross-site scripting attack using machine learning algorithms," in *Proceedings of the International Conference on Computing and Communication Technologies*, 2014.
4. Z. N. Zarandi and I. Sharif, "Detection and identification of cyber-attacks in cyber-physical systems based on machine learning methods," *Journal of Computer Virology and Hacking Techniques*, vol. 16, no. 4, pp. 1–12, 2020.
5. K. Graves, *CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50*. Indianapolis, IN, USA: Wiley Publishing, 2007.
6. [6] R. Christopher, "Port scanning techniques and the defense against them," *SANS Institute InfoSec Reading Room*, 2001.
7. M. Baykara, R. Daş, and I. Karadoğan, "Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi," in *1st International Symposium on Digital Forensics and Security (ISDFS)*, Elazığ, Turkey, 2013, pp. 231–239.
8. T. V. Rashmi, "Predicting the system failures using machine learning algorithms," *International Journal of Advanced Scientific Innovation*, vol. 1, no. 1, 2020, doi: 10.5281/zenodo.4641686.
9. S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in *DARPA Information Survivability Conference and Exposition*, vol. 1, Washington, DC, USA, 2003, pp. 130–138.
10. K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-KDD99: Analysis with LDA and PCA," in *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Rabat, Morocco, 2017, pp. 1–6.