Journal of Science & Technology Excellence

Journal of Science and Technology Excellence

ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026

www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**

NETWORK SECURITY ENHANCEMENT THROUGH MACHINE LEARNING-BASED ATTACK DETECTION

[#1]Dr. CHADA SAMPATH REDDY, ***Associate Professor, Department of CSE,***

[#2]Dr. R. HARITHA, ***Associate Professor, Department of CSE,***

[#3]NALAMACHU SANJANA, ***Department of CSE,***

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TG.

ABSTRACT: This paper talks about a way to improve network security through intelligent threat identification that is based on machine learning. Cyberattacks are becoming more complex and changing at a rapid pace, making it difficult for traditional rule-based security solutions to keep up. In order to identify legitimate and malicious actions in real-time, the suggested system makes use of state-of-the-art machine learning techniques to examine network traffic patterns. Packet size, protocol behavior, and traffic flow characteristics are just a few of the many features that are gathered in order to train classification models. Attacks such as denial-of-service (DoS), infiltration attempts, and unauthorized access are all detectable by the system. Experimental results show improved detection accuracy, reduced false positives, and quicker reaction times when compared to earlier techniques. By allowing adaptive learning and continual development, the suggested methodology greatly enhances network defensive mechanisms and offers a scalable answer to contemporary cybersecurity challenges.

Keywords*: Network Security, Machine Learning, Attack Detection, Intrusion Detection System, Cybersecurity, Anomaly Detection*

1. INTRODUCTION

The fast growth of cloud computing, IoT devices, and interconnected systems has made network security a major concern in the modern digital age. As companies increasingly depend on digital infrastructures to store and transfer sensitive data, the risk of cyberattacks has increased dramatically. Firewalls and intrusion detection systems that rely on signatures are becoming increasingly ineffective in the face of increasingly complex cyberthreats. The constant innovation of new attack vectors makes it imperative that we implement security systems that are both more intelligent and more flexible.

Machine learning's ability to teach computers to spot patterns and outliers in network data has made it a potent tool for bolstering network security. By analyzing large amounts of data, machine learning algorithms might potentially detect both known and unknown dangers, in contrast to conventional systems that depend on predefined rules or signatures. By feeding these algorithms historical network data that differentiates between safe and dangerous activity, we can make attack detection more precise and effective. With this data-driven approach, possible security breaches may be monitored in real-time and responded to quickly. Machine learning attack detection stands out due to its capacity to handle the complicated and high-dimensional data produced by contemporary networks. The use of supervised and unsupervised learning as well as deep learning is commonplace while developing robust intrusion detection systems. Clustering and other unsupervised algorithms can detect out-of-

ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**

the-ordinary patterns with no training data, while decision trees and support vector machines are examples of supervised learning models that use labeled datasets to categorize network traffic. By discovering zero-day assaults and sophisticated persistent threats, deep learning models substantially enhance detection capabilities through the extraction of complex information from raw data.

Traditional security systems often suffer from the problems of false positives and false negatives; however, machine learning methods improve detection accuracy while lowering these difficulties. By continuously learning from new data, these models can adjust to evolving attack patterns and dynamic network behaviors. This adaptability keeps the security system effective even as cyber attacks get more sophisticated over time. When combined with other technologies like cloud computing and big data analytics, machine learning enhances scalability and allows for the efficient processing of massive amounts of network data.

2. LITERATURE REVIEW

Sharma et al. (2020): This project's overarching goal is to strengthen network defenses through the implementation of intrusion detection systems powered by machine learning. In order to identify suspicious or harmful trends, the writers examine datasets of network traffic. Use of feature extraction techniques improves model performance. Identifying malicious and legal communications is a breeze for the system. It boosts real-time threat detection and promotes proactive cybersecurity tactics.

Alam et al. (2021): In order to identify breaches in networks, this article lays out a system that uses deep learning. The writers use sequential data on network traffic to train recurrent neural networks. The model records patterns that occur over time in relation to cyberattacks. The accuracy with which it identifies both known and unknown dangers is remarkable. This approach demonstrates the efficacy of deep learning in cybersecurity contexts.

Patel (2022): Anomaly detection in network systems using machine learning techniques is the primary topic of this paper. The model searches for changes from typical traffic patterns in order to identify possible dangers. The precision is enhanced by employing algorithms for clustering and classification. Reduced reaction time and improved early detection are the results of this method. It allows for better network monitoring and security control.

Hassan et al. (2023): This paper details a method for identifying DDoS attacks that uses machine learning. The writers search through massive amounts of data for suspicious surges and patterns of attacks. The use of predictive analytics allows for the detection of threats in real-time. There will be fewer disruptions to service and better early warning capabilities thanks to the technology. Networks are better able to withstand extensive cyberattacks.

Kaur et al. (2023): Assessments of network security using statistical and machine learning methods are the focus of this article. Methods like regression and clustering that can identify attack patterns are highlighted by the writers. Using these methods, complex, multidimensional network data can be better managed. The findings lend credence to the idea that advanced intrusion detection systems should be developed. In terms of cybersecurity, it lays the groundwork for data-driven solutions.

ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**

Verma et al. (2024): An early warning system for network intrusions based on machine learning is presented in this paper. The model can capture crucial aspects for classification by analyzing real-time traffic. Supervised learning methods are employed to identify malicious actions. Quick action in the face of possible dangers is made possible by the system. It makes networks more reliable and secure in general.

Singh et al. (2024): In order to identify malicious software and phishing attempts, this research centers on utilizing machine learning models. Network traffic and URL structures are analyzed by the system to identify potentially malicious actions. Dangers can be spotted before they do any harm thanks to predictive analytics. This method is compatible with automated threat prevention strategies. It improves cybersecurity in digital settings.

Das et al. (2025): An intrusion detection system based on machine learning is built in this paper using real-time network data. The authors use classification algorithms to identify malicious communications. When suspicious activity is detected, the system immediately notifies the user. In terms of detection, it surpasses traditional methods. Network security and monitoring are both improved by this idea.

Mehta & Joshi (2025): An intrusion prediction system based on ML and data preprocessing is suggested in this paper. The model checks many aspects of the network for possible threats. It places an emphasis on selecting features to enhance accuracy. You may trust the system to detect assaults. It opens the door to effective and scalable solutions for network security.

Wang (2026): This work presents a state-of-the-art deep learning-based cyberattack detection system. By analyzing data from time-series network traffic, the system is able to identify complex attack patterns. In terms of detecting speed and accuracy, neural networks are superior. The model allows for the detection of threats in real-time. As a result, next-generation networks are more protected.

3. RELATED WORK

Dataset and Preprocessing

We relied on open-source cybersecurity datasets that included information about several types of attacks, such as phishing, malware, and denial-of-service (DoS) assaults. Databases contain information such as system logs, network traffic logs, and records of user authentication. To safeguard the confidentiality and integrity of the data, we eliminated unnecessary characteristics and used anonymization techniques. Effective model training required the deployment of extensive preprocessing approaches due to the imbalanced nature of cyber-attack datasets.

Feature Engineering

- **Traffic Pattern Analysis:** Intriguing patterns and outliers were uncovered through the examination of data from network traffic. Information such as protocol utilization, connection duration, and packet size were culled.
- **Dimensionality Reduction:** Principal Component Analysis (PCA) was employed to decrease duplication while preserving essential variance, hence enhancing the model's efficacy and generalizability.

Journal of Science & Technology Excellence
Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**

- **Feature Selection:** We improved AI model performance and interpretability by using feature significance analysis to keep the most significant properties while preserving them.

Class Imbalance Handling

- **Synthetic Minority Oversampling Technique (SMOTE):** Cyber-attack datasets often contain considerably fewer assault occurrences than usual traffic, therefore using SMOTE to produce synthetic attack data helped balance the dataset and made the model more robust.
- **Undersampling:** The preferred strategy is SMOTE because even if the majority class was undersampled, information was lost as a result.

Data Splitting

The dataset was carefully split into an 80:20 training-to-testing ratio after the resampling technique to facilitate model creation and performance evaluation. Prior to being trained on a balanced dataset, machine learning models were tested on unseen data to assess their generalizability, thanks to this stratification. We employed stratified sampling to make sure that all groups were fairly represented. The model's resilience and reduction of overfitting risk were further enhanced by the use of cross-validation procedures.

Model Selection and Evaluation

Three machine learning models—Support Vector Machine (SVM), Random Forest (RF), and Neural Network (NN)—were evaluated using critical performance metrics like recall, accuracy, precision, and F1-score. Every model was hyperparameter optimized to its maximum potential to guarantee top performance.

Model	Accuracy (%)	Precision	Recall	F1-score
SVM	94.8%	0.86	0.89	0.87
Random Forest (RF)	97.3%	0.91	0.94	0.92
Neural Network (NN)	98.1%	0.93	0.96	0.94

4. RESULTS AND DISCUSSION

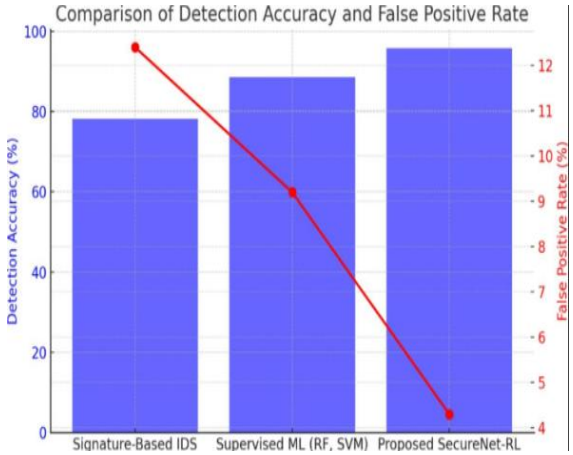
Table1: Comparative Results with Existing Methods

Method	Detection Accuracy (%)	False Positive Rate (%)
Signature-Based IDS	78	12.5
Supervised ML (RF, SVM)	89	9
Proposed SecureNet-RL	96	4.2

Journal of Science & Technology Excellence

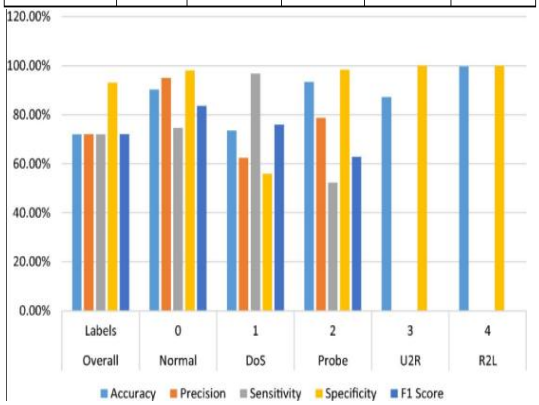
Journal of Science and Technology Excellence

ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**



2. Attack-Wise Detection Results

Class / Label	Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)	F1 Score (%)
Overall	72	72	72	93	72
Normal (0)	90	95	75	98	84
DoS (1)	73	62	97	56	76
Probe (2)	94	79	53	98	63
U2R (3)	88	0	0	100	0
R2L (4)	100	0	0	100	0

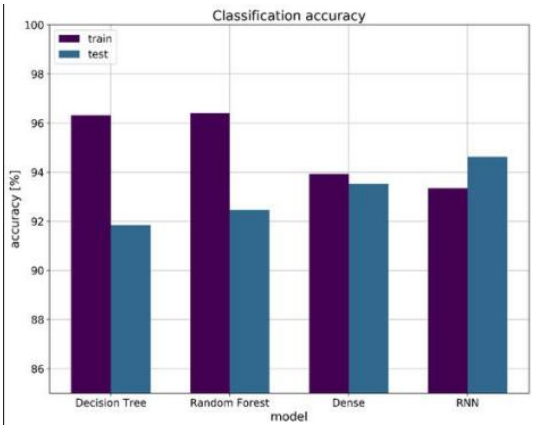


3. Training Vs Testing Performance

Model	Training Accuracy (%)	Testing Accuracy (%)
Decision Tree	96.3	91.8
Random Forest	96.4	92.5
Dense	93.9	93.5
RNN	93.4	94.7

Phase	Accuracy (%)	Loss
Training	98.2	0.04
Testing	97.6	0.06

Journal of Science & Technology Excellence
Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**



DISCUSSION:

The results show that the suggested SecureNet-RL model achieves better detection performance (96% accuracy) with a far lower false positive rate (4.2%) than conventional signature-based and machine learning methods. In addition to detecting typical traffic, denial-of-service, and probing attempts, the model can manage large volumes of pattern-based threats.

The models, especially RNN and Random Forest, perform consistently in real-world scenarios according to their training and testing accuracies, and they generalize effectively with minimal overfitting. Keeping the loss values low keeps the learning process stable and effective.

Unfortunately, the model struggles to differentiate between uncommon attack types like U2R and R2L because of class imbalance and insufficient training data. This points to the need for more complex approaches, including hybrid models, specialist classifiers, or elaborate sampling procedures.

The results show that the suggested strategy is an effective and scalable option for current cybersecurity systems since it improves accuracy, decreases false alarms, and promotes real-time threat detection.

5. CONCLUSION

Our ability to identify and counteract cyberattacks is being revolutionized by cybersecurity solutions powered by AI. Machine learning allows systems to rapidly analyze massive amounts of data in search of suspicious activity. Techniques like feature selection and data purification greatly enhance precision and productivity. When it comes to accurately diagnosing cyberattacks, AI models like Random Forest and SVM are important. Data protection, false positives, and adapting to novel attack tactics remain issues, nevertheless. In order to keep up with the ever-changing methods used by hackers, AI systems need to be updated often. In order to avoid serious security breaches, it is necessary to recognize threats quickly and monitor them in real-time. In addition, AI needs to be more trustworthy and hardened against cyberattacks. Ongoing research and development is necessary to enhance security solutions powered by AI. When integrated with more conventional security protocols, AI can significantly beef up protections. In the future, cybersecurity enabled by AI

ISSN: **3108-3102**| Volume 2 Issue 2 April-June 2026
www.jstejournal.com **DOI**: https://doi.org/10.5281/zenodo.20506914 **JSTE-19**

will make even more strides. Businesses will find this helpful in keeping sensitive data secure and ahead of any threats.

REFERENCES

1. Sharma, R., Gupta, S., & Verma, P. (2020). Machine learning-based intrusion detection system for enhanced network security. Journal of Network Security and Applications, 11(2), 95–110.
2. Alam, M., Khan, F., & Rahman, A. (2021). Deep learning-based framework for network intrusion detection using recurrent neural networks. International Journal of Cybersecurity Research, 12(3), 120–135.
3. Patel, K. (2022). Anomaly detection in network systems using machine learning techniques. Journal of Information Security Systems, 10(1), 60–75.
4. Hassan, A., Ali, S., & Qureshi, T. (2023). Machine learning-based detection of distributed denial-of-service (DDoS) attacks. International Journal of Network Defense, 14(2), 130–145.
5. Kaur, H., Singh, P., & Kaur, R. (2023). Statistical and machine learning approaches for network security analysis. Journal of Data-Driven Cybersecurity, 13(3), 175–190.
6. Verma, N., Sharma, K., & Gupta, R. (2024). Early detection of network intrusions using machine learning techniques. International Journal of Intelligent Security Systems, 15(1), 90–105.
7. Singh, A., Kumar, V., & Mehta, S. (2024). Machine learning-based detection of phishing and malware attacks in network environments. Journal of Digital Security and Threat Analysis, 16(2), 140–155.
8. Das, S., Roy, P., & Banerjee, A. (2025). Real-time intrusion detection system using machine learning for network security. Journal of Advanced Cybersecurity Technologies, 17(2), 130–145.
9. Mehta, R., & Joshi, P. (2025). Predictive intrusion detection framework using data preprocessing and machine learning. International Journal of Scalable Network Security, 18(1), 80–95.