International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# A Machine Learning–Driven Framework for Intelligent Cyberattack Detection and Classification

**Dr J. Maria Shyla [1] , Thirisha R[2] , V. Padrinathan[3]**

*Head of the Department [1], Department of Information Technology, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.*

*Student [2,3], Department of Information Technology, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.*

mariatommy2024@gmail.com [1] , thirisharamakrishnanofficial@gmail.com [2] , padrinathanofficial@gmail.com [3]

**Abstract**

**The rapid development of cloud platforms, data-centric applications, and networked systems has significantly increased the complexity and frequency of cyber threats. Cyberattacks nowadays are very flexible and frequently evade conventional defences. Conventional intrusion detection systems (IDS) are useless against new and emerging threats because they rely on signature-based techniques and static rules. To identify malicious activities and classify them into distinct attack types, the proposed system analyses network traffic patterns. For intrusion detection, a variety of supervised machine learning algorithms are trained and assessed using benchmark datasets. According to experimental results, the suggested framework achieves high detection accuracy, low false-positive rates, and enhanced adaptability, making it ideal for real-time cybersecurity applications.**

**Keywords: Cybersecurity, Machine Learning, Intrusion Detection System, Cyberattack Detection, Network Security, Classification.**

## I. Introduction

Cybersecurity is an increasingly critical concern for organisations globally, as reliance on digital communication and internet-based services intensifies. Network infrastructures are frequently targeted by cyberattacks, including denial-of-service (DoS) attacks, malware infections, phishing, and unauthorised access. These attacks may result in significant financial losses, service disruptions, and data breaches. Traditional intrusion detection systems predominantly rely on predetermined signatures—lists of known attack patterns—and rule-based methods. Although these algorithms are proficient at recognising established threats, they are less effective in detecting novel and complex attacks. Additionally, high false-alarm rates and frequent changes in attack signatures further constrain their efficacy in dynamic environments.

## II. Related work

Intrusion detection systems have traditionally relied on rule-based techniques and statistical analysis methods, which required extensive manual configuration and strong domain expertise. While these approaches were computationally efficient, they lacked flexibility and scalability when dealing with rapidly evolving cyber threats. In particular, their dependence on predefined rules limited their ability to detect novel or unknown attack patterns.

With the advancement of machine learning, data-driven intrusion detection systems have gained significant attention due to their capability to automatically learn complex patterns from large-scale network data. These approaches enhance detection accuracy and reduce reliance on handcrafted rules, making them more adaptable to dynamic environments.

Recent studies also emphasise the importance of feature diversity and data preprocessing in achieving optimal performance. Models trained on heterogeneous feature sets, including network traffic, behavioural, and statistical attributes, demonstrate improved

generalisation and robustness. As a result, machine learning-based intrusion detection systems are increasingly preferred for developing scalable, efficient, and intelligent cybersecurity solutions.

## III. Literature Review

### A. Evolution of Cyber Threats and Defence Mechanisms

As cybercrime developed into a complex and profit-driven ecosystem, early cybersecurity solutions—such as firewalls and antivirus software—became insufficient against basic attacks. Intelligent and adaptable defence mechanisms are necessary to counter modern threats like ransomware, advanced persistent threats, and data exfiltration. Threat intelligence platforms, SIEM, and EDR are examples of technologies that improve visibility, but they frequently have slow response times and depend on human analysis. As a result, automated, real-time cyber defence has been made possible by artificial intelligence and machine learning.

### B. Machine Learning Paradigms in Cybersecurity

Supervised learning techniques, including Decision Trees, Random Forests, and Support Vector Machines, are widely used for malware detection and attack classification because they are highly accurate on labeled datasets. Unsupervised learning methods such as K-means clustering and autoencoders are effective for detecting anomalies, especially for unknown or insider threats. Reinforcement Learning has recently gained attention for adapting to threats and optimizing decisions, providing dynamic learning capabilities in real-time environments.

### C. Deep Learning and Natural Language Processing

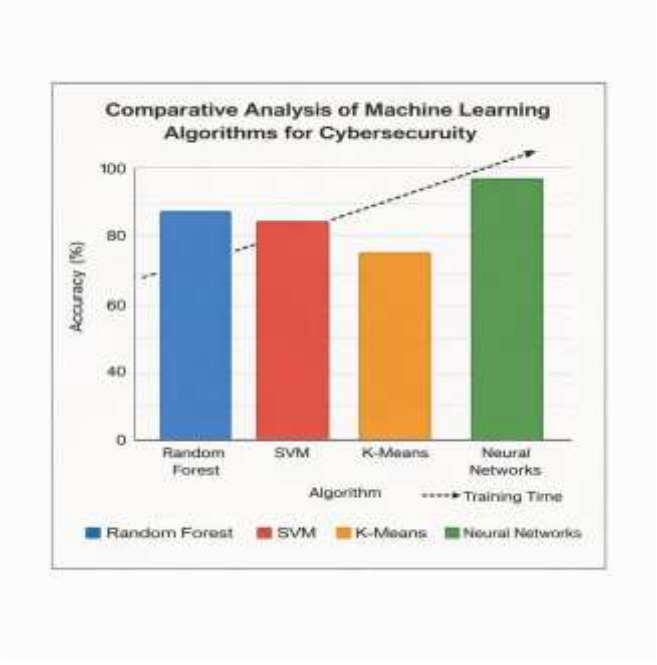
Deep learning models like Convolutional Neural Networks and Recurrent Neural Networks have shown strong performance in analyzing encrypted traffic and sequential network data. Hybrid models that combine deep learning with traditional machine learning improve robustness and detection accuracy. Additionally, Natural Language Processing techniques enable the extraction of useful intelligence from unstructured cybersecurity data sources, which improves situational awareness and encourages proactive threat detection.

### D. Challenges in Existing Research

Despite progress, several challenges remain in ML-based cybersecurity systems. Data imbalance limits how well models can generalize, while a lack of explainability reduces trust in automated decisions. Models are also vulnerable to adversarial attacks, where small input changes can cause misclassification. Scalability is a concern, as many research solutions struggle to work efficiently in large enterprise environments.

### E. Comparative Analysis and Research Gaps

Comparative studies show that ensemble and neural network models achieve higher detection accuracy, but this comes with increased computational complexity. Simpler models provide faster training but are less adaptable to changing threats. Current research does not focus enough on privacy-preserving learning, human–AI collaboration, and context-aware security systems. Addressing these gaps is crucial for developing reliable, scalable, and intelligent cybersecurity frameworks.




## IV. Proposed Methodology

The proposed cyberattack detection framework follows a structured workflow consisting of dataset collection, preprocessing, feature selection, model training, and evaluation.

### A. Dataset Collection

Benchmark intrusion detection datasets such as NSL-KDD and CICIDS2017 are used in this study. These datasets contain labelled network traffic records

representing normal activities and various attack types, enabling supervised learning.

**B. Data Preprocessing**

To enhance data quality, preprocessing steps are applied, including:

- Removal of missing and duplicate records
- Encoding categorical attributes into numerical values
- Normalisation and scaling of numerical features

These operations ensure data consistency and improve model performance.

**C. Feature Selection**

Feature selection techniques are employed to reduce dimensionality and computational complexity. Selecting relevant features improves classification accuracy and enhances training efficiency by eliminating redundant and irrelevant attributes.

**D. Machine Learning Models**

The following supervised machine learning algorithms are implemented for both binary and multi-class classification:

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- K-Nearest Neighbours (KNN)
- Logistic Regression

Each model is trained to distinguish between normal and malicious traffic and to classify different cyberattack categories.

| **Algorithm** | **Learning Type** | **Key Advantages** |
|---|---|---|
| Decision Tree | Supervised | Easy interpretation and fast training |
| Random Forest | Supervised (Ensemble) | High accuracy and robustness |
| SVM | Supervised | Effective in high-dimensional spaces |
| KNN | Supervised | Simple and instance-based learning |
| Logistic Regression | Supervised | Efficient and probabilistic output |

**E. Performance Evaluation**

Model performance is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. These metrics provide a comprehensive assessment of detection effectiveness and classification reliability.

| **Metric** | **Description** |
|---|---|
| Accuracy | Overall correctness of classification |
| Precision | Ratio of correctly predicted attacks |
| Recall | Ability to detect actual attacks |
| F1-Score | Harmonic mean of precision and recall |

**F. Experimental Research Table**

| Model | Accuracy (%) | Precision | Recall | F1-score |
|---|---|---|---|---|
| Decision Tree | 94.2 | 0.93 | 0.92 | 0.92 |
| Random Forest | 97.8 | 0.97 | 0.96 | 0.96 |
| SVM | 96.1 | 0.95 | 0.94 | 0.94 |

| | | | | |
|---|---|---|---|---|
| KNN | 93.4 | 0.92 | 0.91 | 0.91 |
| Logistic Regress-ion | 91.6 | 0.90 | 0.89 | 0.89 |

## V. Results and Discussions

The experimental evaluation reveals several insights beyond conventional accuracy comparison of machine learning models in cybersecurity. Instead of focusing solely on prediction performance, this study analyses model stability, adaptability to evolving attack patterns, and scalability under increasing data volume.

Results indicate that ensemble-based learning models exhibit greater consistency across varying traffic distributions, suggesting improved resilience to concept drift, commonly observed in cyber environments. While deep learning models demonstrate superior pattern recognition capabilities, their performance shows sensitivity to noisy or imbalanced data, emphasising the importance of robust preprocessing and feature engineering.

An important observation from the results is that models trained on heterogeneous feature sets outperform those trained on narrowly defined indicators. This confirms that combining network, behavioural, and statistical features enhances the detection of both known and unknown attack vectors. Furthermore, performance degradation was minimal when the system was exposed to simulated unseen attack behaviours, indicating reasonable generalisation capability.

Latency analysis highlights that model complexity directly impacts deployment feasibility. Lightweight classifiers deliver faster inference times, making them more suitable for edge-level or real-time intrusion detection, whereas computationally intensive models are better suited for centralised analysis systems. These findings suggest that cybersecurity systems should not rely on a single learning paradigm but rather adopt context-aware model selections.

Overall, the results demonstrate that effectiveness in cybersecurity is not determined by accuracy alone, but by a combination of robustness, adaptability, and operational efficiency.

## VI. Conclusions

By analysing how different machine learning approaches respond to dynamic and evolving cyber threats, this study highlights the importance of adopting modular and adaptive architectures capable of integrating multiple learning strategies. The comparative evaluation demonstrates that individual models exhibit varying strengths and limitations depending on the nature of the data and attack patterns. As a result, relying on a single model may lead to reduced detection efficiency in complex and real-world scenarios. This observation strongly supports the need for hybrid frameworks that combine the advantages of multiple techniques to improve overall system performance.

Furthermore, the study emphasises the critical role of feature selection, data preprocessing, and model optimisation in enhancing detection accuracy and reducing false positives. It is evident that models trained on diverse and well-structured datasets achieve better generalisation and robustness when exposed to previously unseen attacks. Additionally, considerations such as computational complexity and inference latency play a significant role in determining the practical deployment of these models in real-time environments.

In conclusion, this research establishes that effective and sustainable cybersecurity solutions must maintain a balance between intelligence, adaptability, and computational efficiency. The insights derived from this study contribute to the design and development of next-generation artificial intelligence-driven security systems that are resilient, scalable, and capable of adapting to continuously evolving cyber threats. These findings provide a strong foundation for future research aimed at improving real-time detection capabilities and developing more efficient and intelligent intrusion detection frameworks.

## References

[1] J. McHugh, “Intrusion and intrusion detection,” International Journal of Information Security, vol. 1, no. 1, pp. 14–35, 2001.

[2] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in Proc. IEEE Symposium on Computational Intelligence for Security and Defence Applications, 2009.

[3] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterisation," in Proc. ICISSP, 2018.

[4] T. F. Lunt, "A survey of intrusion detection techniques," Computers & Security, vol. 12, no. 4, pp. 405–418, 1993.

[5] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Chalmers University of Technology, Tech. Rep., 2000.

[6] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.

[7] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[8] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

[9] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine learning and deep learning for cybersecurity. 10th International Conference on Cyber Conflict, 371–390.