Anomaly-Based Intrusion Detection Systems Using Machine Learning Techniques

Enhancing Network Security Through Intelligent Threat Detection

Snehal Nandkumar Dhaybar
Aishwarya Shivaji Naikare
Rohan Santosh Bankhele
Department of Computer Science
Dr. D.Y. Patil Arts, Commerce and Science College, Pimpri

Abstract

Intrusion Detection Systems (IDS) play a crucial role in safeguarding modern digital infrastructures. Traditional signature-based systems are limited in detecting zero-day and evolving cyber threats. This paper presents a journal-formatted study on anomaly-based intrusion detection systems using machine learning techniques. The study evaluates supervised, unsupervised, and deep learning models for intrusion detection, discusses federated learning approaches for distributed security, and highlights challenges such as high false positives, dataset limitations, adversarial attacks, and encrypted traffic monitoring. The findings suggest that machine learning-based IDS significantly improves detection accuracy, adaptability, and scalability in modern network environments.

Keywords

Intrusion Detection System, Machine Learning, Anomaly Detection, Cybersecurity, Federated Learning, Deep Learning

1. Introduction

With the rapid growth of cloud computing, IoT devices, and distributed network architectures, cybersecurity challenges have become increasingly complex. Traditional intrusion detection systems rely on predefined signatures, making them ineffective against novel and zero-day attacks. Anomaly-based IDS models overcome this limitation by learning normal behavior patterns and identifying deviations. Machine learning techniques enhance this process by modeling complex traffic patterns and adapting to evolving threats in real time.

2. Literature Review

The foundation of intrusion detection research was established by Denning (1987), who introduced anomaly detection concepts. Subsequent research integrated machine learning techniques such as Decision Trees, Support Vector Machines (SVM), Artificial Neural Networks, and ensemble methods. Recent studies emphasize deep learning models including CNN, RNN, and LSTM, which provide improved detection capabilities for large-scale network environments.

3. Methodology

The proposed approach utilizes machine learning-based anomaly detection techniques. Supervised learning models classify labeled traffic data, unsupervised models identify unknown anomalies, and deep learning techniques capture complex traffic patterns. The system architecture includes data collection, feature extraction, model training, anomaly detection, and alert generation.

4. Results and Discussion

Machine learning models demonstrate improved detection accuracy compared to traditional systems. Deep learning approaches achieve higher precision in detecting sophisticated threats. However, challenges such as false positive rates, computational overhead, and dataset imbalance affect performance. Federated learning shows promise for privacy-preserving distributed intrusion detection.

5. Limitations

Despite improved performance, anomaly-based IDS faces several limitations including difficulty in defining normal network behavior, limited generalization across different networks, vulnerability to adversarial attacks, and dependence on high-quality datasets.

6. Future Work

Future research should focus on developing modern benchmark datasets, implementing federated and distributed learning approaches, enhancing encrypted traffic analysis techniques, and improving computational efficiency for real-time deployment.

7. Conclusion

Anomaly-based intrusion detection systems powered by machine learning provide a robust and scalable solution for modern cybersecurity challenges. By leveraging advanced algorithms and distributed learning approaches, IDS systems can effectively detect evolving cyber threats while maintaining privacy and scalability.

Acknowledgement

The authors express their sincere gratitude to the Department of Computer Science, Dr. D.Y. Patil Arts, Commerce and Science College, Pimpri, for providing guidance, resources, and academic support throughout the completion of this research work. We also thank our faculty members for their valuable suggestions and encouragement.

References

[1] Denning, D. E., 'An Intrusion-Detection Model,' IEEE Transactions on Software Engineering, 1987.

[2] Anderson, J. P., 'Computer Security Threat Monitoring and Surveillance,' 1980.

[3] Tavallaee, M. et al., 'A detailed analysis of the KDD CUP 99 dataset,' 2009.

[4] Ferrag, M. A. et al., 'Deep Learning for Cybersecurity Intrusion Detection: Approaches and Datasets,' 2020.

System Architecture Diagram

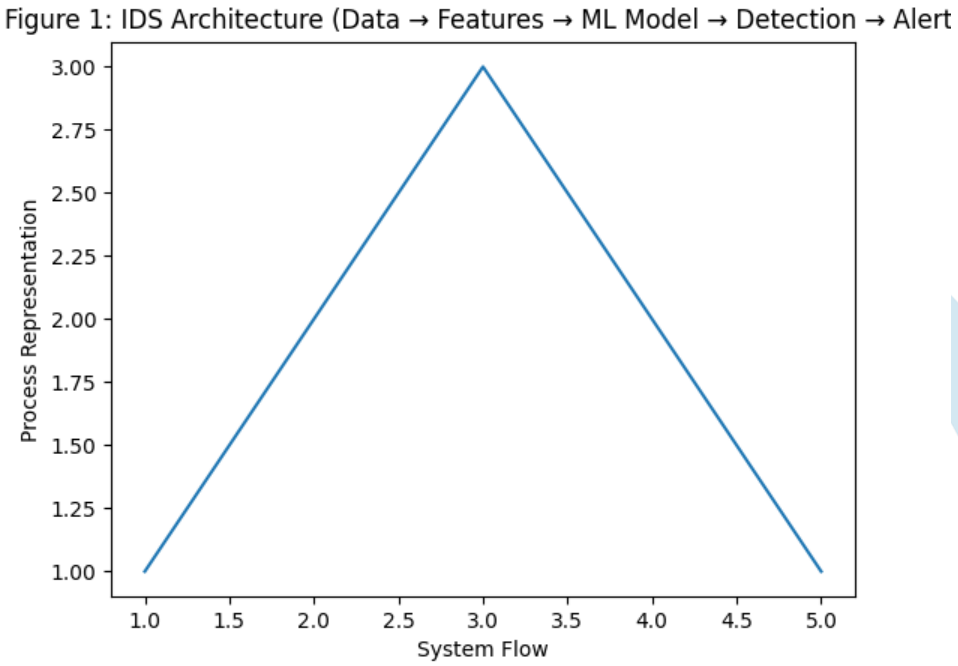

Figure 1: Proposed Anomaly-Based IDS Architecture

Machine Learning Workflow Diagram

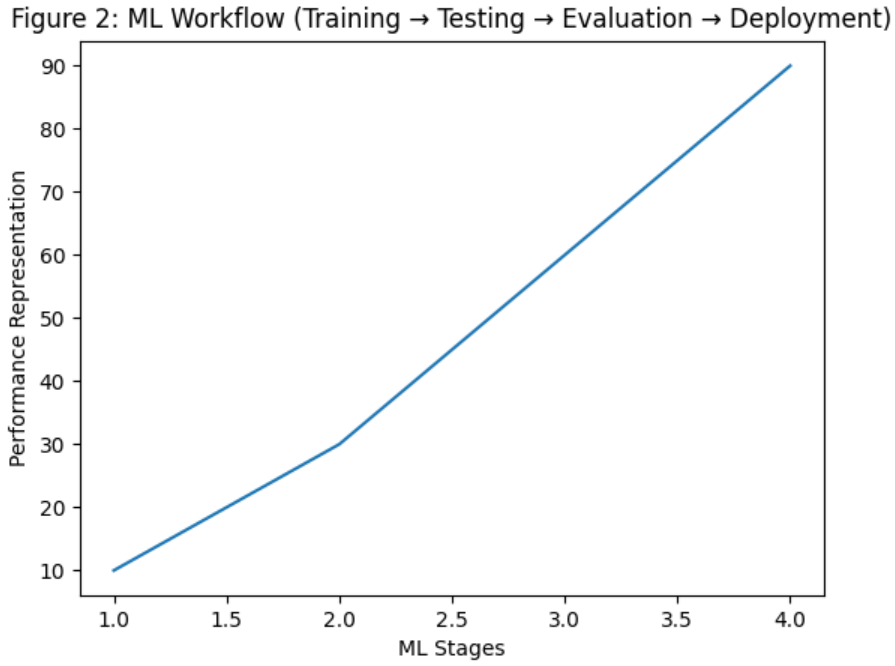

Figure 2: Machine Learning Workflow for Intrusion Detection

Federated Learning Framework Diagram

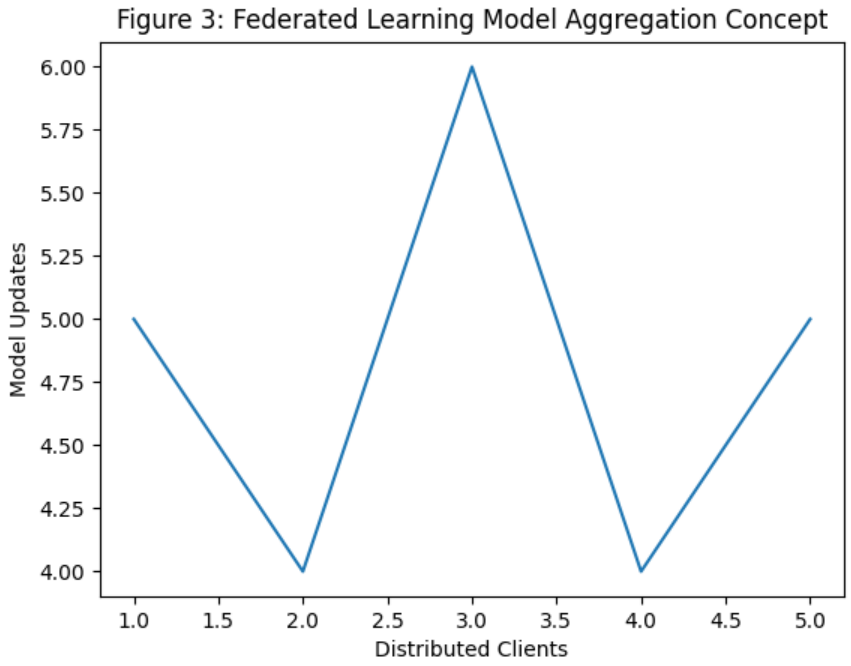

Figure 3: Federated Learning-based Distributed IDS Model