

Network Traffic Analysis using Random Forest Algorithm

Deepali Gobare¹, Ankita Patil², Sahil Pawar³, Ravi Tarate⁴, Prof. Mayuri Agrawal⁵

UG Students, Department of Computer Engineering^{1,2,3,4}

Professor, Department of Computer Engineering⁵

Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Savitribai Phule Pune University, Pune, India

Abstract: *The purpose of project "Network Traffic Detection Using Machine Learning" is to identifying cybersecurity measures and optimizing network performance. In an increasingly interconnected digital landscape, the security and efficiency of network communications are paramount. Network traffic detection using machine learning has emerged as a powerful tool in fortifying cybersecurity measures and optimizing network performance. This report delves into the application of machine learning algorithms for real-time analysis of network data, enabling the identification of anomalies indicative of potential threats. Through a comprehensive exploration of key components, benefits, and considerations, this report aims to provide a detailed understanding of the implementation and impact of machine learning in network traffic detection. By addressing crucial aspects such as data privacy, model accuracy, and scalability, organizations can effectively harness the potential of machine learning to bolster their network security measures. Through insightful analytics and timely threat mitigation, this approach promises to revolutionize the way networks are safeguarded against evolving cyber threats. This report serves as a comprehensive guide for organizations seeking to enhance their cybersecurity posture through the integration of machine learning in network traffic detection.*

Keywords: Network Traffic Analysis, Random Forest Algorithm, Anomaly Detection, Machine Learning

REFERENCES

- [1] Wenke Lee, Sal Stolfo, and Kui Mok, "Adaptive Intrusion Detection: A Data Mining Approach", Artificial Intelligence Review, Kluwer Academic Publishers, 14(6):533-567, December 2000.
- [2] Wenke Lee and Salvatore J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems", ACM Transactions on Information and System Security (TISSEC), Volume 3, Issue 4, November 2000.
- [3] Wenke Lee, Sal Stolfo, Phil Chan, Eleazar Eskin, Wei Fan, Matt Miller, Shlomo Hershkop, and Junxin Zhang, "Real Time Data Mining-based Intrusion Detection", The 2001 DARPA Information Survivability Conference and Exposition (DISCEX II), Anaheim, CA, June 2001.
- [4] W. Lee and S. J. Stolfo, "Data Mining Approaches for Intrusion Detection", the 7th USENIX Security Symposium, San Antonio, TX, January 1998.
- [5] Yongguang Zhang, Wenke Lee, and Yi-An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, Volume 9, Issue 5, September 2003.
- [6] Charles Elkan, "Results of the KDD'99 Classifier Learning", SIGKDD Explorations 1(2): 63-64, 2000.
- [7] L. Breiman, "Random Forests", Machine Learning 45(1):5-32, 2001.
- [8] Daniel Barbarra, Julia Couto, Sushil Jajodia, Leonard Popyack, and Ningning Wu, "ADAM: Detecting Intrusions by Data Mining", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security T1A3 1100 United States Military Academy, West Point, NY, June 2001.