

# Anomaly Detection System

**Prof. K. G. Jagtap,**

Professor, Department of AI & ML  
AISSMS Polytechnic, Pune, India

**Shreeram Shinde**

Student, Department of AI & ML  
AISSMS Polytechnic, Pune, India

**Akshay Adhav**

Student, Department of AI & ML  
AISSMS Polytechnic, Pune, India

**Sahil Kadambande**

Student, Department of AI & ML  
AISSMS Polytechnic, Pune, India

**Abstract:** *The "Network Anomaly Detection System" is a sophisticated software program designed to safeguard computer networks from malicious activities aimed at unauthorized access, data theft, or compromising network agreements. Existing Advanced Detection System (ADS) technologies, despite their effectiveness, face challenges in handling the dynamic and complex security attacks orchestrated by hackers in contemporary computer networks. The pivotal factor influencing the system's efficacy is accuracy, particularly in the context of login activities. With the exponential increase in the volume of data transmitted over the Internet due to the gradual expansion of technology utilization, the imperative to secure this data has become paramount. In response to this, the proposed anomaly detection system (ADS) emerges as a crucial solution by actively monitoring and analyzing data to detect virtual security threats. As intruders deploy diverse methods to infiltrate networks, the ADS is poised to identify anomalies within the system or network proactively. Significantly, the system leverages cutting-edge technology, specifically machine learning algorithms, to classify and detect assaults in real-time. The emphasis is on determining the most appropriate machine learning technique for recognizing the specific nature of the attack, highlighting an adaptive and forward-looking approach to network security. In essence, the "Network Anomaly Detection System" represents a proactive and adaptive defense mechanism, utilizing the power of machine learning to address the evolving landscape of cyber threats in computer networks. Positioned as the final safeguard following a series of preventive measures, anomaly detection plays a crucial role in identifying and thwarting attacks that may have evaded earlier security measures*

**Keywords:** Anomaly Detection System, Network Anomaly Detection System, Secure data, Cyber threats, Intruders, Secure data, Data theft, Accuracy

## REFERENCES

- [1] Hurley, T.; Perdomo, J.E.; Perez-Pons, "A. HMM-Based Intrusion Detection System for Software Defined Networking. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 617–621. 2.
- [2] Shone, N.; Ngoc, T.N.; Phai, V.D.; Shi, "Q. A Deep Learning Approach to Network Intrusion Detection", IEEE Trans. Emerg. Top. Comput. Intell. 2018, 2, 41– 50. 3.
- [3] Gomez, J.; Gil, C.; Banos, R.; Marquez, A.L.; Montoya, F.G.; Montoya, M.G. A, "Pareto-based multi-objective evolutionary algorithm for automatic rule generation in network intrusion detection systems", Soft Comput. 2013, 17, 255–263.
- [4] Sangeetha, S.; Gayathri devi, B.; Ramya, R.; Dharani, M.K.; Sathya, P. Signature Based Semantic Intrusion Detection System on Cloud. In Information Systems Design and Intelligent Applications; Mandal, J.K., Satapathy, S.C., Kumar Sanyal, M., Sarkar, P.P., Mukhopadhyay, A., Eds.; Springer: New Delhi, India, 2015; pp. 657–666.
- [5] Dey, S.K.; Rahman, M.M. , "Effects of Machine Learning Approach in Flow-Based Anomaly Detection on Software-Defined Networking", IEEE 2020

- [6] Vipin, Das & Vijaya, Pathak & Sattvik, Sharma & Sreevathsan & MVVNS. Srikanth & Kumar T, Gireesh, "Network Intrusion Detection System Based On Machine Learning Algorithms", International Journal of Computer Science & Information Technology, 2010
- [7] Choi, J & Choi, Chang & Ko, Byeongkyu & Choi, D & Kim, "Detecting web based Ddos attack using mapreduce operations in cloud computing environment" Journal of Internet Services and Information Security, 2013
- [8] Baig, Zubair & Baqer, M & Khan, Asad, "A Pattern Recognition Scheme for Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks", 2006
- [9] Analyzing Log Files for Post-mortem Intrusion Detection Gamboa, Karen & Monroy, Raúl & Trejo, Luis & Aguirre Bermúdez, Eduardo & Mex-Perera, Carlos. (2012), IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)
- [10] Network Traffic Analysis and Intrusion Detection Using Packet Sniffer Qadeer, Mohammed & Iqbal, Arshad & Zahid, Mohammad & Siddiqui, Misbahur, Communication Software and Networks