

# Machine Learning Based IoT Network Intrusion Detection Classification

**Dr. Jyoti Deshmukh<sup>1</sup>, Pooja Hargude<sup>2</sup>, Divya Ghate<sup>3</sup>, Sacchidanand Linge<sup>4</sup>, Rahul Mahajan<sup>5</sup>**

Faculty, Department of Computer Engineering / Information Technology<sup>1</sup>

Students, Department of Computer Engineering / Information Technology<sup>2,3,4,5</sup>

G H Raison Institute of Engineering and Technology, Pune, Maharashtra, India

**Abstract:** *IoT network is a promising technology, IoT implementation is growing rapidly but cybersecurity is still a loophole, detection of attacks in IOT infrastructures is a growing concern in the field of IoT. With the increased use of Internet of Things in different areas, cyber-attacks are also increasing proportionately and can cause failures in the system. IDS become the leading security solution. Anomaly based network intrusion detection (IDS) detection plays a major role in protecting networks against various malicious activities. Improving the security of IoT networks has become one of the most critical issues. This is due to the large-scale development and deployment of IoT devices and the insufficiency of Intrusion Detection Systems (IDS) to be deployed for the use of special purpose networks. In this article, the performance of several machine learning models has been compared to accurately predict attacks on IoT systems, the case of imbalanced classes was subsequently treated using the SMOTE technique.*

**Keywords:** IoT, Network Intrusion Detection

## REFERENCES

- [1]. Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.
- [2]. Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset." Information Security Journal: A Global Perspective (2016): 1-14.
- [3]. Moustafa, Nour, et al. "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks." IEEE Transactions on Big Data (2017).
- [4]. Moustafa, Nour, et al. "Big data analytics for intrusion detection system: statistical decision-making using finite dirichlet mixture models." Data Analytics and Decision Support for Cybersecurity. Springer, Cham, 2017. 127-156.
- [5]. Feature Extraction for Machine Learning-based Intrusion Detection in IoT Networks <https://arxiv.org/abs/2108.12722>
- [6]. Supervised Machine Learning Based Network Intrusion Detection System for Internet of Things <https://ieeexplore.ieee.org/abstract/document/9225340>
- [7]. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set <https://jwcn-erasipjournals.springeropen.com/articles/10.1186/s13638-021-01893-8>
- [8]. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset) [https://www.researchgate.net/publication/348206258\\_Machine\\_Learning\\_Based\\_IoT\\_Intrusion\\_Detection\\_System\\_An\\_MQTT\\_Case\\_Study\\_MQTT-IoT-IDS2020\\_Dataset](https://www.researchgate.net/publication/348206258_Machine_Learning_Based_IoT_Intrusion_Detection_System_An_MQTT_Case_Study_MQTT-IoT-IDS2020_Dataset)
- [9]. Internet of Things: A survey on machine learning-based intrusion detection approaches <https://www.sciencedirect.com/science/article/abs/pii/S1389128618308739>
- [10]. Towards Machine Learning Based IoT Intrusion Detection Service [https://link.springer.com/chapter/10.1007/978-3-319-92058-0\\_56](https://link.springer.com/chapter/10.1007/978-3-319-92058-0_56)