

Assignment 2 Report

ML and DL Anomaly Detection for Enhancing 802.1X and Network Access Control

By Mohammed Baatiyyah - 261002493

Master of AI - 2026

Problem Statement: Enhance the Accuracy of detecting Anomaly network traffic on 802.1X network access NAC.

Traditional network security systems 802.1X , such as rule-based intrusion detection systems and basic network access control methods, are facing many challenges in detecting modern cyber threats and anomaly detection. As the number of connected devices, and encrypted network traffic continues to grow, these traditional methods often have difficulty identifying unusual network activity and unauthorized access effectively.

Because of these limitations, traditional systems also have difficulty detecting unusual network activity and unauthorized access to network. To address this issue, many researchers have studied the use of machine learning techniques for network anomaly detection. For example, Tyagi and Kumar (2020) investigated supervised machine learning algorithms to detect malicious network traffic. Their study showed that models such as Decision Trees and Random Forest can successfully identify attack patterns when trained with labeled datasets. However, their method depends heavily on the availability of high-quality labeled data, which is often limited in real-world network environments.

Similarly, Abdallah et al. (2021) studied different machine learning models used in intrusion detection systems. Their results showed that ensemble methods can improve detection accuracy. However, the study also pointed out some challenges, such as scalability and the difficulty of detecting new or unknown attacks in dynamic network environments.

Wang et al. (2022) studied different machine learning methods used for network anomaly detection. Their analysis showed that machine learning can improve the accuracy of detecting network attacks. However, they also explained that these models may require high computational resources and may have difficulty adapting to rapidly changing network traffic patterns.

For unsupervised machine learning , Carrera et al. (2021) proposed an unsupervised anomaly detection method that can detect abnormal network traffic without using labeled data. This approach can adapt better to dynamic network environments. However, it may produce more false positive results compared to supervised learning methods.

Ness et al. (2025) studied advanced machine learning techniques for detecting anomalies in network traffic. Their research showed that modern ML models can detect

suspicious even in encrypted network traffic. However, their study mainly focused on traffic analysis and did not address how anomaly detection can be integrated with network authentication systems.

In addition, Sattar et al. (2024) proposed a self-supervised learning method to detect anomalies in encrypted network traffic. Their approach improves detection accuracy and reduces the need for labeled data. However, the study does not focus on integrating this method with network access control systems.

Most existing studies mainly focus on network traffic analysis and intrusion detection. Only a limited number of studies have explored combining machine learning-based anomaly detection with network access control systems such as 802.1X. For this reason, there is a need for smarter security solutions that integrate ML and DL anomaly detection with authentication and access control mechanisms to improve the real-time detection of suspicious devices and unauthorized network activity in enterprise networks.

Research Objectives:

1- To investigate the effectiveness of various supervised machine learning models, such as Decision Trees and Random Forests, in accurately detecting common network anomaly traffic within environments that can help for 802.1X authentication.

2- To find out how to explore anomaly traffic while maintaining the system's response speed to the same suspected data again and speed up the detection process.

3- To evaluate the performance of advanced machine learning algorithms, specifically, in tackling network security issues like class imbalance and high feature complexity to improve overall detection.

4- To explore the use of unsupervised learning approaches, such as Deep Autoencoders and Isolation Forests, for the near real-time detection of unknown Zero-day anomaly traffic that lack prior signatures.

5- To leverage self-supervised contrastive learning for extracting deep representations from encrypted traffic, focusing on flow-level statistical features like packet length and inter-arrival time to enhance detection accuracy.

6- To provide a comprehensive comparison of supervised and unsupervised techniques to guide the selection of the most efficient models for high-speed and resource-constrained network environments that use 802.1X authentication.

Overall, the literature demonstrates a clear evolution from traditional and supervised approaches toward unsupervised and self-supervised learning techniques. Among these, self-supervised learning—particularly contrastive learning—provides a balanced solution by addressing data scarcity, privacy preservation, and detection of unknown threats. However, there is still a need for a unified, scalable, and efficient framework

capable of achieving high accuracy with low false positive rates in encrypted traffic environments.

References:

Tyagi, H., & Kumar, R. (2020). Attack and anomaly detection in IoT networks using supervised machine learning approaches. *Revue d'Intelligence Artificielle*. [Link](#)

Abdallah, E. E., Eleisah, W., & Otoom, A. F. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. *Procedia Computer Science*. [Link](#)

Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Gomez Chavez, K., & Rubinstein, B. (2021). Machine learning in network anomaly detection: A survey. *IEEE Access*. [Link](#)

Carrera, F., Dentamaro, V., Galantucci, S., Iannacone, A., Impedovo, D., & Pirlo, G. (2022). Combining unsupervised approaches for near real-time network traffic anomaly detection. *Applied Sciences*. [Link](#)

Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N. V. P., & Dhanawat, V. (2025). Anomaly detection in network traffic using advanced machine learning techniques. *IEEE Access*. [Link](#)

Sattar, S., Khan, S., Khan, M. I., Akhmediyarova, A., Mamyrbayev, O., Kassymova, D., Oralbekova, D., & Alimkulova, J. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. *Scientific Reports*. [Link](#)