**Paper Title:**
A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning

**Paper Link:**
https://www.mdpi.com/2076-3417/12/22/11752

1 Summary

**1.1 Motivation**

The paper provides an overview of the significance of IDS in detecting network intrusions, the challenges faced by IDS, a review of recent IDS solutions using machine learning, metrics for assessing IDS performance, datasets used, and future trends in the field.

**1.2 Contribution**

The paper identifies the increasing challenge of network attacks, the popularity of machine learning algorithms for intrusion detection, and the study's goals in presenting IDS concepts, recent trends, and outlining future research challenges.

**1.3 Methodology**

The methodology involves a comprehensive overview of IDS concepts, metrics, machine learning understanding, dataset descriptions, and a review of relevant papers, with solutions proposed using CNN, ensemble methods, and feature selection.

**1.4 Conclusion**

The paper discusses the challenges faced by IDS in detecting new and diverse attacks, the issue of imbalanced datasets affecting the detection of minor classes, the importance of testing IDS in real-world environments, the complexity of models due to the use of deep learning methods, the need to detect encrypted traffic, and the benefits of using feature extraction to reduce model complexity. Future work includes developing solutions to address encrypted traffic and improve abnormal instance detection while reducing computing resources.

## 2 Limitations

### 2.1 First Limitation

The first limitation is the lack of testing in real-world environments, which may affect the generalizability of the solutions proposed.

### 2.2 Second Limitation

The second limitation is the complexity and resource-intensive nature of the deep learning models used, which may limit their practical implementation in real-world settings.

### 2.2 Synthesis

The synthesis from the paper suggests the need for further research in developing efficient IDS that can handle the increasing complexity of modern networks, including the detection of encrypted traffic and addressing the imbalance in detecting minor classes of attacks. Future research could focus on developing lightweight IDS solutions for IoT devices, exploring new feature extraction methods, creating up-to-date datasets, investigating cloud computing and GPU platforms, and improving the accuracy of IDS for minor classes of attacks.