# Future Work for NIDS:

* Various issues need to be considered while implementing NIDS, since the nature of the attacks are dynamic. So, adaptability of detection method is required. Developing a feature selection method with classifiers which reduces the dimensions of the dataset is an ongoing challenge. This is another field of research to classify proper dataset using DL techniques.
* To design a centralized SDN controller, that can monitor and implement real-time intrusion detection in high-speed networks is a possible future direction and will be a challenging task. Most of the SDN-based NIDS architectures developed to identify mostly malicious activities in the SOHO network [[39](https://link.springer.com/article/10.1007/s12083-017-0630-0#CR39) . We think that with greater accuracy and scalability of SDN, the researchers can achieve ML/DL based NIDS on critical infrastructure.