A Review on Network Intrusion Detection System using Deep and Shallow Machine Learning Techniques

Mr. N.G. Pardeshi1
1PhD Research Scholar, India,
ngpardeshi@gmail.com

Dr.D.V. Patil2
2Professor and Head, India,
dipakvpatil17@gmail.com

ABSTRACT: Cyber security is obtained by using intrusion detection system. Also, the hardware and software present in the network is being monitored by the intrusion detection system (IDS). Most of the available network intrusion detection systems (NIDS) are facing problems like high false alarm rate, generating alerts for non-attacking situations. These drawbacks of existing NIDS systems are increasing the load of security persons and due to this more dangerous attacks may get ignored. Another drawback of available IDS systems is that they cannot detect the new attacks. In the present scenario networking environment is changing so fast and different types of new attacks are coming into existence constantly.

Also, most of the existing IDS are developed by using old datasets which are captured long back and not representing current network behaviors and present attacks.

Therefore, it becomes necessary, to develop a novel network intrusion detection system using deep and shallow machine learning technologies and recent datasets which are representing the real-world network traffic, current network behaviors and the new types of attacks. Proposed novel NIDS will have low false and missed alarm rates, high detection rate and accuracy. Also proposed NIDS will be able to detect unknown attacks.