

Intrusion Detection System using Decision Tree

Abstract :

With the continuous increase of cyber dangers of all kinds and their rapid spread through networks and the Internet, the need arose to find effective solutions, including intrusion detection systems, but due to the emergence of new and diverse threats over time, we needed to increase the efficiency of these systems, which were previously dependent on the values of Statistical only in making decisions.

In this project, we will employ machine learning in the field of detecting intruders .Specifically , the decision tree (j48 classifier) is applied with (entropy)and (gini index) purity measures in our work, as this algorithm is fast And high accuracy. Also, we used labeled dataset about the network traffic called (CICIDS 2017), which contains 56,662 record and 77 features in training the system. Also, the number of features has been reduced and specified by the system to (60), and the length of the tree limited to 10 levels only. This allowed us to use this system to protect networks and increase their security, and it is also one of the systems that can be developed in the future