Abstract

Of late, research works on Intrusion Detection System have been receiving a lot of attention. An IDS detects hazard patterns of network traffic on the residual open parts through observing user activities [1]. There are several models available as of now, but the major loop hole in most of the existing models is the incapability of cognizing new attacks i.e. novel threats to a system. Anomaly based intrusion detection system has undoubtedly resulted in easing the pain of detecting novel threats for a system when compared to its counterpart, Signature based Intrusion Detection System. This paper gives an overview of various Anomaly Intrusion Detection System techniques like machine learning algorithms, data mining methods and its variants e.g. Entropy data mining, neural network methods etc. We also give an overview of a few hybrid techniques that have been employed and have resulted in better outcomes for e.g. a combination of Neural networks and Fuzzy logic method.
Reference


Index Terms

Computer Science
Security
Key words

Intrusion detection
Data mining
Anomaly intrusion detection
Neural Networks
fuzzy logic