International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 5-14

INTRUSION DETECTION SYSTEM USING OPTIMAL C4.5 ALGORITHM

SACHIN PRAKASH GAVHANE[1] & VIJAY MARUTI SHELAKE[2]

[1]Department of Information Technology, Atharva College of Engineering, Malad, Mumbai, India

[2]Department of Information Technology, YTCEM, Karjat, Maharashtra, India

ABSTRACT

With hacker attacks against well-known businesses and organizations on the rise, network security has made headlines .of course, there are many attacks that do not make headlines and are not reported due to a loss of credibility or embarrassment. Then there are the attacks that are not even detected. The Defense Information Services Agency (DISA) states that up to 98% of attacks go unnoticed. These revelations have caused many businesses to rethink or to start thinking about the security of their own networks. Maximum Processing computation and more time consuming task has always been a limit in processing huge network intrusion data. This problem can be minimized through feature selection to condense the size of the network data involved. Decision tree models allow one to detect anomalies in large databases. In proposed system, we first preprocess dataset (KDD 99 cup). Then we study and analysis of decision tree algorithms (C4.5 and its extension) of data mining for the task of detecting intrusions and compare their relative performances. Based on this study, it can be concluded that even extended C4.5 is complex but decision tree obtained is the most suitable with high true positive (correct detection of attacks) and low false positive (Incorrect detection) with high accuracy.

KEYWORDS: IDS, Security, Attacks, Abnormal Instance