An Analysis of Rule and Decision Tree Based Intrusion Detection System

Yi Yi Aung
yiyiaung123@gmail.com
University of Computer Studies, Mandalay, UCSM

Myat Myat Min
myatiimin@gmail.com
University of Computer Studies, Mandalay, UCSM

We are living in 21st century wherein the number of internet of things is competing with increasing population. Security is becoming a major concern for information technology over network. Therefore, people use technology to overcome every problem that comes in the network intrusions. Now many researchers and developers are trying to protect networks from various attacks but at the same time raise many questions, confusions and conflicts regarding their protecting technology. Because each approaches have advantages and disadvantages in detection. The system use rule based data mining techniques in intrusion detection system for network. And also it compares the approaches of rule based and tree based intrusion detection system by using 10 % kddcup'99 dataset. For rule based approach, we use K-means and JRip algorithms to classify internal and external security threats and attacks. For decision tree based approach, we use K-means and C4.5 algorithms to compare between detection methods.