Shubpreet Kaur

M.Tech. CSE (FT), U.Roll No.1312078

ABSTRACT

In this research work, the problem of 'Insider attacker', a malicious agent, a person or software which has intent to harm organisation either by some breach of trust, or by leaking information is discussed. However the most frequently is the misuse of cloud services and overuse of CPU. The user is authenticated and it is hard to differentiate his activities in terms of normal and abnormal/malicious. The only way out is to put everyone under monitoring trial. The problem becomes more prominent in cloud due to its inherent nature, as it has many loose ends from where user may enter from any end point. The sequence of events/activities is encoded with specific ID's and each activity has particular sequence which may consist of discrete time series sequence represented with code. The current algorithm searches for patterns that are infrequent and that usually do not occur in routine cloud user's working. This is based on the threshold value which acts as support and confidence value for identification of abnormal/infrequent activity sequence. Basically it is solving the problem of approximation of string matching for finding the similar pattern repeats having low frequency or unknown event pattern. This is exactly done in this research work. The activities of the users are observed based on their routine activity sequence and if there is deviation from the normal activity sequence, sequencing mining algorithm detected the abnormal sequence. The work presented here uses algorithm which is faster, memory efficient and accurate as compared to existing algorithm.