**Anomaly Based Intrusion Detection System for Cloud**

**System Model-**

In our IDS, we will use the concept of self-similarity to detect anomalies in the system. It is a host based IDS that will run on each VM.

Every system has its own similarity pattern as the system's internal events depend on the usage pattern of the users, processes and applications. So, any deviation from the normal behaviour of the system would be detected by the violation of its self-similarity pattern. The system will be trained using audit logs generated by the OS.

This is a lightweight model for intrusion detection because the system will use OS generated event logs, so its computational complexity is low.

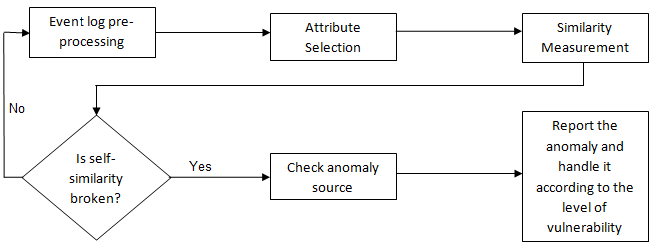


Figure.1 Flow chart of the intrusion detection system

By the next week, we will analyze the log files and decide on the required attributes. We will also decide on the similarity metric to be used and how can we implement our system using CloudSim simulator.

Yashika Jain (TL)

Amala Thampi

Nikita Jain

Nishtha Behal