Detecting Attacks Using Big Data with Process Mining

Ved Prakash Mishra
Department of Computer Science & Engineering
Amity University Dubai, UAE
vmishra@amityuniversity.ae

Yogeshwaran Sivasubramanian
Department of Computer Science & Engineering
Amity University Dubai, UAE
syogeshwaran999@gmail.come

Subheshree Jeevanandham
Department of Computer Science & Engineering
Amity University Dubai, UAE

***Abstract*- In current digital world, Security has become the major issue for the organization. Every day the amount of data is growing in the world. Processing and analyzing of the data is becoming the new challenge for the analyzers. For this purpose, big data is useful to process the high volume of data in less time. Current security tools like existing firewalls and Intrusion Detection Systems are still not able to detect and prevent the attacks and intrusions in full proof manner and giving many false alarms. Big Data analytics concept could be very useful for analyzing, detection and providing full security to the organization because of the ability of handling the large amount of data. In this paper, we have described the concept and the roll of big data. We have also proposed a model using process mining to generate the alerts in the case of attacks.**

***Index Terms*— Big Data, Process Mining, Intrusion Detection System, Logs.**

IJSMS