Anomaly Detection for System Log Analysis using Machine Learning: Recent Approaches, Challenges and Opportunities in Network Forensics

ABSTRACT

Anomaly detection identifies unusual patterns or items in a dataset. The anomalies identified for system logs will signify critical points to help debug system failures and perform root cause analysis. Various system logs are crucial sources to uncover meaningful information on a system condition. Typically, system administrators do manual review using keyword search or rule matching. However, the size of the logs keeps increasing making it a difficult and time-consuming effort to be undertaken manually. Machine learning has been widely used for anomaly detections. In this paper, we reviewed several anomaly detections for system logs using machine learning and discuss emerging research challenges and the opportunities raised from the challenges for network forensics. This paper presents the current research landscape in the area of machine learning and network forensics. It may be beneficial for references to researchers exploring the stated topics.