# Design and Development of a Dashboard for a Real-Time Anomaly Detection System

H.C. Korala (harinduckorala@gmail.com)[1], G.N.R. Weerasooriya[1], M. Udantha[2], G. Dias[2]
[1] Faculty of Information Technology, University of Moratuwa, Katubedda 10400, Sri Lanka.
[2] Department of Computer Science and Engineering, University of Moratuwa, Katubedda 10400, Sri Lanka.

## Abstract

Web logs contain a wealth of undiscovered information on user activities and if analyzed in a proper way they can be utilized for many purposes. Identifying malicious attacks and having a daily summary on user activities are some valuable information that can be extracted from these log files. At present, many tools and algorithms have been developed to extract information from these log files but on most occasions, they have failed to present this information to the user to make decisions in real-time. This paper presents a novel approach taken to design and develop a dashboard for a real-time anomaly detection system with the use of some open source tools to process complex events in real-time, batch process stored data using big data tools and dashboard development techniques. The system accepts web log files as the input; first they are cleaned by a preprocessing unit and then published to WSO2's complex event processor as events to identify and filter out special patterns and summarised by using a set of user specified rules. If an anomaly is detected, an alert or warning will be displayed on the widget based dashboard in real time. Furthermore, each and every event stream that comes to the CEP will be forwarded to WSO2's Data Analytic Server via 'Thrift' protocol. That data will be saved in a Cassandra big data database for further batch processing which is used for drill down purposes. A widget based Dashboard has been developed with the use of modern dashboard concepts and web technologies to display information such as daily summary, possible security breaches in an interactive way allowing system administrators to make operational decisions then and there based on the information provided. Moreover, users can drill down and analyze the historical security breach information and also can customize the dashboard according to their preference. The evaluation techniques used fall under the criteria of evaluation against well-established standards and evaluation by external expert review. Evaluation for security standards has done against the security standard set by the PCI security standards council and evaluation for dashboard has been carried out against the dashboard standards defined by Oracle which describes about the best practices in developing an effective dashboard. Evaluation by external expert review was done in line with the people who have prior experience in dealing with a dashboard in different contexts. Ten expert evaluators from different expertise areas (System Administrators, UX engineers and QA engineers) have been used for this evaluation and a score based model was used to determine how efficient this dashboard is to view and drill information. Based on the results yielded from the evaluation, it is identified that the dashboard meets with the international standards of dashboard designs, well established security standards in dashboard design as well as provides the best user experience for users in different functional areas.

**Keywords:** *Log files analysis*, *Big data*, *Visualization*