Time Series Anomaly Detection in Medical Break The Glass

Qais Tasali
qtasali@ksu.edu
Department of Computer Science
Kansas State University
Manhattan, Kansas

Nikesh Gyawali
gnikesh@ksu.edu
Department of Computer Science
Kansas State University
Manhattan, Kansas

Eugene Y. Vasserman
eyv@ksu.edu
Department of Computer Science
Kansas State University
Manhattan, Kansas

ABSTRACT

The high availability (fail-open) requirement and real-time nature of the communication in distributed medical systems makes it hard to limit clinicians access to bare minimum permissions that are essential to perform life-saving activities in an emergency access (Break the Glass) session. After a BTG session is ended, healthcare facilities perform post-hoc audit to determine the reasons (legitimacy) for overriding access control. Unfortunately, this does not proactively protect against misuse, but provides for identification and punishment of a culprit.

In this work we investigate anomaly detection in the medical Break the Glass (BTG) procedure using statistical analysis. We integrate a semi-supervised learning model into our anomaly detection system to flag anomalous BTG sessions. The model is trained in a supervised fashion with labeled and unlabeled data (pseudo-labeling) simultaneously. Furthermore, by performing real-time log analysis, we limit the extent of uncertainty of the system operating state following an emergency access session, and allow for recovery to a known safe and secure state when needed. We also show that for all but the most permissive BTG authorization policies, the majority of audits currently done manually could be mostly or fully automated.