Time Series Anomaly Detection in Medical Break-the-Glass

Qais Tasali, Nikesh Gyawali, Eugene Y. Vasserman

Department of Computer Science, Kansas State University

KANSAS STATE UNIVERSITY

Department of Computer Science

We investigate the effectiveness of anomaly detection to ease the human burden of post-hoc audits in the medical Break-the-Glass (BTG) context. We use predictive modeling to perform real-time and post-BTG statistical analysis on sequenced session log data for flagging anomalous user actions.

Introduction

- Fail-closed access control (AC) is not always the safest approach
- Post-hoc audit to determine the legitimacy for overriding access control
- Dynamic nature of the environment and complexity of users' behavior
- Uncertainty of the system state following an emergency access session

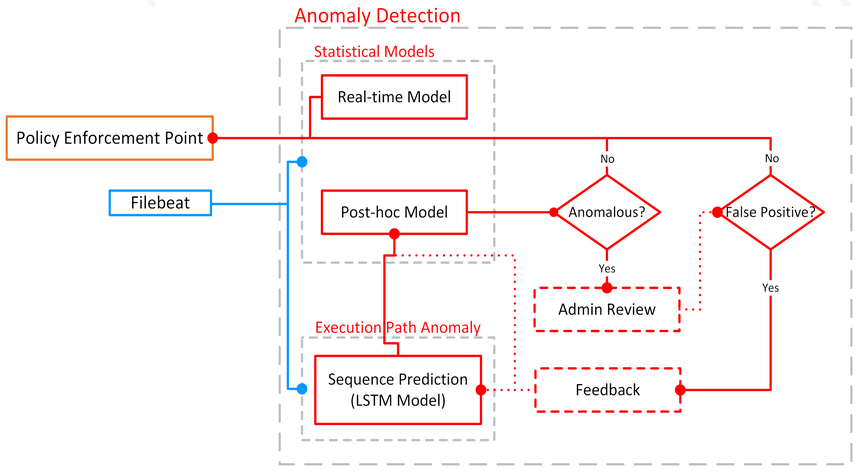


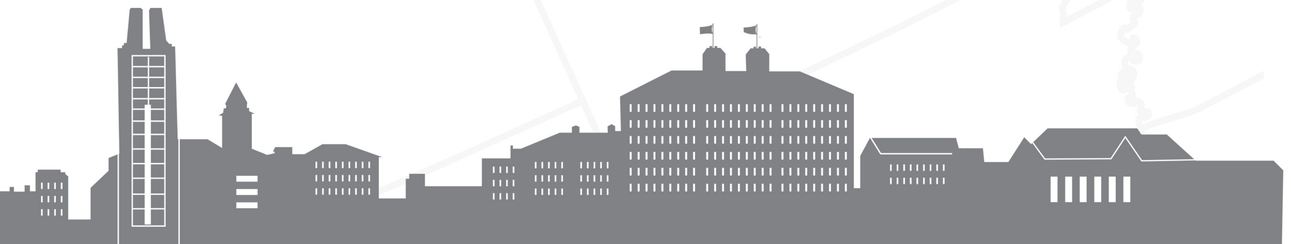
Figure 1: The architecture of the anomaly detection system

Design

- Statistical models for real-time and post-session log monitoring and analysis
- Feature-specific predicators are used to monitor incoming logs for statistical analysis
- Anomalous session detection based on user's behavior analysis
- Sequence prediction model uses LSTM to learn log patterns from normal execution
- Session logs that deviate from normal execution pattern are flagged anomalous

Background

- Routine emergency: use of exceptional mechanisms is too common
- Controlled vs. uncontrolled BTG
- Comparison of constructed behavior with expected behavior profiles
- Frequency of attributes in the log for categorizing transactions
- Efficiency of Long Short-Term Memory (LSTM) neural networks at finding complex relationships in multivariate time series data



Evaluation

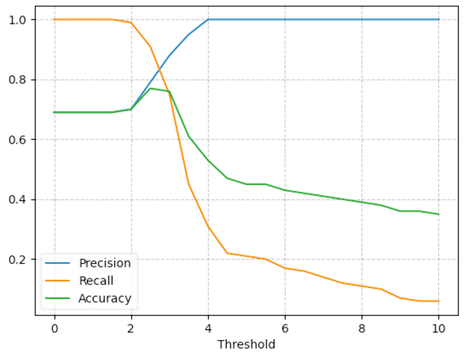


Figure 2: Precision = 88% and recall = 75% with threshold = 3

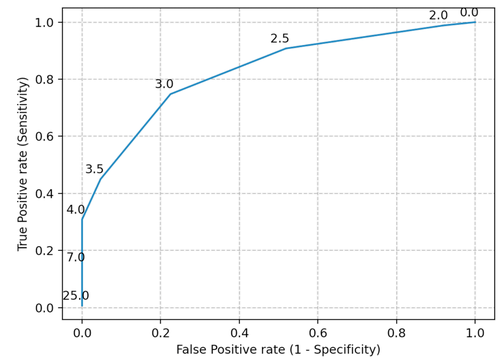


Figure 3: Model's performance for all classification thresholds (ROC curve)

HOTSOS 2020
7TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**
SEPTEMBER 22-23, 2020 | LAWRENCE, KANSAS