ABSTRACT

This disclosure describes a module and method for detecting anomalies in a critical infrastructure (CI) system based on pre-generated rule sets and a trained anomaly detection model. The pre-generated rule sets are automatically generated based on state variables associated with the CI system, while the anomaly detection model is trained on features that are automatically extracted from the CI system. Additionally, the module is configured to dynamically regenerate the rule sets and retrain the anomaly detection model in response to a decline in anomaly detection performance to ensure adaptive and continuous optimization of the anomaly detection system.

Figure 1