METHOD AND SYSTEM FOR ANOMALY DETECTION USING A COLLECTIVE SET OF UNSUPERVISED MACHINE-LEARNING ALGORITHMS

ABSTRACT

An anomaly detection system comprising, one or more distributed sensors for gathering network or log data; one or more generators for generating discovery rules based on a collective set of pattern discovery algorithms including one or more unsupervised machine learning algorithms; one or more detectors for detecting abnormal patterns in the network or log data gathered by the sensors based on the discovery rules generated by the generator; and one or more correlation engine for determining intrusion counter measures based on matching features of one or more detected abnormal patterns with correlation rules.

FIGURE. 1