Abstract

Detecting anomaly behaviors is one of the most challenging tasks for Information Systems (IS) administrators. The anomaly behavior is defined as any behavior from either inside or outside of the organization’s information system that deviates from normal; this includes insider attacks as well as any behavior that threatens the confidentiality, integrity and availability of the
organization's information systems. One of the strategies to detect an anomalous behavior is to create a clustering or classification model by utilizing data mining methodologies. The models could be generated from previous historical data or it could be based on current data. Although these models could identify normal and abnormal behavior, they couldn’t satisfy the growing demand for better information security. The primary drawback of using these methods are a high rate of false positive; the model becomes outdated and there is high demand to maintain the models’ integrity; and they have low response rate. This study attempts to overcome some of the disadvantages in the current data mining models, which have been used to detect anomaly behaviors. Moreover this research will attempt to introduce a model that utilizes stream data mining to actively monitor network traffic for anomaly detection.

Reference


Index Terms

Computer Science  Security

Key words

Stream Data Mining  Anomaly Detection  Data Mining

Supervised Data Mining and Unsupervised Data Mining