A survey of anomaly detection using data mining methods for hypertext transfer protocol web services

ABSTRACT

In contrast to traditional Intrusion Detection Systems (IDSs), data mining anomaly detection methods/techniques has been widely used in the domain of network traffic data for intrusion detection and cyber threat. Data mining is widely recognized as popular and important intelligent and automatic tools to assist humans in big data security analysis and anomaly detection over IDSs. In this study we discuss our review in data mining anomaly detection methods for HTTP web services. Today, many online careers and actions including online shopping and banking are running through web-services. Consequently, the role of Hypertext Transfer Protocol (HTTP) in web services is crucial, since it is the standard facilitator for communication protocol. Hence, among the intruders that bound attacks, HTTP is being considered as a vital middle objective. In the recent years, an effective system that has attracted the attention of the researchers is the anomaly detection which is based on data mining methods. We provided an overview on four general data mining techniques such as classification, clustering, semi-supervised and association rule mining. These data mining anomaly detection methods can be used to computing intelligent HTTP request data, which are necessary in describing user behavior. To meet the challenges of data mining techniques, we provide challenges and issues section for intrusion detection systems in HTTP web services

Keywords: Data mining; Intrusion detection systems; Anomaly detection; Hypertext Transfer Protocol (HTTP); Web services