Abstract

Electronic commerce is a commercial transaction that involves the process of buying and selling goods, services and transfer of information between businesses and customers over an electronic medium. Electronic commerce has expanded rapidly and continues to grow at an unforeseen rate. With the advent of e-commerce, the potential fraudulent activities are prevalent, and therefore hundreds of millions of dollars are lost to fraud every year. The goal of this paper is to implement and evaluate several anomaly detection methods for making predictions using, or finding patterns in, heterogeneous e-commerce data to detect fraudulent activities of users. Various Machine Learning algorithms – K-nearest neighbors, Random-Forest and Isolated forest algorithms are employed to train the model in order to detect fraud and anomalous techniques in e-commerce.

References


**Index Terms**

Computer Science Security

**Keywords**