Abstract

The systems which can be used for pattern classification are used in adversarial application, for example spam filtering, network intrusion detection system, biometric authentication. This adversarial scenario's exploitation may sometimes affect their performance and limit their practical utility. In case of pattern classification conception and contrive methods to adversarial environment is a novel and relevant research direction, which has not yet pursued in a systematic way. To address one main open issue: evaluating at contrive phase the security of pattern classifiers (for example the performance degradation under potential attacks which incurs during the operation). To propose a framework for evaluation of classifier security and also this framework can be applied to different classifiers on one of the application from the
A Review on Security Evaluation for Pattern Classifier against Attack

spam filtering, biometric authentication and network intrusion detection.

References


**Index Terms**

- Computer Science
- Security

**Keywords**

- Machine Learning System
- Security Evaluation
- Adversarial Classification
- Arms-race
- Spam Filtering.