Abstract

From many years, various tools based on pattern classification system have been used in security related applications like, spam filtering, biometric authentication system, network intrusion detection system, pattern classification systems are used, in which brilliant and adaptive adversary may changes data to make the classifier produce false negatives (regular). Measurement of pattern classifier security performance is very important part for making decisions, finding product viability, for differentiate various classifiers. Pattern classification systems may exhibit obligations, exploitation affect their performance, produce limitations to practical utility, if adversarial scenario is not taken into account. At design phase, the system evaluates the classifiers security. The classifiers security means performance degradation for related attacks may acquire when operation runs. A phenomenon is used for classifier security evaluation, adversary model for defining attack scenarios that generates training and testing sets.

References

- B. Biggio, G. Fumera, and F. Roli, "Security evaluation of Pattern Classifiers"

- A. Kolcz and C. H. Teo, &quot;Feature weighting for improved classifier robustness," In 6th Conf. on Email and Anti-Spam (CEAS), 2009.
- D. Lowd and C. Meek, &quot;Adversarial Learning;&quot; Proc. 11th ACMSIGKDD Intapo; l Conf. Knowledge Discovery and Data Mining, pp. 641-647, 2005.
- D. Lowd and C. Meek, &quot;Good Word Attacks on Statistical Spam Filters;&quot; Proc. Second Conf. Email and Anti-Spam, 2005.
- D. B. Skillicorn, &quot;Adversarial Knowledge Discovery;&quot; IEEE Intelligent Systems, vol. 24, no. 6, Nov./Dec. 2009.

Index Terms

Computer Science Security

Keywords

Legitimate samples malicious samples reactive and proactive arms race spoof attack.