Paper ID: MISS21_45

A Predictive Model for Cyberstalking Detection on Twitter Using Support Vector Machine (SVM)

Arvind Kumar Gautam*, and Abhishek Bansal

Department of Computer Science, IGNTU Amarkantak, Madhya Pradesh -484887, India

*Corresponding author

Abstract

Background: Twitter is a real-time social media application that has gained global popularity, and the use of Twitter is also raising serious issues in the form of cyberstalking. Cyberstalking is systematic, repeated, and numerous cyber-attacks and does not occur on a single occurrence. Cyberstalking [1] is a serious cyber-attack in which the attacker uses digital media to harass the victim or group through personal attacks and the disclosure of false or confidential information among other persons. It may categorize as email-stalking, internet-stalking, and computer-stalking.

Objectives: Available preventing mechanism is not sufficient to handle the cyberstalking situations. Filtration, detection, and proper evidence documentation of cyberstalking are challenging tasks. Finding the technological solutions to control cyberstalking more attention is required in the technical aspect.

Methodology: The proposed methodology is inspired by the framework of Frommholz I. et al. [2] for Textual Analysis and Cyberstalking Detection using machine learning algorithms. The proposed framework will work on textual tweets and contain four phases: pre-processing, features extraction, text classification, and cyberstalking detection. Support Vector Machine (SVM) will be used for text classification, while Bag of Word with unigram, bigram, and trigram will be used for feature extraction.

Results and discussion: The experiment was performed on two different datasets containing 1065 and 40116 tweets, respectively, and performance metrics were measured. The proposed machine learning model produced accuracy, 72.4%, and 84.5%, using SVM with Unigrams for dataset-1 and dataset-2, respectively.

Conclusions and future work: We found that SVM with Unigrams produces better accuracy for large cyberstalking dataset-2 while SVM with Ngrams produces better recall on both datasets. It is also found that the performance of algorithms is also dependent on the size and distribution of the dataset and feature extraction methods. Future work will be focused on automatic cyberstalking detection on Twitter in a real-time manner.

References

[1] Ghasem, Zinnar, Ingo Frommholz, and Carsten Maple. "Machine learning solutions for controlling cyberbullying and cyberstalking." J Inf Secur Res 6.2 (2015): 55-64.

[2] Frommholz, Ingo, et al. "On textual analysis and machine learning for cyberstalking detection." Datenbank-Spektrum 16.2 (2016): 127-135.

 DOI: 10.21467/abstracts.120

ISBN: 978-81-954993-2-8