Spam Detection in Social Networks Using Machine Learning Algorithms

Rucha Kibe, Pooja Suryawanshi, Saloni Sonar, Archana Deokate
Department of Electronic and Telecommunication Engineering
Smt. Kashibai Navale College of Engineering, Pune, India

Abstract: *Social networking websites have become more and more popular recently. Users use them to meet new people and communicate their most recent thoughts and actions to their existing acquaintances. The website among these that is growing the quickest is social media. Due to its popularity, many spammers attempt to flood actual users' accounts with spam messages. This paper considers three social networks, Twitter, Facebook, and Instagram, for experimentation. The classification of the data into spam and non-spam using four machine learning techniques, including SVM, KNN, decision trees, and Random Forest. The results obtained from the experiments show that the proposed approach can accurately detect spam in social networks. Implementing such algorithms could help social network platforms improve user experience by reducing the prevalence of spam and fraudulent activity.*

Keywords: Spam detection, social media, Machine learning, SVM, KNN, DT, RF

REFERENCES

[1]. Zhu, K., Zhi, W. and Zhang, L. (2016) 'Exploring mobile users and their effects in online socialnetworks: a Twitter case study,' IEEE 24th International Conference on Network Protocols(ICNP), DOI: 10.1109/icnp.2016.7785319.

[2]. Xu, H., Sun, W. and Javaid, A. (2016) 'Efficient spam detection across online social networks,' IEEE International Conference on Big Data Analysis (ICBDA), DOI: 10.1109/icbda.2016.7509829.

[3]. Jain, G., Sharma, M., & Agarwal, B. (2018). Spam detection on social media using semantic convolutional neural network. International Journal of Knowledge Discovery in Bioinformatics (IJKDB), 8(1), 12-26

[4]. Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010, October). @ spam: the underground on 140 characters or less. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 27-37). ACM

[5]. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," in Proc. CEAS, vol. 6, 2010, p. 12.

[6]. K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine learning," in Proc. 33rd Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR), 2010, pp. 435442.

[7]. G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in Proc. 26th Annu. Comput. Secure. Appl. Conf. (ACSAC), 2010, pp. 19.

[8]. H. Wang, ``Don't follow me: Spam detection in Twitter," in Proc. Int. Conf. Secure. Cryptogr. (SECRYPT), Jul. 2010, pp. 110.

[9]. Z. Chu, I. Widjaja, and H. Wang, ``Detecting social spam campaigns on Twitter," in Proc. Int. Conf. Appl. Cryptogr. Netw. Secure. Cham, Switzerland: Springer, 2012, pp. 455472.

[10]. Meda, F. Bisio, P. Gastaldo, and R. Zunino, "A machine learning approach for Twitter spammers detection," in Proc. Int. Carnahan Conf. Secure. Technol. (ICCST), Oct. 2014, pp. 16.

[11]. Wang, A. Zubiaga, M. Liakata, and R. Procter, ``Making the most of tweet-inherent features for social spam detection on Twitter," 2015, arXiv:1503.07405. [Online]. Available: http://arxiv.org/abs/1503.07405

[12]. X. Zheng, Z. Zeng, Z. Chen, Y. Yu, and C. Rong, ``Detecting spammers on social networks," Neurocomputing, vol. 159, pp. 2734, Jul. 2015.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-10458

259

ISSN
2581-9429
IJARSCT

[13]. Chen, J. Zhang, Y. Xie, Y. Xiang, W. Zhou, M. M. Hassan, A. AlElaiwi, and M. Alrubaian, "A performance evaluation of machine learning-based streaming spam tweets detection," IEEE Trans. Comput. Social Syst., vol. 2, no. 3, pp. 6576, Sep. 2015.