IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.53

Volume 4, Issue 5, March 2024

Fake Social Media Profile Detection and Reporting Using Machine Learning

Aniket Agravat, Umang Makwana, Sahil Mehta, Devashish Mondal, Sushant Gawade

Department of Artificial Intelligence and Machine Learning

Universal College of Engineering, Mumbai, Maharashtra, India

Abstract*: Our research focuses on utilizing machine learning techniques, encompassing natural language processing and computer vision, to create an automated system for the detection and reporting of fake social media profiles across various platforms. Our approach involves feature extraction from both textual and visual content, followed by the application of machine learning models to classify profiles as fake or genuine. This system operates in real-time, monitoring user activity and promptly flagging suspicious profiles for user- initiated reporting. By combining the power of machine learning with cross-platform compatibility and user feedback, our solution aims to enhance online safety by swiftly identifying and addressing fraudulent social media profiles, thus fostering more secure and trustworthy online communities.*

Keywords: Fake profiles, Machine learning, Natural Language Processing, Fraudulent Social media accounts

REFERENCES

[1] E. Karunakar, V. D. R. Pavani, T. N. I. Priya, M. V. Sri, and K. Tiruvalluru, "Ensemble fake profile detection using machine learning (ML)," J. Inf. Comput. Sci., vol. 10, pp. 1071–1077, 2020.

[2] P. Wanda and H. J. Jie, "Deep profile: utilising dynamic search to identify phoney profiles in online social networks CNN" J. Inf. Secur. Appl., vol. 52, pp. 1–13, 2020.

[3] P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter SMS spam," Future Gener. Comput. Syst., vol. 102, pp. 524–533, 2020.

[4] R. Kaur, S. Singh, and H. Kumar, "A modern overview of several countermeasures for the rise of spam and compromised accounts in online social networks," J. Netw. Comput. Appl., vol. 112, pp. 53– 88, 2018.

[5] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, "Automatically dismantling online dating fraud," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1128–1137, 2020.

[6] K. Thomas, C. Grier, D. Song, and V. Paxson, ''Suspended accounts in retrospect: An analysis of Twitter spam,in Proc. ACM SIGCOMM Conf. internet Meas. Conf., 2011, pp. 243–258.

[7] Saeed Abu-Nimeh, T. M. Chen, and O. Alzubi, "Malicious and Spam Posts in Online Social Networks," Computer, vol.44, no.9, IEEE2011, pp.23–28.

[8] B. Viswanath et al., ''Towards detecting anomalous user behavior in online social networks,'' in Proc. Usenix Secur., vol. 14. 2014, pp. 223–238.

[9] R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," Egyptian informatics journal, vol. 17, no. 2, pp. 199–216, 2016.

[10] S.-T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," in Proceedings of the 2010 New Security Paradigms Workshop. ACM, 2010, pp. 61–7

DOI: 10.48175/IJARSCT-16695