

Detection of Fake Profiles on Social Networking

Mrs. J. Sathiya Jothi¹, Mr. A K Akash², Mr. R. Akash³, Mr. M. Deepak⁴

Assistant Professor, Department of Information Technology¹

Students, Department of Information Technology^{2,3,4}

Anjalai Ammal Mahalingam Engineering College, Thiruvarur, Tamil Nadu, India

Abstract: *The detection of fake profiles on social networking platforms is a pressing concern due to the proliferation of fraudulent accounts that undermine user trust and platform integrity. This paper proposes a novel framework for the automatic detection of fake profiles, leveraging the private information available within social networking platforms while respecting user privacy. The proposed scheme utilizes advanced algorithms and machine learning models to analyze various parameters, including user activity patterns, account creation details, and communication behavior, to identify potentially fraudulent accounts. Importantly, this approach ensures the preservation of user privacy by conducting analysis solely within the platform's closed environment without compromising sensitive personal information. Furthermore, the framework incorporates an alert system to notify platform administrators and users of suspicious activity indicative of fake identity creation, enabling proactive measures to prevent the spread of fake profiles and mitigate potential risks. Through the implementation of this framework, social networking companies can effectively combat the proliferation of fake profiles while upholding user privacy and fostering a safer and more trustworthy online environment for all users*

Keywords: Fake Profile

REFERENCES

- [1] (2018) Facebook publishes enforcement numbers for the first time. Internet draft. [Online]. Available: <https://newsroom.fb.com/news/2018/05/enforcement-numbers/>
- [2] (2018) How concerned are you that there are fake accounts and bots on social media platforms that are used to try to sell you things or influence you? Internet draft. [Online]. Available: <https://www.statista.com/statistics/881017/fake-social-media-accounts-bots-influencingselling->
- [3] (2012) Buying their way to twitter fame. Internet draft. [Online]. Available: www.nytimes.com/2012/08/23/fashion/twitter-followers-for-sale.html?smid=pl-share
- [4] (2017) Welcome to the era of the bot as political boogeyman. Internet draft. [Online]. Available: <https://www.washingtonpost.com/news/politics/wp/2017/06/12/welcome-to-the-era-of-the-bot-as-political-boogeyman>
- [5] (2018) Human or 'bot'? doubts over italian comic beppegrillo's twitter followers. Internet draft. [Online]. Available: <https://www.telegraph.co.uk/technology/twitter/9421072/Human>
- [6] (2017) How fake news and hoaxes have tried to derail jakarta's election. Internet draft. [Online]. Available: <https://www.bbc.com/news/world-asia-39176350>
- [7] 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. 61–72.
- [8] S. Fong, Y. Zhuang, and J. He, "Not every friend on a social network can be trusted: Classifying imposters using decision trees," in Future Generation Communication Technology (FGCT), 2012 International Conference on. IEEE, 2012, pp. 58–63.
- [9] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in Proceedings of the 27th annual computer security applications conference. ACM, 2011, pp. 93–102.
- [10] P. Patel, K. Kannoopatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A theoretical review of social media usage by cyber-criminals," in Computer Communication and Informatics (ICCCI), 2017 International Conference on. IEEE, 2017, pp. 1–6.