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
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Recognization of Spurious Profile using Machine Language

S. Jeyaganesh, S. Lokesh, VK. Sudharsan
Students, Department of Electronics and Communication Engineering
Dhanalakshmi College of Engineering, Chennai

Abstract: *In the present generation, the social life of everyone has become associated with online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There are no feasible solutions exist to control these problems. In this paper, I came up with a framework with which the automatic identification of fake profiles is possible and is efficient. This framework uses classification techniques like Random Forest Classifier to classify the profiles into fake or genuine classes. As this is an automatic detection method, it can be applied easily by online social networks that have millions of profiles whose profiles cannot be examined manually. Nowadays, mobile operators in China mainland are facing fierce competition from one to another, and their focus of customer competition has, in general, shifted from public to corporate customers. One big challenge in corporate customer management is how to identify fake corporate members and potential corporate members from corporate customers. In this study, we have proposed an identification method that combines the rule-based and probabilistic methods. Through this method, fake corporate members can be eliminated and external potential members can be mined. The experimental results based on the data obtained from a local mobile operator revealed that the proposed method can effectively and efficiently identify fake and potential corporate members. The proposed method can be used to improve the management of corporate customers. To avoid the spam message, malicious and cyber bullies activities which are mostly done by the fake profile. These activities challenge the privacy policies of the social network communities. These fake profiles are responsible for spread false information on social communities. To identify the fake profile, duplicate, spam and bots account there is much research work done in this area. By using a machine-learning algorithm, most of the fake accounts detected successfully. This paper represents the review of Fake Profile Detection on Social Site by Using Machine Learn.*

Keywords: machine learning

REFERENCES

[1] (2016). PhishMe Q1 2016 Malware Review. [Online]. Available: https://phishme.com/project/phishme-q1-2016-malware-review/
[2] A. Belabed, E. Aimeur, and A. Chikh, ‘‘A personalized whitelist approach for phishing webpage detection,’’ in Proc. 7th Int. Conf. Availability, Rel. Security (ARES), Aug. 2012, pp. 249–254.
[3] Y. Cao, W. Han, and Y. Le, ‘‘Anti-phishing based on automated individual white-list,’’ in Proc. 4th ACM Workshop Digit. Identity Manage., 2008, pp. 51–60.
[4] T.-C. Chen, S. Dick, and J. Miller, ‘‘Detecting visually similar Web pages: Application to phishing detection,’’ ACM Trans. Internet Technol., vol. 10, no. 2, pp. 1–38, May 2010.
[5] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C. Mitchell, ‘‘Clientside defense against Web-based identity theft,’’ in Proc. 11th Annu. Netw. Distrib. Syst. Security Symp. (NDSS), 2004, pp. 1–16
[6] C. Inc. (Aug. 2016). Couldmark Toolbar. [Online]. Available: http://www.cloudmark.com/desktop/ie-toolbar

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
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

[7] J. Corbetta, L. Invernizzi, C. Kruegel, and G. Vigna, ‘‘Eyes of a human, eyes of a program: Leveraging different views of the Web for analysis and detection,’’ in Proceedings of Research in Attacks, Intrusions and Defenses (RAID). Gothenburg, Sweden: Springer, 2014.
[8] X. Deng, G. Huang, and A. Y. Fu, ‘‘An antiphishing strategy based on visual similarity assessment,’’ Internet Comput., vol. 10, no. 2, pp. 58–65, 2006.
[9] Z. Dong, K. Kane, and L. J. Camp, ‘‘Phishing in smooth waters: The state of banking certificates in the US,’’ in Proc. Res. Conf. Commun., Inf. Internet Policy (TPRC), 2014, p. 16.

BIOGRAPHIES

- **JEYAGANESH** is currently pursuing a Bachelor of Engieering in Electronics and communication engineering in Dhanalakshmi College of Engineering , chennai affliated with Anna University
- **LOKESH** is currently pursuing a Bachelor of Engieering in Electronics and communication engineering in Dhanalakshmi College of Engineering, chennai affliated with Anna University
- **SUDHARSAN** is currently pursuing a Bachelor of Engieering in Electronics and communication engineering in Dhanalakshmi College of Engineering, chennai affliated with Anna University