IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11631

Machine Learning Framework For Detecting Spammer And Fake User Identification On Social Networks

Vimala P[1], Nageswari N[2], Naveena Devi M[3], Nisha R[4]

Assistant Professor, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, Tamil Nadu, India[1]

Student, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology,Salem, Tamil Nadu, India[2,3,4]

Abstract: Millions of users throughout the world are active on social networking sites. Users' interactions with social media platforms like Twitter and Facebook have a significant impact on daily life, sometimes in unfavourable ways. Popular social networking sites have become a target for spammers who want to spread a tonne of harmful and unnecessary content. Twitter, for instance, has grown to be one of the most extravagantly used platforms ever and as a result, permits an excessive quantity of spam. False users spam users with unwanted tweets to advertise products or websites that not only negatively impact real users but also disturb resource usage. A popular field of research in today's online social networks is the identification of false Twitter users and the detection of spammers (OSNs). Review the procedures for identifying spammers on Twitter**.** In addition, a taxonomy of Twitter spam detection methodologies is offered, which groups the methods according to how well they can identify I phoney material, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also contrasted based on a number of criteria, including user, content, graph, structure, and time factors. We are optimistic that the study that has been provided will serve as a beneficial tool for scholars looking for the most significant recent advancements in Twitter spam detection on a single platform.

Keywords: Spam Detection, Fake user, online social networks, Detecting URL

I.INTRODUCTION

Using the Internet, spammers can now easily access any information they need Several disputes can be held about diverse themes, such as politics, current affairs, and noteworthy occurrences. When a user tweets something, it is instantaneously sent to his/her followers, allowing them to outspread the received information at a much greater level from any source anywhere in the world. Social media services are becoming popular, allowing users to gather a wealth of user data and information. These websites attract bogus users due to the enormous amounts of data they make available. Twitter has quickly developed into a valuable resource for finding current user data online. Twitter is an Online Social Network (OSN) where users may post anything and anything, such as news, ideas, and even their moods. In order to keep social networks secure, spam identification is a challenging undertaking. To protect users from various dangerous assaults and to maintain their security and privacy, it is crucial to identify spam on OSN sites. In the actual world, the community is severely damaged by the risky tactics spammers deploy. Twitter spammers aim to propagate false information, fake news, rumours and impromptu messages, among other things. Spammers use adverts and other methods to support various causes in order to further their nefarious goals. mailing lists and then randomly send spam letters to advertise their interests. The original users—known as non-spammers—are disturbed by these activities. Additionally, it harms the OSN platforms' reputation. Therefore, it is vital to establish a strategy to recognise spammers so that corrective actions can be taken to fight their malevolent activity. The field of detecting Twitter spam has been the subject of numerous research projects The study also offers a review of the literature that acknowledges the presence of spammers on the social network Twitter. Despite. All the known studies, there is still a void in the existing literature. We therefore evaluate the most recent developments in spammer detection and false user identification on Twitter in order to close the gap. Additionally, this study offers a taxonomy of methods for detecting Twitter spam and makes an effort to provide a thorough summary of current advancements in the field. The purpose of this study is to catalogue several strategies for Twitter spam detection and to give taxonomy by categorising these strategies. For classification, we have identified four means of reporting spammers that can be helpful in identifying fake identities of

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11631

users. Spammers can be found using the following methods: I false content; (ii) spam detection based on URLs; (iii) spam detection in popular subjects; and (iv) fake user identification. Table 1 provides a comparison of existing techniques and helps users to recognize the significance and effectiveness of the proposed methodologies in addition to providing a comparison of their goals and results. Table 2 compares different features that are used for identifying spam on Twitter We hope that this survey will provide readers with comprehensive information about spammer detection methods in one place. The organisation of this article places Section II's taxonomy for Twitter's spammer detection methods first.

II. EXISTING SYSTEM

Spammers currently use social media as a platform since they may use their accounts to target various audiences. One of these objectives is disseminating rumours that could have a significant impact on a certain industry or possibly the entire society. Finding a solution to this problem requires tackling the discretization process because continuous valued features are employed in the bulk of real-world applications of classification learning. Discretization is the conversion of a continuous-valued attribute into an interval-valued attribute. It is useful for transforming numerical numbers that are not regularly distributed into nominal values.

DISADVANTAGE:

- The detection of the spam itself can be effective for filtering spam on real time search whereas the detection of spammers is mainly related with the not detection of existent spam accounts.
- When a spammer is discovered, it is only natural to suspend her account or temporarily block her access to certain IP addresses in order to stop them from posting spam using new accounts.

III.PROPOSED SYSTEM

Proposed a hybrid approach for detecting spammer profiles that makes use of user-based, content-based, and graph-based attributes. Three criteria are used in a suggested model to distinguish between non-spam and spam profiles. to catalogue several strategies for Twitter spam detection and to present a taxonomy by categorising these strategies. Four methods of reporting spammers that can be useful in spotting user impersonation have been discovered by us for classification. Spammers can be found using the following methods:

- Fake Content
- URL Based Spam Detection
- Detecting Spam in Trending Topics
- Fake User Identification

ADVANTAGE:

- The majority of tweets that contained any kind of information were discovered to be made by mobile devices, while non-informative tweets were produced mostly by web interfaces.
- The typical proportion of verified accounts that were spam or not.
- The number of followers of the user accounts.
- The collection of tweets related to Twitter's trending topics. The tweets are then examined after being saved in a specific file format.

IV.SYSTEM REQUIREMENT

A. Hardware Requirements

- System : Pentium IV 2.4 GHz
- Hard Disk : 500 GB
- Monitor : 15 VGA Colour
- Mouse : Logitech
- RAM : 4 GB

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11631

B. Software Requirements

- Operating System : Windows 7/8/10
- Script Language : JavaScript 4.0
- IDE Tools : Dreamweaver CC 2017
- Frontend : PHP 5.1
- Backend : MYSQL 10.0

V.SYSTEM IMPLEMENTATINON

A Module Split Up

- Fake Content Based Spammer Detection
- URL Based Spam Detection
- Detecting Spam in Trending Topics
- Fake User Identification

B Modules Description

Fake Content Based Spammer Detection: The average number of verified accounts that were either spam or non-spam was used to determine the role of user attributes in the detection of fraudulent content. the quantity of user accounts' followers. The indicators that include social, reputation, global engagement, topic engagement, likeability, and credibility were used to detect the spread of bogus information.
URL Based Spam Detection: Evaluated computer learning methods for detecting spam tweets. The spam to non-spam ratio, training dataset size, time-related data, factor discretization, and data sampling are just a few examples of the features that the authors looked at in their analysis of the performance of spam detection.

Detecting Spam in Trending Topics: The collection of tweets related to Twitter's trending topics. The tweets are subsequently evaluated after being saved in a specific le format. Spam labelling is done in order to go through all datasets and find the malicious URL. In order to distinguish between real and false tweets, feature extraction isolates the features construct based on the language model.

Fake User Identification: To find spam accounts on Twitter, a categorization technique is suggested. The dataset that was used in the study was assembled by hand. The classification is done by looking at the user name, profile and background image, friends and followers, tweet content, account description, and tweet count.

VI.CONCLUSION

We looked at the methods for identifying spammers on Twitter. We also offered a taxonomy of Twitter spam detection techniques, categorising them into groups including false user detection, spam detection in trending topics, spam detection based on URLs, and fake content detection. Several features, including user features, content features, graph features, structure features, and temporal features were used to compare the provided strategies. The strategies were also contrasted in terms of the datasets they employed and the goals they were designed to achieve.
It is hoped that the evaluation would provide academics with updated data on methods for detecting Twitter spam in a centralised manner. There are still certain open areas that demand major scholarly attention despite the development of robust and effective algorithms for the detection of spam and false users on Twitter. The concerns are briefly highlighted as under: Due to the grave consequences that false news can have on both an individual and a communal level, the subject of false news detection on social media networks needs to be investigated. Another linked problem that is worth researching is the detection of rumour sources on social media.

REFERENCES

[1].B. Erçahin, Ö. Akta³, D. Kilinç, and C. Akyol, ``Twitter fake account detection,'' in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388_392.
[2]. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, ``Detecting spammers on Twitter,'' in Proc. Collaboration, Electron. Messaging, Anti- Abuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12.

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11631

[3].S. Gharge, and M. Chavan, ``An integrated approach for malicious tweets detection using NLP," in Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), Mar. 2017, pp. 435_438.
[4].T. Wu, S. Wen, Y. Xiang, and W. Zhou, ``Twitter spam detection: Survey of new approaches and comparative study," Comput. Secur., vol. 76, pp. 265_284, Jul. 2018.
[5]. S. J. Soman, ``A survey on behaviors exhibited by spammers in popular social media networks," in Proc. Int. Conf. Circuit, Power Comput. Tech- nol. (ICCPCT), Mar. 2016, pp. 1_6.
[6]. A. Gupta, H. Lamba, and P. Kumaraguru, ``1.00 per RT #BostonMarathon # prayforboston: Analyzing fake content on Twitter," in Proc. eCrime Researchers Summit (eCRS), 2013, pp. 1_12.
[7].F. Concone, A. De Paola, G. Lo Re, and M. Morana, ``Twitter analysis for real-time malware discovery," in Proc. AEIT Int. Annu. Conf., Sep. 2017, pp. 1_6.
[8].N. Eshraqi, M. Jalali, and M. H. Moattar, ``Detecting spam tweets in Twitter using a data stream clustering algorithm," in Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK), Nov. 2015, pp. 347_351.
[9].C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, ``Statistical features-based real-time detection of drifted Twitter spam," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 914_925, Apr. 2017.
[10].C. Buntain and J. Golbeck, ``Automatically identifying fake news in popular Twitter threads," in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2017, pp. 208_215.
[11].G. Stafford and L. L. Yu, ``An evaluation of the effect of spam on Twitter trending topics," in Proc. Int. Conf. Social Comput., Sep. 2013, pp. 373_378.
[12].A. Gupta and R. Kaushal, ``Improving spam detection in online social networks," in Proc. Int. Conf. Cogn. Comput. Inf. Process. (CCIP), Mar. 2015, pp. 1_6.
[13].F. Fathaliani and M. Bouguessa, ``A model-based approach for identifying spammers in social networks," in Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA), Oct. 2015, pp. 1_9.
[14].V. Chauhan, A. Pilaniya, V. Middha, A. Gupta, U. Bana, B. R. Prasad, and S. Agarwal, ``Anomalous behavior detection in social networking," in Proc. 8th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2017, pp. 1_5.
[15].S. Jeong, G. Noh, H. Oh, and C.-K. Kim, ``Follow spam detection based on cascaded social information," Inf. Sci., vol. 369, pp. 481_499, Nov. 2016.