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 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111214

# SPAM DETECTION AND FAKE USER IDENTIFICATION

**Prof.Pawar S.D[1], Holkar Omkar Omkar[2], Waghamare Akash[3]**

Head Of Department, Computer Department, SPCOET College Someshwarnagar, Baramati, India[1]

Student, Computer Department, SPCOET College Someshwarnagar, Baramati, India[2]

Student, Computer Department, SPCOET College Someshwarnagar, Baramati, India[3]

**Abstract**: The popularity of Online Social Networks (OSNs) is often faced with challenges of dealing with undesirable users and their malicious activities in the social networks. The most common form of malicious activity over OSNs is spamming wherein a bot (fake user) disseminates content, malware/viruses, etc. to the legitimate users of the social networks. The common motives behind such activity include phishing, scams, viral marketing and so on which the recipients do not indent to receive. It is thus a highly desirable task to devise techniques and methods for identifying spammers (spamming accounts) in OSNs. With an aim of exploiting social network characteristics of community formation by legitimate users, this paper presents a community-based framework to identify spammers in OSNs. The framework uses community-based features of OSN users to learn classification models for identification of spamming accounts. The preliminary experiments on a real-world dataset with simulated spammers reveal that proposed approach is promising and that using community-based node features of OSN users can improve the performance of classifying spammers and legitimate users.

**Keywords:** Classification, Fake user detection, Online social network, Spammer's identification.

## I. INTRODUCTION

In this paper we examine the approaches used to detect spammers on Twitter in this research. Furthermore, a taxonomy of Twitter spam detection algorithms is offered, which groups the strategies into four categories based on their capacity to detect: I fake content, (ii) spam based on URL, (iii) spam in hot topics, and (iv) false users. The presented methodologies are also compared based on several characteristics, such as user characteristics, content characteristics, graph characteristics, structural characteristics, and temporal characteristics

## II. PROBLEM STATEMENT

The profile data in social networks consist of two main parts, static and dynamic. Former is about the information which is set by the user statically, while the latter is observed by the system and is the result of users' activity on the social network. The static data typically includes users' demographics and interests, and dynamic data relates to user activities and position in the social network. Most of the existing research solutions depend on both static and dynamic data, which is inapplicable to other social networks, where it has merely a smaller number of visible static profiles and no dynamic profile details to the public. Due to its privacy policies and very restricted information visibility, none of the existing practical and theoretical means of fake profile detections are feasible to apply. Therefore, in this research our goal is to identify an approach to determine the spammers and fake profiles in Social Networks.

## III. LITERATURE SURVEY

In recent years, review spam detection has received significant attention in both business and academia due to the potential impact fake reviews can have on consumer behaviour and purchasing decisions. This survey covers machine learning techniques and approaches that have been proposed for the detection of online spam reviews. Supervised learning is the most frequent machine learning approach for performing review spam detection; however, obtaining labelled reviews for training is difficult and manual identification of fake reviews has poor accuracy. This has led to many experiments using synthetic or small datasets. Features extracted from review text (e.g., bag of words, POS tags) are often used to train spam detection classifiers. An alternative approach is to extract features related to the metadata of the review, or features associated with the behaviour of users who write the reviews. Disparities in performance of classifiers on different datasets may indicate the review spam detection may benefit from additional cross domain experiments to

DOI: 10.17148/IJARCCE.2022.111214

help develop more robust classifiers. Multiple experiments have shown that incorporating multiple types of features can result in higher classifier performance than using any single type of feature.

.

**Paper name:** Twitter fake account detection.
**Author:** B. Erçahin, Ö. Aktaş, D. Kilinç, and C. Akyol

Social networking sites such as Twitter and Facebook attracts millions of users across the world and their interaction with social networking has affected their life. This popularity in social networking has led to different problems including the possibility of exposing incorrect information to their users through fake accounts which results to the spread of malicious content. This situation can result to a huge damage in the real world to the society. In our study, we present a classification method for detecting the fake accounts on Twitter. We have preprocessed our dataset using a supervised discretization technique named Entropy Minimization Discretization (EMD) on numerical features and analyzed the results of the Naïve Bayes algorithm.

**2.paper name:** An integrated approach for malicious tweets detection using NLP.
**Author:** S. Gharge, and M. Chavan.

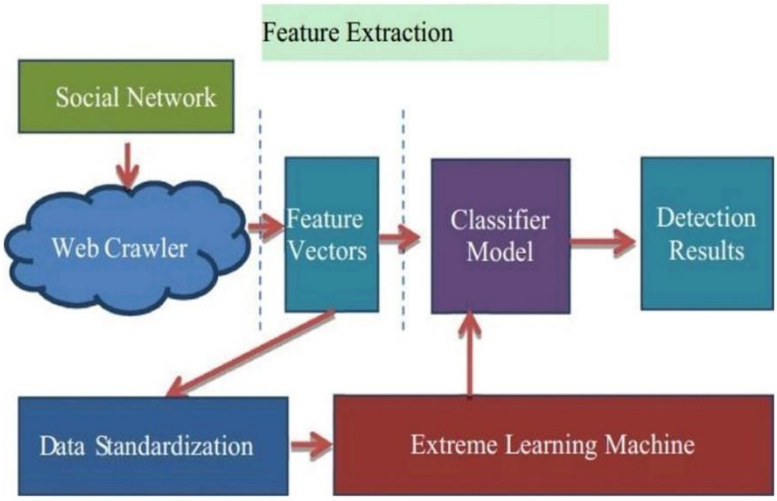
Many previous works have focused on detection of malicious user accounts. Detecting spams or spammers on Twitter has become a recent area of research in social network. However, we present a method based on two new aspects: the identification of spamtweets without knowing previous background of the user; and the other based on analysis of language for detecting spam on twitter in such topics that are in trending at that time. Trending topics are the topics of discussion that are popular at that time. This growing micro blogging phenomenon therefore benefits spammers.

**3.paper name:**：Detecting spammer son Twitter.
**Author:** F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida

With millions of users tweeting around the world, real time search systems and different types of mining tools are emerging to allow people tracking the repercussion of events and news on Twitter. However, although appealing as mech-anisms to ease the spread of news and allow users to discuss events and post their status, these services open opportu-nities for new forms of spam. Trending topics, the most talked about items on Twitter at a given point in time, have been seen as an opportunity to generate traffic and revenue. Spammers post tweets containing typical words of a trend-ing topic and URLs, usually obfuscated by URL shorteners, that lead users to completely unrelated websites.

## IV.PROPOSED SYSTEM

The aim of this paper is to identify different approaches of spam detection on Twitter and to present a taxonomy by classifying these approaches into several categories. For classification, we have identified four means of reporting spammers that can be helpful in identifying fake identities of users. Spammers can be identified based on: (i) fake content, (ii) URL based spam detection, (iii) detecting spam in trending topics, and (iv) fake user identification.



International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111214

## V. METHODOLOGY

An input camera device is required to take the multiple shots of the object/person. As for the algorithm, cascade classication is used for creating the multiple templates of the facial and detects facial features. A database is used for storing the templates along with student's roll number which acts as unique id. Roughout the verication process, the camera detects the facial features and tries to match against the templates which are already stored in the database; if found then it runs through the attendance management system process and marks the attendance for a particular student otherwise absent will be marked for not present student

## VI. CONCLUSION

Face detection is a computer technology that determines the location and size of human face in arbitrary (digital) image. The facial features are detected and any other objects like trees, buildings and bodies etc. are ignored from the digital image. It can be regarded as a specific‘ case of object-class detection, where the task is finding the location and sizes of all objects in an image that belong to a given class. Face detection, can be regarded as a more general‘ case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one). Basically there are two types of approaches to detect facial part in the given image i.e. feature base and image base approach. Feature base approach tries to extract features of the image and match it against the knowledge of the face features. While image base approach tries to get best match between training and testing images.

## REFERENCES

[1] B. Erçahin, Ö. Aktaş, 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, AntiAbuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12
[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. Technol. (ICCPCT), Mar. 2016, pp. 1–6