ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

Spammer Detection and Fake User Identification On Social Networks

M.Naresh Babu[1] , M.Pavani[2] , R.Praveen[3] , M.Sai Santosh[4] , N.S.V.S Vara Prasad[5] ,
[1]Asst.Professor, [2,3,4,5] Students
Department of Computer Science And Engineering
Sri Vasavi Institute Of Engineering and Technology, Pedana, A.P, India

ABSTRACT:-

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Face book have a tremendous impact and occasionally undesirable repercussions for daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased those results in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs). In this paper, we perform a review of techniques used for detecting spammers on Twitter. Moreover, taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also compared based on various features, such as user features, content features, graph features, structure features, and time features. We are hopeful that the presented study will be a useful resource for researchers to find the highlights of recent developments in Twitter spam detection on a single platform.

INTRODUCTION:-

It has become quite unpretentious to obtain any kind of information from any source across the world by using the Internet. The increased demand of social sites permits users to collect

DOI : 10.36893.JK.2022.V12I01N01.934-938

abundant amount of information and data about users. Huge volumes of data available on these sites also draw the attention of fake users [1]. Twitter has rapidly become an online source for acquiring real-time information about users. Twitter is an Online Social Network (OSN) where users can share anything and everything, such as news, opinions, and even their moods. Several arguments can be held over different topics, such as politics, current affairs, and important events. When a user tweets something, it is instantly conveyed to his/her followers, allowing them to outspread the received information at a much broader level [2]. With the evolution of OSNs, the need to study and analyze users' behavior s in online social platforms has intensive. Many people who do not have much information regarding the OSNs can easily be tricked by the fraudsters. There is also a demand to combat and place a control on the people who use OSNs only for advertisements and thus spam other people's accounts. Recently, the detection of spam in social networking sites attracted the attention of researchers. Spam detection is a difficult task in maintaining the security of social networks. It is essential to recognize spam in the OSN sites to save users from various kinds of malicious attacks and to preserve their security and privacy.

EXISTING SYSTEM:-

Find the spam and fake user identification is one of the most emerging problem in the social media. In the existing system used the diff rent kinds of algorithms which can able to find the fake user and spam detection. All the algorithms are used in the existing used based on the database. Initial they used to store the data and features related to the spammers and fake users in the database. After collecting the lots of data related to spammers they used to compare the features of the present user feature with the features in the database. By using this basic approach they developed different types of approaches which can able to solve this problem

DISADVANTAGES:-

1) It requires the more human effort to manage the data.
2) It takes the more time to classify the large amount of data.

DOI : 10.36893.JK.2022.V12I01N01.934-938

PROPOSED SYSTEM:

In the past few years Machine Learning and Deep Learning technologies bring the lots of changes in the world. Natural language processing is the technology which is the sub field of the machine learning which can able to solve this kind of text calcification problems easily. We are using the natural language processing in order to solve the problem because of its high accuracy in the text classification problem.

ADVANTAGES:

1) It requires less human effort compare to existing system.
2) It takes the less time to classify compare to existing system.
3) It has contained the less false rate when it is comparing with the existing system.

ARTICHUTURE:-

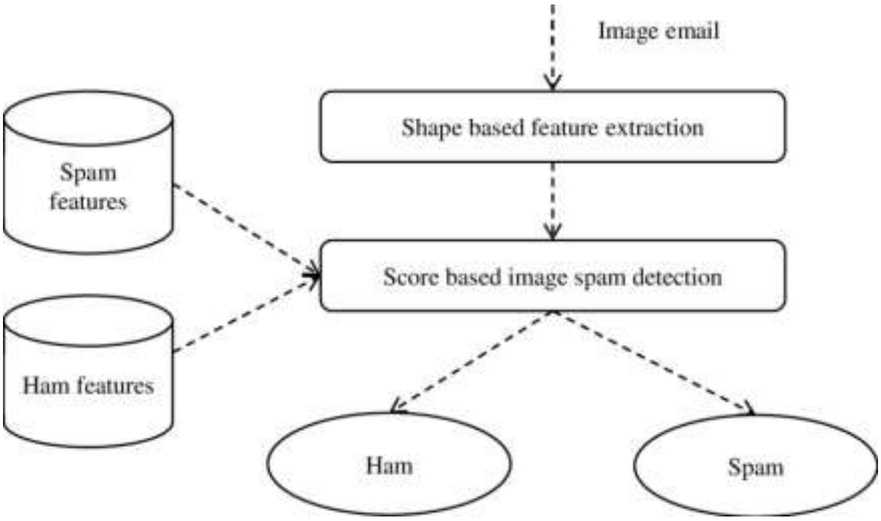


Image email
Shape based feature extraction
Spam features
Score based image spam detection
Ham features
Ham
Spam

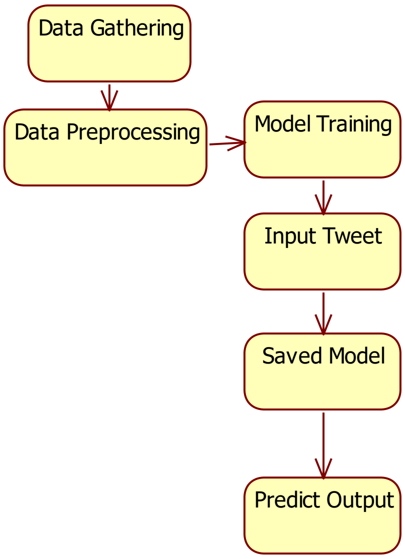
MODULE:

Implementation is the stage of the project when the theoretical design is turned out into a working system. This it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

DOI : 10.36893.JK.2022.V12I01N01.934-938

- **FAKE CONTENT BASED SPAMMER DETECTION**
- **URL BASED SPAM DETECTION**
- **DETECTING SPAM IN TRENDING TOPIC**

DATA FLOW DIAGRAM:-



Conclusion:-

In this paper, we performed a review of techniques used for detecting spammers on Twitter. In addition, we also presented taxonomy of Twitter spam detection approaches and categorized them as fake content detection, URL based spam detection, spam detection in trending topics, and fake user detection techniques. We also compared the presented techniques based on several features, such as user features, content features, graph features, structure features, and time features. Moreover, the techniques were also compared in terms of their specified goals and datasets used. It is anticipated that the presented review will help researchers and the information on state-of-the-art Twitter spam detection techniques in a consolidated form. Despite the development of efficient and effective approaches for the spam detection and fake user identification on Twitter [34], there are still certain open areas that require considerable attention by the researchers. The issues are briefly highlighted as under: False news identification on social media networks is an issue that needs to be explored because of the serious repercussions of such news at individual as well as collective level [25]. Another associated topic that is worth investigating is the identification of rumor sources on social media. Although a few studies based on statistical methods have already been conducted to detect the sources of rumors, more sophisticated approaches, e.g., social network based approaches, can be applied because of their proven effectiveness.

DOI : 10.36893.JK.2022.V12I01N01.934-938

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.

[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.

DOI : 10.36893.JK.2022.V12I01N01.934-938