IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Spammer Detection and Fake User Identification in Social Networks

[1]B.Raghava, [2]M.Amarnath, [3]A D Himavarsha , [4]Dr.Sunil Bhutada, [5]CH.Vijay Bhaskar

[1,2,3]B.Tech Student, [4]Professor, [5]Assistant Professor
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad, India

Abstract: Millions of people utilise social networking services all over the world. Users' interactions with social media sites like Twitter and Facebook have a huge impact on daily life, with some unfavourable consequences. Spammers have converted popular social networking sites into a target platform for disseminating a large number of irrelevant and harmful information. Twitter, for example, has grown to be one of the most widely utilised platforms of all time, allowing for an excessive amount of spam. Fake users send unwanted tweets to users in order to advertise services or websites, which not only harm actual users but also waste resources. Furthermore, the ability of spreading false information to users via fake identities has grown, resulting in the spread of hazardous materials. The detection of spammers and the identification of fraudulent users on Twitter has recently been a popular research topic in today's online social networks (OSNs).

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. We expect that the provided study will be a beneficial resource for academics looking for a single platform to find the highlights of current breakthroughs in Twitter spam detection.

PROBLEM DEFINITION

Obtaining any type of information from any source throughout the world has become relatively simple thanks to the Internet. The rising popularity of social media platforms allows users to amass a large amount of data and information about other people. Fake users are attracted to these sites because of the large amounts of data offered. Twitter has quickly grown in popularity as a way to get real-time information on users. It is now extremely simple to get any type of information from any source anywhere on the planet using the Internet. Users can gather a vast amount of data and information about other users thanks to the growing popularity of social media platforms. Because of the vast volumes of data available on these platforms, fake users are drawn to them. Fake users are drawn to these sites because of the massive amounts of data provided.

Motivation

Researchers have recently become interested in the identification of spam on social networking platforms. Spam detection is a difficult task in keeping social networks secure. To protect users from all types of dangerous assaults and to maintain their security and privacy, it is critical to spot spam on OSN sites. Spammers' risky manoeuvres result in significant community destruction in the real world. Spammers on Twitter have a variety of goals, including distributing false information, fake news, rumours, and spontaneous comments. Spammers achieve their destructive goals using adverts and a variety of other methods, such as supporting several mailing lists and then sending spam messages at random to broadcast their interests. These behaviours annoy the original users, who are referred to as non-spammers. Furthermore, it tarnishes the OSN platforms' reputation. As a result, it's critical to devise a strategy for detecting spammers so that corrective action may be done to stop their unwanted activity.

II. LITERATURE SURVEY

TITLE: Twitter fake account detection.
Authors: 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.

Title: 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. This kind of spam can contribute to de-value real time search services unless mechanisms to fight and stop spammers can be found. In this paper we consider the problem of detecting spam-mers on Twitter. We first collected a large dataset of Twit-ter that includes more than 54 million users, 1.9 billion links, and almost 1.8 billion tweets. Using tweets related to three famous trending topics from 2009, we construct a large la-beled collection of users, manually classified into spammers and non-spammers. We then identify a number of charac-teristics related to tweet content and user social behavior, which could potentially be used to detect spammers. We used these characteristics as attributes of machine learn-ing process for classifying users as either spammers or non-spammers. Our strategy succeeds at detecting much of the spammers while only a small percentage of non-spammers are misclassified. Approximately 70% of spammers and 96% of non-spammers were correctly classified. Our results also highlight the most important attributes for spam detection on Twitter.

TITLE: 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 spam-tweets 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. Our work tries to detect spam tweets in based on language tools. We first collected the tweets related to many trending topics, labelling them on the basis of their content which is either malicious or safe. After a labelling process we extracted a many features based on the language models using language as a tool. We also evaluate the performance and classify tweets as spam or not spam. Thus our system can be applied for detecting spam on Twitter, focusing mainly on analysing of tweets instead of the user accounts.

TITLE: Twitter spam detection: Survey of new approaches and comparative study.
Author: T. Wu, S. Wen, Y. Xiang, and W. Zhou.
Twitter spam has long been a critical but difficult problem to be addressed. So far, researchers have proposed many detection and defence methods in order to protect Twitter users from spamming activities. Particularly in the last three years, many innovative methods have been developed, which have greatly improved the detection accuracy and efficiency compared to those which were proposed three years ago. Therefore, we are motivated to work out a new survey about Twitter spam detection techniques. This survey includes three parts: 1) A literature review on the state-of-art: this part provides detailed analysis (*e.g.* taxonomies and biases on feature selection) and discussion (*e.g.* pros and cons on each typical method); 2) Comparative studies: we will compare the performance of various typical methods on a universal testbed (*i.e.* same datasets and ground truths) to provide a quantitative understanding of current methods; 3) Open issues: the final part is to summarise the unsolved challenges in current Twitter spam detection techniques. Solutions to these open issues are of great significance to both academia and industries. Readers of this survey may include those who do or do not have expertise in this area and those who are looking for deep understanding of this field in order to develop new methods.

TITLE: **A survey on behaviors exhibited by spammers in popular social media networks.**
AUTHOR: S. J. Soman.
Social networking sites have become a major factor of the Web and are playing an important role in the life of human being. People communicate with each other through social networking services (SNSs). Unfortunately, the Blogosphere has been infected by different forms of spam-like contents. The rise of social networking sites made them the targets of spammers as they lead the users to be fed up with irrelevant information while surfing. During early days, researchers were concentrating on the development of Honey pots for detecting spams. Twitter is a target platform for promoters and spammers. The authors survey the related literature that identifies the presence of spam as well as spammers in popular social media networks.

III. METHODOLOGY

Existing System:

In the field of Twitter spam detection, several studies have been conducted. A few polls on false user identification from Twitter were also conducted to cover the current state-of-the-art. Present a review of new methodologies and techniques for detecting Twitter spam. The survey above provides a comparative analysis of existing techniques. The authors of conducted a survey on the various behaviours displayed by spammers on the Twitter social network. The research also includes a literature analysis that acknowledges the existence of spammers on Twitter. Despite all of the studies that have been done, there is still a void in the literature. As a result, we examine the state-of-the-art in spammer detection and fake user identification on Twitter in order to close the gap. Furthermore, this study gives a taxonomy of Twitter spam detection methods and strives to provide a comprehensive overview of current developments in the field.

Proposed System:

The goal of this work is to discover several ways to spam detection on Twitter and to offer a taxonomy that categorises these approaches into different groups. For the purposes of classification, we've identified four methods for reporting spammers that can assist in detecting user impersonation. Spammers can be detected using the following methods: I false content, (ii) URL-based spam detection, (iii) spam detection in popular subjects, and (iv) fake user identification. Table 1 compares existing procedures and aids users in recognising the significance and effectiveness of the proposed methodology, as well as comparing their goals and outcomes. Table 2 examines the many features used to identify spam on Twitter. We hope that by conducting this poll, readers will be able to find a wealth of information on spammer detection strategies in one place.

The taxonomy for spammer detection approaches on Twitter is presented in Section II of this article. In Section III, we compare and contrast various strategies for detecting spammers on Twitter. Section IV contains an overview analysis and debate, while Section V brings the paper to a close and suggests some future research topics.

IV. SYSTEM DESIGN

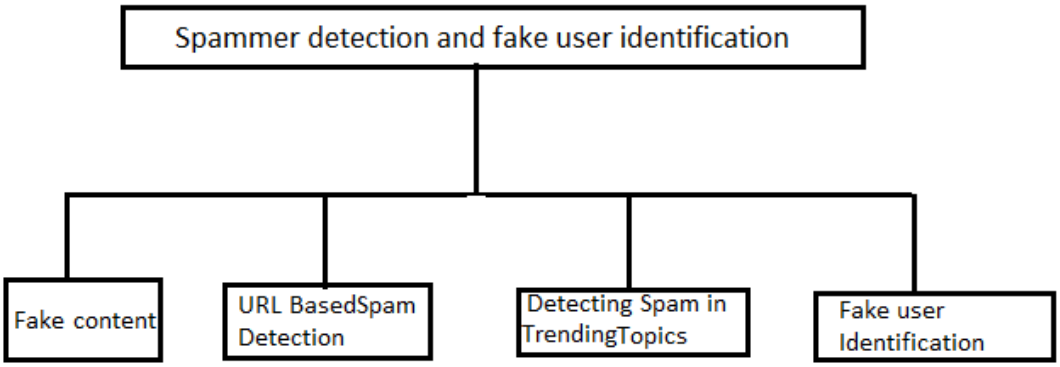

Figure 1) Architecture

MODULES & THEIR OUTPUTS:

User

The user is one of the modules; the user must first register with the programme, then be authorized by the administrator; only then will the user be able to see his personal page.Users can view his profile here, as well as the trending tweets that have been submitted by the compose tweet. Users can also follow each other.

The user can also see who is following them.

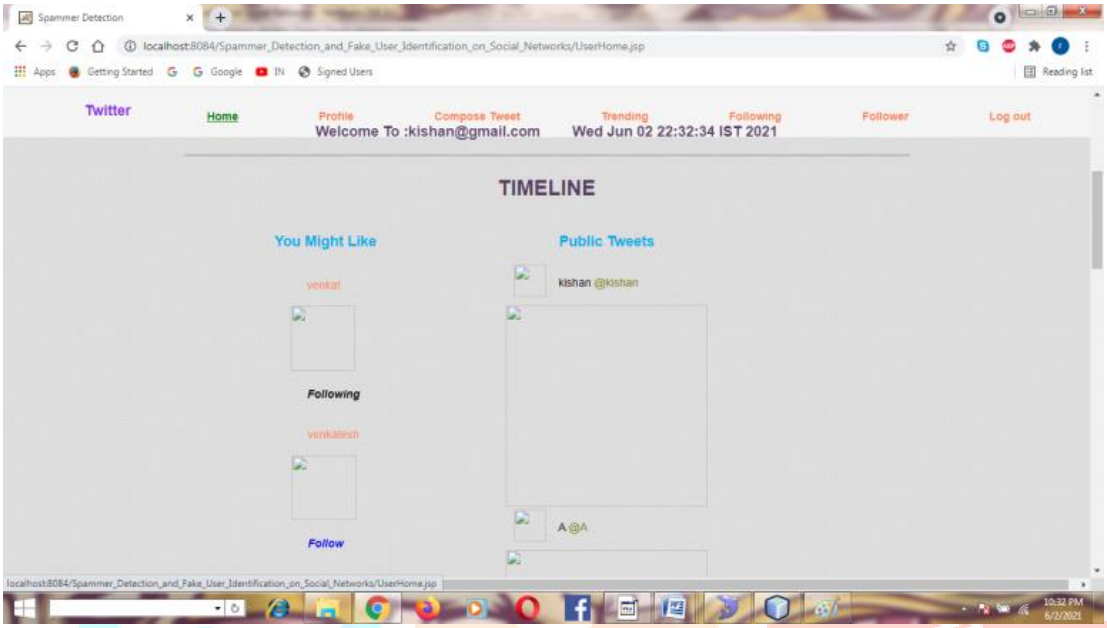

Figure 2) User Interface after logging in to user account

Compose Tweet

This is the user's internal module, and its primary function is to publish tweets to the public.

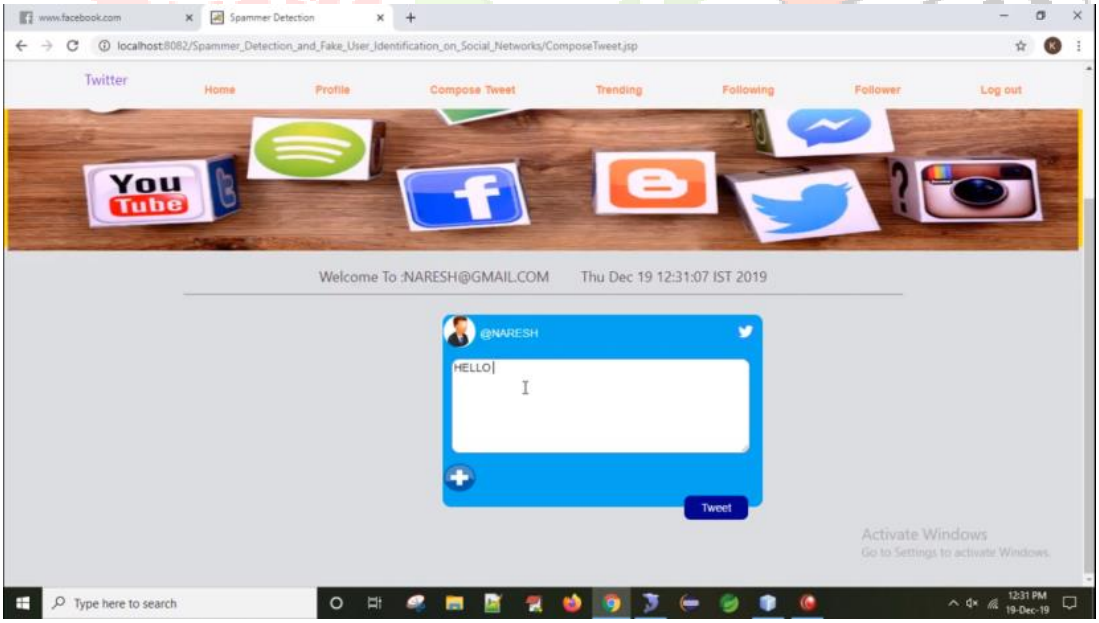

Figure 3) Compose tweet

Admin

The admin module is the main m y. After the administrator has successfully logged in, he can authorise users. Check out all of the users' tweets as well.

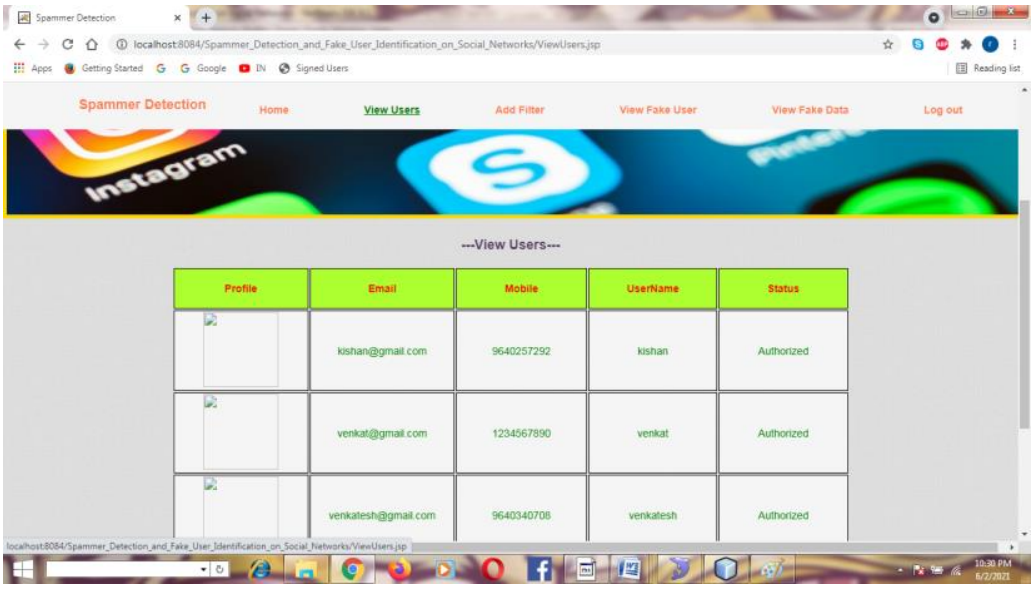

Figure 4) Admin interface after logging in to admin account

Fake User Identification

If any user does not have the appropriate details and does not have the admin's permission, this application will fail. However, these individuals can use the application to view the tweets of approved users. As a result, these individuals are labelled as "fake users."

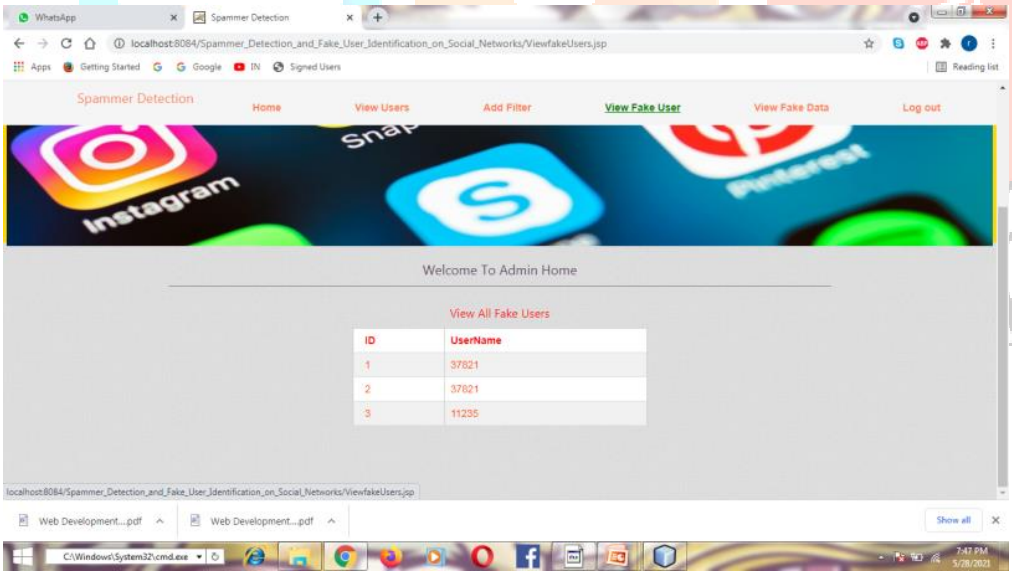

Figure 5) Identified Fake users list

Identifying Fake Data

People can post data into our application even if the user has not been allowed by the administrator. As a result, this type of data is regarded as fictitious.

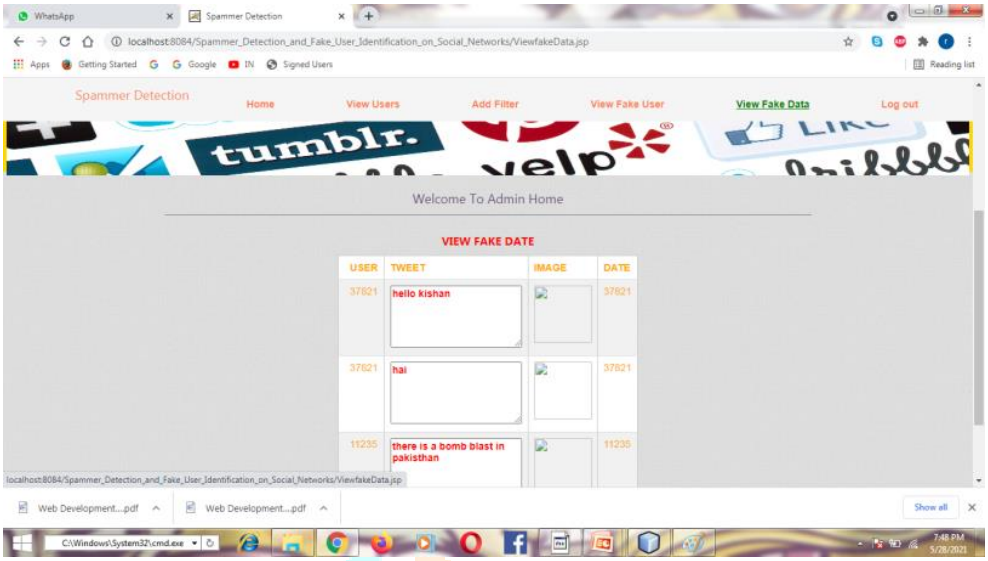

Figure 6) Fake content posted by the fake users

V. CONCLUSION

We conducted a review of approaches for detecting spammers on Twitter in this research. Furthermore, we proposed a taxonomy of Twitter spam detection strategies, dividing them into four categories: fake content identification, URL-based spam detection, spam identification in hot topics, and false user detection strategies. We also examined the offered strategies based on a variety of factors, including user characteristics, content characteristics, graph characteristics, structural characteristics, and temporal characteristics. Furthermore, the strategies were compared in terms of the aims they were designed to achieve and the datasets they employed. The given review is expected to aid academics by providing a comprehensive source of information on state-of-the-art Twitter spam detection systems.

VI. FUTURE SCOPE

Despite the development of efficient and successful ways for spam detection and fake user identification on Twitter , there are still certain gaps in the study that need to be addressed. The following are a few of the issues: Because of the substantial ramifications of false news on an individual and communal level, false news identification on social media networks is a subject that needs to be investigated. The identification of rumour origins on social media is another related topic worth researching. Although a few studies using statistical methods to discover the origin of rumours have already been undertaken, more complex approaches, such as social network-based approaches, can be used due to their demonstrated efficiency.

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 spammersonTwitter,’’inProc.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.
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.BuntainandJ.Golbeck,‘‘Automaticallyidentifyingfakenewsinpopular Twitter threads,’’ in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2017, pp. 208–215.