SPAMMER DETECTION AND FACK USER IDENTIFICATION ON SOCIAL NETWORKS

PRESENTED BY
STUDENT NAME :Mulkala.Anusha
COLLEGE NAME : Jayamukhi Institute Of Technological Sciences
DEPARTMENT : CSE
EMAIL ID : anushamulkala9@gmail.com
AICTE STUDENT ID: STU67c9d91b164581741281563

CONTENTS:

Abstract:

- Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook 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 that 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.

Literature survey:

S.No	Title	Authors	Description
1.	**Statistical features-based real-time detection of drifted Twitter spam**	C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min	Twitter spam has become a critical problem nowadays. Recent works focus on applying machine learning techniques for Twitter spam detection, which make use of the statistical features of tweets.
2.	**Automatically identifying fake news in popular Twitter threads**	C. Buntain and J. Golbeck	Information quality in social media is an increasingly important issue, but web-scale data hinders experts' ability to assess and correct much of the inaccurate content, or "fake news," present in these platforms.

Introduction:

- In this paper, we perform a review of techniques used for detecting spammers on Twitter. Moreover, a 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.

Problem statement:

- 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 that 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).

Existing system and drawback:

- Tingmin*et al*. provide a survey of new methods and techniques to identify Twitter spam detection. The above survey presents a comparative study of the current approaches.
- On the other hand, S. J. Somanet. al. conducted a survey on different behaviors exhibited by spammers on Twitter social network. The study also provides a literature review that recognizes the existence of spammers on Twitter social network.
- Despite all the existing studies, there is still a gap in the existing literature. Therefore, to bridge the gap, we review state-of-the-art in the spammer detection and fake user identification on Twitter

DRAWBACKS:

- No efficient methods used.
- No real time data used.
- More complex

Proposed system and advantages:

- In this paper author is describing concept to detect spam tweets and fake user account from online social network called twitter. To perform detection author is using twitter dataset and 4 different techniques called Fake Content, Spam URL Detection, Spam Trending Topic and Fake User Identification. Using above 4 techniques we can identify whether tweet is normal or spam and then using Random Forest data Mining algorithm we will train above dataset to classify number of spam and non-spam tweets or fake or non-fake accounts. For each technique author is using different data mining techniques to classify tweets as spam or non-spam but here we are using Random Forest classifier.

ADVANTAGES:

- This study includes the comparison of various previous methodologies proposed using different datasets and with different characteristics and accomplishments.
- Tested with real time data.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS :

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- **Operating System:** Windows
- **Coding Language**: Python 3.7

MODULES DESCRIPTION:

- Description of 4 techniques to detect tweet is spam or normal.
- The presented techniques are also compared based onvarious features, such as user features (retweets, tweets, followers etc.), content features (tweet content messages).

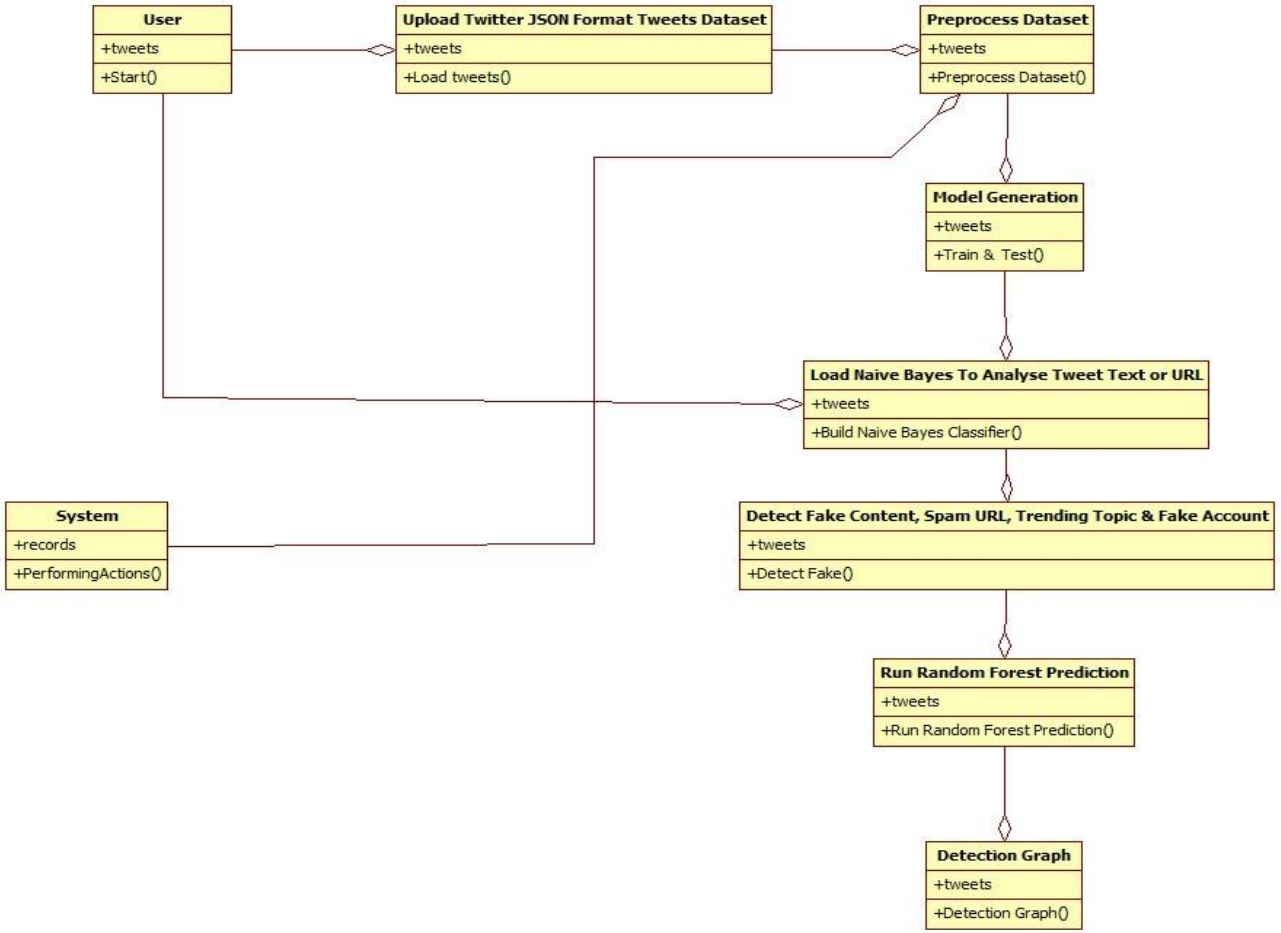
Fake Content: If the number of followers is low in comparison with the number of followings, the credibility of an account is low and the possibility that the account is spam is relatively high.

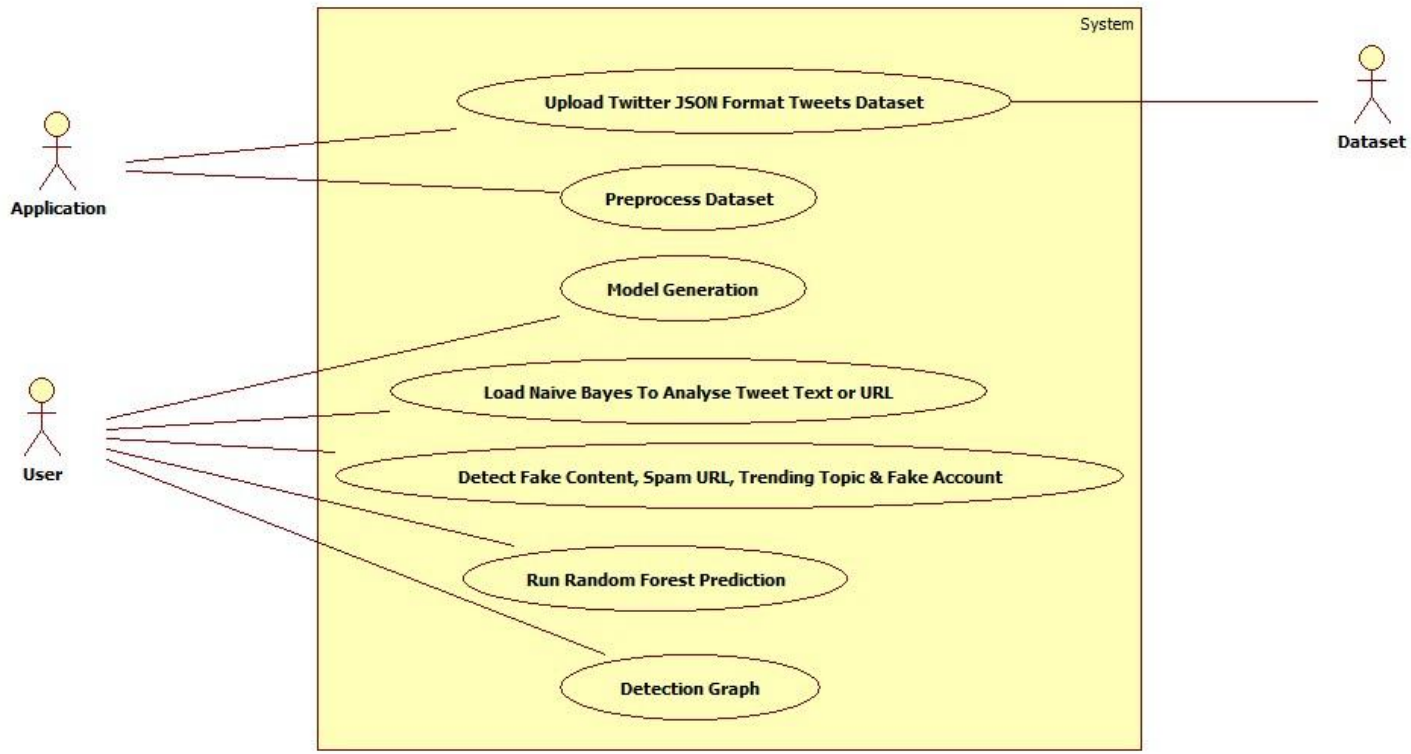
Spam URL Detection: The user-based features are identified through various objects such as account age and number of user favourites, lists, and tweets.

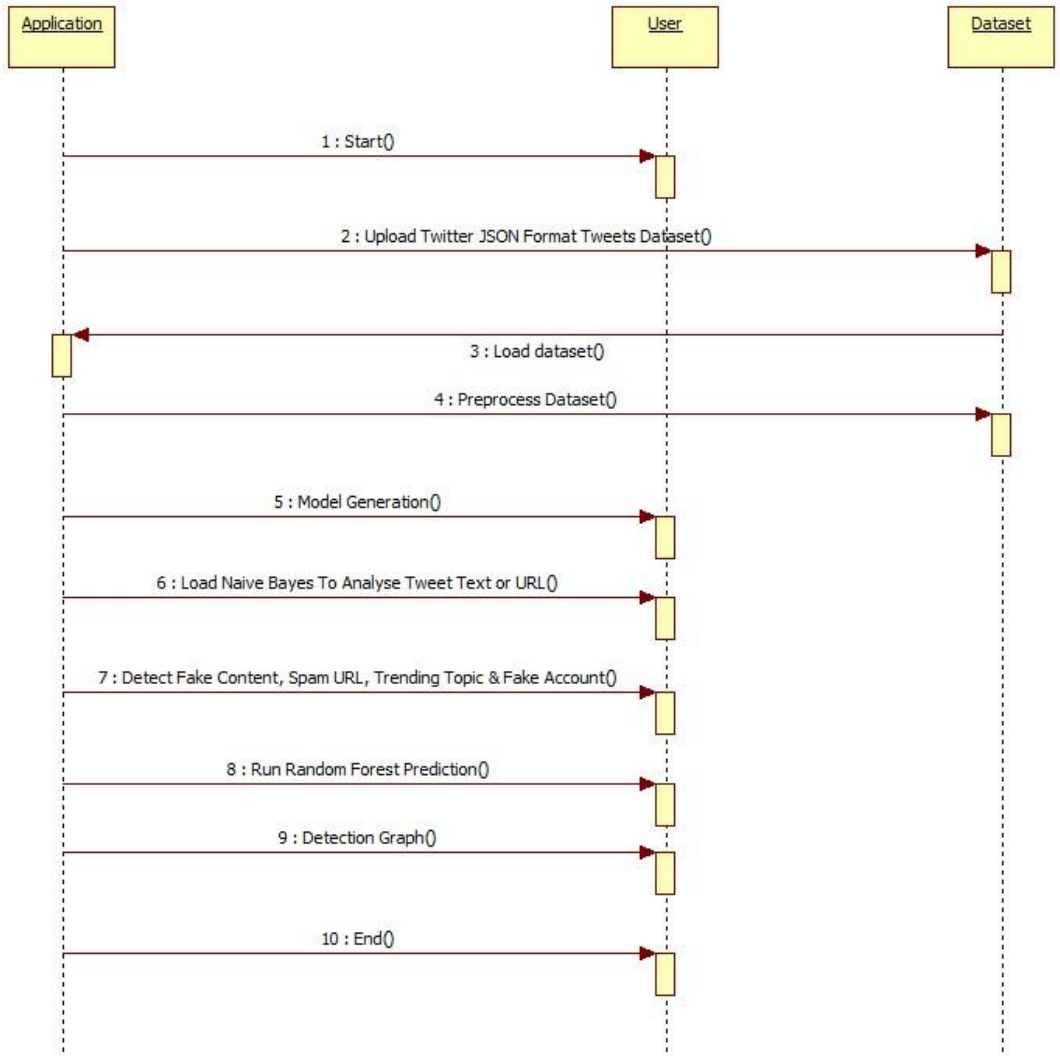
Detecting Spam in Trending Topic: In this technique tweets content will be classified using Naïve Bayes algorithm to check whether tweet contains spam or non-spam words.

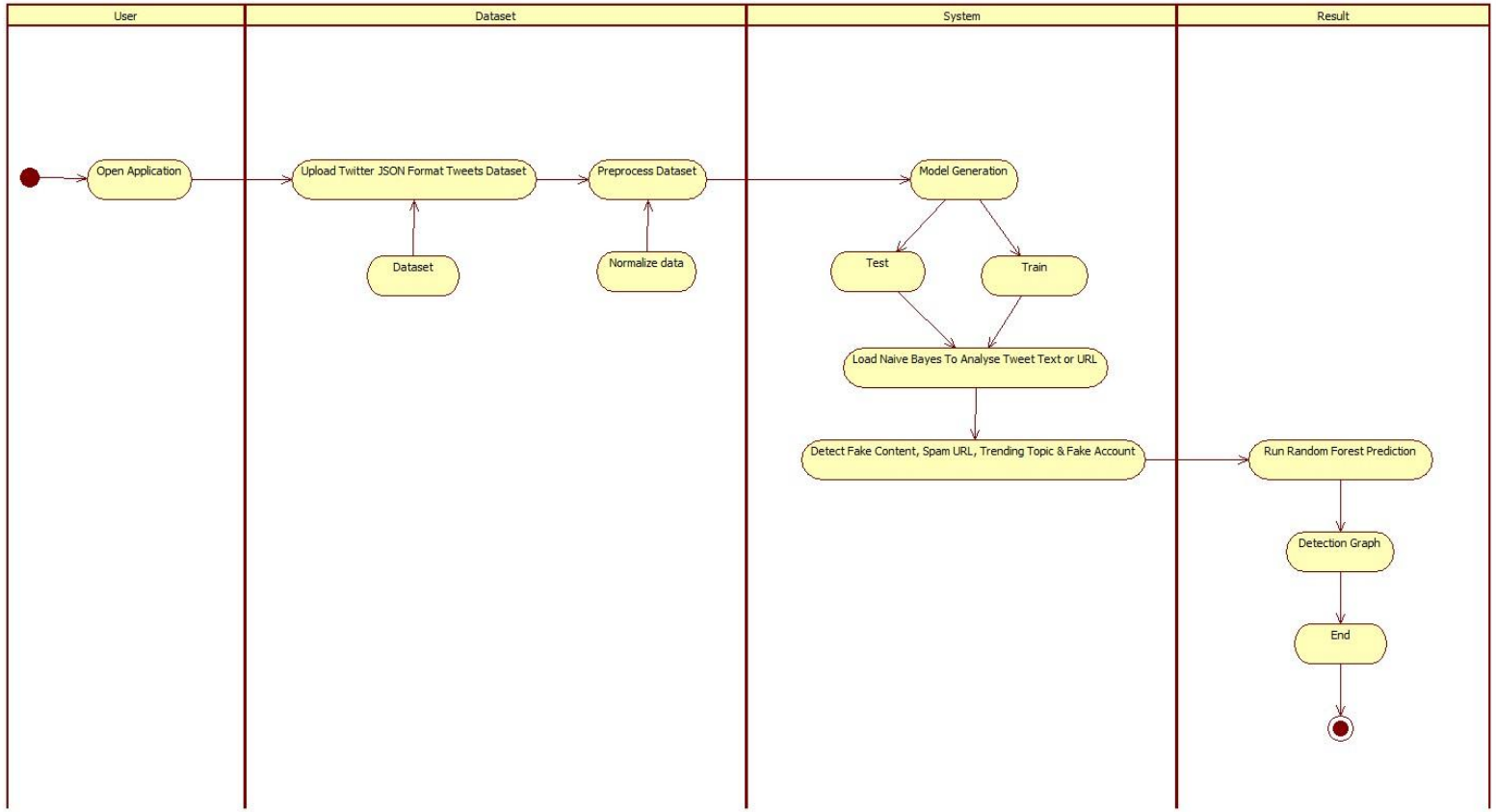
Fake User Identification: These attributes include the number of followers and following, account age etc. Alternatively, content features are linked to the tweets that are posted by users as spam bots that post a huge amount of duplicate contents as contrast to non-spammers who do not post duplicate tweets.

UML DIAGRAMS:




System
Upload Twitter JSON Format Tweets Dataset
Preprocess Dataset
Model Generation
Load Naive Bayes To Analyse Tweet Text or URL
Detect Fake Content, Spam URL, Trending Topic & Fake Account
Run Random Forest Prediction
Detection Graph
Application
User
Dataset


Application
User
Dataset
1 : Start()
2 : Upload Twitter JSON Format Tweets Dataset()
3 : Load dataset()
4 : Preprocess Dataset()
5 : Model Generation()
6 : Load Naive Bayes To Analyse Tweet Text or URL()
7 : Detect Fake Content, Spam URL, Trending Topic & Fake Account()
8 : Run Random Forest Prediction()
9 : Detection Graph()
10 : End()


User
Dataset
System
Result
Open Application
Upload Twitter JSON Format Tweets Dataset
Preprocess Dataset
Dataset
Normalize data
Model Generation
Test
Train
Load Naive Bayes To Analyse Tweet Text or URL
Detect Fake Content, Spam URL, Trending Topic & Fake Account
Run Random Forest Prediction
Detection Graph
End

IMPLEMENTATION:

TECHNOLOGIES:

Python :-

- Below are some facts about Python.
- Python is currently the most widely used multi-purpose, high-level programming language.
- Python allows programming in Object-Oriented and Procedural paradigms. Python programs generally are smaller than other programming languages like Java.
- **Machine Learning :**
- Before we take a look at the details of various machine learning methods, let's start by looking at what machine learning is, and what it isn't. Machine learning is often categorized as a subfield of artificial intelligence, but I find that categorization can often be misleading at first brush.

TESTING:

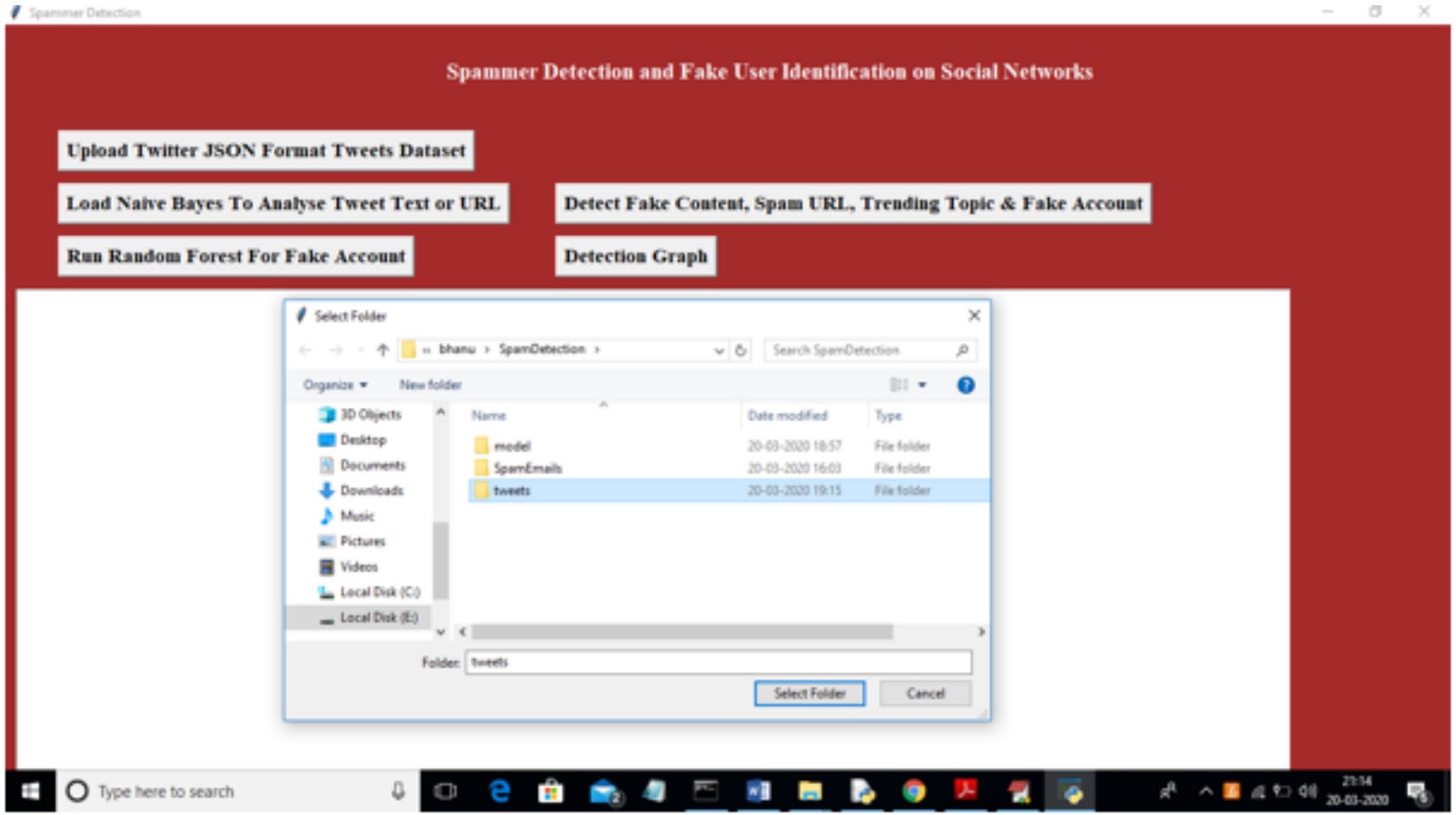
- Testing is a process of executing a program with the aim of finding error.To make our software perform well it should be error free. If testing is done successfully it will remove all the errors from the software.

Types of Testing

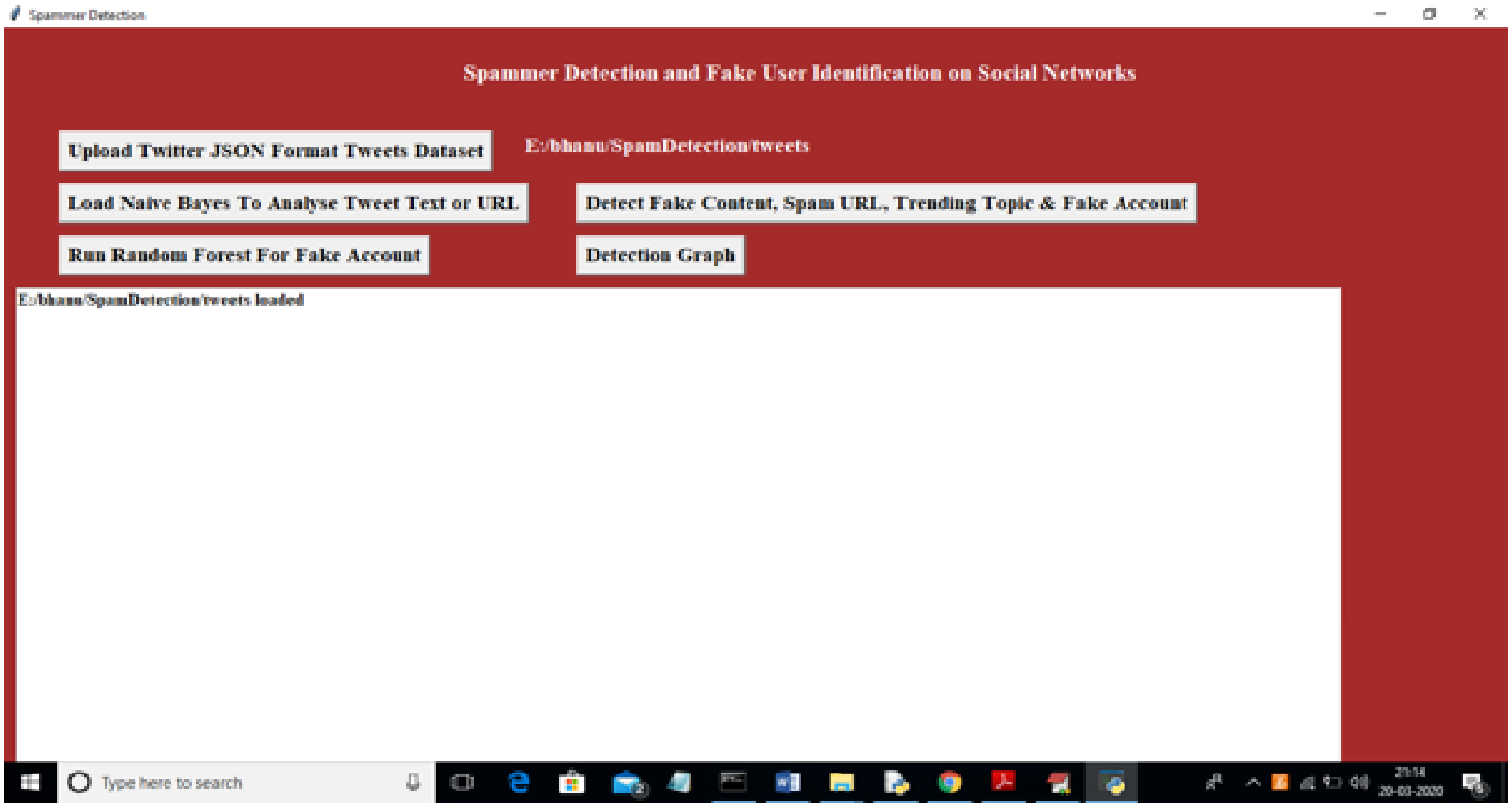
- White Box Testing
- Black Box Testing
- Unit testing
- Integration Testing
- Alpha Testing
- Beta Testing
- Performance Testing and so on

Results:

In above screen click on 'Upload Twitter JSON Format Tweets Dataset' button and upload tweets folder

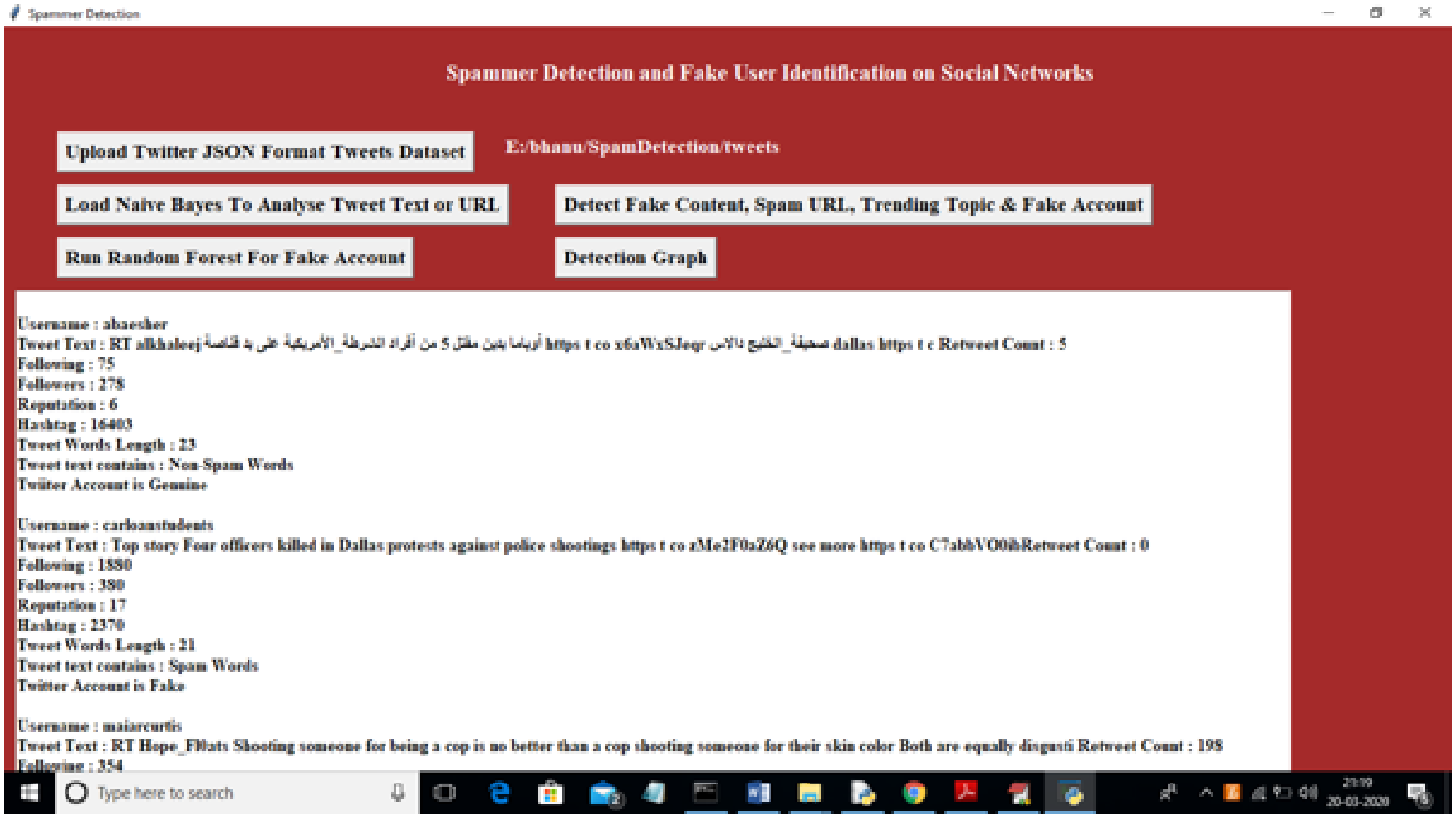


In above screen I am uploading ‘tweets’ folder which contains tweets from various users in JSON format. Now click open button to start reading tweets

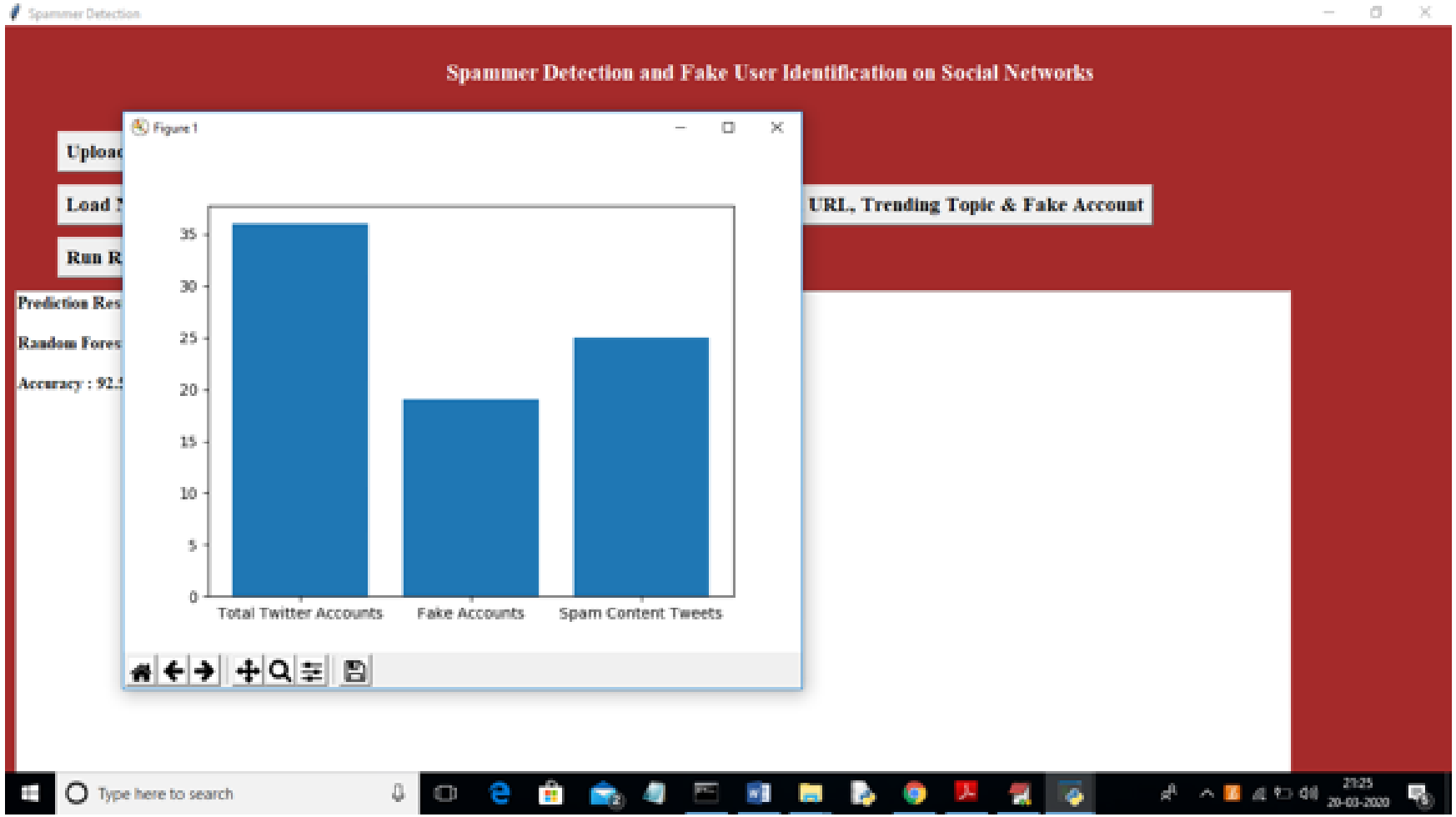


In above screen we can see all tweets from all users loaded. Now click on 'Load Naive Bayes To Analyse Tweet Text or URL' button to load Naïve Bayes classifier


Spammer Detection
Spammer Detection and Fake User Identification on Social Networks
Upload Twitter JSON Format Tweets Dataset
E:/bhanu/SpamDetection/tweets
Load Naive Bayes To Analyse Tweet Text or URL
Detect Fake Content, Spam URL, Trending Topic & Fake Account
Run Random Forest For Fake Account
Detection Graph
Naive Bayes Classifier loaded
Type here to search
21:16
20-03-2020


Spammer Detection
Spammer Detection and Fake User Identification on Social Networks
Upload Twitter JSON Format Tweets Dataset
E:/bhanu/SpamDetection/tweets
Load Naive Bayes To Analyse Tweet Text or URL
Detect Fake Content, Spam URL, Trending Topic & Fake Account
Run Random Forest For Fake Account
Detection Graph
Username : abaesher
Tweet Text : RT alkhaleej أوباما يدين مقتل 5 من أفراد الشرطة الأمريكية على يد القاصة https t co x6aWxSJeqr صحيفة الخليج دالاس https t c Retweet Count : 5
Following : 75
Followers : 278
Reputation : 6
Hashtag : 16403
Tweet Words Length : 23
Tweet text contains : Non-Spam Words
Twitter Account is Genuine
Username : carloanstudents
Tweet Text : Top story Four officers killed in Dallas protests against police shootings https t co zMe2F0aZ6Q see more https t co C7abbVO0hRetweet Count : 0
Following : 1880
Followers : 380
Reputation : 17
Hashtag : 2370
Tweet Words Length : 21
Tweet text contains : Spam Words
Twitter Account is Fake
Username : maiarcurtis
Tweet Text : RT Hope_FHats Shooting someone for being a cop is no better than a cop shooting someone for their skin color Both are equally disgusti Retweet Count : 198
Following : 354
Type here to search
21:19
20-03-2020


Spammer Detection
Spammer Detection and Fake User Identification on Social Networks
Upload Twitter JSON Format Tweets Dataset
E:/bhanu/SpamDetection/tweets
Load Naive Bayes To Analyse Tweet Text or URL
Detect Fake Content, Spam URL, Trending Topic & Fake Account
Run Random Forest For Fake Account
Detection Graph
Prediction Results
Random Forest Algorithm Accuracy & Confusion Matrix
Accuracy : 92.5
Type here to search
21:24
20-03-2020



In above graph x-axis represents total tweets, fake account and spam words content tweets and y-axis represents count of them

conclusion:

- Using above techniques we can detect whether tweets contains normal message or spam message. By detecting and removing such spam messages help social networks in gaining good reputation in the market. If social networks did not remove spam messages then its popularity will be decreases. Now a days all users are heavily dependent on social networks to get current news and business and relatives information and thus protecting it from spammer help it to gain reputation.

FUTURE ENHANCEMENTS:

- Although a few studies based on statistical methods have already been conducted to detect the sources of rumors, more sophisticated approaches, e.g., social networkbased approaches, can be applied because of their proven effectiveness.

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.

THANK YOU