

PROFESSIONAL TRAINING REPORT

at

Sathyabama Institute of Science and Technology (Deemed to be University)

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering Degree in

Computer Science and Engineering

By

1. MALLE RAHUL KUMAR REDDY

Reg.No : 38110290

2. MADITHATI VEERA BHADRA REDDY

Reg.No : 38110287



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

**SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI – 600119. TAMILNADU.**



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with “A” grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



SCHOOL OF COMPUTING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **1. MALLE RAHUL KUMAR REDDY (Reg.No : 38110290) 2. MADITHATI VEERA BHADRA REDDY (Reg.No : 38110287)**

who have done the Project in “**MACHINE LEARNING**” and carried out the project entitled “**Spam Review Detection Using Linguistic Methods for Specified user in Twitter**” under my supervision from JANUARY 2022 to MARCH 2022.

Internal Guide

DR.R.M GOMATHI

Head of the Department

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **1. MALLE RAHUL KUMAR REDDY (Reg.No : 38110290) 2. MADITHATI VEERA BHADRA REDDY (Reg.No : 38110287)** hereby declare that the Professional training report on “**Spam Review Detection Using Linguistic Methods for Specified user in Twitter**” done by me under the guidance of **DR.R.M GOMATHI, at Sathyabama University** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE:

SIGNATURE OF THECANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D, Dean**, School of Computing, **Dr.R.Subhashini M.E., Ph.D. , Head** of the Department of Information Technology for providing necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **DR.R.M GOMATHI** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **COMPUTER SCIENCE AND ENGINEERING** who were helpful in many ways for the completion of the project.

TABLE OF CONTENTS

Chapter No.	Title	Page No.
1.	Abstract	6
2.	Introduction	7-8
3.	Literature Survey	9-11
4.	Proposed Systems	12
5.	Architecture	13
6.	Use Case diagram	14
7.	Algorithm	15
8.	Modules	16-18
9.	Implementation	18
10.	Result	19-21
11.	Conclusion	22
12.	References	23

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO.
5.1	SYSTEM ARCHITECTURE	13
6.1	USE CASE	14
10.1	ABSTRACT	19
10.2	TESTING	20
10.3	DATA COLLECTION	20
10.4	USER CHECK	21
10.5	DETECTION	21

CHAPTER 1

ABSTRACT

- Online review systems play an important role in affecting consumers' behaviors and decision making, attracting many spammers to insert fake reviews to manipulate review content and ratings. To increase utility and improve user experience, some online review systems allow users to form social relationships between each other and encourage their interactions. Here, we aim at providing an efficient and effective method to identify review spammers by incorporating social relations based on two assumptions that people are more likely to consider reviews from those connected with them as trustworthy.
- Review spammers are less likely to maintain a large relationship network with normal users. The contributions are two-fold:
- We elaborate how social relationships can be incorporated into review rating prediction and propose a trust-based rating prediction model using proximity as trust weight.
- We design a trust-aware detection model based on rating variance which iteratively calculates user-specific overall trustworthiness scores as the indicator.
- Experiments on the dataset collected from Yelp.com show that the proposed trust-based prediction achieves a higher accuracy than standard CF method, and there exists a strong correlation between social relationships and the overall trustworthiness scores.

Keywords:

Machine Learning; Spam Detection; Scalability; Twitter

CHAPTER 2

INTRODUCTION

What Is A Social Network?

Wikipedia defines a social network service as a service which “focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software.”

A report published by OCLC provides the following definition of social networking sites: “Web sites primarily designed to facilitate interaction between users who share interests, attitudes and activities, such as Facebook, Mixi and MySpace.”

What Can Social Networks Be Used For?

Social networks can provide a range of benefits to members of an organization:

Support for learning: Social networks can enhance informal learning and support social connections within groups of learners and with those involved in the support of learning.

Support for members of an organization: Social networks can potentially be used by all members of an organization, and not just those involved in working with students. Social networks can help the development of communities of practice.

Engaging with others: Passive use of social networks can provide valuable business intelligence and feedback on institutional services (although this may give rise to ethical concerns).

Ease of access to information and applications: The ease of use of many social networking services can provide benefits to users by simplifying access to other tools and applications. The Facebook Platform provides an example of how a social networking service can be used as an environment for other tools.

Common interface: A possible benefit of social networks may be the common interface which spans work / social boundaries. Since such services are often used in a personal capacity the interface and the way the service works may be familiar, thus minimizing training and support needed to exploit the services in a professional context. This can, however, also be a barrier to those who wish to have strict boundaries between work and social activities.

Opportunities and Challenges

The popularity and ease of use of social networking services have excited institutions with their potential in a variety of areas. However effective use of social networking services poses a number of challenges for institutions including long-term sustainability of the services; user concerns over use of social tools in a work or study context; a variety of technical issues and legal issues such as copyright, privacy, accessibility; etc.

Institutions would be advised to consider carefully the implications before promoting significant use of such services.

Scope of the project:

Social media can also be used for spreading fake news and malicious links (like Ransomware and malware). So, we need to be careful while using social media. Since social media is widely used now-a-days, these spams are increasing rapidly. In this project we are mainly focusing on spam detection in social media (specifically in Twitter) using machine learning techniques.

CHAPTER 3

LITERATURE SURVEY

1) Statistical features-based real-time detection of drifted Twitter spam

Authors: 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. In our labeled tweets data set, however, we observe that the statistical properties of spam tweets vary over time, and thus, the performance of existing machine learning-based classifiers decreases. This issue is referred to as “Twitter Spam Drift”. In order to tackle this problem, we first carry out a deep analysis on the statistical features of one million spam tweets and one million non-spam tweets, and then propose a novel Lfun scheme. The proposed scheme can discover “changed” spam tweets from unlabeled tweets and incorporate them into classifier's training process. A number of experiments are performed to evaluate the proposed scheme. The results show that our proposed Lfun scheme can significantly improve the spam detection accuracy in real-world scenarios.

2) Automatically identifying fake news in popular Twitter threads

Authors: 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. This project develops a method for automating fake news detection on Twitter by learning to predict accuracy assessments in two credibility-focused Twitter datasets: CREDBANK, a crowd sourced dataset of accuracy assessments for events in Twitter,

and PHEME, a dataset of potential rumors in Twitter and journalistic assessments of their accuracies. We apply this method to Twitter content sourced from Buzz Feed's fake news dataset and show models trained against crowd sourced workers outperform models based on journalists' assessment and models trained on a pooled dataset of both crowd sourced workers and journalists. All three datasets, aligned into a uniform format, are also publicly available. A feature analysis then identifies features that are most predictive for crowd sourced and journalistic accuracy assessments, results of which are consistent with prior work. We close with a discussion contrasting accuracy and credibility and why models of non-experts outperform models of journalists for fake news detection in Twitter.

3) A model-based approach for identifying spammers in social networks

Authors: F. Fathaliani and M. Bouguessa

We view the task of identifying spammers in social networks from a mixture modeling perspective, based on which we devise a principled unsupervised approach to detect spammers. In our approach, we first represent each user of the social network with a feature vector that reflects its behavior and interactions with other participants. Next, based on the estimated users feature vectors, we propose a statistical framework that uses the Dirichlet distribution in order to identify spammers. The proposed approach is able to automatically discriminate between spammers and legitimate users, while existing unsupervised approaches require human intervention in order to set informal threshold parameters to detect spammers. Furthermore, our approach is general in the sense that it can be applied to different online social sites. To demonstrate the suitability of the proposed method, we conducted experiments on real data extracted from Instagram and Twitter.

Problem Statement

For real-time spam detection, we further extracted 12 lightweight features for tweet representation. Spam detection was then transformed to a binary classification problem in the feature space and can be solved by conventional machine learning techniques and evaluated the impact of different factors to the spam detection performance, which included spam to no spam ratio, feature discretization, training data size, data sampling, time-related data, and machine learning techniques. From the results it come to know that spam tweet detection is still a big challenge and a robust detection technique should take into account the three aspects of data, feature, and model.

CHAPTER 4

PROPOSED SYSTEM:

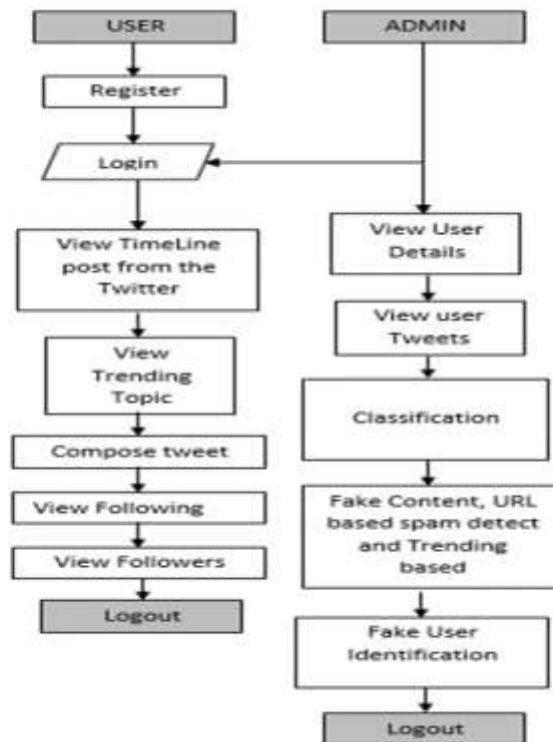
- The aim of the project is to identify fake user detection on Twitter and to present a framework by classifying these approaches into several categories. For classification, we have identified four means of reporting spammers that can be helpful in identifying fake identities of users. Spammers can be identified based on:
 - 1) Fake content
 - 2) URL based spam detection
 - 3) Detecting spam in trending topics
 - 4) Fake user identification.
- Moreover, the analysis also shows that machine learning-based techniques can be effective for identifying fake user on Twitter. However, the selection of the most feasible techniques and methods is highly dependent on the available data.

ADVANTAGES OF PROPOSED SYSTEM

- This study includes machine learning methodology proposed using real time datasets and with different characteristics and accomplishments.
- The proposed system is more effective and accurate than other existing systems.
- Tested with real time data.

CHAPTER 5

Architecture



5.1 SYSTEM ARCHITECTURE

CHAPTER 6

Use Case Diagram



6.1 USE CASE DIAGRAM

CHAPTER 7

Algorithm

Decision Trees for Classification:

Decision Trees are a type of Supervised Machine Learning technique (that is you explain what the input is and what the corresponding output is in the training data) where the data is continuously split according to a certain parameter. The tree can be explained by two entities, namely decision nodes and leaves. The leaves are the decisions or the final outcomes. And the decision nodes are where the data is split.

ID3 Algorithm

- The ID3 algorithm begins with the original set as the root node.
- On each iteration of the algorithm, it iterates through every unused attribute of the set and calculates the entropy or the information gain of that attribute.
- It then selects the attribute which has the smallest entropy (or largest information gain) value. The set is then split or partitioned by the selected attribute to produce subsets of the data.
- The algorithm continues to recurs on each subset, considering only attributes never selected before.

CHAPTER 8

Modules

1. Admin Module
2. Data Collection
3. Train and Test
4. Machine Learning Technique
5. Detection of Fake User

MODULE DESCRIPTIONS:

Admin Module:

In the first module, we develop the Online Social Networking (OSN) system module. We build up the system with the feature of Online Social Networking System, Twitter. Where, this module is used for admin login with their authentication.

Data Collection:

We will be using a Python Library called Tweepy to connect to the Twitter API and collect the data. We download tweets containing certain key words, to incorporate the words or hash tags that contain relevant keyword related to fake users.

Some of the most important fields are:

- Text, which contains the text included in the tweet.
- Created at, which is a timestamp of when the tweet was created.
- User, which contains information about the user that created the tweet, like the username and user id.

Train and Test:

- We present the proposed framework for metadata features are extracted from available additional information regarding the tweets of a user, whereas content-based features aim to observe the message posting behavior of a user and the quality of the text that the user uses in posts.

Machine Learning Technique:

- The number of features, which are associated with tweet content, and the characteristics of users are recognized for the detection of spammers. These features are considered as the characteristics of machine learning process for categorizing users, i.e., to know whether they are spammers or not.
- In order to recognize the approach for detecting spammers on Twitter, the labelled collection in pre-classification of fake user and legitimate user has been done. Next, those steps are taken which are needed for the construction of labeled collection and acquired various desired properties.
- In other words, steps which are essential to be examined to develop the collection of users that can be labelled as fake user or legitimate user. At the end, user attributes are identified based on their behavior, e.g., who they interact with and what is the frequency of their interaction.
- In order to confirm this instinct, features of users of the labelled collection has been checked. Two attribute sets are considered, i.e., content attributes and user behavior attributes, to differentiate one user from the other.

Detection of Fake User:

- In this module, we implement the collection of tweets with respect to trending topics on Twitter. After storing the tweets in a particular file format, the tweets are subsequently analyzed.
- Labelling of fake user is performed to check through all datasets that are available to detect the malignant.

- Feature extraction separates the characteristics construct based on the language model that uses language as a tool and helps in determining whether the user is fake or not.
- The classification of data set is performed by shortlisting the set of tweets that is described by the set of features provided to the classifier to instruct the model and to acquire the knowledge for spam detection.
- The fake user detection uses the classification technique to accept tweets as the input and classify the fake user and legitimate user.

Chapter 9

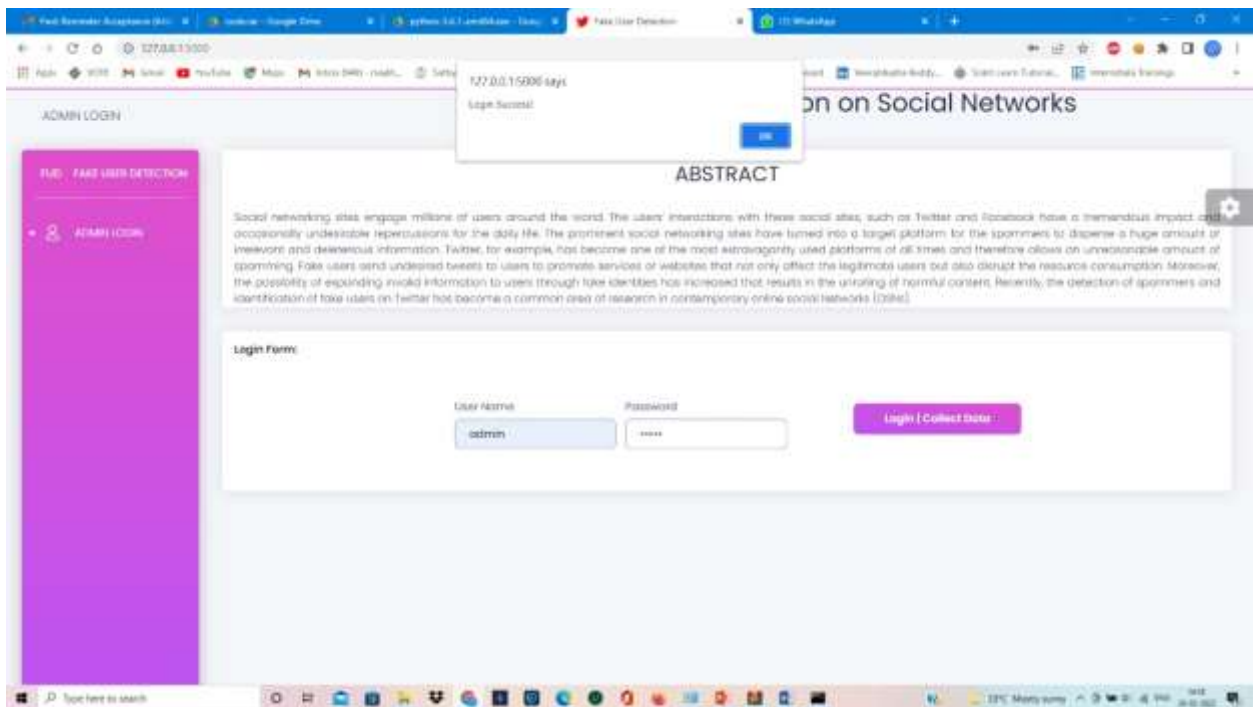
Implementation

- We will be using Flask API, a web framework written in Python.
- Tweepy an open-source python package to access the Twitter API.
- Importing packages like Pandas, NumPy, csv, matplotlib for graphical representation and importing algorithms from Sklearn as we are using python Library.
- Fetching the dataset and training a model to detect fake users by reading the csv file.
- Extracting the features.
- Checking and display the user info from the dataset.
- Building and evaluating the results.
- Displaying whether the user is fake or legitimate with the help of matplotlib.

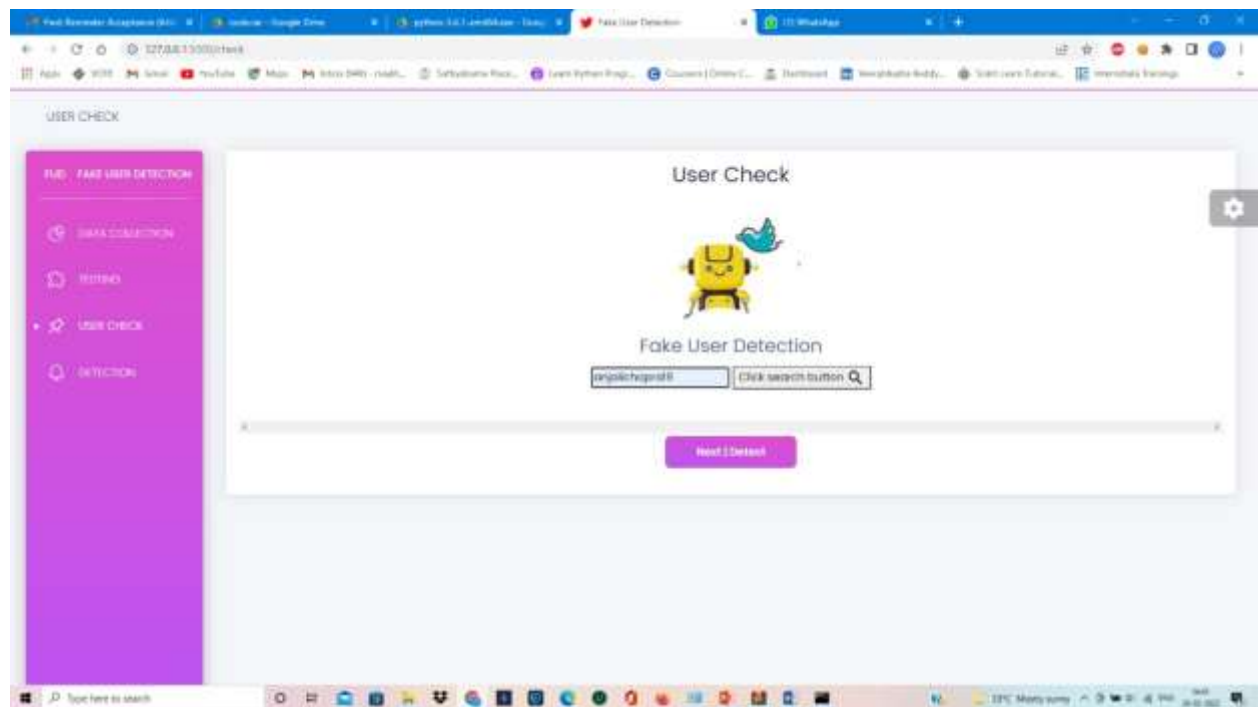
CHAPTER 10

RESULT

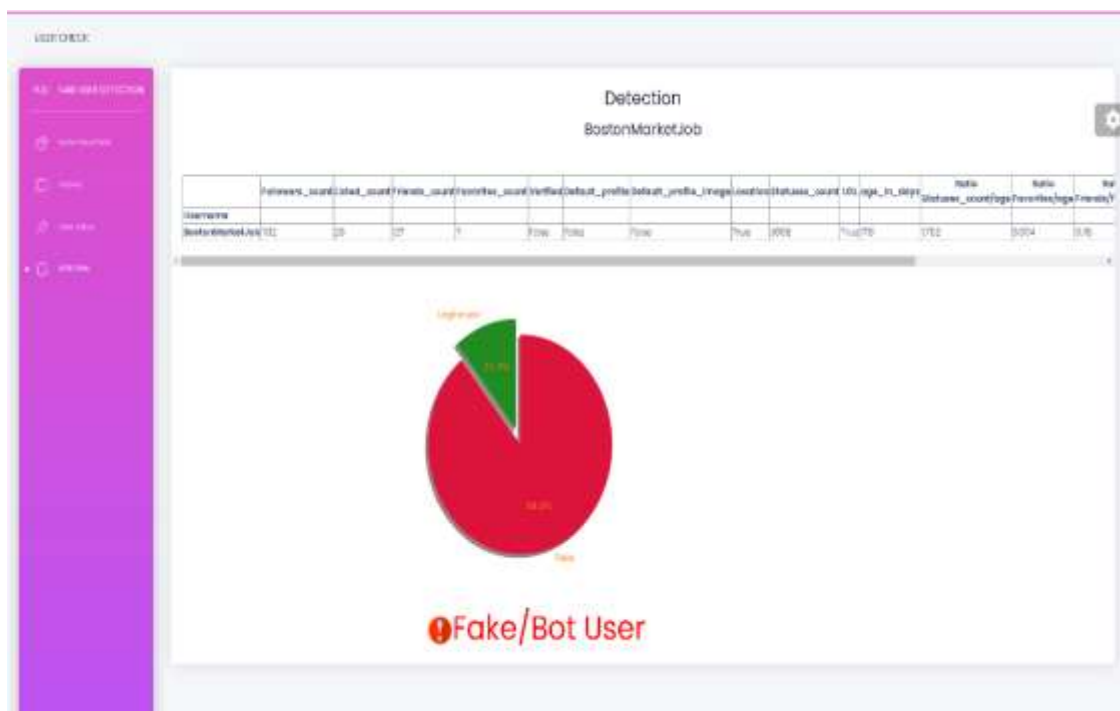
- Algorithm's accuracy depends on the type and size of your dataset.
- More the data, more chances of getting correct accuracy.
- Machine learning depends on the variations and relations
- Understanding what is predictable is as important as trying to predict it.



10.1. ABSTRACT



10.4 USER CHECK



10.5 DETECTION

CHAPTER 11

Conclusion

- We performed a review of techniques used for detecting spammers on Twitter.
- We also presented a 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.
- The techniques were also compared in terms of their specified goals and datasets used.
- It is anticipated that the presented review will help researchers find 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. Twitter, 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.
- 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.

CHAPTER 12

References

- [1] Guanjan Lin, Junyang Qui & Paul Rimba, “Near real-time twitter spam detection with machine learning techniques”, *International Journal of computers and applications*, 16 April 2020.
- [2] I. David, O. S. Siordia, and D. Moctezuma, “Features combination for the detection of malicious Twitter accounts,” in *Proc. IEEE Int. Autumn Meeting Power, Electron. Comput. (ROPEC)*, Nov. 2016, pp. 1–6.
- [3] M. Babcock, R. A. V. Cox, and S. Kumar, “Diffusion of pro- and anti-false information tweets: The black panther movie case,” *Comput. Math. Org. Theory*, vol. 25, no. 1, pp. 72–84, Mar. 2019.
- [4] S. Keretna, A. Hossny, and D. Creighton, “Recognising user identity in Twitter social networks via text mining,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2013, pp. 3079–3082.
- [5] C. Meda, F. Bisio, P. Gastaldo, and R. Zunino, “A machine learning approach for Twitter spammers detection,” in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2014, pp. 1–6.
- [6] W. Chen, C. K. Yeo, C. T. Lau, and B. S. Lee, “Real-time Twitter content polluter detection based on direct features,” in *Proc. 2nd Int. Conf. Inf. Sci. Secur. (ICISS)*, Dec. 2015, pp. 1–4.