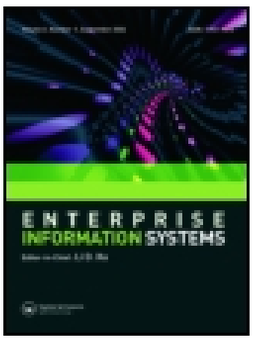

Enterprise Information Systems

ISSN: 1751-7575 (Print) 1751-7583 (Online) Journal homepage: https://www.tandfonline.com/loi/teis20

Classification of spammer and nonspammer content in online social network using genetic algorithm-based feature selection

Somya Ranjan Sahoo & B. B. Gupta

To cite this article: Somya Ranjan Sahoo & B. B. Gupta (2020): Classification of spammer and nonspammer content in online social network using genetic algorithm-based feature selection, Enterprise Information Systems, DOI: 10.1080/17517575.2020.1712742

To link to this article: https://doi.org/10.1080/17517575.2020.1712742

Published online: 21 Jan 2020.

ENTERPRISE INFORMATION SYSTEMS
https://doi.org/10.1080/17517575.2020.1712742

Taylor & Francis
Taylor & Francis Group

Classification of spammer and nonspammer content in online social network using genetic algorithm-based feature selection

Somya Ranjan Sahoo and B. B. Gupta

Department of Computer Engineering, National Institute of Technology Kurukshetra, Kurukshetra, India

ABSTRACT

The emergence of online social network invokes social actors to share their personal information digitally. Moreover, it provides the facility to maintain their links with people of same interest globally. Take advantage of these services; it has become a fascinating testbed to invite various threats like a spammer. Detection of spammer in OSN is one of the most critical tasks. Spammer not only spreads unwanted or bad advertisement but does certain malicious activity in others' profiles. By clearly understanding the activities of different threats, some incremental and accurate approaches are needed for detecting spammer content and profiles involved in these activities by using social network services. Therefore, the focus of this article is to detect spammer content and account, specifically on the leading microblogging platform called Twitter. We propose a hybrid approach which leverages the capabilities of various machine learning algorithms to separate spammer and nonspammer contents and account. Initially, the optimisation algorithm called genetic algorithm analyses the various features and selects the best suitable features that influence the behaviour of user account, and these features are then used to train classifiers. Our framework achieved to severalise spammer and nonspammer content in an effective way. Finally, to prove the efficiency of our proposed framework, a comparative analysis is conducted with some existing state-of-art techniques. The experimental analysis shows that our approach achieves a high detection rate of 99.6%, which is better than other state-of-art techniques.

ARTICLE HISTORY
Received 13 April 2019
Accepted 5 January 2020

KEYWORDS
Online social networking; genetic algorithm; spammer; machine learning

1. Introduction

Online social network (OSNs) sites are the hub for content gathering and information sharing in World Wide Web like Facebook, Twitter, and Instagram by internet users (Sahoo and Gupta, 2019b). Recently, OSN sites have become an essential medium for communication and content sharing. These sites associate the people of the same interests, belongings, acquaintances, and friends of friends in a common platform for sharing their views and contents (Li, Zhang, and Zhang 2018; Gupta and Gugulothu 2018; Zhang et al. 2017). The content protection described as the protection of the user's subject matter from unauthorised access those spreads malicious depicted object in the form of a

CONTACT B. B. Gupta gupta.brij@gmail.com National Institute of Technology Kurukshetra, Kurukshetra, India

spammer in social sites (Sahoo and Gupta, 2019a). Social network users share contents by posting favourite webpage links, multimedia contents like video, images and different files. Furthermore, the social interaction structure of OSN renders trust and network credibility. According to Statista statistics report (https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users), Facebook is the leading OSN sites with 2.1 billion users worldwide, and Twitter is having 336 million users. Instagram covers more than 1 billion active monthly users worldwide for multimedia content sharing and communication like Facebook and Twitter as on December 2018. Due to the escalating number of active users, the content generated is heterogeneous day by day on these social networks. The user postsmultimedia contents like videos and images that are accomplished by the profile holder in the form of like, tags, shared content, hashtag, comments, and direct message transfer. According to Zophoria statistics report (https://zephoria.com/top-15-valuable-facebook-statistics), Facebook has 2.23 billion monthly active users and Facebook users share approximately 300 million photo contents per day. It also describes 1.47 billion people who log onto Facebook daily, which shows the 11 percentage of growth rate. The most common age demographic in social media is between the ages of 24 and 35 years. The analysis represents the involvement of users in social media increasing day by day with five new profiles per second and creates huge traffic in the network between 1 and 3 pm. According to the Statista statistics, Facebook and Twitter play a significant role in the daily activity of the user for sharing the content and communication purposes. Instagram is another photo content medium for users who are very much interested in multimedia contents like photo and video. These social media provide some features like photo editing with some filters that attract the user for multimedia content modification and sharing the same in the network. Due to the increasing content of multimedia, it is used as a gateway for spammers to spread malicious contents in the network using short URLs depicted in Figure 1.

According to the Nexgate statistics report, the spammer contents are increasing day by day with exponential growth in the social network. Spammers use various ways to spread spam contents in the social network like spreading the content in the form of advertising for business, malware contents in the form of malicious URLs attached with text, image, as well as the video also for phishing attack (Qabajeh, Thabtah, and Chiclana 2018) in various profiles. In addition to this, spammer always follows unknown users who are not aware of the security of social networks by spreading spammer contents in the form of link attack

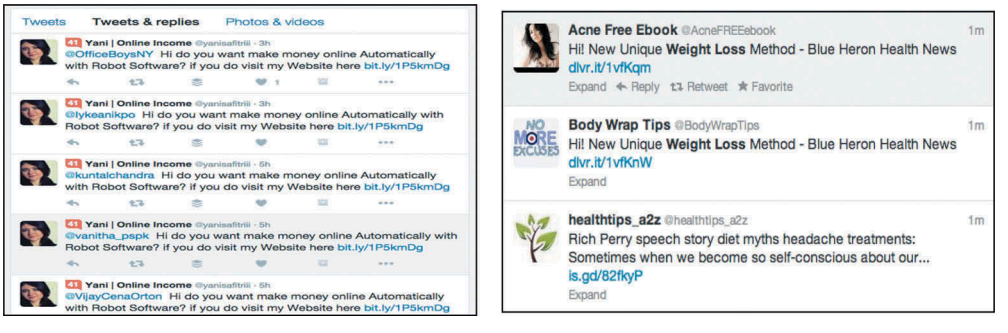

Figure 1. Example of malicious content spreads through short URLs embedded in Tweets.

with various contents. The linked URL activates malwares inside user's profile and steals personal information. Also, these URLs are used to access other profiles remotely. That activity also initiates the bot inside the user's profile and spreads malicious links that are associated with these accounts. The initiated bot leads to a DDoS attack in the network (Chhabra, Gupta, and Almomani 2013; Gupta, Agrawal, and Yamaguchi 2016; Sheng, Su, and Wang 2019; Alieyan et al. 2019; Dahiya and Gupta 2019). The embedded link associated with the message gathers personal information of users like bank account details, user identity and many more related to the user profiles by targeting the legitimate user's profile. Commonly, spammers on social media affected the legitimate users in the network. For detecting, classifying and naming the legitimate user from spammer users is a very tedious job. In the past, detecting spammer content by analysing profile is the easiest job as compared to the current scenario due to the trustworthy nature and automated fashion of the spreading mechanism.

Detecting spammers in OSN's by distinguishing the spammer account from legitimate one is a classification approach in the machine learning (ML) environment by analysing the profile contents of different users and is based on the behavioural issues. The different classification methods undergo various issues and challenges to mitigate the goal. These include various features such as dimension, training time, testing time and accuracy in various terms. To overcome the different issues and challenges, various classification techniques are applied in the ML environment with proper dimensions like SVM (support vector machine) (Gurumurthy et al. 2019), random forest (Liaw and Wiener 2002), KNN (K-nearest neighbour) (Kibanov et al. 2018), JRip (Class JRIP 2015), decision tree (Khan et al. 2018), Bayesian network (Fazil and Abulaish 2018), etc. Finding the optimal parameters for supervised ML is very tedious due to the high dimensionality of features in the profile contents. Therefore, existing methods and frameworks suffer from various numerous issues such as maximum training time, lower true positive rate, and poor classification in terms of features; it is also time-consuming to build a proper model for classifying the content in the form of spammer and legitimate (Zheng et al. 2016). Recently, some effective ML algorithms are introduced such as ELM (extreme learning machine) classifiers. These classifiers are considered promising and effective over other classifiers such as Bayesian and SVM classifiers. Another effective technique is called genetic algorithm (GA), which gives optimised output in the form of different feature analysis for the input values. These techniques are more effective in terms of efficiency and performance. In this approach, user parameters are used as per requirement without any external attributes. The selected suitable features extracted from the rough dataset are the objective function of the GA. The in-depth choice of features would measure a lot of unlike combinations for the functional process. Different studies from an academic perspective show the completeness of the GA for feature selection at high learning speed. Nevertheless, the GA for feature extraction and selection has some limitations. This stochastic algorithm can have trouble obeying equality constraints because of sensitiveness at initial population and a wide diversity of feasible solutions. Also, the solution quality deteriorates with increasing size of the problem. However, detection of a spammer in the social network requires a better feature selection that is suitable for classification of spammer from a legitimate one. For better performance of the classification, GAcombines with extreme ML approach to give a better decision-making environment. Our proposed model based on GA and ML is described below.

In this article, we designed a hybrid framework that uses a GA for feature selection and applied various ML–based classification techniques for better decision-making in the form of spammer and legitimate by reviewing more than 6000 numbers of profile contents. We use a classification method based on the selected dataset with GA for designing the appropriate model for spammer detection in different social network platforms. The main contributions for spammer detection in this article are as follows:

- By analysing the spammer activity on different social networks such as Facebook, Twitter and Instagram, we proposed a framework that facilitates spammer account by classifying the legitimate one. Compared with another detection method, our proposed framework detects the spammer account with higher accuracy by selecting the suitable feature sets.
- Our framework offers a new GA-based feature selection mechanism that is appropriate for the classifier for classifying the spammer content. This method provides a higher detection rate in terms of spammer detection at lesser training time to build the model.
- We construct some level data set for our framework by using crawler. We collect user information that is available publicly and some private information by using Twitter API.
- We also provide some comparative analysis of our framework with other proposed approach for better decision-making and validate the effectiveness of our spammer detection framework.

Our proposed framework helps the OSN users to prevent their accounts from spammers. It helps to analyse various posts shared by the users over a social network platform. Moreover, our framework works under different situations to detect various threats by analysing some other features. The ML approach boosts up the performance of our framework by implementing various classification approaches. It provides a system with the ability to learn and improve from experience without being explicit automatically. It focuses on the development of computer programs that can access data and use it to learn from them. The main practical implication in our framework is learning association. It aims to process developing insights into the association between different features that are used to predict the behaviour of user account and content in social platform. Also, the process of GA enhances the capability of selecting the best suitable features that help in improving the spammer detection rate. By this optimisation principle (Zhao et al. 2019), the features associated with every account in OSNs are tested based on their behaviour in different circumstances and a cluster of features are formed for the next operation. Furthermore, OSN is used as social software in Enterprise Information System (EIS) as a primary component for business and commercial purposes. EIS uses features of OSN for connecting people within the same business interests. When employee and client data are at stake, privacy becomes an immense issue at the enterprise level. Prior to entering the OSN, EIS must address security concerns. Our framework will help to identify misleading information in the form of spammer in Twitter environment by analysing public as well as private profile features of the user.

2. Related work

The advancement of the social network has pulled the tending of many security researchers towards their security that directly or indirectly protect the user contents. The OSN platform is based on the trust of network services and is dependent on the service provider, which might cause various consequences. With the growth of the social network and their service to mankind, the protection of the user content and services is the main research area for the various industry and academician. The primary objective of detecting spammer is based on the classification algorithm implemented in ML environment by using profile features and the spreading content by the user. The researchers and academicians identify the spammer detection methods in various applications like in social network platform, web applications and emails.

The author in (Cao and Caverlee 2015) in the year 2015, analysed and investigate the different behavioural analysis that detects spam URLs in various social networking sites. In (Soiraya, Thanalerdmongkol, and Chantrapornchai 2012), the decision tree technique such as J48 and the various texts of the Facebook messages including several keywords, the average number of keywords, number of links, and length of words are taken into consideration for the detection of the spam content shared by the Facebook users. Thomas et al. (2011a) described five various valuable contents related to Twitter accounts like content filtering, scalability, proper decision-making, ability to retain the model with new content and independence of text model developed for detecting spammers in the social network. The most important factor of this model is that it works on the real-time and content filtering option within a short period. An approach based on the classification with social honeypots is deployed in the network proposed by Lee, Caverlee, and Webb (2010). A spam classification approach was proposed by the author based on the user's profile that made an in-depth study about the spammer behaviour in social network platforms like Twitter. That approach also understands the entire spam ecosystem that spread malicious content in the form of various links and others. Chen et al. (2017) proposed a spam detection method based on the malicious link and that analysed the click rate of spam message by various users in the social platform. Wang et al. (2012) analysed malicious users that are socially connected and spread malicious contents through the network. They also proposed an algorithm based on the inference rule that detects malicious accounts. Yang, Yang, and Wilson (2015) analysed in Sina web environment and designed an LDA-based algorithm and framework that detect who often spread and posted malicious content in the form of a political post. They also use linked structure in the graph approach to detect Sybil nodes and unwanted links that spread malicious content in different social network platforms. Gyongyi et al. (2004) proposed a trust rank-based scheme to detect trust-based links posted by some users in the network. Xue et al. (2013) proposed an invitation graph scheme to defend against social Sybil account in various social networks. Zhang et al. (2018) proposed a method called COLOUR+ that computes and detects spammer account in various social network accounts in mobile devices. It uses the concept of communication and interaction between the various accounts and neighbour accounts also. The author in (Ghosh et al. 2012) proposed one formula based on the famous link farming that widely spreads, and the spammer links are farmed from a fraction of users, who are social people.. Based on the ranking policy, the authors proposed a scheme that tracks users who have followed spammers account in

various microblogging sites in the web. Cao et al. (2012) preceded a Sybil Rank algorithm which trusts on graph structure to rank the various users in the network. It identified a strong node and started some random walk principle to reach other nodes and normalised property. The outcome of this principle has a very high false-positive and false-negative rate between malicious and nonmalicious accounts. Boshmaf et al. (2015) anticipate certain activity at the user level by anticipating victim activities of the user through various ratings, and, this method integrates the various weight into a graph structure. In the next level, random walk algorithm applicable to graph structure and find victim accounts. This method predicts a higher rate of prediction than Sybil rank algorithm. Wei et al. (2012) develop a new tool called Sybil defender that utilises topologies of the graph to defend against various attacks. The tools have certain limitations based on the random walks within the community. When it exceeds 2000 walks, the running time increased by 20% of the original one. Alghamdi et al. (2018) proposed one-hybrid solution to detect spammer contents and filter the spammer content from nonspammer one by analysing the users' focused interest on various modules in social network. The features are selected based on the interest level of the user and the frequent movement of the user from one focused interest to another focused interest. Zhou et al. (2018) analysed and compared the behaviour of malicious and nonmalicious accounts based on some criteria called the viability of account, the sequence of the transaction and spatial correlation among various accounts. The information of the various accounts collected from Tencent QQ global leading OSN with 54 features to analyse the various characteristics. Sohrabi and Karimi (2018) proposed one filtering system based on clustering technique with unsupervised learning called DB index and SVM for higher precision value and decision tree method for better time management to detect spammer account in social network platform. Aslan et al. (2018) proposed an auto-detection system for the cyber security-related accounts on the microblogging platform to detect malicious content by analysing various features through an ML algorithm. Zhang et al. (2019) described the spammer detection method on the basis of pseudo-honey-pot frameworks for monitoring and collecting user's content. The authors also take advantage of the user's diversity and the normal user's behaviour for spammer analysis. The authors used various classifiers for the detection of spammer on Twitter by assigning incomplete samples to the most relevant microcluster with arbitrary distribution (Tajalizadeh and Boostani 2019). As far as EIS environment is concerned, Tse et al. (2018) analysed various texts from social platforms by using a novel comprehensive data analysis framework. The framework captures the customer perception during the crisis and effectiveness of various management practices which the company adopted. Also, Hu et al. (2015) proposed various algorithms to detect influential communities of special interest. By analysing various profile activities and interests, the authors partition various users into different groups of the same interest. The target users for various advertisements and product information are the main concern for e-commerce industries to spread propaganda. By analysing various threats in EIS era, in this work, we detect the malicious accounts that spread spammer contents in the social network. The features that are well suitable for spammer analysis are identified using a GA. The GA analyzes various features based on the content spread by the user. It also uses some ML algorithms that are used for improving the performance in decision-making. A proper set of features are selected from the profile as well as content-based features from various accounts in Twitter by using a crawler. The

crawler extracts public and some private features related to user account with spreading contents. It is imperative to select the best suitable features for performance analysis instead of a blind experiment. The process of best suitable feature selection is a part of the proposed framework. The simple method selects all combinations, i.e. (2^n-1) features for n-dimensional feature vector. Hence, various methodologies are introduced for filtering the best suitable features for our analysis.

3. The proposed architecture for spammer detection

Microblogging site such as Twitter suffers from a lot of spammer contents that are published every day by the social network users. The primary objective of this article is to furnish a framework that detects spammer content by analysing profile content through different features and selects the best suitable features for analysis through ML environment depicted in Figure 2.

3.1. Architectural details

Every day, lots of spam contents are generated rapidly and published over the Internet through OSNs. Our proposed model detects spam specific account by analysing the best suitable features generated using GA and decision predicted through ML as a spammer and legitimate. Our proposed framework is implemented in four different phases called data collection through feature extraction, feature selection based on GA, ML environment and decision-maker as a spammer and nonspammer.

3.2. Characteristic analysis

The analysis of various features that are used to distinguish spammer and nonspammer account in our proposed method depicted below.

- Tweet – posting of multimedia content like text, image and video in the Twitter environment called Tweet for interaction and content sharing between individuals. However, spammer contents are spread through advertising and URLs by the malicious accounts in the form of tweets. People visit those malicious links or advertisement gets affected. We categorise the tweets based on fraudulent content shared by the user with various hashtags and links.
- Tweet permanently or pinned tweet – Fixing a tweet permanently on the top of the profile to stay visible even if the user posts new tweets. Spammer account uses the benefit of this feature to spread malicious contents and attract the user towards their tweets. We selected those tweets that appear more than 20 days on the top of the profile with malicious links in the spammer category.
- Retweet – Posting the same message from an account and other messages shown in the wall in the form of tweet is called retweeting. Adversaries get the benefit of retweet to gain the user attraction regarding that particular tweet. At a later stage, adversaries spread malicious links by attaching to the original content in the network. To analyse the spammer activities, we selected the profiles that frequently retweets the other users' content to attract users to their profile.

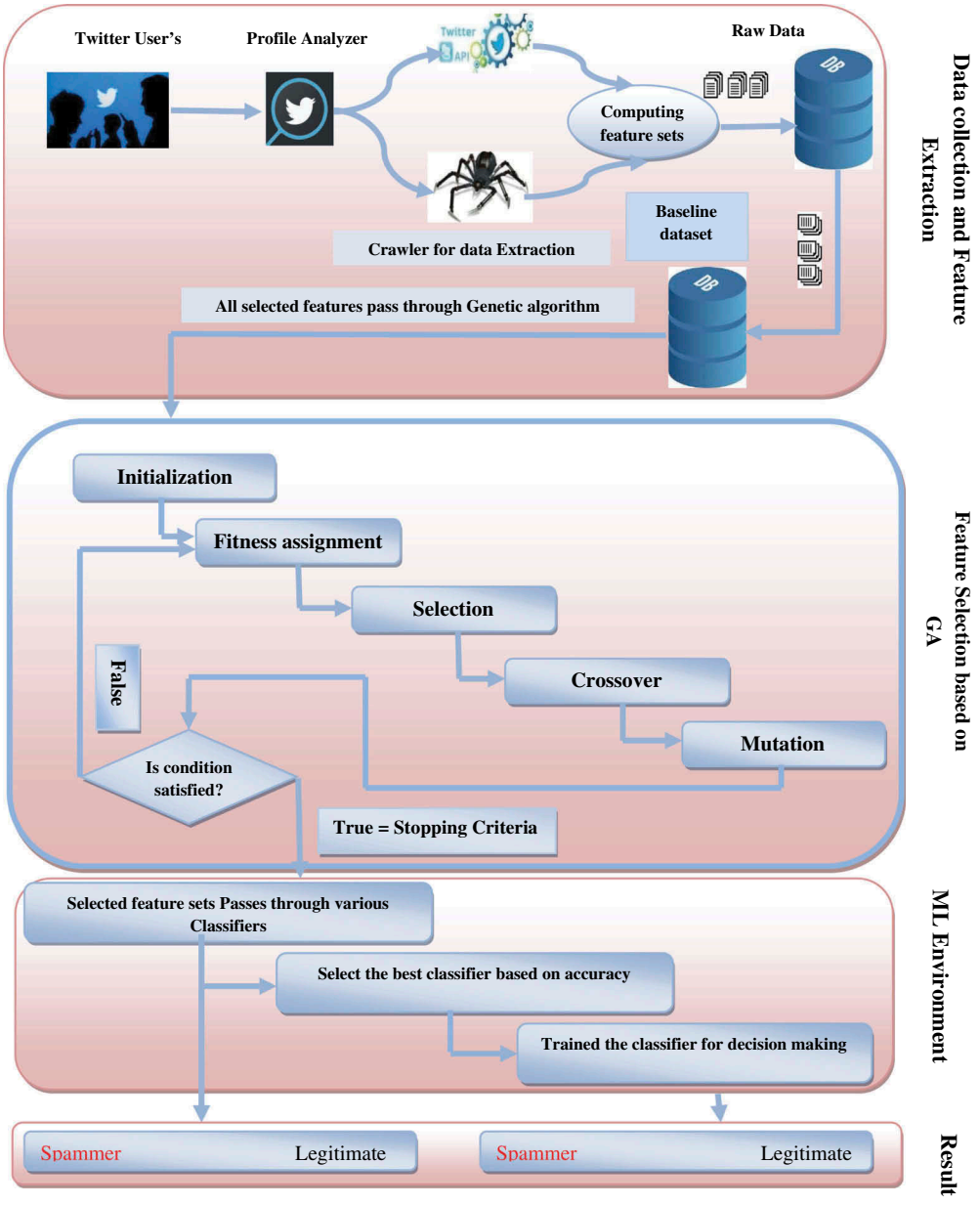

Figure 2. Proposed Framework for spammer detection through various steps.

- Like – By clicking or tapping on a specific moment and appreciate the user content in the Twitter. Sometimes, people enjoy the content without proper investigation regarding the content. Spammer users spread malicious content and highlight the spammer content by like every tweet in their list.
- Replies through direct message – User directly communicates with other users who are in the user group without disclosing the content publically. It is a one-to-one communication facility provided by Twitter for sharing of information in the form of

text. Those users who use this feature frequently and send malicious links are categorised as spammer groups.

- Replies on Tweet: Another promising feature provided by Twitter for answering the question or direct opinion regarding that particular content by responses to a specific tweet. If the malicious user is one of the friends of that specific account, then he/she sends malicious content in the form of replies.
- Sharing of multimedia content – Twitter provides the facility for sharing video, image and live performance activity of the users with other users in the network. Malicious account holder takes the advantages of these services to spread malicious content. Sometimes they use certain hashtag and other services for highlighting the content for attraction through pornographic images and videos. We categorised those accounts as spammer group.
- URLs – Sharing of some information through URL is another promising area of Twitter. Through URLs, a malicious user spreads malware and other services that redirect the users to indivisual malicious pages. People use certain online services to shorten the URLs to hide the originality of the URLs and redirect the user to some different sites.
- Following – The connection of one user account with others by showing interest in them is one of the promising features of Twitter. When the user accepts others' friend request, then the requesting user added to the following list. If the user follows some statement, that account may contain some malicious content and get affected.
- Followers – To gain the attraction of some specific users, spammers always follow the content of user by showing interest. At a later stage, the person is also willing to follow that particular person by following that account. By taking advantage of this fact, malicious account holders spread malicious content in their account in the form of a link, hashtag or by tagging certain content in their account. By this process, the malicious account holder spreads malicious content in the form of multimedia content and URLs. We selected those accounts which frequently follow other users without any specific interest.

3.3. Reckoning feature sets

To compute various features, we analyse different Twitter characteristics such as tweets, retweets, reply on tweets, direct message service, like followers, followings, sharing multimedia contents and some other features. For experimental purposes, we collected dataset related to various Twitter profiles by using our crawler described in Algorithm 1.

Algorithm1: Dataset collection based on the extracted feature

---

Input: A list of theTwitter profile user
Output: A label data set generation
for each User Profile (UP) in the crawler list **do**
Pull out UP's features using crawler;

Store the feature sets in an EXCEL file;
Based on the available content, Extract new features by using Twitter API and crawler;
for each shared content by various profiles i.e. Post shared P_{shared} **do**
Extract set of the crude dataset from various features like $\#^{Tweet}$, $\#^{pinned\ tweet}$ $\#^{Retweet}$, $\#^{likes}$, $\#^{Multimedia\ content}$,$\#^{Follower}$, $\#^{Followings}$ from P_{id} as an input parameter to the crawler.
Extracted feature store in EXCEL file.
end
Parse EXCEL files and calculate the total and average values for each user post
Analyse the performance based on the stored result in the file.
end

By distinguish various characteristics associated with profiles, the spammer and nonspammer content can be detected. In general, spammer accounts have fewer friends as compared to nonspammer accounts according to the previous research analysis. The legitimate account spreads malicious content in the form of a spammer by using multimedia content and linked activities. Most of the time, spammer attracts normal users towards their account by posting certain video and images. We selected various features for our spammer detection framework based on the page content and profile features described in Table 1. We selected some of the features used in previous research and some new page content features for detecting spammer content and account in the Twitter environment. We measure different activity behaviors of each profile by analyzing characteristics like spreading malicious URLs, video containing pornographic activity, images that degrade the behavior of individuals, large numbers of hashtag in a single tweet, like different fraudulent posts such as advertising, and publicity of personals, etc. Spammer contents are separated from nonpammer content by analysing malicious content through URLs, pornographic content in videos, images with a link, tweet with many hashtags, fraudulent posts and some other methods.

3.4. Crude dataset construction

For the analysis of detecting spammer contents and accounts, we generate baseline dataset from various Twitter profiles. Most significant features are processed through our crawler in the python environment and Twitter API for content gathering. Our baseline dataset collects applicable information by crawling each page of the user's profile that is available publicly and some private information on request. The fraction of our Twitter dataset is depicted in Figure 3.

Our crawler collected 6824 profile information associated with both spammer and nonspammer accounts. The extraction of public information is more accessible than private information. For extracting private content, crawler uses Twitter API, and it boosts up the performance of crawler.

3.5. Extraction of the labelled dataset from the crude dataset

The labelled dataset is required for detecting spammer accounts in the ML environment and is a suitable feature selection using a GA. We built label dataset from a crude one by

Table 1. Various features pertained with a Twitter account for analysis.

Details of Twitter profile and page content features	Feature number	Twitter features (tf)		Feature number	Twitter features (tf)	
	F_1	$\#_{1}^{\text{Prof ID (tf)}}$		F_{21}	$\#_{21}^{\text{shared live video stream (tf)}}$	
	F_2	$\#_{2}^{\text{Description (tf)}}$		F_{22}	$\#_{22}^{\text{Notification (tf)}}$	
	F_3	$\#_{3}^{\text{Date of Creation (tf)}}$		F_{23}	$\#_{23}^{\text{Hiding abusive tweets (tf)}}$	
	F_4	$\#_{4}^{\text{Protected (tf)}}$		F_{24}	$\#_{24}^{\text{Pinned tweets (tf)}}$	
	F_5	$\#_{5}^{\text{Tweet (tf)}}$	$\#_{5}^{\text{Total Tweets (tf\_1)}}$ $\#_{5}^{\text{Favourite Tweets (tf\_2)}}$ $\#_{5}^{\text{Avg. Tweets per day (tf\_3)}}$ $\#_{5}^{\text{Tweet with URLs and Hashtag (tf\_4)}}$ $\#_{5}^{\text{Tweet with images (tf\_5)}}$	F_{25}	$\#_{25}^{\text{Using IFTTT(If this then that) (tf)}}$	
	F_6	$\#_{6}^{\text{Followers (tf)}}$	$\#_{6}^{\text{Total Followers (tf\_1)}}$ $\#_{6}^{\text{Total Followers with the direcrt message (tf\_2)}}$ $\#_{6}^{\text{Total followers per day (tf\_3)}}$	F_{26}	$\#_{26}^{\text{Using mobile and desktop (tf)}}$	
	F_7	$\#_{7}^{\text{Following (tf)}}$	$\#_{7}^{\text{Total Followings (tf\_1)}}$ $\#_{7}^{\text{Total followings per day (tf\_2)}}$	F_{27}	$\#_{27}^{\text{Using in app live diveo streaming (tf)}}$	
	F_8	$\#_{8}^{\text{Replies on Tweet (tf)}}$	$\#_{8}^{\text{Total number of replies (tf\_1)}}$ $\#_{8}^{\text{Average number of replies per day (tf\_2)}}$	F_{28}	$\#_{28}^{\text{profile image (tf)}}$	0(Own image) 1(Others Image)
	F_9	$\#_{9}^{\text{Multimedia Content (tf)}}$	$\#_{9}^{\text{Total Audio content (tf\_1)}}$ $\#_{9}^{\text{Total Video content (tf\_2)}}$ $\#_{9}^{\text{Content with URL's (tf\_3)}}$			
	F_{10}	$\#_{10}^{\text{Retweet (tf)}}$	$\#_{10}^{\text{Total number of retweet (tf\_1)}}$ $\#_{10}^{\text{Avg. number of retweets (tf\_2)}}$ $\#_{10}^{\text{Retweet with hashtag or URLs. (tf\_3)}}$			
	F_{11}	$\#_{11}^{\text{Like (tf)}}$	$\#_{11}^{\text{Total Likes (tf\_1)}}$			
	F_{12}	$\#_{12}^{\text{Direct message service (tf)}}$				
	F_{13}	$\#_{13}^{\text{URLs (tf)}}$	$\#_{13}^{\text{Total URL's (tf\_1)}}$ $\#_{13}^{\text{URL's with the hashtag (tf\_2)}}$			
	F_{14}	$\#_{14}^{\text{Listed Count (tf)}}$				
	F_{15}	$\#_{15}^{\text{Verified account (tf)}}$				
	F_{16}	$\#_{16}^{\text{Background Image (tf)}}$				
	F_{17}	$\#_{17}^{\text{Defaulu profile view (tf)}}$	0(Default) 1(Changed)			
	F_{18}	$\#_{18}^{\text{Translator used (tf)}}$				
	F_{19}	$\#_{19}^{\text{Notifications (tf)}}$				
	F_{20}	$\#_{20}^{\text{Hashtags (tf)}}$	$\#_{20}^{\text{Total number of Hashtag (tf\_1)}}$ $\#_{20}^{\text{Average number of Hashtag (tf\_2)}}$ $\#_{20}^{\text{Total unique hashtag (tf\_3)}}$ $\#_{20}^{\text{Hashtag with URLs (tf\_4)}}$			
	F_{21}	$\#_{21}^{\text{Mentions (tf)}}$				

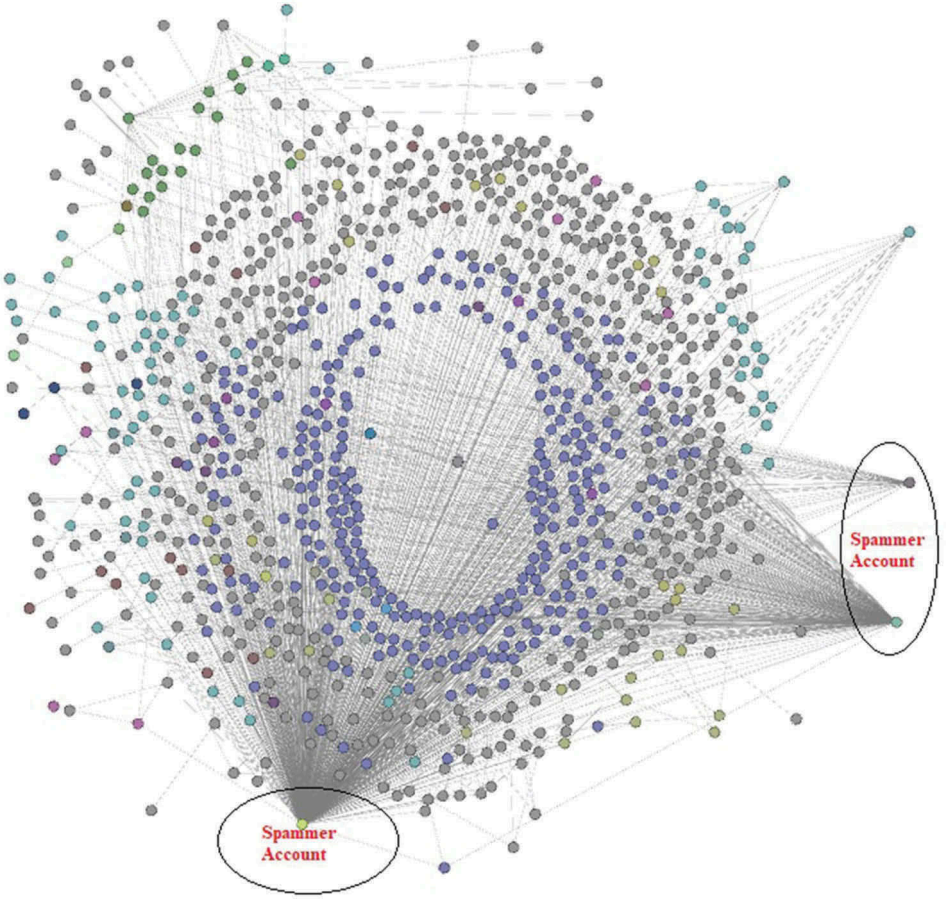

Figure 3. Visualisation of the Twitter account using open-source software Gephi.

analysing features associated with user accounts. Every user profile labelled with a spammer and nonspammer is based on profile characteristics and activities. The interaction and sharing of profile contents is through the dissemination of spammer in the form of links, tweet and direct messaging. By using existing approaches and service provider guidelines, the different accounts are labelled as a spammer and non-spammer. The user profile is labeled as fake or legitimate by the manual process on the basis of parameters like tweets with embedded URLs and hashtags, posts with pornographic videos and other videos that degrade the personality of users and so on. Some profiles spread advertisement for promoting any organisation and product for their benefit. After collecting the profile contents from different profiles, we analyse every profile characteristic by using a GA for better feature selection and decision-making described in Section 4. Some of the contents related to our crawled dataset are shown in Table 2.

Table 2. Details of the extracted dataset.

Profile parameters (spammer)	Total number of contents
Total profiles	6824
Total tweets	59,153,788
Total followers	4,899,493
Total followings	3,439,937
Total likes	16,236,669
Total listed count	67,976
Total URL's shared	1367

3.6. Various classification techniques

Various classification techniques such as SVM, NF (neurofuzzy) classifier, RF (random forest), JRip, Bagging and other classification techniques are used to distinguish spammer and legitimate account in our proposed model. Some of the techniques are described below.

3.6.1. Support vector machine (SVM)

SVMs use the concept of statistical learning theory that is formally defined by a separating hyperplane. By estimating the boundaries, the hyperplane separates the input content into two different parts wherein each class lay on either side (Zheng et al. 2015). If two different classes are separable by a linear fashion, the decision boundary that separates the two classes maximum will be chosen. A margin can be specified or drawn between the sums of the measure to the hyperplane from the nearest data point (called support vector) of the two different class labels. The issues related to margin maximisation can be solved by using quadratic programming (QP). Various issues related to nonlinear data structure are minimisation of the misclassification error and margin maximisation. That can be avoided by using some user-defined parameters.

3.6.2. Neurofuzzy classifier

To avoid the limitation of different supervised learning classification approaches, neuro-fuzzy classifier is used. In this classification, the input parameter or features are distributed with various fuzzy subspaces based on the if-then rule. The rule for fuzzy classifier is depicted in Figure 4. The neurofuzzy classifier is a multilayer feed-forward network that contains five different sublayers called input, membership function, fuzzy layer, defuzzification, normalisation and class label.

3.6.3. Random forest classifier

The outcome of several tree classifiers is called RF. In this process, each tree classifier selected some random features from the input set. The class selected with more votes helps decide class label. The two essential methods that are used to select the various attributes in the decision tree are information gain ratio criterion and Gini index. The combination of various features gathered from training set generates maximum depth tree. The selected dataset base on various features avoids the overfitting condition in decision-making due to purring approaches. Hence, the effectiveness of the RF depends on several trees generated through a random selection process.

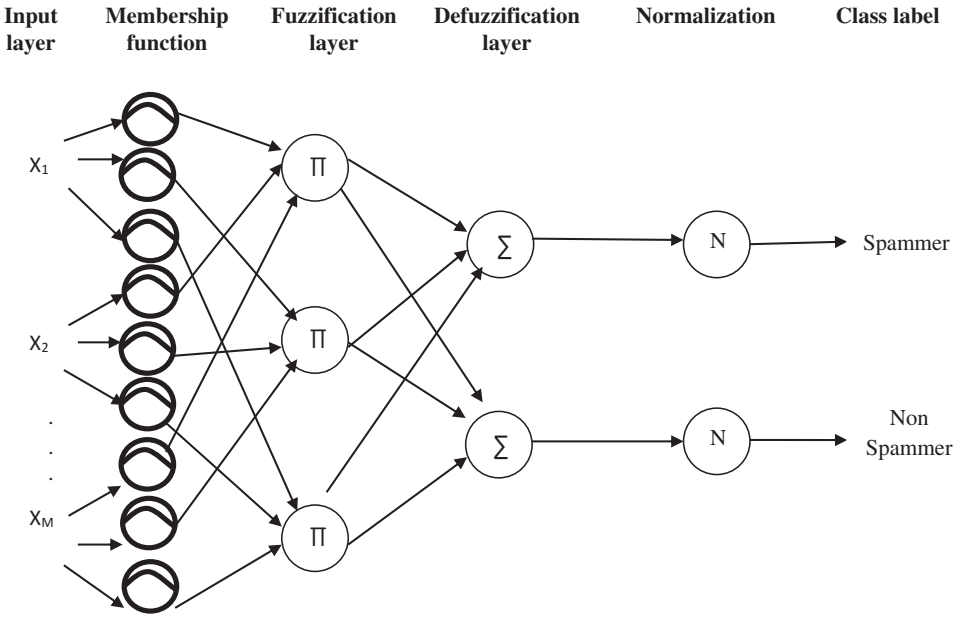

Figure 4. Neurofuzzy classifier for classifying the content as spammer and nonspammer.

4. Metaheuristic approach for feature selection

Evolutionary computation in the computing world is one of the radical developments to optimise and solve various issues. A GA is an effective evolutionary mechanism and subset of a large community, which is based on natural phenomena and genealogy. Charles Darwin suggested the concept of GA based on the precept of survival of the fittest. The basic principle behind the genetic algorithm is to identify the best solution by optimizing the process and discard remaining feasible solutions. Similar to other optimisation algorithms, the GA follows randomised operations over the selected content. Moreover, this technique is found to be more efficient also and commits the best possible solutions for the problem that do not have enough information and linearity. The various advantages of GAs are multiple suitable solutions, optimal solutions, the better analytical output for large-scale problems, and many others. Some of the drawbacks are also associated with GAs. One of the main disadvantages is that it cannot be implemented for the small dataset. The advent of GA motivated us to use the same principle for selecting appropriate features from a set of features for detecting spammer content in Twitter account. The various operations that are associated with the GA are mainly classified into five different stages such as initialisation, fitness assignment, selection, crossover, and mutation as described in Section 4.1.

4.1. Steps of genetic algorithm

4.1.1. Initialisation

By using random number generator, the initial sets of chromosomes have been rendered. The technique selected optimal sets of features from a master feature vector of length 38, including subfeatures. The arrangement of every row contains 38-bit feature vectors in the form of 38

elements in the form of 0's and 1's describing the selection and rejection of features. For the selection of appropriate bits from the master, random selection process is required. The chromosomes are formed from the randomly generated numbers by using binary encoding schemes. Based on the size of the feature vector, a number of random numbers is decided. Similarly, to produce the initial population, 'N' number of chromosomes are created as shown in Figure 5. Those features corresponding to bit 1 are selected from the generated initial population. The random value-based generated chromosome is shown below.

$$[15, 3, 31 \ldots] = [001111\ 000011\ 011111] \rightarrow \text{Chromosome } X_1$$
$$[32, 7, 12 \ldots] = [100{,}000\ 000111\ 001100] \rightarrow \text{Chromosome } X_2$$

4.1.2. Fitness assignment

By selecting various features as described in previous section, the fitness function processes the execution with some classification techniques. Here we use an artificial neural network (ANN) as a classification technique to verify and test each feature associated with the Twitter account. The fitness value is estimated using different features in different chromosomes and the performance of the classifier. The equating weight is given to performance accuracy and count. Our results are rendered in the form of fitness function by enforcing different values shown in Equation (1).

$$\text{Fitness}\,(i) = (.8^{*}\text{Acc}) - (.2^{*}\,F_C) \ldots\ldots\ldots\ldots \quad (1)$$

where

i = Chromosome index

FC = Selected features

Acc = Accuracy generated based on the classifier

The fitness compute column of Figure 4 contains three different columns representing accuracy, a number of the feature selected and obtain fitness value.

4.1.3. Selection

To maintain the fitness chromosome, various selection techniques are available. These are tournament selection, steady-state selection, roulette wheel selection, proportionate selection, and rank selection. Our work uses the concept of tournament selection for the proposed methodologies. The process of selecting various fitness chromosomes is

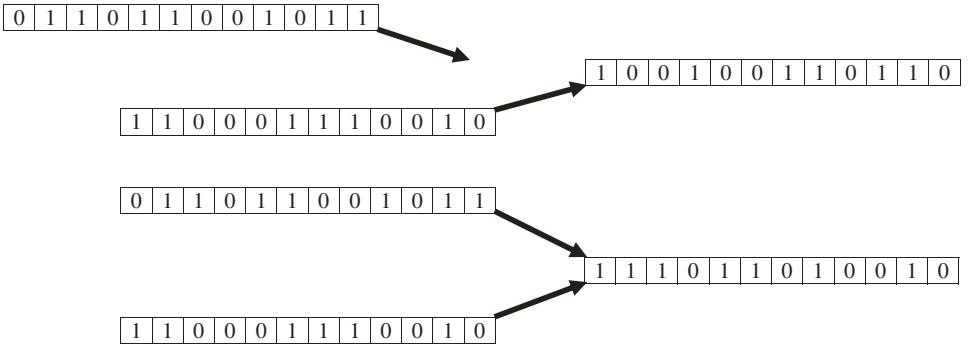

Figure 5. Different crossover techniques.

based on the threshold cut-off of fitness value. The chromosomes having higher probability are selected for the next level of operations.

4.1.4. Crossover

The main objective of the crossover technique is to select the next appropriate child chromosome. In GA, various forms of crossover techniques are implemented. Some of the crossover techniques are a single point, uniform, two-point and arithmetic crossover. In a single-point crossover, only one random number is required for two different chromosomes. Based on the random value, the two chromosomes get exchanged to make new offspring. In the uniform crossover, two or more random numbers are applied to elicit more features of two parent chromosomes to create a new offspring. As compared to a single point and uniform crossover, arithmetic crossover is used to find out similarities and dissimilarities of two different chromosomes that are generated in subsequent phases using AND, OR and other operators depicted in Figure 5.

4.1.5. Mutation

The mutation operation in GA involves enriching the tone of child chromosomes by inverting bit values or interchanging the multiple bits within the chromosome. The various processes continue until the optimal solution is found. The better chromosomes are produced by selecting the majority of chromosomes are in steady-state.

4.2. Feature selection based on GA

To analyse the characteristics of any user profile on Twitter, we select the best features by using our Algorithm 2. The algorithm takes all the selected features for operation and chooses the best optimal features that can analyse the profile by eliminating the junk one. The proposed algorithm runs in a python environment using five different phases discussed in Section 4.1. In each step, the algorithm selects certain features randomly and processes the content to find accuracy. The similar processes continue up to getting the accuracy as 1 with suitable feature selections shown in Figure 6. As the variation in the feature sets due to random selections, reaching to the optimal one is taking more time as a comparison to manual selection approaches. All the selected features after applying GAwith 100^{th} iteration depicted in Table 3. Figure 6 illustrates the simplification of various operations associated with the GA

Algorithm 2: Genetic algorithm for Feature selection

Input: $\prod \leftarrow$Number of instances
$\alpha \leftarrow$Size of chromosomes
$^{\beta}\leftarrow$Rate of elitism
$^{\gamma}\leftarrow$Rate of Mutation
N$\leftarrow$Number of iteration
$N^{e}\leftarrow$Number of elitism
$N^{c}\leftarrow$Number of crossover
C$\leftarrow$Chromosomes

Output: X $\leftarrow$ Best solution

//Initialisation

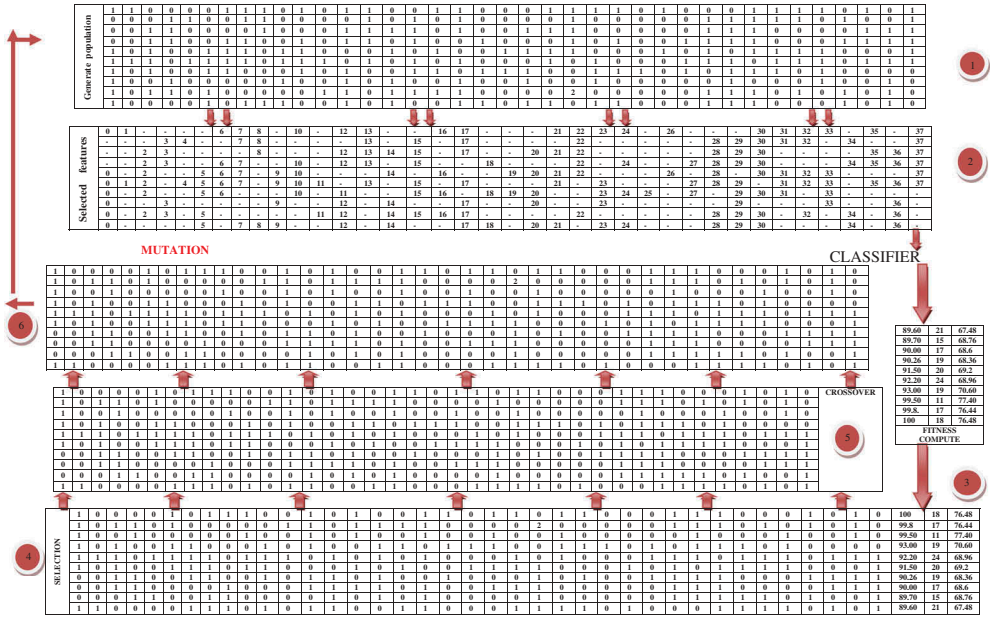

Figure 6. Various steps for feature selection based on GA.

Table 3. Selected features by using genetic algorithm after 100th iteration.

Selected Feature No.	Feature	Selected Feature No.	Feature
0	Profile ID	20	Total number of retweets
5	Total tweets	21	Average number of retweets
7	Average Tweets per day	23	Total number of like
8	Tweet with URL and Hashtags	24	Direct message service
9	Tweet with images.	28	Verified account
12	Total Follower per day	29	Background images
14	Total Following per day	30	Default profile view (0/1)
17	Total audio content	34	Pinned tweets
18	Total Video content	36	Using In app line video stream

Generate a number of feasible solutions randomly i.e.

α ← Number of feasible solutions

Save the content in chromosome i.e. C

//Continue the loop until the termination step

For i = 1 to N do

//Elitism based on selections

Number of elitism $N^e = \alpha * \beta$

Select the best chromosome in Chor and save them in next i.e. C_1

//Crossover

$N^c = (\alpha - N^e)/2$

For = 1 to N^c do

Random selection of two different output X^A and X^B from C

Generate X^C and X^D using one point crossover to X^A and X^B

$C_2 = X^C$ and X^D

endfor

```
//Process for mutation
        For j = 1 to N^C do
          Select any solution 'X^Z' from C_2
           Mutate every bit of 'X^Z' under γ
           Generate a new solution i.e. X_Z'
              if X_Z' is unfeasible
                 Update X_Z' with some feasible solution by fixing X_Z'
              endif
           Update X^Z with X_Z' in C_2
        endfor
//Update the content
        Update C = C_1 + C_2
    endfor
//Gather best solution
Return X
```

The resultant analysis of different iteration is depicted in Figure 7. Also, variation in the validation set accuracy and test case accuracy for population ordered by increasing the test set is shown in Figure 8. As the sizes of the features are increasing, the test set and validation set accuracy grow accordingly. Changing of accuracy with respect to the order of population depends on features and their activities related to profile. Our proposed algorithm works on python environment with core i7 7^{th} generation processor with 8 GB RAM for implementation. The input values to the program are in the form of 38 various features related to any Twitter account with public and private contents, including profile activities. The random selection of various features in the way of chromosomes predicts the accuracy by analysing the feature contents. The process continues up to 100 iterations and selected 21 best suitable features for classification. Various classification techniques are processed with selected features for decision-making. In the proposed algorithm, the sizes of the chromosomes are directly proportional to the training time of the entire execution. In the first step, numbers of feasible solutions are generated randomly and store the selected chromosomes in a variable for performance. The number of iteration denotes the number of executable steps for choosing the best suitable chromosomes for implementation. The selected chromosomes process the dataset associated with every feature by assigning some binary values for every record. After selecting some chromosomes, the crossover techniques are applied to every portion and generate new chromosomes based on accuracy. The mutation technique mutates every bit of new chromosomes and generates a new solution for the next operation.

5. Performance analyser based on experimental evaluation

Processing of manual selection of features may not be sufficient to discriminate spammer and nonspammer content and accounts in Twitter. Hence, some useful feature extraction and selection techniques are required. The selection of various features (public features and some private features) such as tweet, follower, following, replies on a tweet, media content shared, retweet, URLs shared, direct message service, tagging and hashtag are extracted by our crawler based on user's behaviour and profile activities. In addition to them, a set of new

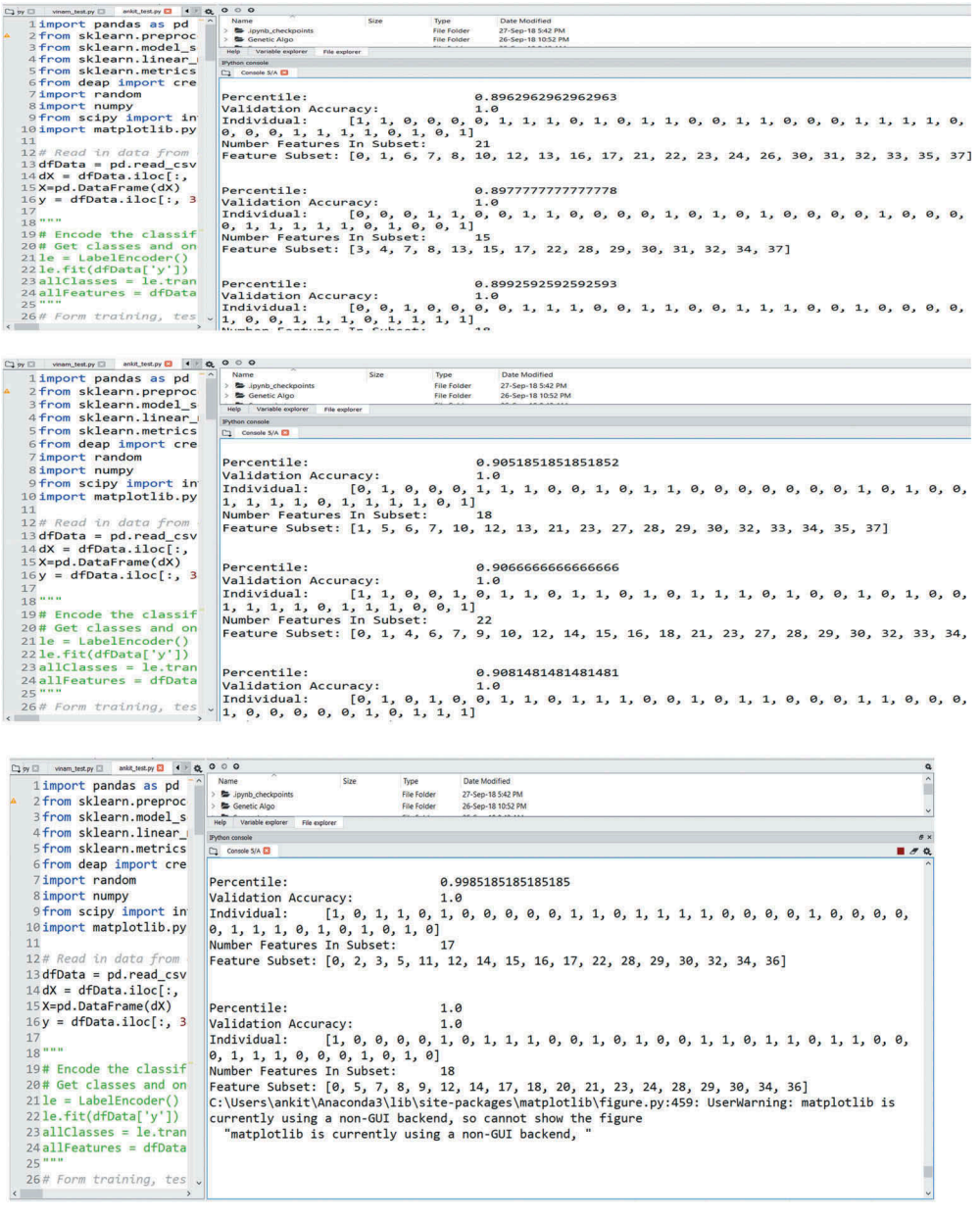

Figure 7. Selection of various features through genetic algorithm.

features, namely recent tweets, recent photo shared, newly added friends and other features, are extracted by our crawler through Twitter API as the booster. We evaluated the performance of various features associated with profiles in the python environment. To train and test the dataset, we use 10-fold cross-validation techniques for given input dataset. In each set, the model separates the contents in 9:1 ratio for operation. The objective of our model is how accurately our framework distinguishes the spammer content from a legitimate one. After successful operations of various modules related to label dataset, the

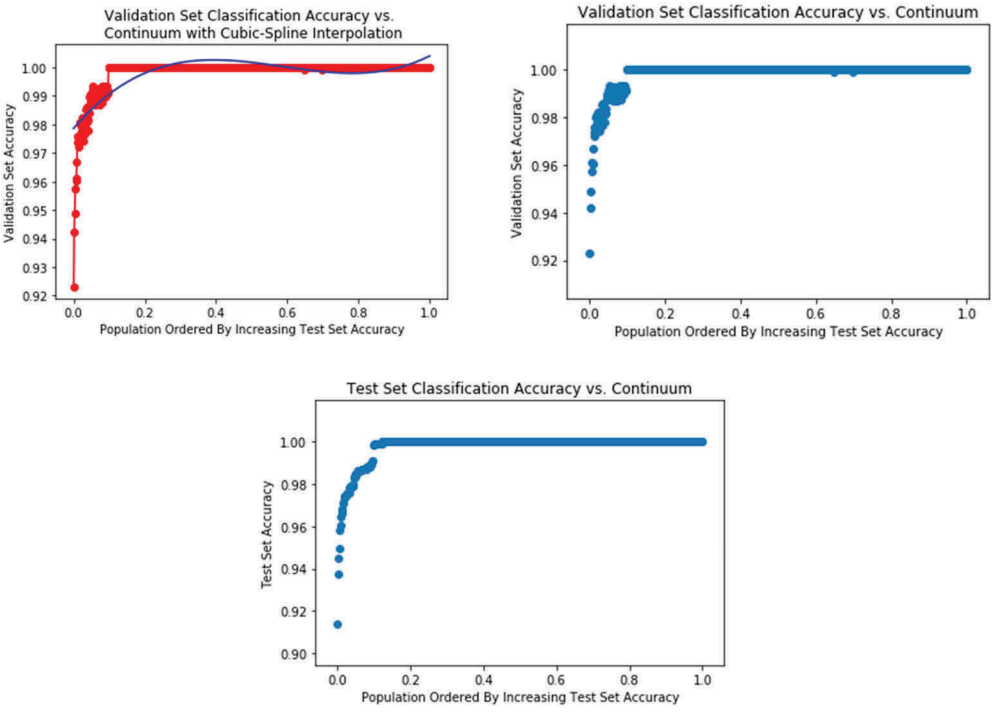

Figure 8. Accuracy obtained for various selected features using GA.

Table 4. Confusion matrix.

		Classification in the form of actual output	
Accuracy		Spammer	Nonspammer
Classification in the form of predictive output	Spammer	TP	FN
	Nonspammer	FP	TN

outcome of the final result pop up with the average value calculated in the form of confusion matrix shown in Table 4.

The predicted result is in the form of confusion matrix generated from various measures like sensitivity (recall), specificity (true negative rate), precision (positive predictive value), receiver operating curve (ROC) values, root mean square error, false-positive rate, Matthews correlation coefficient (MCC) and F-score based on precision and recall. The performance results based on the selected features with various classifications are depicted in Table 4. It is found that all the feature selection approaches are equally important for the detection mechanism. However, our feature selections based on GA select the best combination in optimal time. If the feature sets are large, the evolutionary algorithm uses a randomised method using conventional approaches for output. Evaluation of the performance analysis of each and every feature associated with any Twitter account with various classification algorithms versus the obtained accuracy has been depicted in Table 5. When observing the output of various classifiers, the random forest gives better accuracy in terms of TP rate and ROC with 6779 correctly classified instances and 45 incorrectly classified instances. As compared to the random forest, SVM

Table 5. Various analyses based on classifiers.

Analysis →													
Classification ↓	TP rate	FP rate	Precision	Recall	F-measure	MCC	ROC Area	PRC area	Kappa statistics	Mean absolute error	Root mean square error	Correctly classified	Incorrectly classified
Naïve Bayes	.831	.008	.990	.831	.904	.832	.983	.983	.820	.040	.297	6210	614
Logistic	.957	.008	.992	.957	.975	.950	.995	.995	.949	.048	.142	6650	174
Bagging	.995	.010	.990	.995	.992	.984	.999	.990	.984	.015	.082	6770	54
JRip	.993	.011	.989	.993	.991	.982	.992	.989	.981	.014	.045	6761	63
PART	.992	.010	.990	.992	.991	.982	.992	.988	.981	.012	.094	6762	62
Random Forest	.996	.010	.991	.996	.994	.987	.999	.999	.986	.013	.075	6779	45
J48	.992	.011	.989	.992	.991	.981	.994	.991	.980	.013	.093	6759	65
SMO	.734	.195	.736	.734	.764	.540	.770	.720	.538	.231	.480	5247	1557
IBK	.954	.034	.967	.954	.960	.919	.961	.950	.919	.040	.200	6549	275

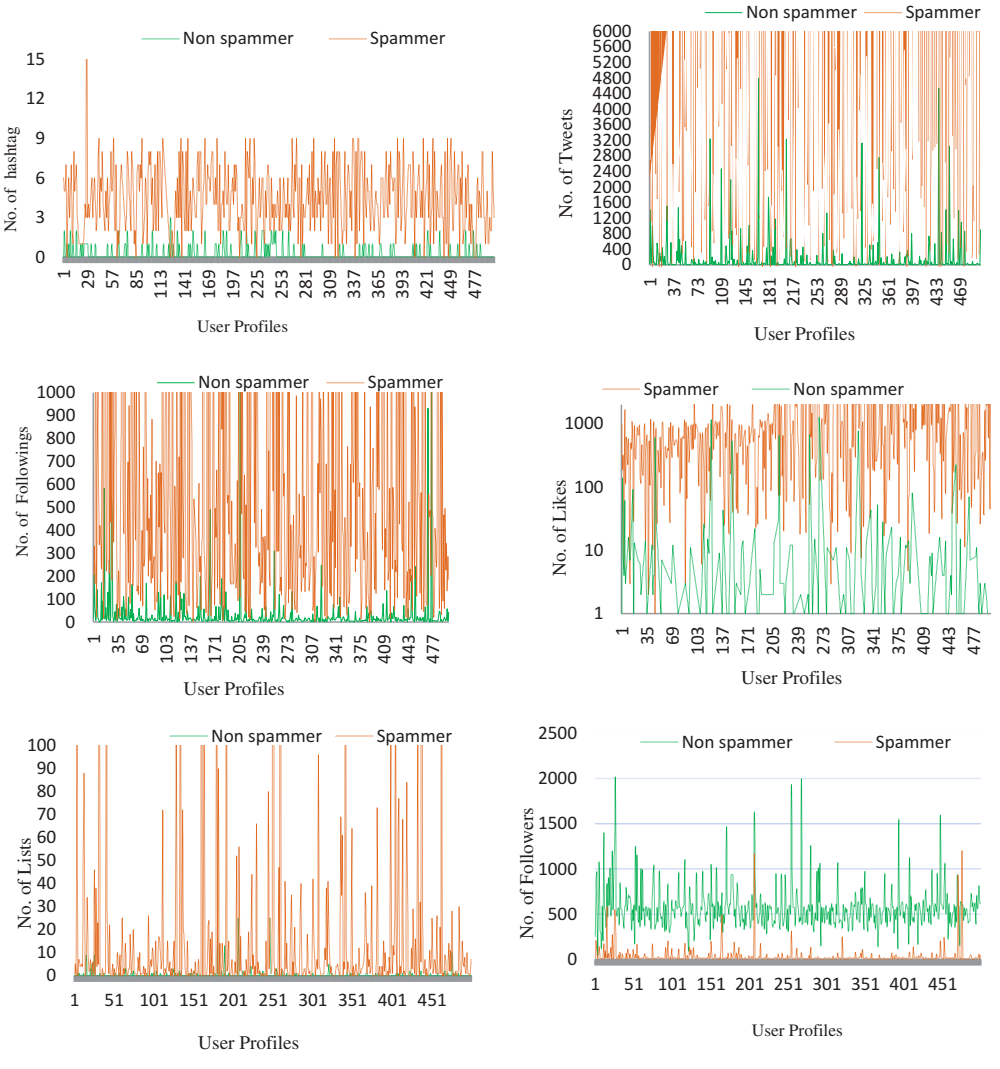

Figure 9. Classifying spammer and non-spammer behaviour based on different features.

and ANN give lower predicted result due to structured data. It is observed that when feature sets are increasing the accuracy factor also increases with better accuracy. Sometimes, the decision of feature selection gives more impact for analysing spammer contents in the Twitter environment. In logistic regression, the FP rate is low as compared to other classification but that cannot correctly classify the data content. The classifier with more ROC sometimes gives lower accuracy and lower F-measure. Our various classification results show we can effectively classify spammer account by misclassifying some nonspammer content. Based on the selected features, analysis with various classifications that separate spammers and legitimate content is depicted in Figure 9 and 10 . We observe our framework gives better result with 21 features selected through GA. From our analysis, we can see that, the number of followings replies on tweets and direct message service for spammer users can be very large as compared to legitimate users. The

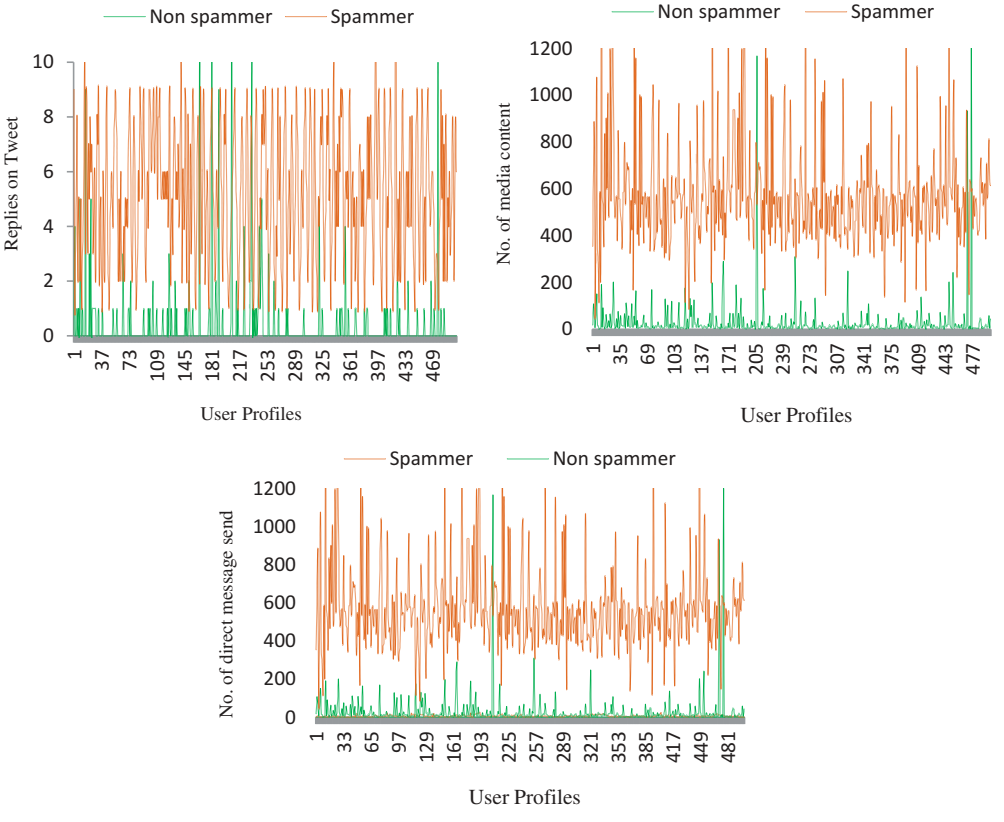

Figure 10. Classifying spammer and non-spammer behaviour based on different features.

number of followers for each spammer user is typically smaller than that of legitimate users. We also observed that some profile contents are not appropriately classified due to sporadic misclassification in spammer and nonspammer segments.

6. Comparison of results with existing approaches

To detect the spammer in the OSN platform, our proposed model analyses various characteristics associated with the Twitter account. Our detection framework reveals the fast rate of detection as compared to other methodologies described in Table 6. Also, our proposed model works on private and public features associated with users' account.

7. Conclusion and future work

In this article, we proposed an intelligent spammer detection framework using GA for suitable feature selections and various MLi algorithm for analysing feature sets. The proposed framework performs various operations like crawling the data content from the Twitter profile, selecting appropriate features by the heuristic approach and developing a spammer detection framework. The proposed framework evaluated based on the public as well as private features of Twitter accounts and obtained

Table 6. Comparison of our approach with other methodologies.

Sl. No.	Title of a research article	Dataset used	Accuracy (%)	Techniques used	Future research direction	Limitations
1	Automatic Detection of Cyber Security Related Accounts on Online Social Networks Aslan, Sağlam, and Li (2018)	424 Twitter profiles data.	97.17	Selection of the profile and behavioural features using machine learning approach with different methodologies like prototypical words, weirdness and if-idf values.	Generate automated cyber security event detection using selected features for OSN research.	The selection of profile content through a heuristic approach with limited feature selection for processing. The ratio between the secure account and nonsecure account is natural.
2	A feature selection approach to detect spam in the Facebook social network. Sohrabi and Karimi (2018)	200,000 wall posts from Facebook	91.20	Design of hybrid algorithm for spam filtering method using PSO based feature selection, DB index and differential evaluation algorithm	Develop deep learning based spam detection system by analysing public and private features.	Selection of features is very less for detecting spam content from various posts due to public features only.
3	Who is Who on Twitter–Spammer, Fake or Compromised Account? A Tool to Reveal True Identity in Real-Time. Singh, Bansal, and Sofat (2018)	74,000 tweets related to pornographic adult content.	92.1	The framework contains a behavioural analysis of pornographic users, Twitter followers related to marketing activities and detection of spam content trough machine learning approach.	Constantly monitor and update classification features based on spammer's behaviour. To improve the detection method NLP can be used.	Manual selection of approaches for feature selections leads to lower accuracy in detecting spam content. Public features are not sufficient to detect the fake accounts that spread malicious content in the network.
4	Detecting Indonesian spammer on Twitter Setiawan, Widyantoro, and Surendro (2018)	450 user data including Indonesian users.	93.67	The model used some machine learning techniques to separate spammer accounts from a legitimate one.	For better decision making in machine learning environment, large dataset required.	The smaller dataset cannot predict the accurate result in terms of spammer detection. Manual selection of features leads to a lower detection rate.
5	Discovering spammer communities on Twitter. Ho et al. (2018)	5,643,297 tweet posts.	86.7	Spamcom: Spammer communities' detection by employing community-based features, robust structural characteristics.	Collection of the real-time dataset can help to predict the proper analysis to detect the spammer content.	The honey pot dataset cannot properly represent the Twitter ecosystem. The follower network layer construction using honey pot data is not complete.
6	Collective classification of spam campaigners on Twitter: A hierarchical meta-path based approach. Gupta et al. (2018)	3370 campaign dataset.	67.3	(HMPS) Hierarchical meta path score to measure the proximity of unknown users to detect spammer.	To generate more and more features to analyse spammer contents at real-time.	The accuracy of the proposed model for detection of spammer is very low as compared to others. To increase accuracy, suitable feature selections are required.

evaluation results and hit very promising detection rate compared to other approaches. It identifies the most relevant features and optimises its classifier based on the selected tuple. It is also noticed that the change of features in a GA with random selection process gives a proper selection of features with a higher true positive rate. Overall, it can be concluded that the spammers targeted the users by sending malicious contents through public as well as private features. However, spammers can spread with various methods and techniques for a convertible and evolvable spammer-spotting system. In addition to our proposed method, suitable filtering techniques can be developed for removing spammer contents that reduce the performance of user account. As a future work, a framework can be developed for sentiment analysis to be used in other social networks like Facebook, Instagram, and LinkedIn.

Acknowledgments

This publication is an outcome of the R&D works undertaken under (i) YFRF grant and (ii) the project Visvesvaraya Ph.D. Scheme of Ministry of Electronics & Information Technology, Government of India and being implemented by Digital India Corporation.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Ministry of Electronics & Information Technology, Government of India.

References

Alghamdi, B., Y. Xu, and J. Watson 2018. "A Hybrid Approach for Detecting Spammers in Online Social Networks." In *International Conference on Web Information Systems Engineering*, 189–198. Cham: Springer, November.

Alieyan, K., A. Almomani, M. Anbar, M. Alauthman, R. Abdullah, B. B. Gupta. 2019. "DNS Rule-based Schema to Botnet Detection."*Enterprise Information Systems*: 1–20. doi:10.1080/17517575.2019.1644673.

Aslan, Ç. B., R. B. Sağlam, and S. Li. 2018. *Automatic Detection of Cyber Security Related Accounts on Online Social Networks,* Proceeding of the 9th International Conference on Social media and Society.

Boshmaf, Y., D. Logothetis, G. Siganos, L. Jorge, J. Lorenzo, M. Ripeanu, and K. Beznosov 2015. "Integro: Leveraging Victim Prediction for Robust Fake Account Detection in Osns." In *NDSS*. Vol 15, 8–11. Citeseer

Cao, C., and J. Caverlee 2015. "Detecting Spam URLs in Social Media via Behavioral Analysis." Proceedings of Advances in Information Retrieval, 703–714. Europe: Springer.

Cao, Q., M. Sirivianos, X. Yang, and T. Pregueiro. 2012. "Aiding the Detection of Fake Accounts in Large Scale Social Online Services." In *Presented as part of the 9th USENIX symposium on networked systems design and implementation (NSDI 12)*, 197–210, USNIX association, United State.

Chen, C., S. Wen, J. Zhang, Y. Xiang, J. Oliver, A. Alelaiwi, and M. M. Hassan. 2017. "Investigating the Deceptive Information in Twitter Spam." *Future Generation Computer Systems* 72: 319–326. doi:10.1016/j.future.2016.05.036.

Chhabra, M., B. Gupta, and A. Almomani. 2013. "A Novel Solution to Handle DDOS Attack in MANET." *Journal of Information Security* 4 (03): 165. doi:10.4236/jis.2013.43019.

Class JRIP 2015. http://weka.sourceforge.net/doc.stable/weka/classifiers/rules/JRip.html

Dahiya, A., and B. B. Gupta. 2019. "A PBNM and Economic Incentive-based Defensive Mechanism against DDoS Attacks." *Enterprise Information Systems* 1–21. doi:10.1080/17517575.2019.1700553.

Fazil, M., and M. Abulaish. 2018. "A Hybrid Approach for Detecting Automated Spammers in Twitter." *IEEE Transactions on Information Forensics and Security* 13 (11): 2707–2719. doi:10.1109/TIFS.2018.2825958.

Ghosh, S., B. Viswanath, F. Kooti, N. K. Sharma, G. Korlam, F. Benevenuto, N. Ganguly, and K. P. Gummadi. 2012. "Understanding and Combating Link Farming in the Twitter Social Network." In *Proceedings of the 21st International Conference On World Wide Web*, 61–70, Lyon France

Gupta, B., D. P. Agrawal, and S. Yamaguchi, Eds. 2016. *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. IGI global, USA.

Gupta, S., and N. Gugulothu. 2018. "Secure Nosql for the Social Networking and E-commerce Based Bigdata Applications Deployed in Cloud." *International Journal of Cloud Applications and Computing (IJCAC)* 8 (2): 113–129. doi:10.4018/IJCAC.

Gupta, S., A. Khattar, A. Gogia, P. Kumaraguru, and T. Chakraborty. 2018. "Collective Classification of Spam Campaigners on Twitter: A Hierarchical Meta-Path Based Approach." *arXiv Preprint arXiv* 1802: 04168.

Gurumurthy, S., C. Sushama, M. Ramu, and K. S. Nikhitha. 2019. "Design and Implementation of Intelligent System to Detect Malicious Facebook Posts Using Support Vector Machine (SVM)." In *Soft Computing and Medical Bioinformatics*, 17–24. Singapore: Springer.

Gyongyi, Z., H. Garcia-Molina, and J. Pedersen. 2004. "Combating Web Spam with Trustrank." In *Proceedings of ¨ the Thirtieth international conference on very large data bases, vol. 30, VLDB '04*, 576–587, Brighton, England

Ho, K., V. Liesaputra, S. Yongchareon, and M. Mohaghegh. 2018. . "Evaluating Social Spammer Detection Systems." In Proceedings of the Australasian Computer Science Week Multiconference, 18. ACM, January, Brisband Queensland, Australia, 2018.

Hu, W., Z. Gong, U. Leong Hou, and J. Guo. 2015. "Identifying Influential User Communities on the Social Network." *Enterprise Information Systems* 9 (7): 709–724. doi:10.1080/17517575.2013.804586.

Khan, M. U. S., M. Ali, A. Abbas, S. U. Khan, and A. Y. Zomaya. 2018. "Segregating Spammers and Unsolicited Bloggers from Genuine Experts on Twitter." *IEEE Transactions on Dependable and Secure Computing* 15 (4): 551–560.

Kibanov, M., M. Becker, J. Mueller, M. Atzmueller, A. Hotho, and G. Stumme. 2018. "Adaptive kNN Using Expected Accuracy for Classification of Geo-spatial Data." In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 857–865. ACM. April, Pau, France

Lee, K., J. Caverlee, and S. Webb. 2010. "Uncovering Social Spammers: Social Honeypots + Machine Learning." In *Proceedings of the 33rd international ACM SIGIR Conference On Research And Development In Information Retrieval, SIGIR '10*, 435–442, Geneva, Swizerland, 2010.

Li, C., Z. Zhang, and L. Zhang. 2018. "A Novel Authorization Scheme for Multimedia Social Networks under Cloud Storage Method by Using MA-CP-ABE." *International Journal of Cloud Applications and Computing (IJCAC)* 8 (3): 32–47. doi:10.4018/IJCAC.

Liaw, A., and M. Wiener. 2002. "Classification and Regression by randomForest." *R News* 2 (3): 18–22.

Qabajeh, I., F. Thabtah, and F. Chiclana. 2018. "A Recent Review of Conventional Vs." *Automated Cybersecurity Anti-phishing Techniques. Computer Science Review* 29: 44–55.

Sahoo, S. R., and B. B. Gupta. 2018. "Security Issues and Challenges in Online Social Networks (Osns) Based on User Perspective." In *Computer and Cyber Security*, 591–606. Auerbach Publications, Taylor & Francis.

Sahoo, S. R., and B. B. Gupta. 2019a. "Classification of Various Attacks and Their Defense Mechanism in Online Social Networks: A Survey." *Enterprise Information Systems* 13 (6): 832–864. doi:10.1080/17517575.2019.1605542.

Sahoo, S. R., and B. B. Gupta. 2019b. "Hybrid Approach for Detection of Malicious Profiles in Twitter." *Computers & Electrical Engineering* 76: 65–81. doi:10.1016/j.compeleceng.2019.03.003.

Setiawan, E. B., D. H. Widyantoro, and K. Surendro. 2018. "Detecting Indonesian Spammer on Twitter." In *2018 6th International Conference on Information and Communication Technology (ICoICT)*, 259–263. IEEE, Bandung, Indonesia.

Sheng, G., Y. Su, and W. Wang. 2019. "A New Fractal Approach for Describing Induced-fracture Porosity/permeability/compressibility in Stimulated Unconventional Reservoirs." *Journal of Petroleum Science and Engineering* 179: 855–866. doi:10.1016/j.petrol.2019.04.104.

Singh, M., D. Bansal, and S. Sofat. 2018. "Who Is Who on Twitter–Spammer, Fake or Compromised Account? A Tool to Reveal True Identity in Real-Time." *Cybernetics and Systems* 49 (1): 1–25. doi:10.1080/01969722.2017.1412866.

Sohrabi, M. K., and F. Karimi. 2018. "A Feature Selection Approach to Detect Spam in the Facebook Social Network." *Arabian Journal for Science and Engineering* 43 (2): 949–958. doi:10.1007/s13369-017-2855-x.

Soiraya, M., S. Thanalerdmongkol, and C. Chantrapornchai. 2012. "Using a Data Mining Approach: Spam Detection on Facebook." *International Journal of Computer Applications* 58 (13): 26–31. doi:10.5120/9343-3660.

Tajalizadeh, H., and R. Boostani. 2019. "A Novel Stream Clustering Framework for Spam Detection in Twitter." *IEEE Transactions on Computational Social Systems* 6 (3): 525–534. doi:10.1109/TCSS.6570650.

Thomas, K., C. Grier, J. Ma, V. Paxson, and D. Song 2011a. "Design and Evaluation of a Real-time Url Spam Filtering Service." Proceeding of IEEE Symposium on Security and Privacy (SP), Oakland, California.

Tse, Y. K., H. Loh, J. Ding, and M. Zhang. 2018. "An Investigation of Social Media Data during a Product Recall Scandal." *Enterprise Information Systems* 12 (6): 733–751. doi:10.1080/17517575.2018.1455110.

Wang, G., C. Wilson, X. Zhao, Y. Zhu, M. Mohanlal, H. Zheng, and B. Y. Zhao. 2012. "Serf and Turf: Crowdturfing for Fun and Profit." In *Proceedings of the 21st International conference on World Wide Web, WWW '12*, 679–688. doi:10.1007/s10856-012-4832-y.

Wei, W., X. Fengyuan, C. C. Tan, and Q. L. Sybildefender. 2012. "Defend against Sybil Attacks in Large Social Networks." In *INFOCOM, 2012 Proceedings IEEE*, 1951–1959, Florida, USA, IEEE.

Xue, J., Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai. 2013. "Votetrust: Leveraging Friend Invitation Graph to Defend against Social Network Sybils." In *Proceeding of the 32Nd IEEE international conference on computer communications, INFOCOM '2013*. Turin, Italy.

Yang, X., Q. Yang, and C. Wilson. 2015. "Penny for Your Thoughts: Searching for the 50 Cent Party on Sina Weibo." In *ICWSM*, 694–697. Oxford, UK

Zhang, J., Q. Li, X. Wang, B. Feng, and D. Guo. 2018. "Towards Fast and Lightweight Spam Account Detection in Mobile Social Networks through Fog Computing." *Peer-to-Peer Networking and Applications* 11 (4): 778–792. doi:10.1007/s12083-017-0559-3.

Zhang, Y., H. Zhang, X. Yuan, and N. F. Tzeng. 2019. "TweetScore: Scoring Tweets via Social Attribute Relationships for Twitter Spammer Detection." In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 379–390. ACM, July. doi:10.1177/1753193418809771.

Zhang, Z., R. Sun, C. Zhao, J. Wang, C. K. Chang, and B. B. Gupta. 2017. "CyVOD: A Novel Trinity Multimedia Social Network Scheme." *Multimedia Tools and Applications* 76 (18): 18513–18529. doi:10.1007/s11042-016-4162-z.

Zhao, H., L. Xu, Z. Guo, W. Liu, Q. Zhang, X. Ning, G. Li, et al. 2019. "A New and Fast Waterflooding Optimization Workflow Based on INSIM-derived Injection Efficiency with A Field Application". *Journal of Petroleum Science and Engineering* 179: 1186–1200. doi:10.1016/j.petrol.2019.04.025.

Zheng, X., Z. Zeng, Z. Chen, Y. Yu, and C. Rong. 2015. "Detecting Spammers on Social Networks." *Neurocomputing* 159: 27–34. doi:10.1016/j.neucom.2015.02.047.

Zheng, X., X. Zhang, Y. Yu, T. Kechadi, and C. Rong. 2016. "ELM-based Spammer Detection in Social Networks." *The Journal of Supercomputing* 72 (8): 2991–3005. doi:10.1007/s11227-015-1437-5.

Zhou, Y., X. Wang, J. Zhang, P. Zhang, L. Liu, H. Jin, and H. Jin. 2018. "Analyzing and Detecting Money-Laundering Accounts in Online Social Networks." *IEEE Network* 32 (3): 115–121. doi:10.1109/MNET.2017.1700213.