International Journal of Research in Advent Technology, Vol.7, No.6, June 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Supervised Feature Based Malicious Profile Detection System in Online Social Media

Ms. Anamika Joshi, Dr. D.S. Bhilare

Abstract: The raging and ever growing popularity of social media, with its reach and depth, also gained the attention of cyber-criminals for the dissemination and distribution of malicious contents and link. In order to achieve this, they create fake and doctored profiles to send malicious messages to social media users on various platforms, leading to misinformation campaigns, fraud, spam or malware promotions. Thus it is very important that such malicious profiles are detected and remedied at the earliest possible, so that the resulting harm could be minimized. The objective of this research work is to develop a modified model for detection of malicious profiles on Twitter. In this modified model, we have identified simple and derived salient features by examining the public information available on the twitter in order to classify malicious and legitimate profiles with accuracy over 96.92%. Experiment illustrates that our modified model to detect malicious profile in social media has significant improvement over the previous work.

Keywords: Online social media analysis, security and privacy, malicious profile, fake profile**.**

I. INTRODUCTION

Across the world, Online Social Media such as Facebook, Twitter, or LinkedIn, allow users to present themselves as an online profile, using these profiles, users are able to share their ideas, feelings and information [1]. Online social networks are also becoming an essential part of any business or government strategy and communication. Online social network like Twitter is growing on a daily basis and as a result, cyber criminals and attackers have developed interest in distributing malicious contents and links on this platform. In order to send malicious messages and links to legitimate users they have also been creating and using fake profiles.

In a social network like Twitter it is easy to have access to all public information like users names, profiles and users contents in comparison with, for example, email where even getting a large number of email addresses for massive complaints is a very hard task. This is a huge advantage to cybercriminals.

Manuscript revised June 15, 2019 and published on July 10, 2019
Ms. Anamika Joshi, *Research scholar in School Of Computer Science, Devi Ahilya University Indore, India*
Dr. D.S. Bhilare, Head, IT Centre, *Devi Ahilya University Indore, India*

It is very easy for them to get all the information they need for both sending malicious messages and links. They can easily create clone or fake profiles to attract the victims.

Sybil attacks are one of the most widespread attacks against online social media [2], in this attack, it impersonate the real users' identities across online social media via creating several fake accounts known as Sybil accounts. The Koobface, Petya, Wannacry virus family types are an example of computer viruses attempted to collect sensitive information, such as credit card numbers and personal details, from social media users [3] and [4].

Although the researchers introduced several approaches for detecting malicious or fake profiles, but they do not provide the desired effectiveness and accuracy [5]. In present research work we have used user's profile, activity and previous behavior to detect malicious profiles as soon as possible.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 describes our proposed model to detect malicious profile. Section 4 presents our evaluation and experiments results and the last section draws a conclusion and future work.

.

II. RELATED WORK

The detection of malicious content has been studied since email spam [6]. Now it is extended to the online social media where cybercriminals can easily find their targets and information. Malicious content are unwanted content in social media includes unrelated tweet content, sharing malicious links or fraudulent information. These types of messages express a different behavior from what the normal social media is intended for. By identifying this different behavior we can filter theses messages from social media.
The most of the previous work in this field has focused on the detection of malicious profiles that produce malicious content. The recent malicious profile detection work can be classified into three categories as depicted in figure 1.1:

1. ***Examine The URLS:*** The first category of work, such as [7], [8], [9] and [10] detects malicious accounts by examining the URLs or domains of the URLs posted along with the tweets. The messages could be classified on the basis of whether they are tagged as malicious or not by publicly blacklisted URLs/domains. They used several URL blacklists for detecting malicious tweets from their retrieved dataset, therefore they can classify only tweets contains a URL link, and is not able to detect other types of malicious tweets.

doi: 10.32622/ijrat.762019109

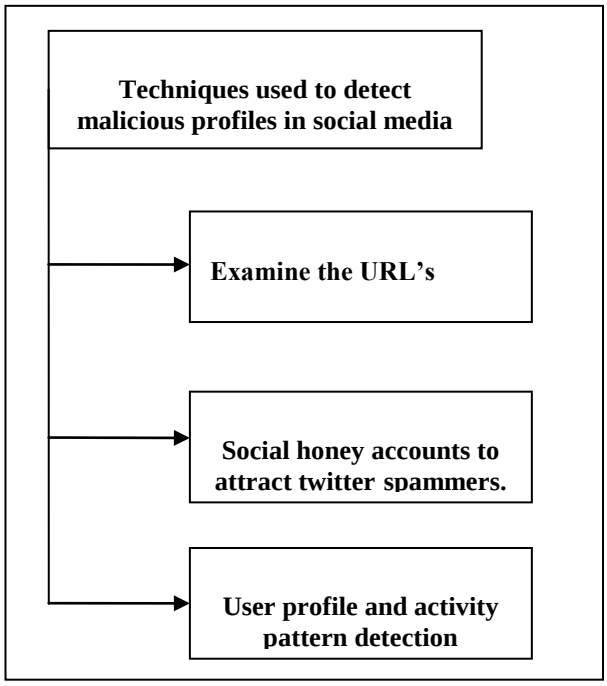


Figure 1.1: Techniques used to detect malicious profiles

2. ***Social honey accounts to attract twitter spammers***: *The* second category of work, e.g. [11] and [12] detects spam accounts by utilizing social honey accounts to attract twitter spammers. Honeypot techniques help to detect malicious users by attracting them to their sites and entering themselves into their networks with the goal of harvesting information from them. Then by analyzing and finding their distinguished behavior we can classify malicious users from legitimate users. This technique is very effective but time consuming. It is generally useful to trap targeted cybercriminals.

3. ***User profile and activity pattern detection:*** The third category of work, such as [11], [13], [14], [15] and [16] mainly utilizes machine learning techniques to classify legitimate accounts and malicious accounts on the basis of their selections of classification features. They used users profile, tweet contents, user's historical and network information that is publicly available to detect malicious users in the social media.

In this research work we have used user's profile, activity and previous behavior that is publicly available to detect malicious users. As the creation and maintenance of malicious accounts is mostly done automatically, profile-pattern detection method provides a better way to classify malicious users from legitimate users without detailed analysis of Tweets [17], [18], [14], [19] and [20].
Benevenuto et al. (2010) used profile information such as ''number of followers and number of followings'' to detect fake profile [14]. Many researchers as in [20], [21] and [22] extracted different features from user's previous behaviors such as average number of hashtags, average number of URL links and average number of user mentions that appear in their tweets. They also extracted other non-historical features such as number of followers, number of followings and age of the account.

Thomas et al. (2013) purchased fake accounts from an underground market and found that there is strong correlation between the three features userprofile-name, screen-name, and email parameters for all fake accounts [17]. Such a pattern recognition method could be used as a pre-identifier of malicious profiles.

Lee et al. [22] and Yang et al. [23] used different techniques to study the spammers' behavior. They both used features based on user's previous behavior and their social networks such as tweeting rate, following rate, percentage of bidirectional friends, FOFO rato and local clustering coefficient of its network graph.

Miller et al. [24] solved spammer detection problem as an anomaly detection problem. They built a clustering model in which spammers are considered as outliers.
Most recent method to detect malicious accounts in social media is based on their activity patterns. For example, Jiang et al. (2014, 2016) detect suspicious profiles in Twitter based on abnormal user activity [25] and [26]. Similarly, Clark et al. (2016) used linguistic features with other features to classify fake profiles [27].

III. PROPOSED METHOD

In present research work we have used user's profile, activity and previous behavior to detect malicious profiles. The goal of this work is to obtain a set of features derived from the public information available in order to correctly classify malicious and legitimate profiles in the social media. In this section we describe malicious profile detection system that classifies malicious and legitimate profiles in the social media.

A. Problem Statement

As we have seen, Malicious Profile detection is a basically a classification problem. Formally, a malicious profile detection is a model M that predicts the class label $\hat{y}$ for a given input example x, that is, $\hat{y} = M(x)$, where $\hat{y} \in \{1; 0\}$. Where 1 is for malicious profile and 0 is for legitimate profile. To build the model we require a set of points with their correct class labels, which is called a training set. After learning from this model M, we can then predict the class for any other set.

B. Proposed Model

Malicious profile detection is a classification model and we have used supervised classifier to classify Tweeter profiles into malicious and legitimate profiles. It is based on the features extracted from the data and metadata publicly available on Tweeter. Supervised classifiers that attempt to discover the relationship between independent variables and dependent variables. Supervised classifier need labeled dataset that is known as training dataset to learn and build classification rules. Then classification rules are tested on test data set. After that the classifier is ready to be used on any data set. Our approach for understanding and developing a malicious profile detection model is depicted in figure 1.2.

doi: 10.32622/ijrat.762019109

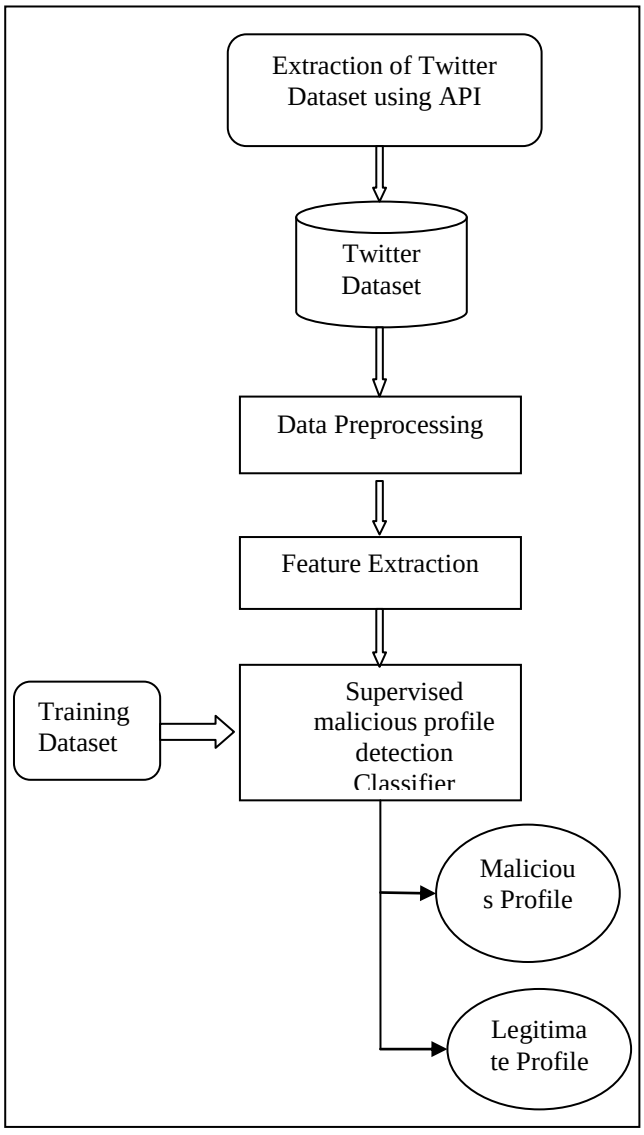


Figure 1.2: The Framework of proposed malicious profile detection model

C. Feature Extraction

This section details all the significant features used to classify profiles as malicious or legitimate. The information is obtained directly through the twitter API. Further needed information is collected by further crawling twitter or by analyzing the tweet contents and user profile. We have started with simple features easily available for any user and which is quick to calculate. In first analysis, these set of features did not seem enough to classify profiles as malicious or legitimate. So we have considered some other derived features that provide more information when classifying malicious users. We have added some features that have been proposed in previous work [28], [24], [29], [30] and [31] to strengthen our model. In this way we have extracted total 15 set of features to detect if a profile is malicious or not. These features are listed in table 1.1.

Table 1.1: Significant features for malicious profile detection

Feature	Feature Name	Description	Value
F1	FOFO Ratio	It is a ratio of total number of following and followers	Numeric
F2	Tweets URLRatio	It is the ratio of tweets posted by a user contains URL to a total number of tweets posted	Numeric
F3	AvgTime Between Messages	It is an average of time interval between messages(tweets)	Numeric
F4	APITweetRatio	It is a ratio of total number of tweets posted by a profile using tweet source API to total number of tweets posted	Numeric
F5	Tweeting Rate	It is a ratio of total number of Tweets to the age of profile	Numeric
F6	Tweets Known Friends Ratio (TKF Ratio) and Tweets UnknownFriends Ratio (TUF Ratio)	Compare between tweets to known friends ratio and tweets to unknown friends ratio	Numeric
F7	Follow Back	Count total number of friends following a user	Numeric
F8	Tweets ViasUsed	Count of different channels used to send tweets	Numeric
F9	TotalHashTags	It is total number of Hash Tags(#) used by an user	Numeric
F10	Total Followers and	It is the ratio between total no of followers and	Numeric

doi: 10.32622/ijrat.762019109

	Total Followees	followees	
F11	Account Age	Total number of Months since a profile connected to the twitter	Numeric
F12	FollowingRate	It is a ratio of the total number of following to age of the account	Numeric
F13	Verified	Whether a account is verified by twitter or not	Boolean
F14	ListCount	The number of public lists that this user is a member of.	Numeric
F15	Has ProfileImg and HasProfileDescription	Whether a twitter account has profile image and description or not	Boolean

IV. DESIGN OF THE EXPERIMENT

A. Experimentation Platform:

In our model for malicious profile detection we have used following platforms:

- ***R programming language with IDE RStudio***: R is an open source software package that provides a wide variety of statistical, machine learning, classification, clustering etc. It is highly extensible.

  To extract Twitter data and metadata we have used R programming language. We have used R programming language further for data preprocessing, JSON to excel conversion, feature extraction and its significance test and also to test the model fitness.
- ***Weka***: Weka is an open source, freely available, platform-independent and easily useable software package that is a collection of machine learning algorithms for data mining tasks.

  We have used Weka to implement and to evaluate the performance of five classifiers *naive bayes (NB), logistic regression (LR), linear support vector machine (SVM), Randon Tree (RT) and J48*.

B. Data Collection and Dataset

The first step of our analysis is to gather data.

- Our Model is trained and also evaluated on dataset collected from twitter.
- Twitter shares its data in JSON – JavaScript Object Notation format and allows developers to access it using Twitter APIs.
- Twitter uses Open Authentication and each request must be signed with valid Twitter user credentials.
- Data has been collected using TwitterR package of R programming language.

These data will be used to analyze the features that will be used for supervised classification in order to detect legitimate and also malicious profiles. For supervised classification we need annotated or tagged data so that we could find the ways to get both legitimate and malicious data. Our emphasis in this study is on using more accurate and target data for the analysis rather than on larger size data so that we could determine a more reliable model to detect malicious profiles.

Twitter data is publicly available; almost all information about users and the tweets are available. We have collected two categories of data sets to test our model – one set is of genuine users and another one of malicious users. Getting clean profiles is easy, as more than the 95% of Twitter users are legitimate users. The difficult task is detecting and gathering data for malicious users.

For tagging legitimate users two different methods were used:

1. The first method takes the advantage of the 'verified field' provided by Twitter. When the field is true it means that twitter has verified this account and belonging to a real person or company. The field is intended for VIPs', celebrities and big companies mainly.
2. In the second method, we have sampled all the users followed by my user account in Twitter which are trustworthy. Once we get them we do the same in a second iteration. We have sampled all the users followed by my friends with the trust that they are reliable users and which are also not following any malicious user.

Taking malicious users is a bit more complicated. We have used two methods for it.

1. Twitter shuts down all malicious profiles when identified. We trekked and collected for malicious and suspicious users for a period of 3 months and the main analysis of the data one month later. We are giving some time to Twitter to identify and detect some malicious users and close these profiles. Then we have checked that how many of the previously suspicious users were unreachable after one month and tagged as malicious in case Twitter closed them down.
2. The second method for collecting malicious accounts takes the help of the websites displaying malicious URL[1],[2]. The tweets containing these URLs are tagged as malicious.

Using these methods for tagging, we have collected our data as shown in table 1.2 below:

[1] https://quttera.com/lists/malicious
[2] https://www.malwaredomainlist.com

doi: 10.32622/ijrat.762019109

Table 1.2: Annotated dataset for malicious profile detection system

Malicious Users	1,043
Legitimate Users	1,395

C. Result Analysis and Evaluation

The objective of this study is to identify features of twitter users and their behavior which can help in detecting malicious profiles. The study analyzed users' suspicious behavior based on the trust score. These trust scores are treated as features along with user profile features like number of followings, presence of profile image and description etc. If the calculated trust score of features is less than the threshold value of 0.5 then the user is a legitimate user. However, if the trust score is greater than the threshold value of 0.5 then the user is not trustworthy and is thus malicious in nature. So our dependent variable is binary. We used 15 user and trust score features as independent predictors for twitter profile classification.

There are three main goals to evaluate the malicious detection model:

1. Measure the accuracy at which our model detects the malicious profile.
2. Measure the contribution and significance of each feature to detect malicious profile.
3. Measure the contribution of all features together in detecting malicious profiles.

To model malicious profile detection, we used 1,395 legitimate users' data and 1,043 malicious users' data. We used 10 fold cross validation to evaluate the model. To make comprehensive evaluation on how effective our proposed framework is in detecting malicious profiles on twitter, we conducted series of experiments.

We used 'Binomial Logistic Regression' as a classifier to check the significance of independent variable(s) and fitness of the model. The results of the regression are given in Table 1.3. It can be seen from the results, that all included features are significant as hypothesized. The ratio between tweets posted by a user containing URL and total number of tweets posted is found to be the most significant predictor of malicious profile detection with highest estimate value. The sign of the feature estimates shows the relationship between various features and malicious profile detection. The McFadden R2 value of the model is 0.938 which means model is a good-fit.

Table 1.3: Results of Logistic Regression – Malicious Profile Detection Model

Variable Names	**Malicious Profile Detection Model**		
	Estimates	St. Error	Z-Value
(Intercept)	15.809***	1.662	9.515
TweetsURLRatio	-7.525***	0.767	-9.811
AvgTimeBetween Messages	-3.822***	0.485	-7.877
HasProfileImg.and .HasProfileDescription	-1.661**	0.554	-3.000
TotalHashTags	-3.309***	0.508	-6.509
TKFRatio.and. TUFRatio	-2.790***	0.477	-5.853
ListCount	-1.587***	0.407	-3.901
FollowBack	-3.356***	0.490	-6.851
FOFO Ratio	1.520***	0.438	3.472
TotalFollowers.and. TotalFollowees	-2.652***	0.469	-5.654
TweetsViasUsed	1.260**	0.404	3.117
TweetingRate	1.717***	0.406	4.228
APITweetRatio	2.508***	0.438	5.721
AccountAge	-3.294***	0.501	-6.577
Verified	-1.517***	0.415	-3.655
FollowingRate	-1.224**	0.408	-3.003
McFadden R2	0.938		

***, **, * significant at 1%, 5%, 10% respectively

We have trained five different classifiers on our significant set of features given in the previous section using the following methods: *naive bayes (NB), logistic regression (LR), linear support vector machine (SVM), Randon Tree (RT) and J48*. The results are given in table 1.4 and Figure 1.3 shows that Random Tree performance is better than other classifiers. The various evaluation metrics

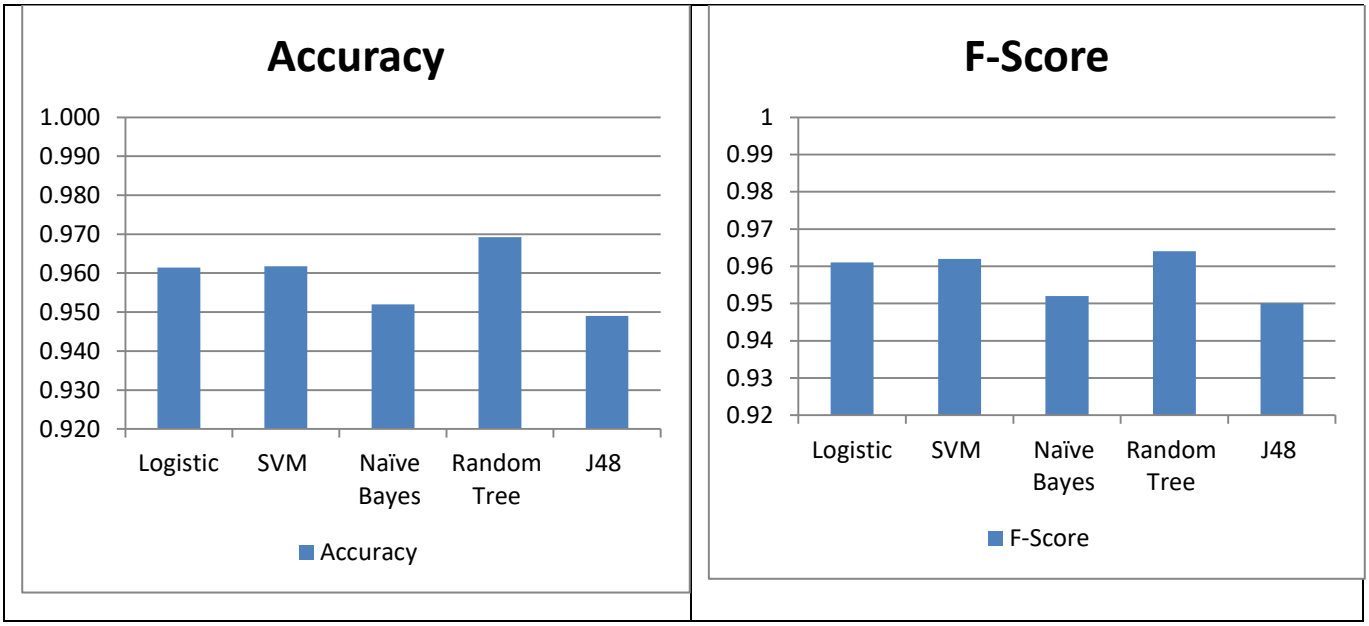
doi: 10.32622/ijrat.762019109

of the classifier are given in Table 1.5. With our dataset, the proposed model obtained an accuracy of **96.92**% with a false positive rate of only 0.032. The false positive rate tells us about the number of legitimate users classified as malicious users. The True Positive rate (TPR) is equal to 96.9%, which means that it correctly classifies 96.9% of malicious users. Only 3.1% malicious users are classified as legitimate. The F-score which is the weighted average of precision (PPR) and recall (TPR) is at high of 0.969. Table 1.5 shows the evaluation metrics for proposed model.

Table 1.4: Performance Result of five classifiers

Classifier / Metrics	Accuracy	DR	FPR	PPR	F-Score	AUC	Kappa
Logistic regression	**96.14%**	**0.961**	**0.040**	**0.961**	**0.961**	**0.993**	**0.921**
SVM	**96.18%**	**0.962**	**0.039**	**0.962**	**0.962**	**0.961**	**0.922**
Naïve Bayes	**95.20%**	**0.952**	**0.044**	**0.953**	**0.952**	**0.990**	**0.903**
Random Tree	**96.92%**	**0.963**	**0.032**	**0.965**	**0.964**	**0.970**	**0.937**
J48	**94.95%**	**0.950**	**0.053**	**0.950**	**0.950**	**0.972**	**0.897**

Figure 1.3: Performance result of five classifiers



doi: 10.32622/ijrat.762019109

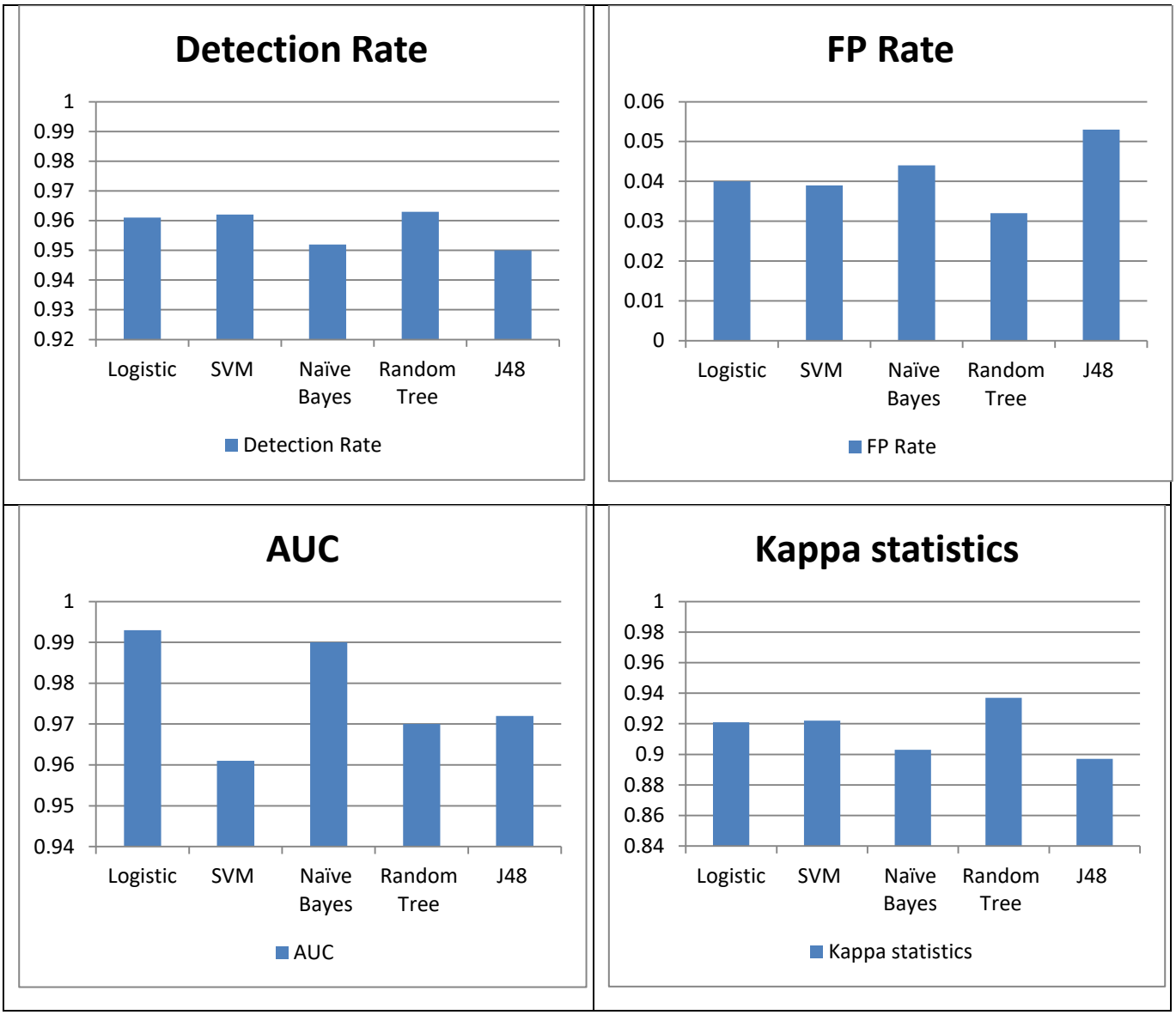


Table 1.5: Evaluation Metrics for the proposed model

Accuracy	Kappa statistic	Precision	Recall	F-Measure	ROC Area
96.9%	0.9371	0.965	0.963	0.964	0.970

From the above discussion, we conclude that our model has been successful in getting better accuracy, precision, recall and F-score and it has a very low value of false positive rate.

V. CONCLUSION AND FUTURE WORK

It is very important that one could efficiently identify and monitor the miscreants in the social media. Finding malicious profiles require a significant set of static and dynamic features that define its behavior. So we have identified 15 salient features that are significantly contributing in classification. We have used supervised classification model for classifying legitimate profiles and malicious profiles in Twitter with the 96.90% accuracy. This will be helpful for security, digital forensic and emergency agencies to identify malicious profiles and indirectly monitor malicious contents and misinformation in the social media.

Current system only works on the data from twitter. So in future data from heterogeneous sources (such as Facebook, Google+ and many more) can be collected for analysis.

REFERENCES

[1]. Qiang Cao, Michael Sirivianos, Xiaowei Yang, and Tiago Pregueiro, "Aiding the detection of fake accounts in large scale social online services", in Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, 2012.

[2]. Z. Yang, C. Wilson, X. Wang, T. Gao, B.Y.Zhao, and Y.Dai," Uncovering Social Network Sybils in the Wild", ACM Transactions on Knowledge Discovery from Data (TKDD), 8(1), 2014.

[3]. "Petya cyber attack: Ransomware virus hits computer servers across globe, Australian office affected", Available : http://www.abc.net.au/news/2017-06-28/ransomware-virushits-computer-servers-across-the-globe/8657626

[4]. "Ransomware 'Nyetya' behind new global cyber attack: Cisco ", *Economic Times*, Available : http://economictimes.indiatimes.com/articleshow/59349471.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[5]. Srinivas Rao Pulluri, Jayadev Gyani and Narsimha Gugulothu, "A Comprehensive Model for Detecting Fake Profiles in Online Social Networks ", *International Journal of Advanced Research in science and engineering*, **6** (6), 385 – 394, 2017.

[6]. E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering", *Artificial Intelligence Review*, vol. 29(1), 2008.

[7]. C. Grier, K. Thomas, V. Paxson, et al., "@ spam: The underground on 140 characters or less", *In: Proceedings of the 17th ACM conference on computer and communications security*, 27–37, 2010.

[8]. F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, C. Zhang and K. Ross , "Identifying Video Spammers in Online Social Networks", *in Int'l Workshop on Adversarial Information Retrieval on the Web (AirWeb'08)*, 2008.

[9]. F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida and M. Gonalves , "Detecting Spammers and Content Promoters in Online Video Social Networks", *in ACM SIGIR Conference (SIGIR)*, 2009.

[10]. Sangho Lee and Jong Kim, "WarningBird: A Near Real-Time Detection System for Suspicious URLs in Twitter Stream", *IEEE Transactions on Dependable and Secure Computing*, **10** (3), 183-195, 2013.

[11]. Lee K, Caverlee J and Webb S, "Uncovering social spammers: Social honeypots + machine learning", *In:Proceedings of the 33rd international ACM SIGIR conference on research and development in information retrieval*, 435–442, 2010.

[12]. G. Stringhini, S. Barbara, C. Kruegel and G. Vigna, "Detecting Spammers On Social Networks", in *Annual Computer Security Applications Conference (ACSAC'10), 2010.*

[13]. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting Spammers on Twitter", *in Collaboration, Electronic messaging, Anti-Abuse and Spam Conffference (CEAS), 2010.*

[14]. A. Wang, "Don't follow me: spam detecting in Twitter", *in Int'l Conference on Security and Cryptography (SECRYPT), 2010.*

[15]. Almaatouq, Abdullah et al., "If It Looks like a Spammer and Behaves like a Spammer, It Must Be a Spammer: Analysis and Detection of Microblogging Spam Accounts.", *International Journal of Information Security*, **15**(5), 475–491, 2016.

[16]. K. Thomas, D. McCoy, C. Grier C, et al., "Trafficking fraudulent accounts: The role of the underground market in Twitter spam and abuse", *In: USENIX Security*, 195–210, 2013.

[17]. K. Thomas and D.M. Nicol, "The Koobface botnet and the rise of social malware", *In: Proceedings of the 5th international conference on malicious and unwanted software*, 63-70, 2010.

[18]. A. Aggarwal, J Almeida and P Kumaraguru, "Detection of spam tipping behavior on foursquare", I*n: Proceedings of the 22nd international conference on World Wide Web, ACM*, 641-648, 2013.

[19]. Anhai Doan, Raghu Ramakrishnan and Alon Y Halevy, "Crowdsourcing systems on the world-wide web". *Commun. ACM*, **54**(4), 86–96, 2011.

[20]. Chu Zi, Indra Widjaja and Haining Wang, "Detecting social spam campaigns on twitter", *Applied Cryptography and Network Security, Springer Berlin Heidelberg, 455-472*, 2012.

[21]. Yang Chao, Robert Harkreader, Jialong Zhang, Seungwon Shin and Guofei Gu , "Analyzing Spammers' Social Networks for Fun and Profit", *in Proceedings of the 21st international conference on World Wide Web*, 71-80, 2012.

[22]. K. Lee, B. D. Eoff, and J. Caverlee ,"Seven months with the devils: A long-term study of content polluters on twitter", *In L. A. Adamic, R. A. Baeza-Yates, and S. Counts, editors, ICWSM*, 2011.

[23]. Chao Yang, Robert Harkreader, and Guofei Gu . "Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers", *IEEE Transactions on Information Forensics and Security*, **8** (8), 1280 – 1293, 2013.

[24]. Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering". *Information Sciences*,**260**, 64 – 73, 2014

[25]. M. Jiang, P. Cui, A. Beutel, et al, "Detecting suspicious following behavior in multimillion-node social networks", *In: Proceedings of the 23rd International Conference on World Wide Web, ACM*, 305–306, 2014.

[26]. M. Jiang, P. Cui, A. Beutel, et al.,"Catching synchronized behaviors in large networks: A graph mining approach", *ACM Transactions on Knowledge Discovery from Data (TKDD). Vancouver*, 2016.

[27]. EM Clark, JR Williams, CA Jones, et al.,"Sifting robotic from organic text: a natural language approach for detecting automation on Twitter". *Journal of Computational Science*, **16**, 1–7, 2016.

[28]. Carlos Castillo, Marcelo Mendoza and Barbara Poblete, "Predicting information credibility in timesensitive social media", *Internet Research*, ***23***(5), 560–588, 2013.

[29]. C. Grier, K. Thomas, V. Paxson, et al., "@ spam: The underground on 140 characters or less", *In: Proceedings of the 17th ACM conference on computer and communications security*, 27–37, 2010.

[30]. Supraja Gurajala, Joshua S White, Brian Hudson, Brian R Voter and Jeanna N Matthews, "Profile characteristics of fake Twitter accounts", *Big Data & Society* , 1–13, 2016.

[31]. Ali M. Meligy, Hani M. Ibrahim, and Mohamed F. Torky**, "** Identity Verification Mechanism for Detecting Fake Profiles in Online Social Networks", *I. J. Computer Network and Information Security*, 1, 31-39 ,2017.

AUTHORS PROFILE

Ms. Anamika Joshi is a research scholar in School Of Computer Science, Devi Ahilya University Indore, India. She worked as an Assistant Professor in International Institute of Professional Studies - [IIPS], Devi Ahilya University Indore, India. Her area of interest are online social media analysis and information security.

D.S. Bhilare received his M.Tech.(Computer Sc.), M.Phil.(Computer Sc.), Ph.D.(Computer Sc.), and MBA from Devi Ahilya University, Indore. Worked as a senior project leader for ten years in the industry and developed various business applications for different industries. Worked in the University for 30 years as a Head IT Centre. His areas of interest are Information Security, Network Management and Project Management.