International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Detecting Fake Accounts on Twitter using Machine Learning Technique

Vaishali Govind Bharane and Prof. Bere Sachin S. Assistant Professor

Department of Computer Engineering , Dattakala Group of Institution, Faculty of Engineering, Bhigwan

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

In the present generation number of clients can communicate with each other through social networking sites such as Facebook, Twitter, WhatsApp, etc. The social networking sites are used in the world a huge number of clients can communicate with each other. Online Social Networks (OSNs) have become increasingly popular. People's lives have become more associated with these sites. People are used to Online Social networks to keep in touch with each other and communication between social networks for share news, organize events and advertisement of own e-business. The increasing growth of OSN and the more amount of personal data of its subscribers have attracted attackers and imposters to steal personal details, share fake news and spread malicious activities. On the other side, researchers have started to research efficient techniques to detect abnormal activities and fake accounts relying account on different features and classification algorithms. However, some of the accounts exploited features have a negative contribution in the final results or it has no impact it has using standalone classification algorithms does not achieve satisfactory results. In this paper, we present a machine learning technique to identify fake accounts on twitter. We have a preprocessed dataset of numerical highlights. The Support Vector Machine algorithm is proposed to provide efficient detection of fake accounts of twitter it has used feature selection and dimensionality reduction techniques. The machine-learning algorithm was used to decide accounts to identify accounts that are fake or real. SVM algorithm is used to identify account is fake or real. SVM has used a smaller number of features hence it is being able to correctly classify about 98% of the accounts of our provided training dataset.

Keywords: *Machine learning; online social media; Twitter*

Introduction

Online Social Networking has grown extremely throughout the last few years. Online Social networks such as Facebook, Twitter, RenRen, Linked In, Google + have become increasingly popular over the last few years [1]. People use online social network to keep in touch with each other's, share news, organize events and even advertisement of their own e– businesses. For the period between 2013 and 2019 around 3.14 million U.S dollars have been spent on sponsoring political ads on Facebook by nonprofit organizations [2]. The continues growing Facebook community more than 2.3 billion monthly active users with an increase of 12% on a year –over-year basis [3].

In the second social networking sites twitter has reported about one billion of subscribers with 337 million monthly active users [4] .online social network has also attracted interest of researchers for mining and analyzing their massive amount of data, exploring and studying users behaviors as well as detecting abnormal activities [5] In scientist have made a study to predict analyze and explain customer loyalty of social media online community [6]. The online social network operator can increase the credibility of user metrics and enable third parties to consider user account [7]. In the present generation, information security and privacy are among the primary requirements of social network users, maintaining security and privacy are more important. As recently banks and financial institutions have started to analyze the loan of Facebook and Twitter accounts [8]. The open nature of online social networks the amount of personal data for a subscriber to vulnerable attack [9]. In this paper, a support vector machine classification algorithm has been used. The support vector machine algorithm uses fewer features hence it can correctly classify about 98% of the accounts of our provided training data set [7][11]. We also validated the detection performance of our classifier classifies that the account is fake or real.

Literature Survey

In the 2013 Sentiment analysis on twitter it has used the machine learning technique it deals with identifying and classifying opinions or sentiments in the source text. Twitter sentiment analysis difficult

compared to general sentiment analysis due to the presence of slang words and misspellings. It has analyzed twitter posts about electronics products like mobiles, laptops, etc. The new feature vector for classifying the tweets as positive or negative and extract people's opinions about products. In 2015 Facebook estimated that nearly 14 million monthly active users [11].

First time Facebook shared a report in the first quarter of 2018.In 2018 that shows their internal guidelines used to enforce community standards covering their efforts between October 2017 to March 2018, this report illustrates the amount of undesirable content that has been removed by Facebook [12].

Statistics shows that 40% of parents in the US and 18% of teens have a great concern about the use of fake accounts and bots on social media to sell or influence products [13].Another example, during the year 2012 United States election campaign, the Twitter account "Romney" experienced a sudden jump in the number of followers. The great majority of them were later claimed to be Fake follower [14]. Before the general Italian elections of Feb 2013 online blogs and newspapers reported statistical data over a supposed percentage of Fake followers of major candidates [16].

In 2017 fake posts have shared a roamer on social media that the actor clint Eastwood has been dead, however, the claims were proven to be false. In general, attackers follow the concept of having Online Social Networks user accounts are "keys to walled gardens" [18]so the deceive themselves off as somebody else, by using photos and profiles to spread fake news, and steal personal information. These fake accounts are generally called imposters [11][19].

To enhance their effectiveness, these malicious accounts are often armed with stealthy automated tweeting programs, to mimic real users, known as bots [20].

In 2018 detecting spam accounts on twitter has investigated the nature of spam users on twitter of the goal to improve existing spam detection mechanisms. In 2018 Trending topicsbased Spam detection from social media it has to detect Spam and classify a dataset taken from social media into trending and non-trending topics. In 2018 Social Bot Hunter it has Botnet detection in twitter to detect social botnets in an accurately detect social bots involved in distributing social spam is also called social spambots. In 2018 Detecting pathogenic social media accounts it has identifies pathogenic social media account in comparison with random and existing bot detection methods.

Proposed Methodology

This section presents the proposed system for predicting fake accounts. The twitter account has mining data i.e. tweets and accounts. It has account details are stored i.e. follows_count, friends_count, statuses_count, favourite_count and listed_count. This feature vector dataset is storing on social media. The provided tweets and accounts compare it is the non-relational or relational database. The relational database has cleaned data it gives accounts only. Then relational database it has applied a machine learning technique. It has used a machine learning technique to classify users. This method is divided into three parts.
A. Data pre-processing:
The dataset features are presented in two types.
a. Categorical Features: Categorical Features has various categories of data for e. g languages, different tweets, profile colors.
b. Numerical Features: It has a numerical type of data.

Table: Feature Vector Dataset

1.	Follows_Count
2.	Friends_Count
3.	Statuses_Count
4.	Favourites_Count
5.	Listed_Count

B. Feature Extraction:
In feature reduction phase has extracted the different features and reduce the dimensionality of features. Feature reduction has used four different techniques to reduce the dimensionality of features.
1.Principal Component Analysis (PCA)
2.Spearman's Rank-Order Correlation
3.Relevance and Redundancy analysis technique
4.Markov Blanket Technique
Those techniques are discussed as follows:

1. Principal Component Analysis (PCA):

PCA is a dimension reduction technique this is used to reduce feature vector dimensions. It finds the top number of features that best describe the data and covers as much variance of it, unnecessary features by assigning a lower weight so they did not impact on the data mining process.

2. Spearman's Rank-Order Correlation:
Spearman's Rank-Order Correlation is a type of feature selection filtering method. It measures the strength and direction of the monotonic relationship between two variables P and Q.

3.Relevance and Redundancy analysis technique: Relevance and Redundancy analysis technique is used for feature selection. In Relevance and Redundancy analysis technique Spearman's Rank-Order Correlation Was used to eliminate all pairs of features and user input as selected features.

Table. Pairs of correlated features

#	Feature1	Feature 2
Set 1	4	1
Set 2	3	1
Set 3	10	6
Set 4	11	9
Set 5	14	11
Set 6	13	11
Set 7	8	5

4. Markov Blanket Technique:

The Markov Blanket Technique for a node B in a Bayesian network is the set of nodes composed of B's Parents of its children. In Markov Blanket Technique the Markov Blanket of a node is its neighboring node.

Table. Two selected feature set

#	F1	F2	F3	F4	F5	F6	F7	F8
Set 1	0	1	1	0	1	1	1	1
Set 2	1	1	0	1	1	0	0	1

5.Wrapper Feature Selection using SVM:

One of the well-known feature selection methods is wrapper feature selection methods, where different feature subsets are selected and qualified by a learning model. The features subset with the highest predictive performance would be selected. All subsets of a set can be found using bit manipulation, there will be 2^n subsets for a given set, where n is the number of features F, in a set. For example, there will be 2^3 subsets for the set {1, 2, 3}. This method provides the best performing feature set for that particular learning model.

F1	F2	F3
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Feature Subset
{0}
{1}
{3,2}
{1}
{2}
{1,2}
{1,3}
{1,2}

Fig. All available subsets for the set {1, 2,3} presented using bit manipulation, each 1 in the binary representation indicate an element in that position.

space it might need intensive computational requirements. The baseline dataset has been split into 70% training and 30% testing. Then, all feature subsets have been trained and tested using Support vector machine "SVM".

C. Data Classification:

Data classification has used Support Vector Machine Algorithm to classify accuracy. The five features were used as input to train and test the SVM Classifier. It has the feature sets it was calculated that there is a feature subset that provides a better classification accuracy.

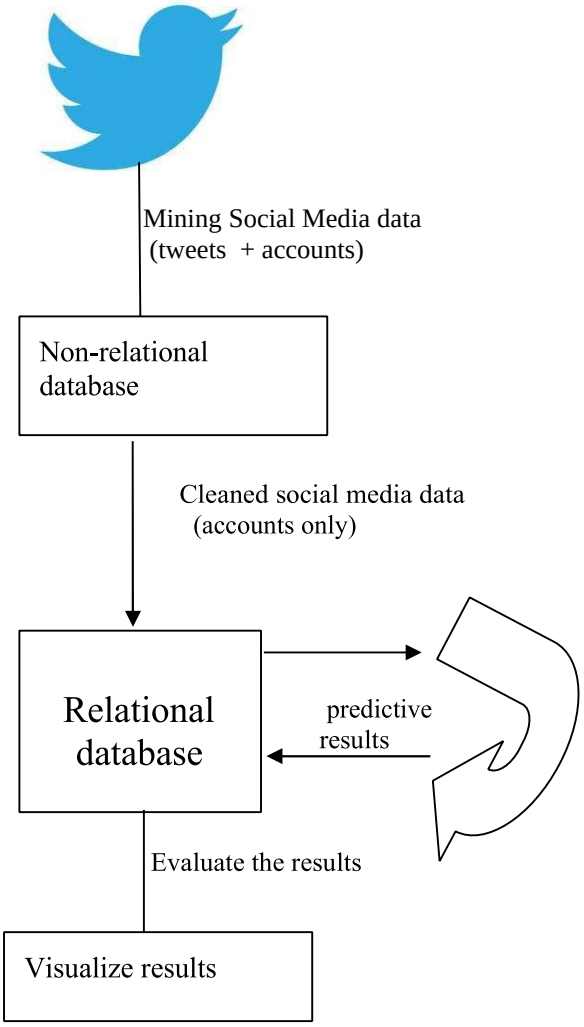

Fig. Architecture diagram of Proposed system

Algorithm Support Vector Machine

In machine learning, the algorithm support vector machine is a supervised learning method. The support vector machine is analysis data and it is used for classification and regression analysis. The support vector machine is used for classification and used to separating the hyperplane. The supervised learning algorithm is used labeled training data.

Input: Dataset of a twitter account. This dataset is a preprocessed & restructured version data. Characteristics of data set

Output: Binary classification Method. We have a set of observations called training data set which comprises the sample data with actual classification results. We train a model, called classifier on this data set, and use that model to predict whether a
certain account will be fake or not.
The outcome, thus now depends upon:
1. How well these features can "map" to the outcome.
2. The quality of our data set. By quality, I refer to statistical And Mathematics qualities.
3. How well our Classifier generalizes this relationship between the features and the outcome.
4. The values of the y1 and y2.

Steps to perform:

1.M: pre-classified data, in the form of a P*Q matrix. Q is the no. of observations and P is the number of features 2.N: An P -d vector corresponding to predicted classes for each of the P observations. 3. Feature Extraction: Extracting valuable information from input M using a series of transforms. 4. Machine Learning Model: support vector machine classifier. 5. N: Labels predicted by the classifier. 6. Quality Metric: Metric used for measuring the performance of the model. 7. Support vector machine Algorithm: The algorithm that is used to update weights w, which update the model and " learns" iteratively.

Performance and Evaluation

In this section, we present the results of the proposed algorithm and discuss them. Initially, two different classification algorithms have been trained and tested using four feature sets. The neural network classification algorithm was used as the principles mining techniques in many social network researches, so they have been applied to the feature sets and compared with the proposed SVM algorithm. Neural Networks: Currently, there are many neural network algorithms used to train models and predict results based on the trained models. NN does not calculate the prediction accuracy implicitly, so the prediction accuracy has to be calculated separately using the following formula

$$\%\text{Accuracy} = \frac{\text{All correctly identified accounts}}{\text{a total number of accounts}} \text{ X } 100$$

As mentioned above the feature subsets with the highest accuracy was highlighted, as following: spearman's rank order Correlation

Feature Set	SVM			NN		
	Accuracy	False Positive	False Negative	Accuracy	False Positive	False Negative
Yang et al.	0.886	0.111	0.001	0.737	0.059	0.203
PCA	0.914	0.039	0.046	0.53	0.278	0.067
Correlation	0.923	0.036	0.046	0.8222	0.079	0.097
Regression	0.947	0.035	0.016	0.888	0.04	0.071
Wrapper SVM	0.986	0.039	0.004	0.833	0.052	0.114

Fig. Accuracy result of SVM and NN

As mentioned above the feature subsets with the highest accuracy was highlighted, as following: spearman's rank order Correlation best pattern was (1000001000110110), Multiple Linear Regression best pattern was (0110110111001111), WrapperSVM best pattern was (0110111111011111). SVM classifier has the highest accuracy while using the Wrapper-SVM feature set and the lowest accuracy was with Yang et al. feature set. while the accuracy results for the NN classifier were lower than SVM classifier, with the highest accuracy 0.98 from the wrapper feature set and lowest accuracy using the PCA feature set. By comparing the accuracy results of all the two classification algorithms, it was illuminated that the SVM classification algorithm has the highest classification accuracy results on all the feature subsets compared with the neural network with the highest accuracy 0.98. Fig. Accuracy result of SVM and NN SVM classification: As a proposed SVM classification algorithm, researchers used an SVM classification algorithm to distinguish between fake accounts and real accounts. Hence, SVM was applied to the provided dataset and compared with NN. Radial Basis Function (RBF) was exploited as an SVM classifier kernel, and it was trained using the libSVM machine learning algorithm. It was noticed that there is a feature subset that has the maximum prediction accuracy results compared with the other subsets. As in Spearman's rank-order correlation best pattern was (1 0 0 0 0 0 1 0 0 0 1 1 0 1 1 0), Multiple Linear Regression best pattern was (0011110111001111), and Wrapper-SVM best pattern was (0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1). The detailed accuracy results of this experiment are presented in Figure.

Result and Discussions

In this section, we present the result of the proposed algorithm and discuss them. Initially, we use the Support vector machine algorithm. It is a supervised learning method. It infers a function from labeled training data. This algorithm analyzes the training data and produces an inferred function.

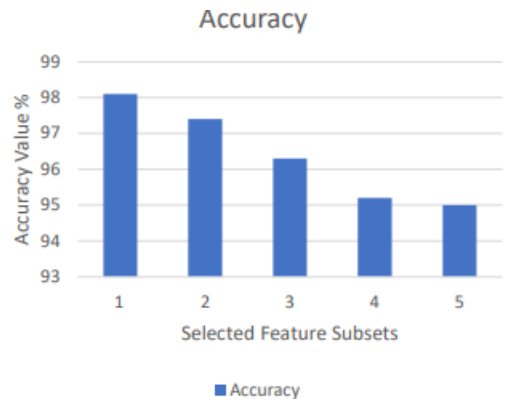

Fig. Feature Subsets with performance accuracy > 98%

The support vector machine provided a predictive model accuracy greater than 98%. To reach our goal we need training dataset and run into the pre-processing phase where different feature reduction techniques were used to reduce the feature vector. In the classification phase SVM learning algorithm were used. The result of SVM archived better accuracy result with all features set comparing.

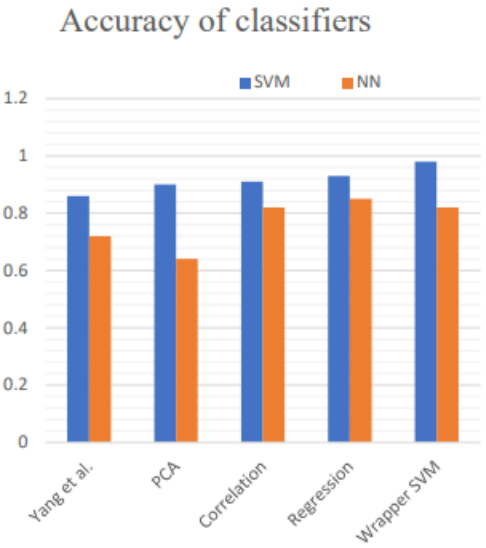

Fig. SVM Classification accuracy result

Conclusion

In this paper, a new classification algorithm was proposed to improve detecting fake accounts on social networks, where the SVM trained model decision values were used to train a Neural Network model. To reach our goal we used dataset run it into the pre-processing phase where different feature reduction techniques were used to reduce the feature vector. In the classification phase, SVM learning algorithms were used. The results of the analyses showed that "SVM" has archived better accuracy results with all feature sets comparing with other classifiers, with classification accuracy around 98%. It was noticed that the Neural Network algorithm has the lowest classification accuracy compared with SVM. This occurred because the SVM algorithm reaches the global minimum of the optimized function, while the Neural Network using the gradient descent technique, and may reach the local minimum, not global minimum like SVM. It was also noticed that using the feature set provided by PCA, encountered a very low classification accuracy, while the wrapper SVM feature set achieves high classification accuracy. This happened because PCA performs dimension reduction and generates new features base on a linear combination of original features. But the wrapper SVM approach, and other feature selection techniques select the best set of original features, not a linear combination of all features. On the other words, feature selection selects the most effective original features, but PCA performs a linear combination of the original features event they are not effective. The Wrapper SVM feature set records a remarkable accuracy among the other feature selection technique sets because the Wrapper SVM technique not only selects the best features but also removes the redundancy.

References:

[1] (2018) Detecting Fake Accounts on Social Media. [Online].Available:https://www.researchgate.net/publication/3 30629456_Detecting_Fake_Accounts_on_Social_Media [2] Political advertising spending on Facebook between 2014 and 2018.Internet draft. [Online].Available:https://www.statista.com/statistics/891327/ political-advertisingspending-facebook-by-sponsor-category/

[3]Quarterly earning reports. Internet draft.[Online].Available:https://investor.fb.com/home/default.a spx(2018)

[4] Statista.twitter: number of monthly active users 2010-2018. Internet draft. [Online]. Available: https://www.statista.com/statistics/282087/number-of-monthly active-twitter-users/

[5] R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," Egyptian informatics journal, vol. 17, no. 2, pp. 199–216, 2016.

[6] L. M. Potgieter and R. Naidoo, "Factors explaining user loyalty in a social media-based brand community," South African Journal of Information Management, vol. 19, no. 1, pp. 1–9, 2017.

[7] Y. Boshmaf, D. Logothetis, G. Siganos, J. Ler´ıa, J. Lorenzo, M. Ripeanu, K. Beznosov, and H. Halawa, "´ Integro: Leveraging victim prediction for robust fake account detection in large scale osns," Computers & Security, vol. 61, pp. 142–168, 2016.

[8] (2013) Banque populaire dis-moicombiendamistu as sur Facebook, je tediraisi ta banquevataccorder un prłt. Internet draft.

[Online].Available:http://bigbrowser.blog.lemonde.fr/2013/09/1/ popularitedis-moi-combien-damis-tu-as-sur-facebook-je-te-diraisi-ta-banqueva-taccorder-un-pret/

[9] J. R. Douceur, "The sybil attack," in International workshop on peerto-peer systems. Springer, 2002, pp. 251–260.

[10] (2012) Cbc.facebook shares drop on news of fake accounts. Internetdraft.[Online].Available:http: //www.cbc.ca/news/technolo gy/facebook-shares-drop-onnews-of-fake-accounts-1.1177067

[11] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, "Thwarting fake osn accounts by predicting their victims," in Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015, pp. 81–89.
[12] (2018) Facebook publishes enforcement numbers for the first time.Internet draft [Online]. Available:https://newsroom.fb.com/news/2018/05/enforcementnumbers/
[13] (2018) How concerned are you that there are fake accounts and bots on social media platforms that are used to try to sell you things or influence you? Internet draft. [Online]. Available: https://www.statista.com/statistics/881017/fake social-media-accounts-bots-influencing-selling-purchases-usa/
[14] (2012) Buying their way to twitter fame. Internet draft. [Online].Available:www.nytimes.com/2012/08/23/fashion/twitterf ollowers-for-sale.html?smid=pl-share [15] (2017) Welcome to the era of the bot as political boogeyman. Internet draft.[Online]. Available:https: //www.washingtonpost.com /news/politics/ wp/2017/06/12/welcometo-the-era-of-the-bot-as-political-boogeyman
[16](2018)Human or'bot'?doubts over italiancomicbeppegrillo's twitter followers. Internet draft.[Online].Available:https://www.telegraph.co.uk/technology/t witter/9421072/Human-orbot-Doubts-over-Italian-comic-BeppeGrillos-Twitter-followers.html
[17] S.-T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," in Proceedings of the 2010 New Security Paradigms Workshop. ACM, 2010, pp. 61–72.
[18] S. Fong, Y. Zhuang, and J. He, "Not every friend on a social network can be trusted: Classifying imposters using decision trees," in Future Generation Communication Technology (FGCT), 2012 International Conference on. IEEE, 2012, pp. 58–63. [19] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in Proceedings of the 27th annual computer security applications conference. ACM, 2011, pp. 93–102.
[20] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A theoretical review of social media usage by cybercriminals," (ICCCI), 2017 International Conference