Volume: 7 Issue: XII Month of publication: December 2019

DOI: http://doi.org/10.22214/ijraset.2019.12038

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

Spam Account Detection on Social Media using Machine Learning Methods: A Survey

Jaladhi Pandya[1], Prof. Gayatri Pandi (Jain) [2]
[1, 2]Information Technology, L J Institute of Engineering and Technology

Abstract: Internet has become a world of social media and communication. In our daily life usually every person is using a social media like a Facebook, twitter and LinkedIn for communication and knowledge widening. These social media sites are misused for communication by creating fake accounts. These accounts do not have genuine data. Fake accounts mean some people are using other's personal data for creating fake profile. Fake accounts frequently spam legitimate users, posting inappropriate or illegal content. These social media sites are being used to spy, send malicious links and carry out financial frauds. Platforms of social media are more effectual for conman since they give permission to striker to build a bond with their targets. We are using several new features, which are more effective and robust compared to existing features like selection, generalize batter, interpretable. In our proposed system, we are using classification and regression method for detecting fake accounts on social media which are more efficient and accurate as compared to the existing ones.

Keywords: Social Media, Fake accounts, Spam account detection, Machine learning

I. INTRODUCTION

Current generation we are using so many different social media. There is different social media like a Facebook, Twitter, etc. A social networking service work for as a platform to built social networks or social relation among people who, share interests, activities, backgrounds, or real life connections. A social network generally offered to participants who register this site with their unique representation. One of the most common ways of performing a large scale data gathering attack is the use of fake accounts. Where hostile users are present themselves in profiles impersonating fictitious or real persons. At attempt has been made in this paper to use of Machine learning.

A. Machine Learning

Machine learning means there is a machine which is automatically improve and learn and study from experience without crystal clear programmed. In the artificial intelligence one of the applications is machine learning. The basic bourn is to permit the computers study instinctively without human involvement or encouragement and adjust steps appropriately.

B. Random Forest (RF)

Random forest is one of the most appropriate classifier. In machine learning there is a different type of classifier. Random forest is one kind of ensemble technique. Ensemble technique means we are using a different models or classifier on applying a same database or different database and then we get the output from different models after that combine that output from different models and create one strong model. So, random forest is ensemble model where there is using a different decision trees.

C. Artificial neural Network (ANN)

An artificial neural network is a mutually related group of nodes, inspired by neurons in a brain. In artificial neural network there are three layers: Input layer, Hidden layer, Output layer. Artificial neural network have n number of input and n number of weight with input data. And then n number of input data and n number's weight consider as input data for hidden layer and in this layer there is also a weight. And after that we can get the output.

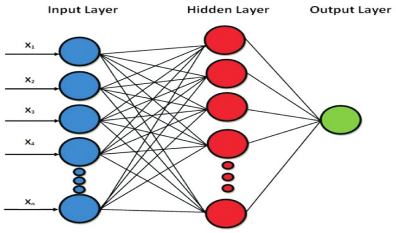

Fig.1 Artificial neural network

D. Spam

Spamming is the fruition of messaging systems to send an unsought or blackballed, especially advertisement, fake messaging using fake account. Spammers are targeting users of instant messaging service or private number or SMS. Some people they want harm others so they are creating fake accounts on different social media.

II. RELATED WORK

In this section we are focusing on some different papers and they are using different proposed system and the different classifiers and they mostly use of supervised machine learning's classification algorithm. Rewinding different paper this will be helpful for our proposed work and we can evaluate and solve the problem. [1] The graph adjacency matrix, the similarity matrices between accounts was calculated, and then PCA algorithm was used for feature extraction. Then the linear SVM, Medium Gaussian SVM and regression, and logistic algorithms were used to classify the nodes. Detecting fake users in a complex network use the graph technology. There is also use an approach known as the minority class artificial sampling which creates the synthetic minority oversampling technique. [1] Authors used map-reduction techniques and pattern recognition approaches to discover fake accounts. [2], authors use seven machine learning algorithms, namely: kNearest Neighbor (k-NN), Decision Tree (DT), Naive Bayesian (NB), Random Forest (RF), Logistic Regression (LR), Support Vector Machine (SVM), and eXtreme Gradient Boosting (XGBoost) to classify spam and legitimate users and also used feature like graph-based and content-based features that have been proved to be powerful for spam account detection on Twitter. Content-based and graph based feature have been to be powerful for spam account detection. [2] Authors are detecting a fake accounts using twitter dataset and using a twitter dataset and where 168 real accounts' and 157 spam users. [3], the classifier is being trained regularly as new training data set is feed into the classifier.

The classifier determines whether the profile is fake or real. Dataset is divided into training and testing data. Classification algorithm is trained using training dataset and testing data set is used to determine the efficiency of algorithm. [3], the authors using machine learning algorithm like random forest and support vector machine and deep learning. Confusion matrix is used for what your classification model is getting right and what type of error occurs. Authors using different feature like number of friends, number of, followers, language. They are using a publicly available dataset of 1337 fake users and 1481 real accounts.

[4], The Reaserch have preprocessed our dataset using a supervised discretization technique named Entropy Minimization Discretization (EMD) on numerical features and analyzed the results of the Naïve Bayes algorithm. In this paper research using twitter social account for detecting fake accounts. There is using confusion matrix which most common evolution metrics.

[5], the proposed algorithm (SVM-NN) uses less number of features, while still being able to correctly classify about most of the accounts of our training dataset. In this paper researcher combine the classification algorithm support vector machine and neural network. Authors were using PCA for identifying features.

III.COMPARISION TABLE

TABLE 1 Comparison Table

NO	Paper Title	Author	Methods	Limitation
1	Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms	Mohammadreza Mohammadrezaei , MohammadEbrahimShiri , andAmirMasoudRahmani	linear SVM Medium Gaussian SVM Regression	In this paper, the method which is used it will not recognize properly and not work in network
2	Detecting spam accounts on Twitter	Zulfikar Alom, DiSTA, Barbara Carminati DiSTA,Elena Ferrari DiSTA	kNearest Neighbor Decision Tree Naive Bayesian Random Forest Logistic Regression Support Vector Machine eXtreme Gradient Boosting	In this paper complex method and not give batter efficiency
3	Detecting Fake Accounts in Media Application Using Machine Learning	Gayathri A , Radhika S , Mrs. Jayalakshmi S.L.	Random forest Support vector machine	In this paper support vector machine not get good accuracy.
4	Twitter Fake Account Detection	Buket Ershin; Ozlem Aktas; Deniz Kilinc; Ceyhum Akyol	supervised discretization technique Naïve Bayes	In this paper Authors can improve accuracy using different model or classifier.
5	Detecting Fake Accounts on Social Media	Sarah khaled; Neamat El-Tezi; Hoda M. O. Mokhtar	Support vector Neural network	In this paper, authors using PCA and so that the accuracy rate goes down.

IV. PROPOSED SOLUTION

In this paper we are using machine learning classifier random forest. Random forest gives best accuracy comparatively other classifier and also more efficient compare to other classifier. Also use an artificial neural network for detecting fake accounts.

Using neural network we can improve efficiency and accuracy.

So, we are using RF-ANN model for accurate result. We are using some different features like following list, common friends, family member, message frequency, and Language type.

Random forest is kind of ensemble classifier which is using decision tree algorithm in random fashion. First of all creates a fictitious accounts and then inject the data and for a detection of fake account we are using machine learning algorithm.

We are using the machine learning algorithms for improve an efficiency and accuracy. First we select the profile which would be tested from extracting our database. We are creating a database where we are tested on that profile. Then extracting features what we are needed to help an evolution of that there is a profile is fake or real and then we are using a classification algorithm and then we evaluate the result.

We are evaluating result in five steps:

1) *Step 1:* We need to select profiles or account which we are wanted to testing on that database. So, we first need a dataset. Creating a database where we are using a twitter data set. In this data set there will be some data set are real and some data set are fake. So in first phase we create fake and real accounts.
2) *Step 2:* After extracting database or dataset we should extract features and then applying on the database. There is different types of feature which have a different type of characteristics. In this paper we are using simplest features like who is following the account, what is the relation between that follower and the user account.
3) *Step 3:* After step 2, we have to go through data preprocessing. Data preprocessing is necessary because suppose there is data which is unnecessary and also redundant data or garbage data then data preprocessing clean this type of data. And after this and also after extracting feature, this data pass through Classification algorithm. In this paper we are using a Random forest and artificial neural network.
4) *Step 4:* This phase is the evolutions phase that, where we properly extract data from the database?, where there is extracting features properly?, so this is the evolution of overall of process flow and every phase work properly.
5) *Step 5:* After step 4, this phase is last phase where we are obtaining result.

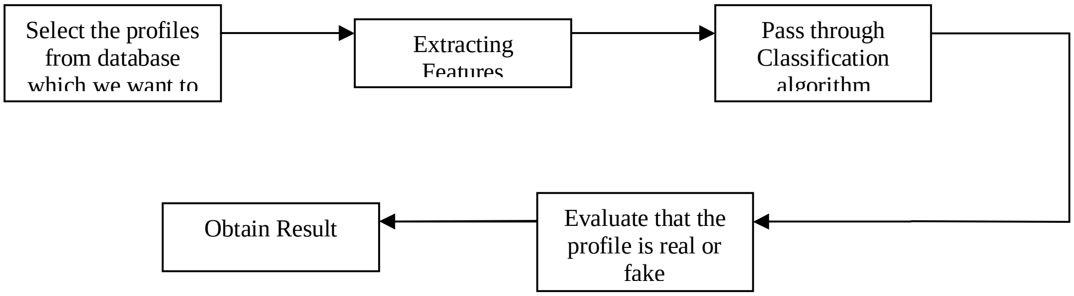
Select the profiles from database which we want to
Extracting Features
Pass through Classification algorithm
Evaluate that the profile is real or fake
Obtain Result

Fig.2 Proposed flow

V. CONCLUSIONS

In this paper we are using a machine learning algorithms and where we are using supervised machine learning. In supervised machine learning's algorithm there are a different classification models.

But Random forest model is better than the other models. So using a Random forest and artificial neural network we can get more accuracy and also efficiency. And we can reduced the malicious activity and detect the fake accounts on social media.

REFERENCES

[1] Sarah khaled; Neamat El-Tezi; Hoda M. O. Mokhtar, “Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms,” , Hindwai, 2018.

[2] Zulfikar Alom, DiSTA, Barbara Carminati DiSTA,Elena Ferrari DiSTA; Ceyhum Akyol, “Detecting spam accounts on Twitter,” IEEE International Conference,2017

[3] Gayathri A , Radhika S , Mrs. Jayalakshmi S.L.; “Detecting Fake Accounts in Media Application Using Machine Learning ,“ International Journal of Advanced Networking & Applications, 2018

[4] Buket Ershin; Ozlem Aktas; Deniz Kilinc; Ceyhum Akyol; “Twitter Fake Account Detection,” IEEE International Conference,2017

[5] Sarah khaled; Neamat El-Tezi; Hoda M. O. Mokhtar;“Detecting Fake Accounts on Social Media ,” IEEE International Conference,2018

[6] Abdulla Amin Aburomman; Mamun Bin Ibne Reaz;“ Ensemble of binary SVM classifiers based On PCA and LDA feature extraction for intrusion detection,” IEEE International Conference,2016

[7] Marc-André Kaufhold, Christian Reuter, “Cultural Violence and Peace in Social Media,”Information Technology for Peace and Security Springer, 2019

[8] Patxi Gal´an-Garc´ıa, Jos´e Gaviria de la Puerta, Carlos Laorden G´omez, Igor Santos, Pablo Garc´ıa Bringas, “Supervised Machine Learning for the Detection of Troll Profiles in Twitter Social Network: Application to a Real Case of Cyberbullying,” Springer International Publishing ,2014

[9] Arnu Pretorius∗, Surette Bierman and Sarel J. Steel, “A Meta-Analysis of Research in Random Forests for Classification,”,IEEE, 2016

[10] Mehmet ŞİMŞEK, Oğuzhan YILMAZ , Asena Hazal KAHRİMAN , Levent SABAH ,” Detecting Fake Twitter Accounts with using Artificial Neural Networks,”Artificial Intelligence Studies, 2018

[11] Sun Bo, Du Junping, Gao Tian, “Study on the Improvement of K-Nearest-Neighbor Algorithm,” International Conference on Artificial Intelligence and Computational Intelligence, 2009

[12] P. Srinivas Rao, Dr. Jayadev Gyani, Dr.G.Narsimha, “Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP ,”International Journal of Applied Engineering Research, 2018

[13] Rohit Raturi, “Machine Learning Implementation for Identifying Fake Accounts in Social Network,” International Journal of Pure and Applied Mathematics, 2018

[14] G´erard Biau, Erwan Scornet, Johannes Welbl, “Neural Random Forests,” Mathematics Subject Classification, 2010