International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Fake Account Detection using Machine Learning and Data Science

S. P. Maniraj, Harie Krishnan G, Surya T, Pranav R

Abstract- ***Nowadays, Online Social Media is dominating the world in several ways. Day by day the number of users using social media is increasing drastically. The main advantage of online social media is that we can connect to people easily and communicate with them in a better way. This provided a new way of a potential attack, such as fake identity, false information, etc. A recent survey suggest that the number of accounts present in the social media is much greater than the users using it. This suggest that fake accounts have been increased in the recent years. Online social media providers face difficulty in identifying these fake accounts. The need for identifying these fake accounts is that social media is flooded with false information, advertisements, etc.***

Traditional methods cannot distinguish between real and fake accounts efficiently. Improvement in fake account creation made the previous works outdated. The new models created used different approaches such as automatic posts or comments, spreading false information or spam with advertisements to identify fake accounts. Due to the increase in the creation of the fake accounts different algorithms with different attributes are use. Previously use algorithms like naïve bayes, support vector machine, random forest has become inefficient in finding the fake accounts. In this research, we came up with an innovative method to identify fake accounts. We used gradient boosting algorithm with decision tree containing three attributes. Those attributes are spam commenting, artificial activity and engagement rate. We combined Machine learning and Data Science to accurately predict fake accounts.

Keyword: ***Data science, Fake account detection, Machine learning, Online social media***

I. INTRODUCTION

In today's Modern society, social media plays a vital role in everyone's life. The general purpose of social media is to keep in touch with friends, sharing news, etc. The number of users in social media is increasing exponentially. Instagram has recently gained immense popularity among social media users. With more than 1 Billion active users, Instagram has become one of the most used social media sites. After the emergence of Instagram to the social media scenario, people with a good number of followers have been called Social Media Influencers. These social media influencers have now become a go-to place for the business organization to advertise their products and services.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
S. P. Maniraj*, Assistant Professor, SRM Institute of Science and Technology, Chennai, India.
Harie Krishnan G, UG Scholar, SRM Institute of Science and Technology, Chennai, India.
Surya T, UG Scholar SRM Institute of Science and Technology, Chennai, India.
Pranav R, UG Scholar SRM Institute of Science and Technology, Chennai, India.

The widespread use of social media has become both a boon and a bane for the society. Using Social media for online fraud, spreading False information is increasing at a rapid pace. Fake accounts are the major source of false information on social media. Business organizations that invest huge Sum of money on social media influencers must know whether the following gained by that account is organic or not. So, there is a widespread need for a fake account detection tool, which can accurately say whether the account is fake or not. In this paper, we use classification algorithms in machine learning to detect fake accounts. The process of finding a fake account mainly depends on factors such as engagement rate and artificial activity.

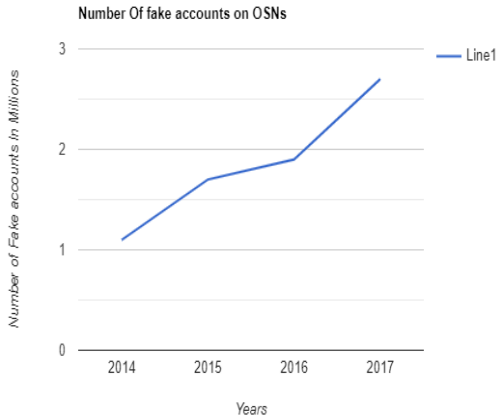

Fig 1.1 Graph Showing increase in number of Fake accounts over the years

II. EXISTING SYSTEM

The existing systems use very fewer factors to decide whether an account is fake or not. The factors largely affect the way decision making occurs. When the number of factors is low, the accuracy of the decision making is reduced significantly. There is an exceptional improvement in fake account creation, which is unmatched by the software or application used to detect the fake account. Due to the advancement in creation of fake account, existing methods have turned obsolete. The most common algorithm used by fake account detection Applications is the Random forest algorithm. The algorithm has few downsides such as inefficiency to handle the categorical variables which has different number of levels. Also, when there is an increase in the number of trees, the algorithm's time efficiency takes a hit.

III. PROPOSED SYSTEM

The existing system uses random forest algorithm to identify the fake account. It is efficient when it has the correct inputs and when it has all the inputs. When some of the inputs are missing it becomes difficult for the algorithm to produce the output. To overcome such difficulties in the proposed systems we used a gradient boosting algorithm. Gradient boosting algorithm is like random forest algorithm which uses decision trees as its main component. We also changed the way we find the fake accounts i.e., we introduced new methods to find the account. The methods used are spam commenting, engagement rate and artificial activity. These inputs are used to form decision trees that are used in the gradient boosting algorithm. This algorithm gives us an output even if some inputs are missing. This is the major reason for choosing this algorithm. Due to the use of this algorithm we were able to get highly accurate results.

IV. DETECTION STRATEGY

In Our Research, we define an account as fake when it doesn't meet the minimum engagement rate, have artificial activities or when the account has a history of Spam comments.

A. Web Scraper

Web Scraper is used to extract data from a website. When a user pastes a link of a Social media Account, Using OutWit hub, a Web scraper tool, we extract necessary pieces of information from the social media site.

We extract data such as login activity, Total Likes, Total Comments, Number of posts, Number of followings and Number of Followers.

B. Calculation of Engagement rate

An engagement rate is a metric that measures the level of engagement of a Post or Story received on social media. It is the percentage by which the audience interact with a post. By checking the number of interactions with the number of followers we can evaluate the engagement rate. Interactions can be of likes, comments, and shares. Most Fake accounts will boast of 1000s of followers and a very minimum number of likes. Since the engagement rate is relatively calculated, comparisons between popular accounts and semi-popular accounts are comparatively easy. This metric is one of the most vital ones because lesser audience engagement signifies that the account is fake.

$$\text{Engagement rate percentage} = \left(\frac{\text{Total number of interactions}}{\text{Total number of followers}} \right) \times 100$$

Fig 4.1 Engagement rate Calculation

C. Artificial Activity

Normal social media activities such as liking, commenting and sharing turns into an artificial activity when the frequency of the above mentioned are very high. Around the clock activity also signifies that the account is used by a Bot. At this stage, we look into the number of likes, comments, and shares this particular account has made since its creation. If an enormous amount of likes or comments are found, then that account will be considered as fake. By enormous we mean a number which is not achievable by an average social media user. Also, the amount of time the account was online will be looked upon before concluding. Other factors that are considered are insufficient information on the account and Status of verification of the mobile number and email.

D. Spam Comments

BOT comments are always known to be very Generic and often lack Substance. At this stage, the comments made from the account will be gone through in a detailed manner. Total number of comments by the user made since the creation of the account will be compared with average comments of users in that particular OSN's. If there is a big difference the account may be considered fake. Commenting links will lead to the account being termed as Fake account. Same or Similar type of comments will also be considered as spam comments.

E. Detection of Fake Accounts

In this step, we combine all the data we extracted from the website. In this paper we mainly focus on engagement rate, artificial activity and spam comments. The data collected using web scraper is used to compute the values for the factors mentioned above. Using these factors different decision tress is formed. Using gradient boosting algorithm and with the formed decision trees fake accounts are detected.

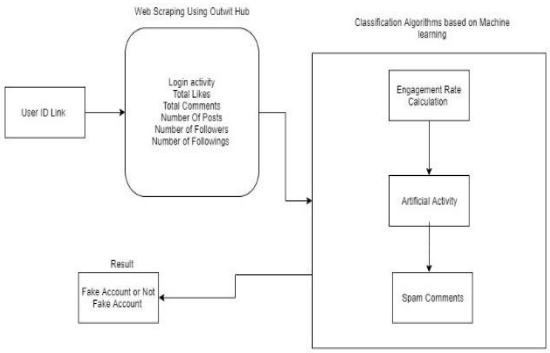

Fig 4.2 Architecture Diagram

V. EVALUATION

A. Decision Trees

Decision trees are made seeing the success rate i.e., in our case taking the value which contains more fake accounts. The first tree is made using an engagement rate as the root node and artificial activity as its child node along with spam comments as another node. The second tree is made keeping artificial activity as the root node, engagement rate and spam comments as subsequent nodes. The third tree is formed using spam comments as the root node, artificial activity and engagement rate as subsequent nodes.

B. Gradient boosting

Gradient boosting is the most effective algorithm for classification problems. When the values are given accurately and with a lot of training data sets this algorithm works efficiently. The basic principle of gradient boosting is that it forms a strong rule from multiple weak learners. The main advantage of this algorithm is that it predicts perfectly in the absence of any one of the used factors. The decision trees formed are combined and predicted value is found. This value is used to predict the result. The main terminologies in this algorithm are pseudo residuals, shrinkage, decision trees, and prediction value.

VI. ALGORITHM

Input: training set $\{(x_i, y_i)\}_{i=1}^{n}$ a differentiable loss function L(y,F(x)), number of iterations *M*.
Algorithm:

I. Initialize model with a constant value:
$F_0(x) = argmin \sum_{i=1}^{n} L(y_i, \gamma)$.

II. For *m* = 1 to *M*:

1. Compute so-called *pseudo-residuals*:
$$r_{im} = -[\frac{\partial(L(y_i, F(x_i))}{\partial(F(x_i)}]_{F(x)=F_{m-1}(x)}$$
For i =1, . . . , n.
2. Fit a base learner (e.g.tree) $h_m(x)$ to pseudo-residuals, i.e. train it using the training set $\{(x_i, y_i)\}_{i=1}^{n}$.
3. Compute multiplier γ_m by solving the following one-dimensional optimization problem:
$$\gamma_m = argmin \sum_{i=1}^{n} L(y_i, F_{m-1}(x_i) + \gamma h_m(x_{i)})).$$
4. Update the model:
$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x).$$

III. Output $F_m(x)$.

VII. CONCLUSION

In this research, We have come up with an ingenious way to detect fake accounts on OSNs By using machine learning algorithms to its full extent, we have eliminated the need for manual prediction of a fake account, which needs a lot of human resources and is also a time-consuming process. Existing systems have become obsolete due to the advancement in the creation of fake accounts. The factors that the existing system relayed upon is unstable. In this research, we used stable factors such as engagement rate, artificial activity to increase the accuracy of the prediction.

VIII. LITERATURE SURVEY

Detecting fake accounts in social media has become a tedious problem for many Online Social Networking sites such as Facebook and Instagram. Generally, fake accounts are found using machine learning. Previously used methods to identify fake accounts have become inefficient. In [1], Multiple algorithms like decision tree, logistic regression and support vector machine algorithms were used for detection. A major drawback of the decision tree algorithm is that the tree contains data sets for a feature and not for multiple features. Thus, the models which came after this minimized the number of features as done in [2] where comparing the age entered with their registered mail id and location of the users were used as features. Improvement in creating fake accounts made these methods inefficient in detecting it. Thus, service providers changed their way to predict fake accounts by changing their algorithms as done in [3] where the METIS clustering algorithm was used. This algorithm gets the data and clusters it into different groups which made it easier to separate fake accounts from real accounts. Whereas in [4] Naïve Bayes algorithm is used. The probability for the used features was calculated and is substituted in the naïve Bayes formula and the computed value is checked with a reference value. If the computed value is less than the reference value, then that account is considered to be fake.

REFERANCES

1. ”Detection of Fake Twitter accounts with Machine Learning Algorithms” Ilhan aydin,Mehmet sevi, Mehmet umut salur.
2. ”Detection of fake profile in online social networks using Machine Learning” Naman singh, Tushar sharma, Abha Thakral, Tanupriya Choudhury.
3. ”Detecting Fake accounts on Social Media” Sarah Khaled, Neamat el tazi, Hoda M.O. Mokhtar.
4. ”Twitter fake account detection”, Buket Ersahin, Ozlem Aktas, Deniz kilinc, Ceyhun Akyol.
5. ” a new heuristic of the decision tree induction” ning li, li zhao, ai-xia chen, qing-wu meng, guo-fang zhang.
6. ” statistical machine learning used in integrated anti-spam system” peng-fei zhang, yu-jie su, cong wang.
7. ” a study and application on machine learning of artificial intellligence” ming xue, changjun zhu.
8. ” learning-based road crack detection using gradient boost decision tree” peng sheng, li chen, jing tian.
9. ” verifying the value and veracity of extreme gradient boosted decision trees on a variety of datasets” aditya gupta, kunal gusain, bhavya popli.
10. ” fake account identification in social networks” loredana caruccio, domenico desiato, giuseppe polese.

AUTHOR PROFILE

S P Maniraj Assistant Professor (Sr.G) SRM Institute of Science and Technology, (PhD) School of Computing, Specialization-Medical Image Processing. Email: *maniraj.p@rmp.srmuniv.ac.in*

Harie Krishnan G (B.tech) UG Scholor SRM Institue of Science and Technology Email: hariekrishnan60@gmail.com

Surya T (B.tech) UG Scholor, SRM Institue of Science and Technology. Email: surya11012000@gmail.com

Pranav R (B.tech) UG Scholor, SRM Institue of Science and Technology. Email: pranavron112@gmail.com