International Journal of Recent Advances in Multidisciplinary Topics
Volume 2, Issue 6, June 2021
https://www.ijramt.com | ISSN (Online): 2582-7839

Fake Profile Identification Using Machine Learning

M. Naveen Babu[1], Giragani Anusha[2*], Aleti Shivani[3], Chenchu Kalyani[4], Jangalla Meenakumari[5]
[1]*Assistant Professor, Department of Computer Science and Engineering, JB Institute of Engineering and Technology, Moinabad, India*
[2,3,4,5]*Student, Department of Computer Science and Engineering, JB Institute of Engineering and Technology, Moinabad, India*

***Abstract*: The social network, a crucial part of our life is plagued by online impersonation and fake accounts. According to the 'Community Standards Enforcement Report' published by Face book on March 2018, about 583 million fake accounts were taken down just in quarter 1 of 2018 and as many as 3-4% of its active accounts during this time were still fake. In this project, we propose a model that could be used to classify an account as fake or genuine. This model uses Support Vector Machine as a classification technique and can process a large dataset of accounts at one, eliminating the need to evaluate each account manually. The community of concern to us here is Fake Accounts and our problem can be said to be a classification or a clustering problem**

***Keywords*: SVM**

1. Introduction

In the present generation, the social life of everyone has become associated with the online social networks. Adding new friends and keeping in contact with them and their updates has become easier. The online social networks have impact on the science, education, grassroots organizing, employment, business, etc. Researchers have been studying these online social networks to see the impact they make on the people. Teachers can reach the students easily through this making a friendly environment for the students to study, teachers nowadays are getting themselves familiar to these sites bringing online classroom pages, giving homework, making discussions, etc. which improves education a lot,, the employers can use these social networking sites to employ the people who are talented and interested in the work, their background check can be done easily.

2. System Overview

The previously engineered features that were used to detect fake accounts are not similarly successful in the detection of genuine user's accounts. The current method is focused on detecting fake accounts, as opposed to those genuine accounts. The results from past methods to detect fake accounts could be applied successfully to defect genuine human accounts. A corpus of genuine human accounts is enriched with engineering features that had previously been used to detect fake accounts created be fake users to some extent. These features were applied to various supervised machine learning models. The machine learning models were trained to use engineered features without relying on behavioral data. This made it possible for these machine learning models to be trained on very little data, compared to when behavioral data is included (SVM). The finding indicates that engineered features that were previously used to detect fake accounts, at best predicted genuine accounts with an F1 score of 49.75%. This can be attributed to the fact that genuine users have different characteristics and behaviors' than fake users which cannot be modeled similarly. The community of concern to us here is fake us here is Fake Accounts and our problem can be said to be a classification or a clustering problem. As, this is an automatic detection method, it can be applied easily be online social networks which has millions of profiles, whose profiles cannot be examined manually.

3. Literature Survey

1) Facebook immune system

Popular Internet sites are under attack all the time from phishes, fraudsters, and spammers. They aim to steal user information and expose users to unwanted spam. The attackers have vast resources at their disposal. They are well-funded, withfull-times killed labor, control over compromised and infected accounts, and access to global botents. Protecting our users is a challenging adversarial learning problem with extreme scale and load requirements. Over the past several years we have built and deployed a coherent, scalable, and extensible real time system to protect our users and the social graph. This Immune System performs real time checks and classifications on every read and writes action. As of March 2011, this is 25 B checks per day, reaching 650 K per second at peak. The system also generates signals for use as feedback in classifiers and other components. We believe this system has contributed to making Face book the safest place on the Internet for people and their information. This paper outlines the design of the Face book Immune System, the challenges we have faced

*Corresponding author: giraganianusha@gmail.com

and overcome, and the challenges we continue to face.

2) Existing system

1. Naïve Bayes algorithm having less accuracy.
2. Several approaches that seem promising towards the aim of perfectly classify the misleading articles.
3. They note that simple content-related- grams and shallow parts-of-speech (POS) tagging have proven insufficient for the classification task, often failing to account for important context information.

3) Disadvantages

Because of Privacy Issues the Face book dataset is very limited and a lot details are not made public.

4. Proposed System

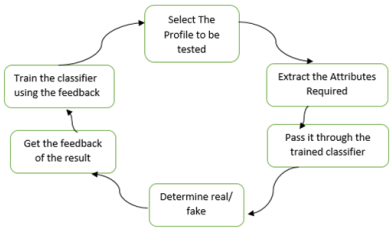
The Application Domain of the following project was Community Detection. Community detection is key to understanding the structure of complex networks, and ultimately extracting useful information from them. In this project, we came up with a framework through which we can detect a fake profile using machine learning algorithms so that the social life of people becomes secured.

1. Classification starts from the selection of profile that needs to be classified.
2. Once the profile is selected, the useful features are extracted for the purpose of classification.
3. The extracted features are then fed to trained classifier.
4. Classifier is trained regularly as new data is fed into the classifier.
5. Classifier then determines whether the profile is genuine or fake.
6. The result of classification algorithm is then verified and feedback is fed back into the classifier.
7. As the number of training data increases the classifier becomes more and more accurate in predicting the fake profiles.

1) Advantages

1. The social networking sites are making our social lives better but nevertheless there are a lot of issues with using these social networking sites.
2. The issues are privacy, online bullying, potential for misuse, trolling, etc. these are done mostly by using fake profiles.
3. In this project, we came up with a framework through which we can detect a fake profile using machine learning algorithms so that the social life of people becomes secured.

5. System Architecture



1) Modules: Pre-processing

Pre-processing refers to the transformations applied to our data before feeding it to the algorithm. Data Preprocessing is a technique that is used to convert the raw data into a clean data set. In other words, whenever the data is gathered from different sources it is collected in raw format which is not feasible for the analysis. For achieving better results from the applied model in machine learning projects the format of the data has to be in a proper manner. Some specified Machine Learning model needs information in a specified format, for example, Random Forest algorithm does not support null values, therefore to execute random forest algorithm null have to be managed from the original raw dataset.

2) Feature extraction

Feature selection is also called as variable selection or attributes selection. It is the automatic selection of attributes in your data (such as columns in tabular data) that are most relevant to the predictive modeling problem you are working on. Feature selection is the process of selecting a subset of relevant features for use in model construction.

3) Classification

Ordinary Least Squares Regression: If you know statistics, you probably have heard of linear regression before. Least squares are a method for performing linear regression. You can think of linear regression as the task of fitting a straight line through a set of points. There are multiple possible strategies to do this, and ordinary least squares strategy go like this – you can draw a line, and then for each of the data points, measure the vertical distance between the point and the line, and add these up: the fitted line would be the one where this sum of distances is as small as possible. Linear refers the kind of model you are using to fit the data, while least square refers to the kind of error metric you are minimizing over.

Logistic Regression: Logistic regression is a powerful statistical way of modeling a binomial outcome with one or more explanatory variables. It measures the relationship between the categorical dependent variable and more independent variables by estimating probabilities using a logistic function, which is the cumulative logistic distribution.

4) Support vector machines

SVM is binary classification algorithm. Given a set of points of 2 types in N dimensional place, SVM generates a (N-1) dimensional hyper plane to separate those points into 2 groups. Say you have some points of 2 types in a paper which are linearly separable. SVM will find a straight line which separates those points into 2 types and situated as far as possible from all those points.

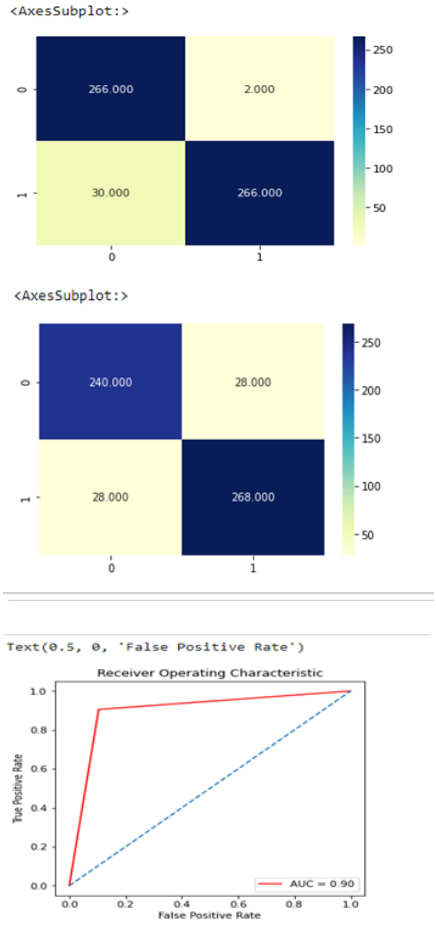
5) Generating confusion matrix and accuracy finding

Confusion Matrix is a technique for summarizing the performance of a classification algorithm. Calculating a confusion matrix can give you a better idea of what your classification model is getting right and what types of errors it is making.

True Positive Rate (T P R) = TP / TP + FN
False positive Rate (F P R) = FP / FP / + TN
True Negative Rate (T N R) = TN/ FP + TN
False Negative Rate (F N R) = 1 – TPR

Recall – How many of the true positives were recalled (found), i.e. how many of the correct hits were also found.

6. Result



7. Conclusion

The model presented in this project demonstrates that Support Vector Machine (SVM) us an elegant and robust method for binary classification in a large dataset. Regardless of the non-linearity of the decision boundary, SVM is able to classify between fake and genuine profiles with a reasonable degree of accuracy (>90%). This method can be extended on any platform that needs binary classification to be deployed on public profiles for various purposes. This project uses only publicly available information which makes it convenient for organization that want to avoid any breach of privacy, but organizations can also use private data available to them to further extend the capabilities of the proposed model.

8. Future Work

Since we have limited data to train the classifier, our approach is facing a high variance problem which can be observed in the learning curve as follows High variance problems can usually be mitigated by increasing the size of the dataset which should not be of much concern to Social Networks Organization which already have fairly large datasets.

References

[1] C. Beleites, K. Geiger, M. Kirsch, S.B. Sobottka, G. Schackert, and R. Salzer, “Raman spectroscopic grading of astocytoma tissues: Using soft reference information,” Anal. Bioanal. Chem., vol. 400, no.9, pp.2801, 2011.

[2] G.Gu, R. Perdisci, J.Zhang, and W.Lee, “BotMiner: Clustering analysis of network traffic for protocol-and structure-independent botnet detection,” in Proc. USENIX Secur.Symp., vol. 5, pp. 139-154, 2008.

[3] W.Wu, J.Alvarez, C.Liu, and H.-M.Sun, “Bot detection using unsupervised machine learning,” Microsyst. Technol., vol. 24, no. 1, pp. 209-217, 2018.