International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Fake Profile Identification Using Machine Learning

K.Pavankumar,K.Sandeep Varma, M.Pavithra

Department of C.S.E, SCSVMVdeemed Universityrsity, Kanchipuram.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 Facebook 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 once, 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: Social media, Twitter, Facebook, Random Forest Classifier, Classification, Frame work, Dataset

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. Literature Survey

• Statistical features-based real-time detection of drifted Twitter spam
AUTHORS:C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Mi

•Automatically identifying fake news in popular Twitter threads
AUTHORS:C. Buntain and J. Golbeck

•A performance evaluation of machine learning-based streaming spam tweets detection
AUTHORS:C. Chen, J. Zhang, Y. Xie, Y. Xiang,W. Zhou, M. M. Hassan, A. AlElaiwi, and M. Alrubaian

* *Corresponding author.*
E-mail address: rethinakumars66@gmail.com

3. Proposed Model

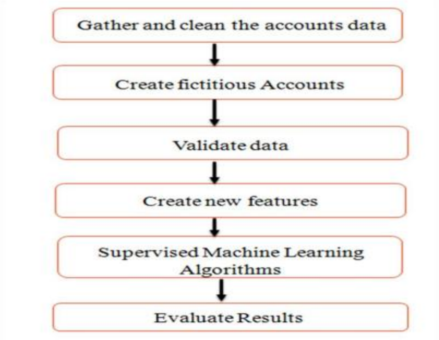
The Application Domain of the following project was Community Detection. Community detection is key to understanding the stru cture of complex networks, and ultimately extracting useful information from them. In this project, we came up with a framework through which we can detect a fake profile using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

4. Software Requirements

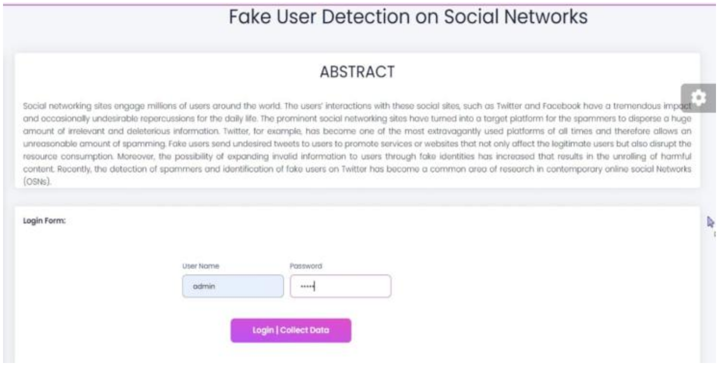
CODING LANGUAGE : Python 3.7
MODULES : Anaconda,Numpy,Pandas,Jupytor
OPERATING SYSTEM : Windows

5. Block Diagram


Gather and clean the accounts data
Create fictitious Accounts
Validate data
Create new features
Supervised Machine Learning Algorithms
Evaluate Results

6. Result and Implementation

Whenever the program is ready to run,it will ask for input,the input is home page .In home page we have login account.After log in we get a Data collection after that testing the data and seaching a account is Real or Fake.



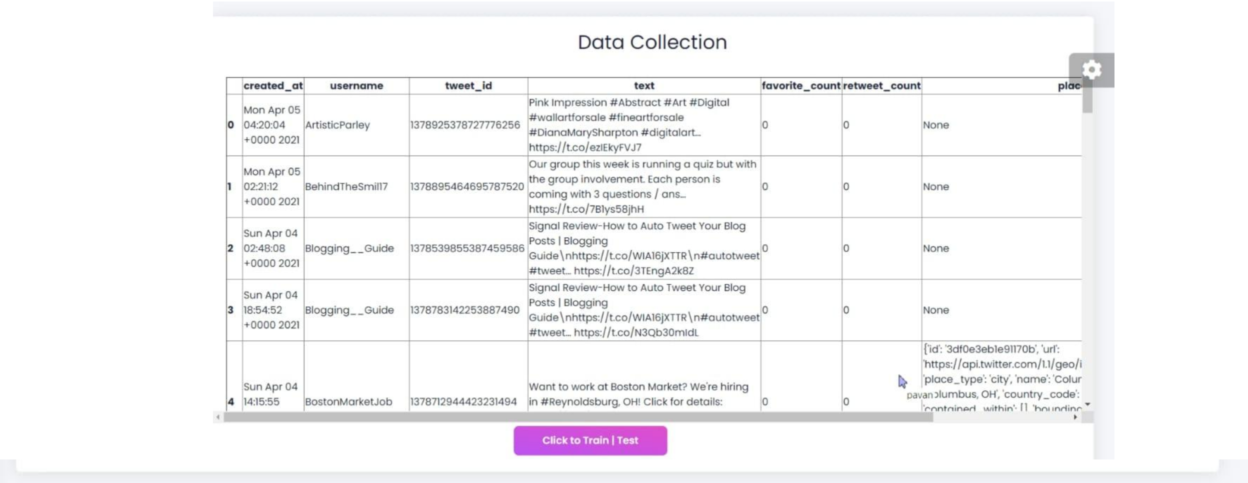
Fake User Detection on Social Networks

ABSTRACT

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook have a tremendous impact and occasionally undesirable repercussions for the daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spamming. Fake users send undesired tweets to users to promote services or websites that not only affect the legitimate users but also disrupt the resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased that results in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs).

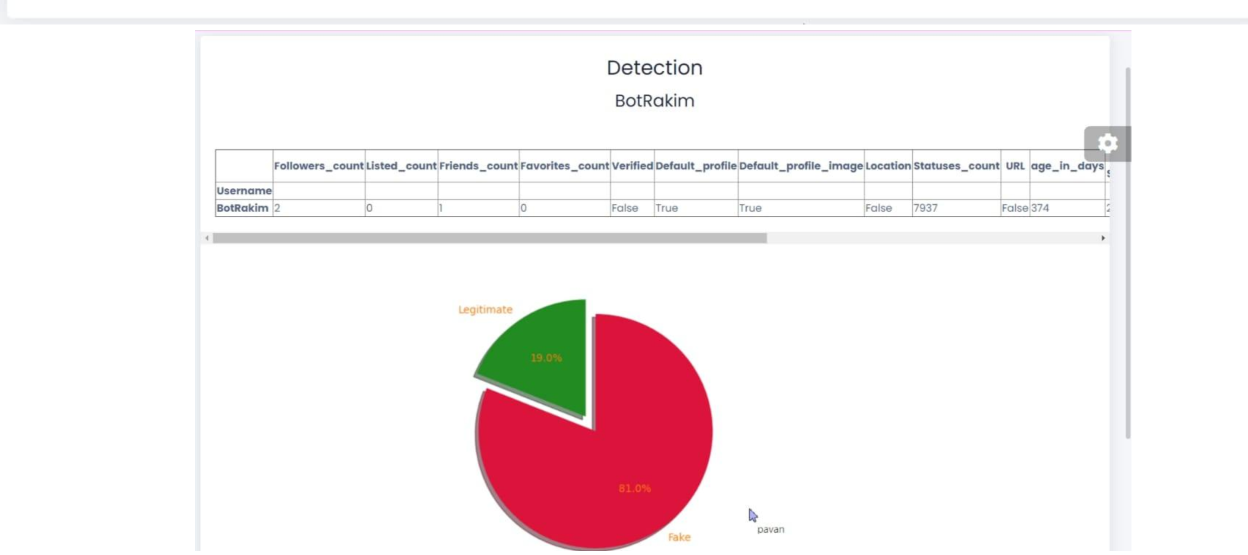
Login Form:

User Name: admin
Password: •••••



Data Collection

	created_at	username	tweet_id	text	favorite_count	retweet_count	plac
0	Mon Apr 05 04:20:04 +0000 2021	ArtisticParley	1378925378727776256	Pink Impression #Abstract #Art #Digital #wallartforsale #fineartforsale #DianaMarySharpton #digitalart… https://t.co/ezIEkyFVJ7	0	0	None
1	Mon Apr 05 02:21:12 +0000 2021	BehindTheSmil17	1378895464695787520	Our group this week is running a quiz but with the group involvement. Each person is coming with 3 questions / ans… https://t.co/7B1ys58jhH	0	0	None
2	Sun Apr 04 02:48:08 +0000 2021	Blogging__Guide	1378539855387459586	Signal Review-How to Auto Tweet Your Blog Posts | Blogging Guide\nhttps://t.co/WIA16jXTTR\n#autotweet #tweet… https://t.co/3TEngA2k8Z	0	0	None
3	Sun Apr 04 18:54:52 +0000 2021	Blogging__Guide	1378783142253887490	Signal Review-How to Auto Tweet Your Blog Posts | Blogging Guide\nhttps://t.co/WIA16jXTTR\n#autotweet #tweet… https://t.co/N3Qb30mIdL	0	0	None
4	Sun Apr 04 14:15:55	BostonMarketJob	1378712944423231494	Want to work at Boston Market? We're hiring in #Reynoldsburg, OH! Click for details:	0	0	{'id': '3df0e3eb1e91170b', 'url': 'https://api.twitter.com/1.1/geo/i 'place_type': 'city', 'name': 'Colur olumbus, OH', 'country_code': 'contained_within': [], 'boundinc



Detection

BotRakim

	Followers_count	Listed_count	Friends_count	Favorites_count	Verified	Default_profile	Default_profile_image	Location	Statuses_count	URL	age_in_days
Username											
BotRakim	2	0	1	0	False	True	True	False	7937	False	374

7. Advantages:

- The social networking sites are making our social lives better but nevertheless there are a lot of issues with using these social networking sites.
- The issues are privacy, online bullying, potential for misuse, trolling, etc. These are done mostly by using fake profiles.
- 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 become secured.

8. Conclusion

The model presented in this project demonstrates that Support Vector Machine (SVM) is 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 organizations 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.

References

[1] C. Chen, S. Wen, J. Zhang, Y. Xiang, J. Oliver, A. Alelaiwi, and M. M. Hassan, ‘‘Investigating the deceptive information in Twitter spam,’’ Future Gener. Comput. Syst., vol. 72, pp. 319–326, Jul. 2017.

[2] I. David, O. S. Siordia, and D. Moctezuma, ‘‘Features combination for the detection of malicious Twitter accounts,’’ in Proc. IEEE Int. Autumn Meeting Power, Electron. Comput. (ROPEC), Nov. 2016, pp. 1–6.

[3] M. Babcock, R. A. V. Cox, and S. Kumar, ‘‘Diffusion of pro- and anti-false information tweets: The black panther movie case,’’ Comput. Math. Org. Theory, vol. 25, no. 1, pp. 72–84, Mar. 2019.

[4] S. Keretna, A. Hossny, and D. Creighton, ‘‘Recognising user identity in Twitter social networks via text mining,’’ in Proc. IEEE Int. Conf. Syst., Man, Cybern., Oct. 2013, pp. 3079–3082.

[5] C. Meda, F. Bisio, P. Gastaldo, and R. Zunino, ‘‘A machine learning approach for Twitter spammers detection,’’ in Proc. Int. Carnahan Conf. Secur. Technol. (ICCST), Oct. 2014, pp. 1–6.

[6] W. Chen, C. K. Yeo, C. T. Lau, and B. S. Lee, ‘‘Real-time Twitter content polluter detection based on direct features,’’ in Proc. 2nd Int. Conf. Inf. Sci. Secur. (ICISS), Dec. 2015, pp. 1–4.

[7] H. Shen and X. Liu, ‘‘Detecting spammers on Twitter based on content and social interaction,’’ in Proc. Int. Conf. Netw. Inf. Syst. Comput., pp. 413–417, Jan. 2015.

[8] G. Jain, M. Sharma, and B. Agarwal, ‘‘Spam detection in social media using convolutional and long short term memory neural network,’’ Ann. Math. Artif. Intell., vol. 85, no. 1, pp. 21–44, Jan. 2019.

[9] M. Washha, A. Qaroush, M. Mezghani, and F. Sedes, ‘‘A topic-based hidden Markov model for real-time spam tweets filtering,’’ Procedia Comput. Sci., vol. 112, pp. 833–843, Jan. 2017.