Fake Profile Identification in Social Network using Machine Learning and NLP

1st Mr.T.MURALI,
(Assistant professor)
Dept of computer science andEngineering,
Paavai Engineering College, Namakkal, India

2nd CHERUB EBENEZEER
dept of computer science andEngineering
Paavai Engineering College Namakkal,India

3rd KIRUTHIKA.M
dept of computer science andEngineering,
Paavai Engineering College
Namakkal, India

***Abstract*—In present times, social media plays a key role in every individual life.Everyday majority of the people are spending their time on social media platforms. The number of accounts in these social networking sites has dramatically increasingday-by-day and many of the users are interacting with others irrespective of their timeand location.These social media sites have both pros and cons and providesecurity problems to us also for our information.To scrutinize,who are giving threats in thesenetworking sites we need to organize these social networking accounts into genuine accountsand fake accounts.Traditionally, we are having different classification methods to point outthe fake accounts on social media. But we must increase the accuracy rate in identifying fakeaccounts on these sites.In our paper we are going with Machine Learning technologies and Natural Language processing (NLP) to increase the accuracy rate of detecting the fake accounts. We opted for Random Forest tree classifier algorithm.**

Keywords: Machine Learning, NLP, Random Forest classifier, Gradient Boost classifier

1. INTRODUCTION

Social media has become most entertaining platform for present world, admiring users who are spending millions of minutes on such services. These social media services solve almost every problem ranging very small to big problems [1]. And upgrading security and protecting from harmful sites also plays a vital role and became a challenge. Using social media everybody interacts with other new user and share their personal information. this may lead to cause threats. Some social media methods have been proposed;however, they often rely on data that is not publicly available for LinkedIn accounts. [2]. A FeatureBased Approach to Detecting Fake Twitter Profiles [3,4], There are many types of attacks in social media and the major one is file theft. When someone uses others information for their personal use then the theft occurs, and it becomes a problem.

978-1-6654-7995-0/22/$31.00 ©2022 IEEE

Victims may face penalties. For example, people use other's identity and do mistakes which affects the reputation that person in the society. Truly, many Social Networkapplications have the lowest level of data protection set by default.Therefore,Social Network has become the best platform for fraud and abuse.Social media makes it easier for serious and naive attackers to conduct identity theft and phishing attacks.Make matters worse,users need to create an account on the social media.Loss, especially if such accounts are hacked.The configuration file information in the online network is also static or dynamic.Individuals can provide detailed info during the profile period.Creation is called static knowledge.Static knowledge covers a person's demographics and interests while dynamic knowledge includes a person's leadership habits and position in most current studies which are based accordingly on static and dynamic data.The network you see some static and dynamic configuration files is usually. This unique research has proposed several techniques that can find nonauthentic(fake) identities and malicious content in the social networking platforms.Every technique has their own advantage and Disadvantage-Bullying,abuse,trolls,etc.In many cases, false personal information is used on specifici.e., there can be male as well as female profiles with incorrect data.Fake Facebook personal information is mostly used for malicious problems for customers in social communities.People create false social engineering materials,phishing aims to demean a male or female,promote or inspire a group of people.With spam,fake identity etc., it is also commonly referred to as the Facebook Immune System (FIS).It is not currently ready to closely check the false personal profiles created for customers on Facebook.

Artificial intelligence (AI) refers to a computer program's or machine's ability to think and learn.It's also a branch of research that aims to make computers "smarter" [5]. Artificial intelligence is the use of computer science programming to simulate human cognition and behaviour by analysing data and surroundings, solving or predicting problems, and learning or self-teaching to adapt to a variety of activities.

Machine learning is a rapidly evolving technology that allows computers to learn from earlier data automatically. Machine learning uses a range of techniques to developmathematical models and make predictions based on previously collected data or expertise. It is currently utilised for a variety of activities, including image recognition [6], Facebook auto-tagging [7][9],Many algorithms and approaches for detecting fraudulent profiles have been presented, the majority of which make advantage of the huge number of unstructured data created by social networks [8], social networks [10][11], Speech recognition, email filtering, recommender systems, and a variety of other applications are just a few examples. There are many machine learning algorithms are developed like mathematical modelling [12], clustering [13], deep learning [14], artificial neural network models [15]. Machine learning are used in various fields like face recognition [16], Speech recognition [17], tumour classifications [18].

2. IMPLEMENTATION

The following six steps as shown in fig.1 need to be followed to implement the machine learning model which detects the fake profile in the social media sites.

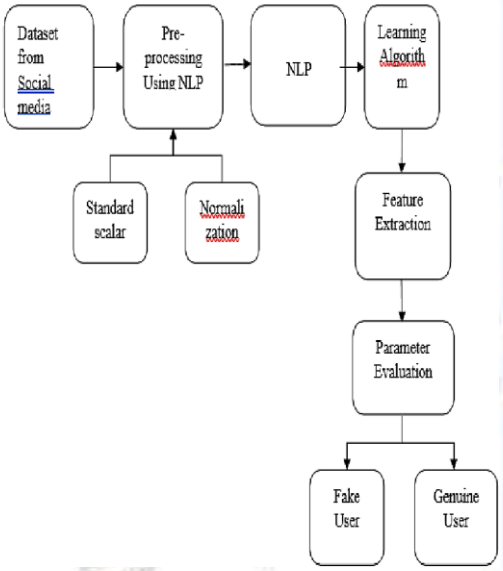


Fig1. System Architecture

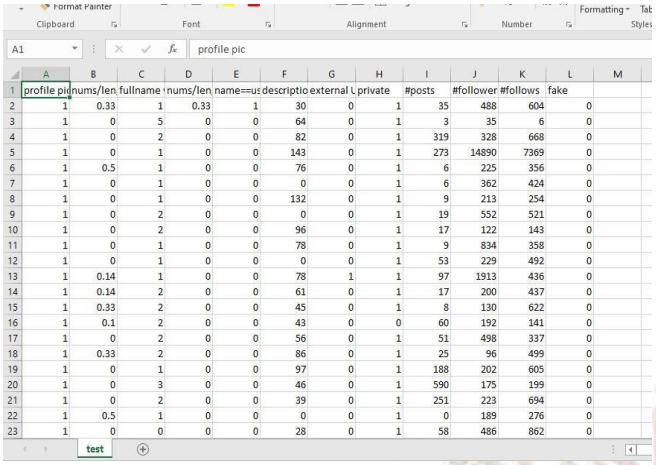
System Architecture Consists of:
1.Collect the dataset 2.Preprocess the dataset
3.Validate the information needed to determine if something is false or not 4. Tunning the dataset.
5. Applying random forest Algorithm.
6. Theresults of precision, recall, accuracy, f1 score parameters is evaluated.

Dataset:

We'll need to gather a dataset having data from both false and real profiles. Among the attributes in the dataset are the number of followers, follows, username length, if the profile is secret, and the number of posts. Table 1 lists the qualities and their descriptions. The information is separated into two groups: training and testing. The testing dataset is used to evaluate the model, whereas the training dataset is used to train it. The dataset is divided in half in a 4:1 ratio, with 4/5 of the data utilised for training and 1/5 for testing. Table 1. Attributes and its explanation.

Fig 2. Shows Collected Data

Attributes	Explanation
Profile Pic	In most of the cases profile picture will not be there when it is a fake account.
followers	In most of the cases there will not more followers for the fake profile users.
follows	The fake Profile uses mostly follow more person.
post	In most of the cases the number of posts created by fake profile will be very less.
Description length	The Description length of the fake profiles will be very less for most of the cases.
Private	Most of the fake profiles will not be private.
External URL	There will be more external URL in the fake profile.
Full name	This attribute gives the full name of the user of social media profile.
Length of Full name	This attribute gives the length of full name of the user of social media profile.
Length of username	This attribute gives the length of username of the social media profile.
Username==full name	In most of the cases username will not be same as full name when it is fake profile.



profile pic	nums/len	fullname	nums/len	name==us	descriptio	external L	private	#posts	#follower	#follows	fake
1	0.33	1	0.33	1	30	0	1	35	488	604	0
1	0	5	0	0	64	0	1	3	35	6	0
1	0	2	0	0	82	0	1	319	328	668	0
1	0	1	0	0	143	0	1	273	14890	7369	0
1	0.5	1	0	0	76	0	1	6	225	356	0
1	0	1	0	0	0	0	1	6	362	424	0
1	0	1	0	0	132	0	1	9	213	254	0
1	0	2	0	0	0	0	1	19	552	521	0
1	0	2	0	0	96	0	1	17	122	143	0
1	0	1	0	0	78	0	1	9	834	358	0
1	0	1	0	0	0	0	1	53	229	492	0
1	0.14	1	0	0	78	1	1	97	1913	436	0
1	0.14	2	0	0	61	0	1	17	200	437	0
1	0.33	2	0	0	45	0	1	8	130	622	0
1	0.1	2	0	0	43	0	0	60	192	141	0
1	0	2	0	0	56	0	1	51	498	337	0
1	0.33	2	0	0	86	0	1	25	96	499	0
1	0	1	0	0	97	0	1	188	202	605	0
1	0	3	0	0	46	0	1	590	175	199	0
1	0	2	0	0	39	0	1	251	223	694	0
1	0.5	1	0	0	0	0	1	0	189	276	0
1	0	0	0	0	28	0	1	58	486	862	0

Fig2. Collected dataset

Pre-processing:

In the Pre-processing section we need to check whether the data set is having any null values and the type of value each column having if there is any null value, we need to find the mean and we need to update the mean value in the null value box or else we can remove the row itself also if there is any column with object datatype we also need to change to integer. Fig 3 shows the Pre-processed results of our dataset.

Tuning and Applying algorithm:

In the Tuning we are using grid search algorithm to tune the data and we are applying the Random Forest algorithm to create the machine learning model which will detect the fake profile in the social media.

```
In [16]: # Finding Missing  Values
         X_data.isnull().sum()

Out[16]: profile pic            0
         nums/length username   0
         fullname words         0
         nums/length fullname   0
         name==username         0
         description length     0
         external URL           0
         private                0
         #posts                 0
         #followers             0
         #follows               0
         dtype: int64

In [17]: # Check if Imbalance in Labels
         #Labels is about 1:1 which means there is no imbalance in the labels.
         #but here the ratio would be more 2:1.

         unique, freq = np.unique(y_data, return_counts = True)

         for i, j in zip(unique, freq):
             print("Label: ", i, ", Frequency: ", j)

         Label:  0 , Frequency:  288
         Label:  1 , Frequency:  288
```

]

Fig 3. Pre-processed results

3. EVALUATION OF MODEL

Confusion Matrix: For the classification algorithmthe overall performance can be summarized by using Confusion matrix. By getting the confusion matrix we can know whether our classification algorithm is predicting correct or what kind of mistake it is doing. Fig.4 explains the confusion matrix of our model.

True Positive Rate (TPR)TPR=TP/(TP+ FN)
True Negative Rate (TNR)TNR=TN / (FP+ TN)
False Positive Rate (FPR)FPR=FP/(FP+ TN)
False Negative Rate (FNR)FNR=1- TPR

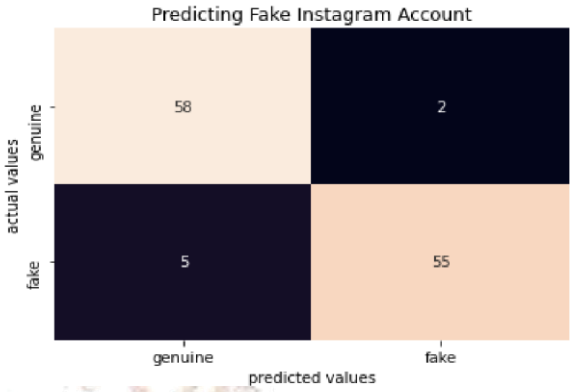


Fig 4. Confusion matrix for our model

Precision: The ratio of relevant instances to all retrieved instances is called as Precision.

Precision = TP/(TP+FP) Precision = 58/(58+5) = 0.92

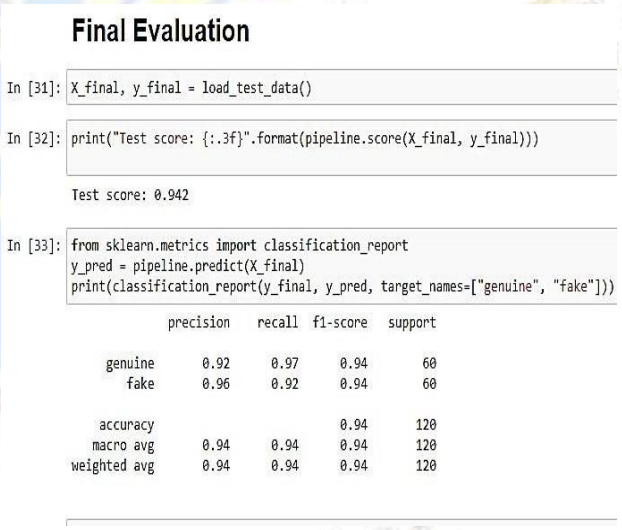
Recall: The ratio of retrieved instances to all relevant instances is called as Recall. sometimes it is also referred as sensitivity.

Recall = TP /(TP+FN) Recall = 58/(58+2) = 0.96

Accuracy: It is defined as the how accurately the model predicting the correct output.

Accuracy = (TP+TN)/(TP+TN+FP+FN) Accuracy = (58+55)/(58+55+5+2) = 0.94

The evaluation metrics of our model is shown in the Fig.5



Final Evaluation

```
In [31]: X_final, y_final = load_test_data()

In [32]: print("Test score: {:.3f}".format(pipeline.score(X_final, y_final)))

         Test score: 0.942

In [33]: from sklearn.metrics import classification_report
         y_pred = pipeline.predict(X_final)
         print(classification_report(y_final, y_pred, target_names=["genuine", "fake"]))

                      precision    recall  f1-score   support

             genuine       0.92      0.97      0.94        60
                fake       0.96      0.92      0.94        60

            accuracy                           0.94       120
           macro avg       0.94      0.94      0.94       120
        weighted avg       0.94      0.94      0.94       120
```

Fig5. Evaluation metrics of our model

4. CONCLUSION

Here this idea came up with machine learning algorithms besides NLP techniques. From the social media sites, we can easily find the fake profiles by implementing these techniques. In this Paper to point out the fake profiles we have taken the Instagram dataset. Examine the dataset, we used the NLP pre-processing techniques and to organize the profiles we used machine learning algorithm such as Random Forestclassifier and Gradient Boost classifier. By using these learning algorithms, thedetection accuracy rate has been improved in this paper.

5. FUTURE WORK

Our major complication is that a person can have numerous Instagram accounts which is an added benefit for those who create fake profiles and accounts in social media sites. Our aim is to add 12-digit Aadhar card number while creating an account, as a result we can limit single account for single user and there is no probability of fake profiles in social networks.

REFERENCES

[1] Understanding User Profiles on social media for Fake News Detection. Shu, S. Wang and H. Liu, 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2018, pp. 430-435, doi:
10.1109/MIPR.2018.00092.

[2] "Identifying fake profiles in linkedin." Adikari, Shalinda, andKaushik Dutta. arXiv preprint arXiv:2006.01381 (2020).

[3]. Fake Twitter accounts: profile characteristics obtained using an activity-based pattern detection approach.Gurajala, S., White, J.S., Hudson, B. and Matthews, J.N., 2015, Julyin Proceedings of the 2015 International Conference on social media & Society (pp. 1-7).

[4] "A feature-based approach to detect fake profiles in Twitter." Kaubiyal, Jyoti, and Ankit Kumar Jain. In Proceedings of the 3rd International Conference on Big Data and Internet of Things, pp. 135-139. 2019.

[5] Fake news detection within online social media using supervised artificial intelligence algorithms.Ozbay, F.A. and Alatas, B., 2020. Physica
A: Statistical Mechanics and its Applications, 540, p.123174.

[6] Contour tracking based knowledge extraction and object recognition using deep learning neural networks (2016).Reddy, A.
V. N., &Phanikrishna, C. Paper presented at the Proceedings on 2nd International Conference on Next Generation Computing Technologies in 2016, NGCT 2016, 352-354. doi:10.1109/NGCT.2016.7877440.

[7] Hybrid Scheme for Detecting Fake Accounts in Facebook"N., Smruthi.M.,"A ISSN: 2277- 3878, (IJRTE)International Journal of Recent Technology and Engineering (2019), Issue-5S3, Volume-7.

[8] 2 Fake profile detection techniques in large-scale online social networks: A comprehensive review. (2018)Ramalingam, D. and Chinnaiah, V., Computers & Electrical Engineering, 65, pp.165- 177.

[9. "Detection of fake profiles in social media-Literature review."]Romanov, Aleksei, Alexander Semenov, Oleksiy Mazhelis, and Jari Veijalainenin International Conference on Web Information Systems and Technologies, vol. 2, pp. 363-369. SCITEPRESS, 2018

[10] Recognition of fake currency note using convolutional neural networks (2016).Sai Pooja, G., Rajarajeswari, P., YaminiRadha, V., NavyaKrishna.G., Naga Sri Ram.B.,International Journal of Innovative Technology and Exploring Engineering, 58-63,8(5).

[11] Predicti-Ngcyber Bullying on Social Networks. Mohammed Ali Al- Garadi, Mohammad Rashid Hussain, HenryFriday Nweke,Ihsanali,Ghulammujtaba1,HarunachiroMa,Hasanalikhattak,And abd ullahgani

[12] "Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP (2018)",Dr.Narsimha.G, Dr.JayadevGyani, P. Srinivas Rao ," International Journal of Applied Engineering Research ISSN 0973-4562, Number 6, Volume 13.

[13]. Automatic detection of illegitimate websites with mutual clustering. (2016) V. Rama Krishna,&K.KanakaDurgaInternational Journal of ElectricalandComputer Engineering, 6(3), 995-1001. doi:10.1151/ijece. v6i3.9878

[14] Tan Qiaoyu, Liu Ninghao, Hu Xia.," Deep Representation Learning for Social Network Analysis" Frontiers in Big Data Vol.2 ,2019 ,.frontiersin.org/article/10.3389/fdata.2019.00002, ISSN=2624-909X .

[15 "Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial,"]M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3039-3071, Fourthquarter 2019, doi: 10.1109/COMST.2019.2926625. [16]KH Teoh et al 2021 Face Recognition and Identification using Deep Learning Approach, Journalof Physics: Conference Series.

[17] "Machine Learning Paradigms for Speech Recognition: An Overview," L. Deng and X. Li,in IEEE Transactions on Audio, Speech, and Language Processing, vol. 21, no. 5, pp. 1060-1089, May 2013, doi: 10.1109/TASL.2013.2244083.

[18] Fotiadis, Machine learning applications in cancer prognosis and prediction,Computational and Structural BiotechnologyKonstantina Kourou, Themis P. Exarchos, Konstantinos P. Exarchos, Michalis V. Karamouzis, Dimitrios I. Journal, Volume 13,2015,Pages 8-17,ISSN 20010370,https://doi.org/10.1016/j.csbj.2014.11.005.