International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET2293158

Fake Accounts and Clone Profiles Identification on Social Media Using Machine Learning Algorithms

Ajith M*[1], M. Nirmala*

*[1]MC Student, Department of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India

*[2]Department of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Article Info
Volume 9, Issue 3

Page Number : 551-560

Publication Issue :
May-June-2022

Article History
Accepted : 12 June 2022
Published: 30 June 2022

ABSTRACT

Fake and Clone profiles are creating dangerous security problems to social network users. Cloning of user profiles is one serious threat, where already existing user's details are stolen to create duplicate profiles and then it is misused for damaging the identity of original profile owner. They can even launch threats like phishing, stalking, spamming etc. Fake profile is the creation of profile in the name of a person or a company which does not really exist in social media, to carry out malicious activities. In this paper, a detection method has been proposed which can detect Fake and Clone profiles in Twitter. Fake profiles are detected based on number of abuse reports, number of comments per day and number of rejected friend requests, a person who are using fake account. For Profile Cloning detection two Machine Learning algorithms are used. One using Random forest Classification algorithm for classifying the data and Support Vector Machine algorithm. This project has worked with other ML algorithms, those training and testing results are included in this paper.

Keywords — Machine Learning, Fake and Clone Profiles, Twitter, Social Media, Classification Algorithms.

I. INTRODUCTION

Social networking sites have commonly used the channel of communication between people. Users of social networking sites can share their information and daily activities which attract a number of people towards these sites. One of the most widely used social networking sites is 'Twitter'. Online social media allow the users to add friends and share various kind of information such as personal, social, political, business etc. Moreover, they can also share photos, videos, travels and another day to day affairs. However, some people don't use these sites with good intent. Therefore they create fake accounts on social networking sites. Fake accounts do not have any real identity.

On the other hand some privacy issues related to information leakage, identity based frauds, discloser of private and sensitive information invites malicious attacks. Using these information reputation slanders, personalized spamming, and phishing kinds of attacks are deployed.

II. LITERATURE SURVEY

Fake profile Identification using Natural Language Processing [1], also known as, NLP and Machine Learning approach was introduced to evaluate the problems involving social networking like privacy, online bullying, misuse, and trolling and many others.

Adikari [2] and Dutta (2014) [2] describe identification of fake profiles in LinkedIn. The paper shows that fake profiles can be detected with 84% accuracy and 2.44% false negative, using limited profile data as input.

Stringhini [3] et al. (2010) describe methods for spam detection in Facebook and Twitter. The authors created 900 honeypot profiles in social networks, and performed continuous collection of incoming messages and friend requests for 12 months. User data of those who performed these requests were collected and analyzed, after which about 16000 spam accounts were detected. Authors further investigated the application of machine learning for further detection of spamming profiles.

Detection of Fake Profiles in Social Media by [4] Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and Jari Veijalainen, was introduced to aware identity is an object attached to a human being, separate from him or her.

Malicious users' circle detection in social network based on spatiotemporal co-occurrence," [5] was described to a typical scenario for using false identities is using social media platforms to impersonate someone or create a fake identity to establish trust with the target, which is then exploited: for gathering further information for a spear phishing attack, mounting a spear phishing attack, or for directly interacting to get the information of interest.

Stein T, Chen E, Mangla K [6] described different privacy settings to secure user's personal information in network.

Because of the openness of Facebook, users are likely disclosing many personal details about themselves and their friends as presented by [7]

Malicious and Spam Posts in Online Social Networks, Stein Maclean, J. Melton, J. Melton, A. R. Simon, and M. Chisholm, Data Mining : Concepts and Techniques. 1999, [8] was introduced a number of fake account detection approaches rely on the analysis of individual social network profiles, with the aim of identifying the characteristics or a combination thereof that help in distinguishing the legitimate and the fake accounts.

S. Kiruthiga, [9] evaluated study trending memes that attract attention and designed a ML system to recognize campaigns. With hashtags a millions of posts were used to prove accurate recognition is possible up to 95%.

An attempt has been made in this work[10] to use a hybrid model based on machine learning and skin detection algorithms to detect the existence of fake accounts. The experimentation process clearly brought out the strength of the proposed scheme in terms of detecting fake accounts with high accuracy labels from the testing dataset are eliminated and are left for determination by the educated classifier

III. RESEARCH METHODOLOGY

The various methods adopted during the research process have been portrayed. This is a Descriptive Research problem where the study of Fake Profile details from twitter social media is explored. It performs the classification of profile as fake or original based upon various parameters by applying various methodologies with respect to Machine Learning.

3.1 Overview of proposed system

In the proposed system we used to detect fake Twitter profiles. Here fake profiles are detected based on rules that effectively distinguish fake profiles from genuine ones. Some of the rules that are used to detect fake profiles are - usually fake profiles do not have profile name or image. They do not include any description about the account. They usually make large number of tweets or sometimes the profiles would not have made any tweets etc. A detection method has been proposed which can detect Fake and Clone profiles in Twitter. Fake profiles are detected based on number of abuse reports, number of comments per day and number of rejected friend requests, a person who are using fake account.

The proposed system contains 9 features described in Table 3.1 which is numerical data type and the category feature is the target variable which identifies the profile as fake or not fake is a categorical variable The system architecture diagram depicts the working model of the system is given in Figure 3.1.

Table 3.1 : Profile Features and Descriptions

Feature	Data type	Description
User ID	Numerical	Id od user
Number of Abuse Report	Numerical	Number of abuse report in social media
Number of rejected friend requests	Numerical	Number of rejected friend requests in social media
Number of friend requests that are not accepted	Numerical	Number of friend requests that are not accepted in social media
Number of friends	Numerical	Number of friends in social media
Number of followers	Numerical	Number of followers in social media
Number of likes to Unknown account	Numerical	Number of likes to Unknown account in social media
Number of comments per day	Numerical	Number of comments per day in social media
Category	Categorical	Based on above reports, classified account as genuine category or not.

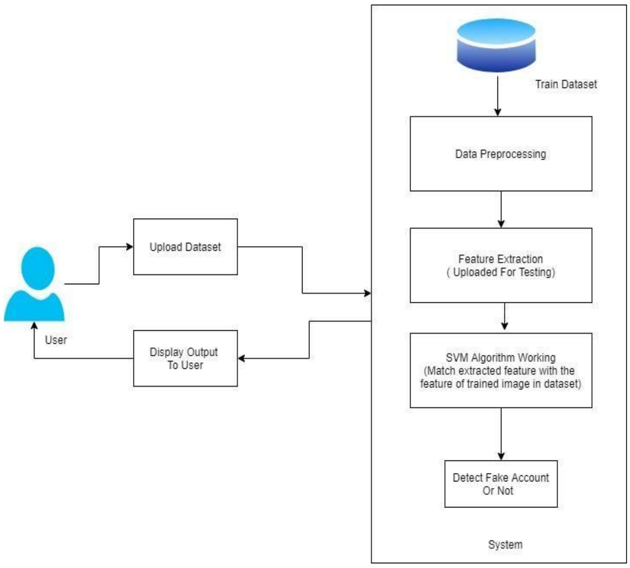


Figure 3.1 : System Architecture

3.2 Machine Learning Process

- Object has features and the collective features are named under the term Label. The features + label are called as Training Data.
- The model is trained by the above given Training Data
- Once the model has become well trained, it should be evaluated by Test Data. The test data are just the Features (given as Input) and not the labels.
- Based on the Training received from the Training data, the train model will be evaluated by the Test data.
- If the trained model has evaluated the data correctly then it is ready for prediction. The flow diagram of machine learning pipeline is depicted in Figure 3.2

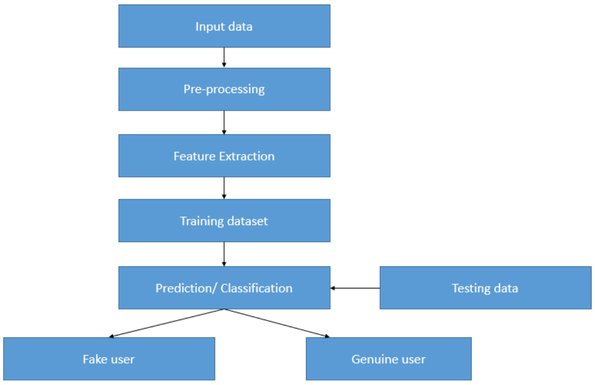


Figure 3.2 Machine Learning Flow Diagram

3.3 DATA PRE-PROCESSING

This is the first real step towards the real development of a machine learning model, collecting data. This is a critical step that will cascade in how good the model will be, the more and better data that we get, the better our model will perform. There are several techniques to collect the data, like web scraping, manual interventions and etc. The dataset contains 10 columns and 692 rows.

This module will transform the data. By getting rid of missing data and removing some columns. First we will create a list of column names that we want to keep or retain. Next we drop or remove all columns except for the columns that we want to retain. Finally we drop or remove the rows that have missing values from the data set. In the used dataset missing values are absent and so that data has be directly applied for model building.

3.4 UNIVARIATE ANALYSIS

Individual Features / Variables

The Univariate Analysis Data Visualization consists of single variable and it is a descriptive type of analysis and not infer its relationship with any other variables. In general count plot could be used for this analysis. It helps to portray the data and its respective patterns for the user to get a better insight about the single variable and the graphical representation helps us to view maximum, minimum, mean values etc.

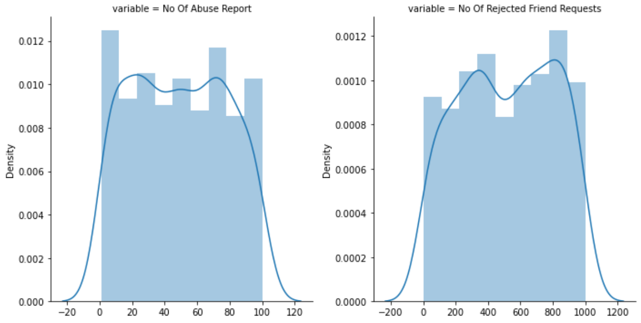


Figure 3.3 Analyzing number of abuse reports and rejected friend requests.

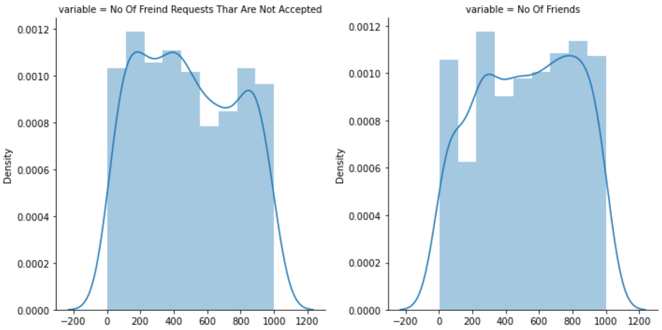


Figure 3.4 Analyzing number of friends and friend requests that are not accepted.

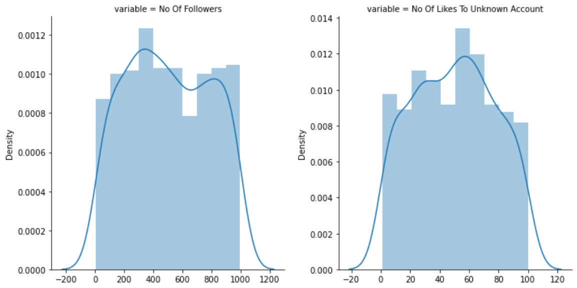


Figure 3.5 Analyzing number of followers and number of likes to unknown account.

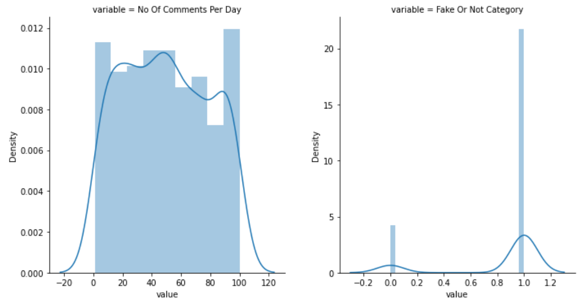
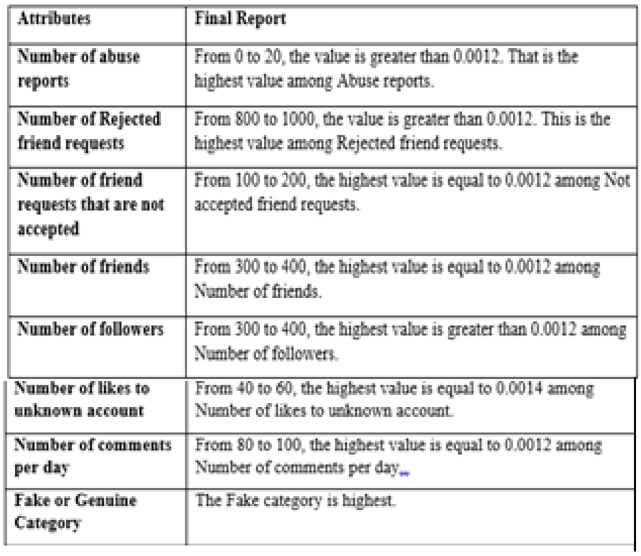


Figure 3.6 Analyzing number of comments per day and fake or not category.

3.5 UNIVARIATE ANALYSIS REPORT

Table 3.2 : Univariate Analysis Report



Attributes	Final Report
Number of abuse reports	From 0 to 20, the value is greater than 0.0012. That is the highest value among Abuse reports.
Number of Rejected friend requests	From 800 to 1000, the value is greater than 0.0012. This is the highest value among Rejected friend requests.
Number of friend requests that are not accepted	From 100 to 200, the highest value is equal to 0.0012 among Not accepted friend requests.
Number of friends	From 300 to 400, the highest value is equal to 0.0012 among Number of friends.
Number of followers	From 300 to 400, the highest value is greater than 0.0012 among Number of followers.
Number of likes to unknown account	From 40 to 60, the highest value is equal to 0.0014 among Number of likes to unknown account.
Number of comments per day	From 80 to 100, the highest value is equal to 0.0012 among Number of comments per day.
Fake or Genuine Category	The Fake category is highest.

HISTOGRAM REPRESENTATION OF FEATURES ACCORDING TO UNIVARIATE ANALYSIS REPORT

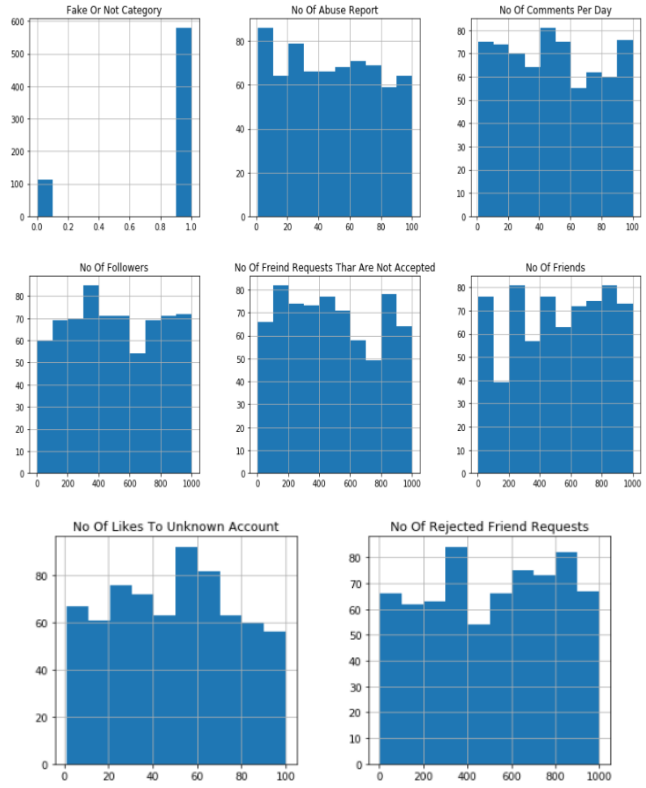


Figure 3.7 Histogram Representation.

BIVARIATE ANALYSIS – RELATIONSHIP OF A FEATURE WITH TARGET VARIABLE

Bivariate Analysis is performed to find the associativity between every variable in the data set with the Target Variable (Fake Or Not Category in this system). It also checks for association and the strength of this association or whether there are differences between two variables and the significance of these differences.

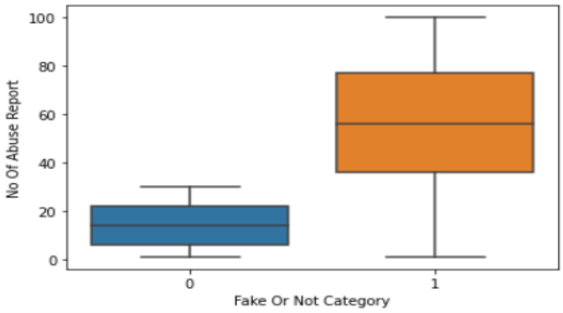


Figure 3.8 Bivariate Analysis – No of Abuse Report & Target Variable

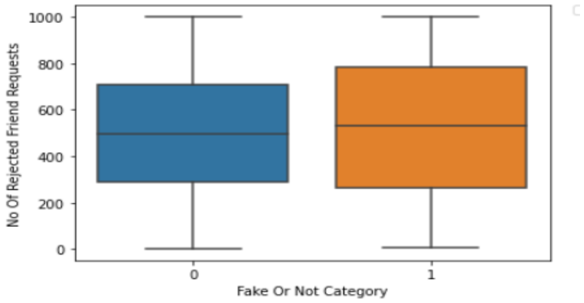


Figure 3.9 Bivariate Analysis – No of Rejected Friend requests & Target Variable

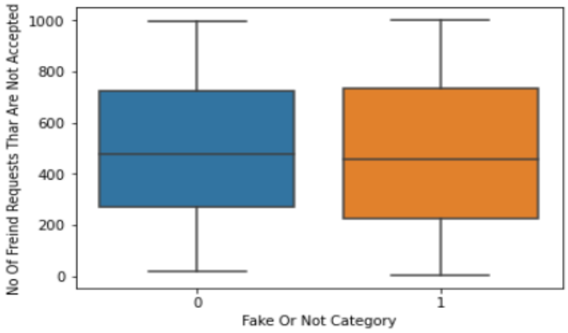


Figure 3.10 Bivariate Analysis – No of Friend request that are not accepted & Target Variable

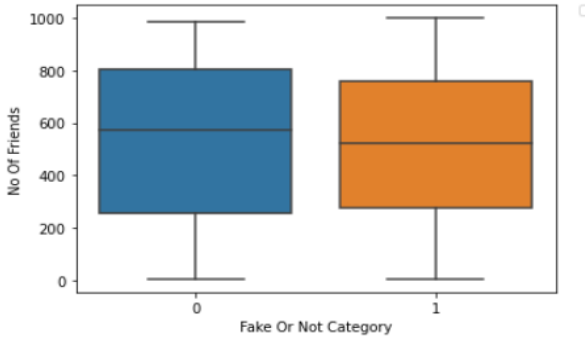


Figure 3.11 Bivariate Analysis – No of Friends & Target Variable

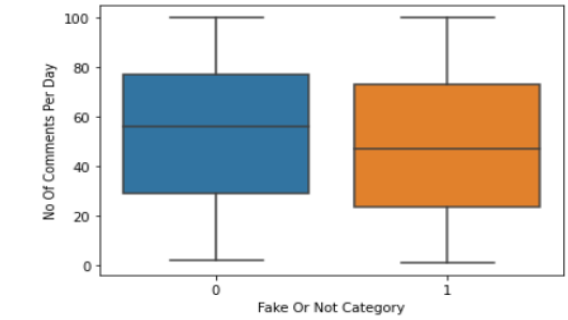


Figure 3.12 Bivariate Analysis – No of Comments per day & Target Variable

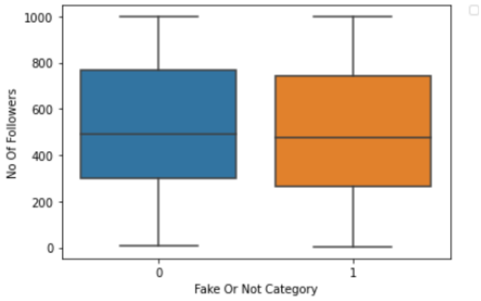


Figure 3.13 Bivariate Analysis – No of Followers & Target Variable

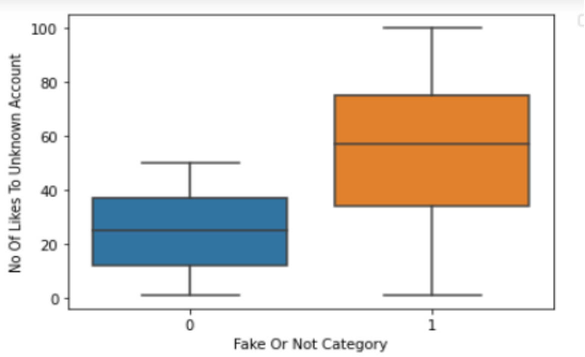


Figure 3.14 Bivariate Analysis – No of likes to unknown Account & Target Variable

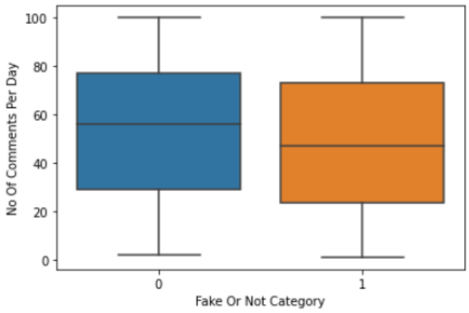


Figure 3.15 Bivariate Analysis – No of Comments per day & Target Variable

CORRELATION OF FEATURES

Correlation [11] is a bivariate analysis that measures the strength of association between 2 variables and the direction of the relationship. The correlation value will be between +1 and -1.

Types of Correlation are

Numeric Vs Numeric	Categorical (Binary Feature) Vs Numerical	Ordinal With Ordinal	Categorical vs categorical
Pearson	Pointbiserialr	Spearman Rho	Cross Tab

Numeric vs Numeric –Pearson Correlation

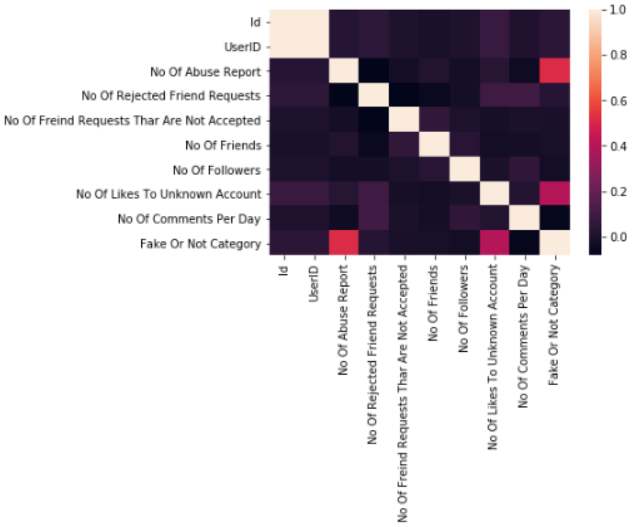


Figure 3.16 Pearson Correlation

High level of correlation between Number of abuse reports and Fake or not category (60%).
High level of correlation between Number of likes to unknown account and Fake or not category (40%).
Medium level correlation between Number of rejected friend requets and Fake or not category (20%).
Low level correlation between Number of comments per day and fake or not category (10%).

IV. PROPOSED ALGORITHMS

Various proposed Classification Algorithms [12] used in this paper are :

- Logistic Regression
- Decision Tree
- Random Forest

- XG Boost
- K Nearest Neighbors Algorithm
- Support Vector Machine

4.1 PERFORMANCE AND EVALUATION

In this section the results and findings of this work would be explained and evaluated.

4.2 MODEL SELECTION

While creating a machine learning model, we need two dataset, one for training and other for testing. But now we have only one. So splitting this in two with a ratio of 80:20. We will also divide the data frame into feature column and label column. Here we imported train_test_split function of sklearn. Then use it to split the dataset. Also, test_size = 0.2, it makes the split with 80% as train dataset and 20% as test dataset.
The random_state parameter seeds random number generator that helps to split the dataset. The function returns four datasets. Labelled them as train_x, train_y, test_x, test_y. If we see shape of this datasets we can see the split of dataset. We will use Random Forest Classifier, which fits multiple decision tree to the data. Finally I train the model by passing train_x, train_y to the fit method. Once the model is trained, we need to Test the model. For that we will pass test_x to the predict method.

Table 4.1 : Parameters For Model Fitting

Model Type	Parameters for Fitting the Model
Logistic Regression	solver='lbfgs',multi_class='auto', max_iter=2000
Random Forest	RandomForestClassifier(n_jobs=-1, random_state=123, criterion='gini', max_depth=3,)
KNN	KNeighborsClassifier(n_neighbors=7
SVM	svm.SVC(kernel='rbf',gamma='auto') # Linear Kernel
XGBOOST	xgb.XGBClassifier(max_depth=10, learning_rate=0.1, n_estimators=100, seed=10)
DECISION TREE – Gini	DecisionTreeClassifier(criterion = "gini", random_state = 100, max_depth=7, min_samples_leaf=5)
DECISION TREE - Entropy	DecisionTreeClassifier(criterion = "entropy", random_state = 100, max_depth=7, min_samples_leaf=5)

V. EXPERIMENTAL RESULTS

JupyterLab is the next-generation user interface for Project Jupyter offering all the familiar building blocks of the classic Jupyter Notebook (notebook, terminal, text editor, file browser, rich outputs, etc.) in a flexible and powerful user interface. JupyterLab will eventually replace the classic Jupyter Notebook. Installation. JupyterLab can be installed using condo or pip. In this system Anaconda3-2019.10-Windows-x86 64 has been installed with Jupyter Lab 1.1.4 which comes within it.

The following libraries are used for effective implementation.

Pandas is the most popular python library that is used for data analysis. It provides highly optimized performance with back-end source code is purely written in C or Python

SciPy is an Open Source Python-based library, which is used in mathematics, scientific computing, Engineering, and technical computing.

Seaborn is a Python data visualization library based on matplotlib. It provides a high-level interface for drawing attractive and informative statistical graphics.

Matplotlib is a Python 2D plotting library which produces publication quality figures in a variety of hardcopy formats and interactive environments across platforms. Matplotlib can be used in Python scripts, the Python and IPython shells, the Jupyter notebook, web application servers, and four graphical user interface toolkits.

NumPy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

Table 5.1 : Experimented Results

Name of the Algorithm	Training Score	Testing Score
Logistic Regression	96.69	94.23
Random forest	98.14	94.71
KNN	84.50	82.21
SVM	100	82.21
Xgboost	100	100
DECISIONTREE (gini)	100	100
DECISION TREE (ENTROPY)	100	100

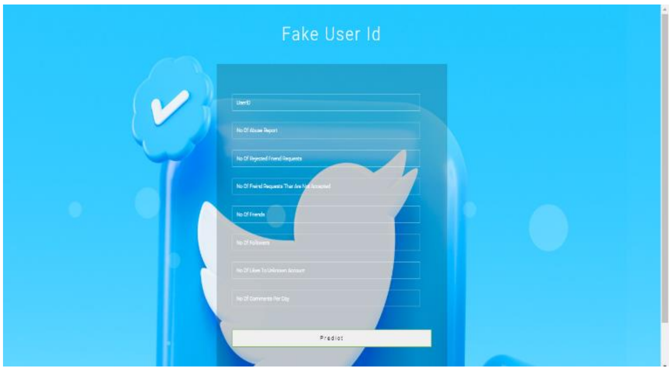

Fake User Id
UserID
No Of Abuse Report
No Of Rejected Friend Requests
No Of Friend Requests That Are Not Accepted
No Of Friends
No Of Followers
No Of Likes To Unknown Account
No Of Comments Per Day
Predict

Figure 5.1 Testing the model

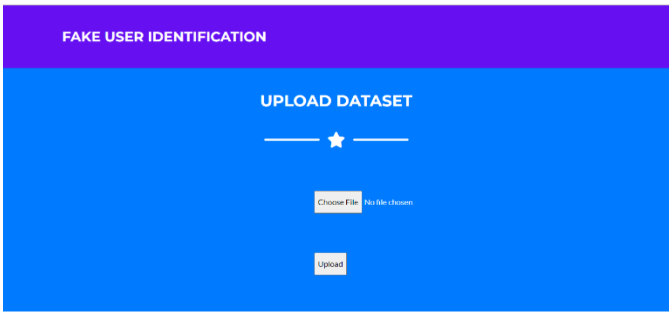
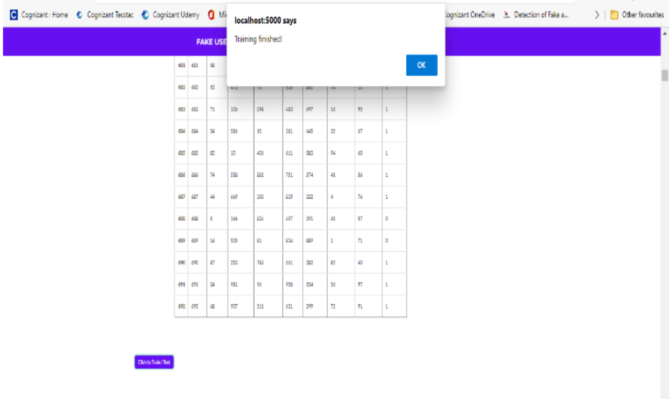


Figure 5.2 Upload dataset to train the model

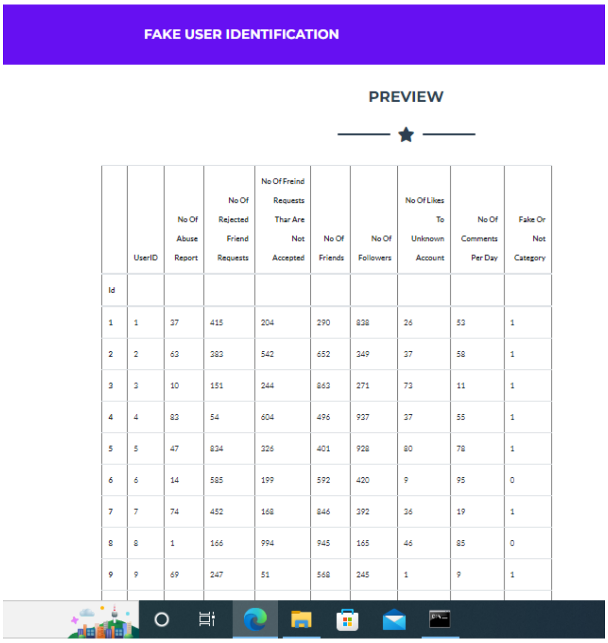


localhost:5000 says

Training finished!

681	681	56							
682	682	52							
683	683	71	106	398	483	697	16	95	1
684	684	54	586	10	381	645	35	67	1
685	685	82	10	406	611	583	94	60	1
686	686	74	558	681	751	574	41	56	1
687	687	44	669	150	839	322	4	76	1
688	688	5	166	624	497	391	41	57	0
689	689	14	535	61	634	889	1	71	0
690	690	87	253	783	661	282	85	40	1
691	691	24	981	96	958	504	56	97	1
692	692	68	937	511	631	299	72	91	1

Figure 5.3 Training finished by the model


FAKE USER IDENTIFICATION

PREVIEW

	UserID	No Of Abuse Report	No Of Rejected Friend Requests	No Of Freind Requests Thar Are Not Accepted	No Of Friends	No Of Followers	No Of Likes To Unknown Account	No Of Comments Per Day	Fake Or Not Category
Id									
1	1	37	415	204	290	838	26	53	1
2	2	63	383	542	652	349	37	58	1
3	3	10	151	244	863	271	73	11	1
4	4	83	54	604	496	937	37	55	1
5	5	47	834	326	401	928	80	78	1
6	6	14	585	199	592	420	9	95	0
7	7	74	452	168	846	392	36	19	1
8	8	1	166	994	945	165	46	85	0
9	9	69	247	51	568	245	1	9	1

Figure 5.4 After uploading, dataset view for training

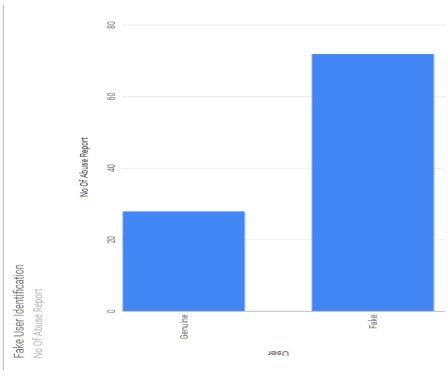


Figure 5.5 Analysis graph between fake and genuine cases - After prediction

VI. CONCLUSION AND FUTURE WORK

This project titled Fake Accounts and Clone Profiles Identification on Social Media Using Machine Learning Algorithms is mainly developed to create awareness of Fake Users between customers. In this project, administrator controlling the entire application, admin should train the model and make it ready to process. If model needs to get further trained, that process would be handled by admin. This software has been computed successfully.

Fake and clone profiles have become a very serious problem in online social networks. We hear some or the other threats caused by these profiles in everyday life. So a detection method has been proposed which can find both fake and clone Twitter profiles. The problem can be further extended to Natural Language Processing Techniques.

VII. REFERENCES

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

[2]. Adikari, S., Dutta, K., 2014. Identifying Fake Profiles in Linkedin, in: PACIS 2014 Proceedings. Presented at the Pacific Asia Conference on Information Systems.

[3]. Stringhini, G., Kruegel, C., Vigna, G., 2010. Detecting Spammers on Social Networks, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC '10. ACM, New York, NY, USA, pp. 1–9. doi:10.1145/1920261.1920263.

[4]. Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and Jari Veijalainen, Detection of Fake Profiles in Social Media Literature Review, University of Jyväskylä, Finland.

[5]. Michael Fire et al. (2012). "Strangers intrusion detection-detecting spammers and fake profiles

in social networks based on topology anomalies." Human Journal 1(1): 26-39.Günther, F. and S. Fritsch (2010).

[6]. Stein T, Chen E, Mangla K," Facebook immune system. In: Proceedings of the 4th workshop on social network systems", ACM 2011, pp.1-8.

[7]. Saeed Abu-Nimeh, T. M. Chen, and O. Alzubi, "Malicious and Spam Posts in Online Social Networks," Computer, vol.44, no.9, IEEE2011, pp.23–28.

[8]. Maclean, J. Melton, J. Melton, A. R. Simon, and M. Chisholm, Data Mining : Concepts and Techniques. 1999.

[9]. S. Kiruthiga, "Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques," IEEE, 2014.

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

[11]. https://www.statisticssolutions.com/correlation-pearson-kendall-spearman/

[12]. https://www.cs.princeton.edu/~schapire/talks/picasso-minicourse.pdf

Cite this article as :

Ajith M, M. Nirmala, "Fake Accounts and Clone Profiles Identification on Social Media Using Machine Learning Algorithms", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 3, pp. 551-560, May-June 2022. Available at doi : https://doi.org/10.32628/IJSRSET2293158
Journal URL : https://ijsrset.com/IJSRSET2293158