Social Media Fake Profile Detection

Tejaswini S Patil[1], Siddhali A More[2], Trupti V Todkar[3], Dr. Divya Chirayil[4]

[1,2,3]Department of Information Technology Engineering, Pillai HOC College of Engineering and Technology, Rasayani, Maharashtra, India
[4]Associate Professor,Department of Information Technology Engineering, Pillai HOC College of Engineering and Technology, Rasayani, Maharashtra, India

---***---

Abstract - *In the current generation, online social networking (OSNs) has become more popular, and social media is becoming more and more associated with these sites. They use OSN to communicate with others, share news, organize events, and run their own e-business. The strong growth of OSNs and the large number of personal information of its subscribers has led attackers, and hypocrites to steal their information, share false news, and spread malicious activities. Fake or man-made fake profiles designed to spread rumors, identity theft etc. So, in this project, we are trying to propose a discovery model, which distinguishes between fake profiles and real profiles on Twitter based on visual features such as fan counts, friends counts, status calculations and more using various machine learning methods.*

1. INTRODUCTION

Artificial intelligence can take many different meanings in different contexts, but a very brief description of Britannica, defines artificial intelligence as the 'computer power to perform tasks that are usually associated with humans'. In today's world, it seems that the A is everywhere, from the most obvious use of self-driving cars to the most obscure as the complimentary programs available on popular platforms like Netflix and Amazon. Machine learning is a subset of AI that contains any computer program that can predict without human intervention. They are able to correct themselves by responding to the data they have been exposed to, like a human child. The ML learning feature refers to the fact that these algorithms attempt to amplify their results, by minimizing error or increasing the probability of their prediction being true. The focus will be on this project the discovery of fake profiles and smart BOTS on social media like twitter. These days fake profile bots are used because they are automatic and can work without anyone. A lot of bots where they are made into tweets and sent to US elections and that can be dangerous because the spread of rumors and false ideas can affect the results by defaming the party in the election and even they can use it to spread publicity, propaganda, war, etc. we are advancing technologically, AI is taking the place of humans and now finding bots are much more sensitive than humans. We have therefore proposed a model that detects smart bots with a fake profile based on the limits of twitter data like followers,tweets, followers, etc. We use twitter data for our model as we can download real-time user twitter data via twitter API

2. BACKGROUND

Social media profiles and bots have been around since the advent of social media. There is often a negative impact on them, as many of them are designed to jeopardize democracy, cause panic attacks, disclose confidential information, affect the stock market, and wreak havoc on the world. However, bots can also be useful for useful purposes such as encouraging users to get shot in the flu, give earthquake warnings, health tips, share automatic drawings, etc. Identifying bad bots can help us understand their behavior and determine which emotional traits make them as prominent as bots. In addition, by easily identifying Twitter accounts as bots, the public can be taught not to be a victim of bot or malicious messages on Twitter. In addition, when bots are detected earlier, their tweets can be quickly protected from spreading on the platform.

Acquisition of Bot

Bot detection is the process of using various tools as well ways to identify bots in a collection. The complexity of this varies depending on the type of bot and the set of symbols it contains. The goal here is to reduce the number of false positives (bots are actually human) and misalignments (humans are actually bots).

Twitter

Twitter is a micro-blogging (condensed blogging) communication platform launched in 2006. Users communicate via tweets, limited to 280 characters in length, in order to convey their message effectively and efficiently. Communication can be in the form of tweeting (messaging), replying (replying to messages), and direct messaging (private chat). Users can access others by tagging them with their handle, the '@' symbol followed by the username of the target account. Users can also interact with others by using the hashtag '#' tag to discuss specific topics, and segment tweets to make it easier to search and retrieve. Additionally, users can select the content they want to see in their timeline by following specific accounts. With the growing popularity of Twitter over the years, companies, schools, celebrities, and politicians have a Twitter account. The platform also offers the opportunity to 'like' and 'rewrite' users 'tweets. Repeated tweets were added to the user's timeline, which is a collection of posts made or mentioned by the user. Account fans can see all the content in their timeline. Since Twitter became an effective tool to spread political messages in the presidential election, the number of active US accounts in the US has grown from 45 million during the 2012 US presidential election to 67 million during the 2016 US presidential election.

Fake Profile

A false profile is the representation of a person, organization or company that does not exist, on social media. These accounts often use names and identities that are not only real but also intended to gain greater access to specific individuals and audiences. These accounts are used to conceal the identity of the person while sending abusive or threatening messages, impersonating him or her in an attempt to damage his or her reputation or to cause distress or to deceive his or her friends and family by contacting the victim profile to trick them into engaging in malicious content.

Internet bots

An internet (bot) is any automated software program that can repeatedly perform 5 different tasks. The use of bots on the web is so common that they currently make up 40% of all online traffic. The most common tasks performed by these bots are business crawling, downloading, monitoring, and ticketing.

Twitter Bots

A Twitter bot is a bot that works on a Twitter platform from an account. Certain tasks can be performed automatically from the Twitter bot such as tweeting, rewriting and liking. There are no restrictions on creating a Twitter bot account as long as it does not violate their Terms of Service by tweeting default spam messages or misleading links. Twitter bots, like regular bots, do a variety of things enough to use different types of objectives ranging from basic functions like user tracking to more complex ones like conducting a conversation with other users Social bots are a type of bot that communicates with users, the purpose of which is to produce content that develops a particular idea. Approximately 9 to 15 percent of Twitter accounts for bots

Fake Profile Separation

For our purposes, false profile classification is a process of deleting a profile that is already positive, negative or neutral depending on various factors such as followers, following, likes, tweets and more. Here it is very important that we be able to distinguish the negative from the good and neutral tweets.

Machine learning

Machine reading is a method of automatic data analysis to build an analytical model. A branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Supervised learning

Supervised learning is a learning algorithm process from a training database to find map activity from input to output. These problems can be categorized and subdivided.

Unsupervised learning

Unregulated learning is an algorithm process for trying to model a structure or distribution of data to learn more about it. These problems are more complex than supervised learning and can be collected and collected and combined. Other popular examples are vector support machines, line layout and random forest.

Classification

Separation is a way of dividing data into different categories where we can assign a label to each class. Dividing data into two distinct categories is called binary categories (e.g. male and female). Dividing into more than two different categories is called different categories (e.g. plant species).

The Naive Bayes

Naive Bayes is an opportunity-divisive divider inspired by the Bayes theorem, in which it assumes that attributes are independent under certain conditions. One of its major benefits involves the need for only a small amount of training data to measure the required parameters. Moreover, it is much faster compared to more complex methods. However, the worst is the worst. Continuing the demolition of the stairs, the inexperienced bayes divider first calculates the opportunities before the category labels provided. It then finds opportunities for each attribute in each class, places these numbers in the Bayes formula and calculates the probability of the background. Ultimately it decides who has the highest chances, if you are given the input it belongs to the high probability category. The power of this type of differentiation lies in its ability to handle audio data. That is to say, prices are simply ignored and unimportant factors are evenly distributed so that they do not have a significant impact on the outcome of the phase.

Decision Tree Decisions

The decision tree is a flowchart-like tree structure where the internal node represents a feature (or attribute), the branch represents the rule of thumb, and the node of each leaf represents the result. The highest node in the decision tree is known as the root node. It learns to distinguish on the basis of the value of the attribute. It separates the tree in a repetitive manner and calls for repeated divisions. This structural flowchart helps you make decisions. Views similar to a flowchart diagram that easily mimics human-level thinking. That is why decision trees are easy to understand and interpret. The tree resolution is a kind of white box ML algorithm. Share an internal decision- making concept, not found in the black box type algorithms like Neural Network. Its training time is much faster compared to the neural network algorithm. The duration of the treatment decision is the function of the record number and the number of symptoms in the data provided. Decision medicine is a method of distribution or non-parameter, independent of possible distribution ideas. Decision trees can handle high-resolution data with good accuracy.

Direct Profile(Positive)

We identify a positive profile such as a man-made one or a bot designed for good purpose such as earthquake warnings, health tips, etc and avoid using bad or inappropriate language.

Invalid Profile(Negative)

Identifies a profile with a false or man-made account or bots such as those designed to spread negative, misleading or false information (eg Russian bots tweeting about US elections), impersonating others, or posting spam content

NLTK

NLTK is the leading platform for building Python programs is used in human language data to apply for mathematical language analysis (NLP) analysis. Contains libraries for token processing, classification, classification, marking, marking and semantic consultation. Includes graphical representations and sample data samples, which also explain the basic principles of language processing activities supported by the NLTK.

SCIKITLEARN

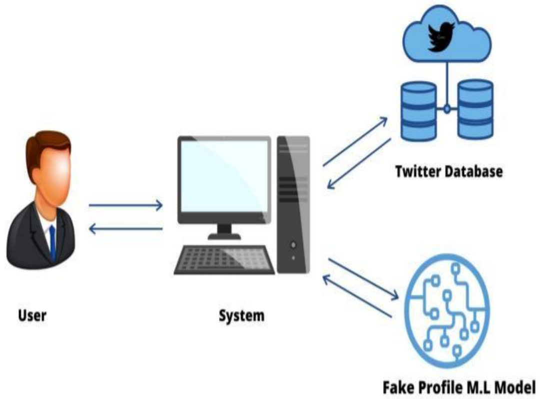
Scikit-learn (Sklearn) is a very useful and robust library of machine learning in Python. Provides a selection of effective machine learning and modeling tools including division, deceleration, merging and reduction of size using the Compatible interface in Python. This library, mostly written in Python, is built on NumPy, SciPy and Matplotlib.

3. System

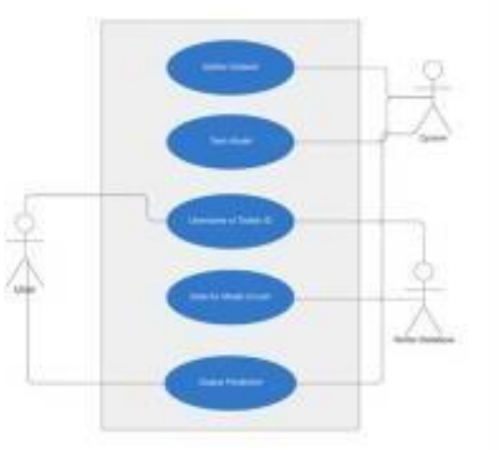
In the current system, the targeted algorithm for learning the targeted reading machine is Random Forest, Decision Tree, and Naïve Bayes. The algorithms used have good accuracy but the model is not compatible to get a fake profile in real time. Allows the user to test only on selected databases. Used Twitter Database. Also, it only gets a fake profile but there are even non-BOT or BOT accounts on various social media platforms that can be used to disrupt and spam like many BOT social / bad BOTs trying to spread false information to the public like the US election 2015. There is even a good BOT made with good intentions such as posting health tips, news alerts, matching points, etc.

Random forest planning

Random Forest is a supervised learning algorithm used for both split and reverse. However, it is also used mainly for planning problems. As we know the forest is made up of trees and many trees mean a strong forest. Similarly, an algorithm in a random forestprodure multiple decision trees in data and receives predictions from each of them and ultimately the result is the result of a collection of all decision trees. It is a better combination than a single decision tree because it reduces over-equilibrium by obtaining a measure. We used the random forest route to find the profile. Details are entered into the model and corresponding results are available. Fig: First Random Editor.



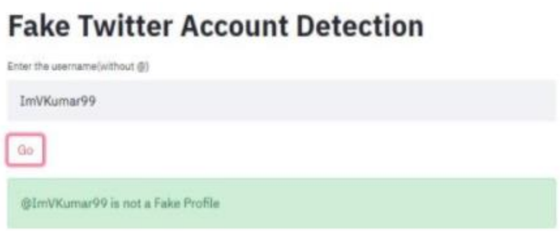
Workflow Diagram



UseCaseDiagram

4. RESULT

Entered Account ID is not fake



Fake Twitter Account Detection

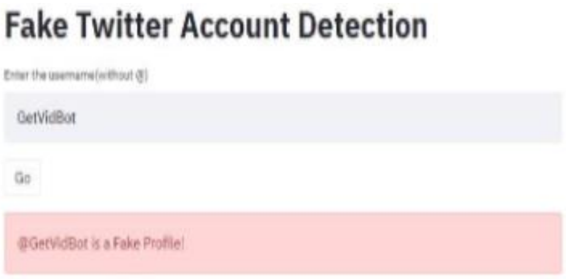
Enter the username(without @)

ImVKumar99

Go

@ImVKumar99 is not a Fake Profile

Entered Account ID is Fake



Fake Twitter Account Detection

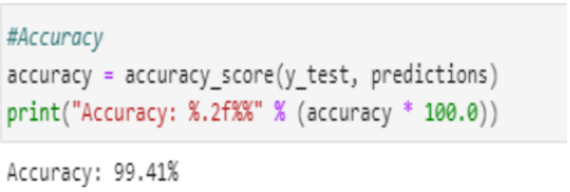
Enter the username(without @)

GetVidBot

Go

@GetVidBot is a Fake Profile!

Accuracy



```
#Accuracy
accuracy = accuracy_score(y_test, predictions)
print("Accuracy: %.2f%%" % (accuracy * 100.0))
```

```
Accuracy: 99.41%
```

5. CONCLUSIONS

The model presented in this project demonstrates that the Division of Decision split is a good and powerful way of binary planning on a large database. Despite the inconsistency of the decision boundary, the Decision Tree Verification is able to distinguish between false and real profiles with the correct truth (> 97%). This method can be extended to any platform that requires binary separation to be included in public profiles for various purposes. This project uses only publicly available information that makes it easier for organizations that want to avoid any breach of privacy, but organizations can also use the personal information available to them to maximize the potential of the proposed model.

ACKNOWLEDGMENT

We remain very committed to Dr. DIVYA CHIRAYIL for providing us technical support and guidance. We would also like to thank our guide for providing us with his professional opinion and good suggestions for all stages of the project. We would like to take this opportunity to thank Professor Dr.J.E.NALAWADE Head of Information Technology for his motivation and invaluable support. This acknowledgment is incomplete without thanking academic and non-academic staff for their department for their kind support. We would also like to thank Dr.J.MATHEW Principal of Pillai HOC College of Engineering and Technology, Rasayani for providing the necessary infrastructure and resources for the project.

REFERENCES

I. References

1. (2018) How concerned are you that there are fake accounts and bots on social media platforms that are used to try to sell you things or influence you? Internet draft.[Online]. Available: https://www.statista.com/statistics/881017/fake-social-media-accounts-bots-influencing-selling-purchases-usa
2. (2012) Buying their way to twitter fame. Internet draft.[Online].Available: https://investor.fb.com/home/default.aspx https://www.nytimes.com/2012/08/23/fashion/twitter-followers-fo r-sale.html?smid=pl-share

II. References

1. Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: The socialbot network: when bots socialize for fame and money. In: Proceedings of the 27th Annual Computer Security Applications Conference, pp. 93–102. ACM (2011)
2. Adikari, S., Dutta, K.: Identifying fake profiles in Linkedin. Presented at the Pacific Asia Conference on Information Systems PACIS 2014 Proceedings (2014).
3. Elyusufi, Y., Seghiouer, H., Alimam, M.A.: Building profiles based on ontology for recommendation custom interfaces. In: International Conference on Multimedia Computing and Systems (ICMCS) Anonymous IEEE, pp. 558–562(2014).