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/IJSRSET2310292

Fake Profile Identification in Online Social Networks Using Machine Learning

Dr. P. Shanthakumar[1], S. Jeyasri Pooja[2], R.Jenifer[2]

[1]Professor, Department of Information Technology Kings Engineering College, Chennai-Banglore Highway, Irungattukottai, Sriperumbudur, Chenna, Tamil Nadu, India

[2]B Tech IT, Department of Information Technology Kings Engineering College, Chennai-Banglore Highway, Irungattukottai, Sriperumbudur, Chenna, Tamil Nadu, India

ARTICLEINFO

Article History:

Accepted: 05 April 2023
Published: 27 April 2023

Publication Issue

Volume 10, Issue 2
March-April-2023

Page Number

679-684

ABSTRACT

Social networking platforms are now a common aspect of daily life for most people. Every day, a large number of people create profiles on social networking sites and interact with others, regardless of their location or time of day. Social networking platforms not only benefit users, but also put their security and personal information at danger. To find out who is spreading hazards on social media, we must classify user profiles. The classification allows us to distinguish between legitimate profiles on social networks and fake profiles. We generally employ a range of methods for categorising fraudulent profiles on social networks. As a result, we must improve the social network phoney profile identification system's accuracy rate. In this research, we propose machine learning and natural language processing (NLP) approaches for fraudulent profile detection. Both the Nave Bayes algorithm and the Support Vector Machine (SVM) can be employed.

Keywords: Machine Learning, Natural Learning Processing, Classification, Naïve Bayes Algorithm, Support Vector Machine.

I. INTRODUCTION

Currently, social networking on the internet attracts hundreds of thousands of users and generates billions of minutes of usage per year. Online social network (OSN) services include everything from platforms that focus on social interaction, like Facebook or Myspace, to those that focus on information sharing, like Twitter or Google Buzz, to those that have social interaction aspects built right into them, like Flicker. The protection of OSN privacy and rising security concerns, on the other hand, continue to be a significant challenge.

One-of-a-kind people share one-of-a-kind amounts of their private information when using social networks (SNs). We may have all or some of our personal information made public, making us a potential target for many types of attacks, the worst of which may be identity theft. Identity theft happens when someone assumes another person's identity in order to further their own interests or goals. Online identity theft used to be a significant problem because it affected millions

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

of individuals worldwide. Even if such bills were fraudulent, basic online consumer monitoring would cause enormous losses.

Internet networks will also have profile data, either static or dynamic. Dynamic knowledge is information that is communicated by a system inside a network, whereas static knowledge is information that can be contributed by a person at the time of profile creation. Static information just provides a person's demographic details and areas of interest, but dynamic knowledge also includes a person's runtime behaviours and location within the network.

Social networking problems, including trolling, abuse, cyberbullying, and many others. In social networking platforms, fraudulent profiles are frequently used. False profiles are those that lack specificity, i.e., they are those of men and women with phoney credentials. People frequently use the internet as a means of earning money, but it's also usual for it to be utilised as a means of earning money. Fake profiles are created by individuals for marketing, campaigning, online impersonation to disparage an individual or group of individuals, social engineering, and other purposes. In order to secure user credentials against spamming, phishing, and other types of fraud, Facebook has its own security mechanism in place. The Facebook Immune is another name for the comparable.

II. LITERATURE SURVEY

Prominent websites on the Internet are constantly under attack from spammers, scammers, and phishers. They intend to expose people to unwanted spam while stealing their personal information. The attackers have access to a tremendous amount of resources. They have access to the world's botnets, are well-funded, have full-time dedicated labour, and control over compromised and infected accounts. A difficult adversarial learning challenge with high scale and load requirements is protecting our users. To safeguard our users and the social network, we have developed and implemented a real-time system that is coherent, scalable, and extendable over the past few years. Every read and write operation is subject to real-time classifications and inspections by this immune system .[1]

Online impersonation and false identities are rife on the social network, a vital component of our daily lives. Over 583 million false accounts were removed in just the first quarter of 2018, according to Facebook's "Community Standards Enforcement Report," and as many as 3-4% of its active accounts at the time were still fake. In this project, we offer a methodology that might be applied to determine whether an account is real or false. [2] This model uses Support Vector Machine as a classification technique and can process a big dataset of accounts at one, removing the need to evaluate each account individually .[3]

In today's world, Online Social Media is king in a number of forms the number of individuals who use the service is expanding every day. Social media usage is rapidly increasing. The main advantage is that via social media websites, we may easily and more effectively communicate with people .[4] This opened up a fresh line of attack potential, such as a fake identity or fraudulent information. A recent study found that the number of accounts on social media is significantly larger than the total number of users .[5]

We can use machine learning algorithms to identify such fraudulent and real accounts. Using the various models that are created, machine learning algorithms are used to forecast and categorise datasets .[6] It can be challenging to distinguish between the outcomes of many models at times, therefore we can simplify this work by using a hybrid approach to a machine learning method.[7]

III. PROPOSED SYSTEM

In this study, we demonstrated a system for detecting bogus users in online social networks using machine learning and natural language processing.Also, we are including the Random Forest Classifier, Gradient Boost

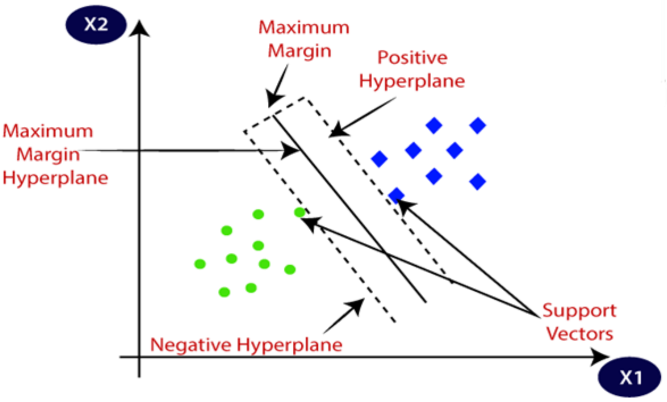
Classifier, Naive Bayes, and Logistic Regression Algorithm in addition to the Five Algorithms to assess the most effective model for improving the fake profile detection efficiency. We acquire the values of accuracy, classification report, and confusion matrix in the final forecast.High accuracy is acquired and time consumption for detecting the Fake profiles. More datasets are included. We may find all different kinds of profiles on various social media platforms as well.

1. Collect the data
2. Pre-process the collected data
3. Reduction of the feature
4. Training the data
5. Apply the machine learning algorithm
6. Evaluate the classification result into fake and real

IV. LEARNING ALGORITHM:

(i) Support Vector Machine (SVM):

An SVM categorises data by locating the exceptional hyperplane that separates all information components of one kind from those of the other type. The ideal hyperplane for an SVM approach is the one with the longest line connecting the two classes. An SVM classifies data by locating the exceptional hyperplane that separates all knowledge facets of one category from those of the other. The assist vectors are the informational components that are closest to the separating hyperplane.



1. NLP Pre-Processing

Each NLP technique must include text pre-processing, and its importance lies in:

1. Reducing the size of the text content records' indexing (or knowledge) records.

i. In a special text content record, stop words account for 20–30% of the total phrase counts.

ii. Stemming may only reduce indexing size by up to 40%–50%.

2. To increase the IR method's effectiveness and efficiency

i. Stop words aren't useful for searching or mining textual content, therefore they could merely confuse the retrieval system ii. Stemming is a technique used to match similar words in a text record.

The objective of NLP is to enable computers to interpret texts and languages in a manner similar to that of humans.

After achieving this, computers will be able to understand, infer, summarise, interpret, and produce precise, human-like text and language.

Real-world data is unorganised and frequently produced, processed, and saved by a range of people, business operations, and software programmes. Because of this, a data set can be incomplete, have manual input errors, have duplicate data, or use several names to refer to the same object. In the data that they use for their line of work, humans can frequently spot and fix these issues, but data used to train machine learning or deep learning algorithms needs to be automatically preprocessed.

Information Retrieval
Doc A
Doc 1
Doc 2
Doc 3
Sentiment Analysis
Information Extraction
Machine Translation
文
A
Natural Language Processing
QuestionAnswering
?
Human: When was Apollo sent to space?
Machine: First flight - AS-201, February 26, 1966

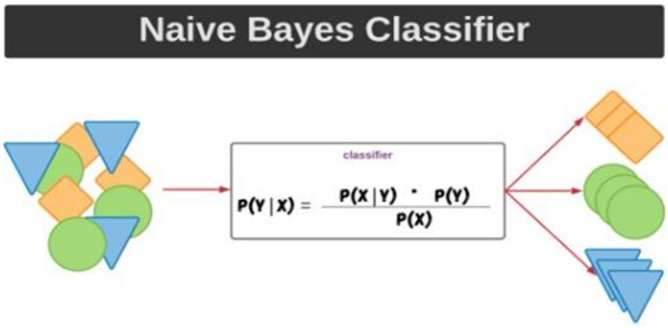
(ii) NAVIS BAYES:

The Naive Bayes algorithm calculates the probability that an object with precise characteristics belongs to a given group or category. To put it plainly, it's a probabilistic classifier. Because it is assumed that the prevalence of one feature stands apart from the prevalence of other features, the Naive Bayes approach is so named. Using language, location, and the time, date, or publication of the postings as an example, let's say we wish to spot bogus profiles. Even if they are all dependent on one another or the existence of other variables, all of these traits, in my opinion, increase the possibility that the false profile will exist.

It is mostly employed in text categorization with a large training set.

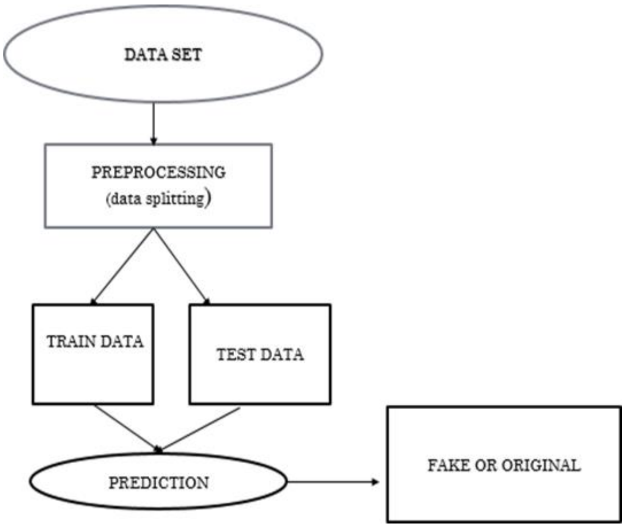
The Naive Bayes Classifier is one of the most straightforward and efficient classification algorithms available today. It aids in the development of quick machine learning models capable of making accurate predictions.

Being a probabilistic classifier, it makes predictions based on the likelihood that an object will occur.



it's ideal for scenarios where you have very little data but still want to classify your new data into several discrete categories. It will even work with very small datasets of only 10 or 20 items

V. ARCHITECTURE:



Data collection:

Making a decision about what information to gather is one of the most crucial steps in the data collection process and ought to come first. We must decide which topics the data will cover, which sources we will use to collect it from, and how much data we need. Depending on our objectives—or what we want to accomplish using your data—our answers to these questions will vary. For instance, we could decide to find out which article categories website users between the ages of 20 and 50 most regularly access.

Data pre-processing:

Data pre-processing is the process of turning unstructured data into sets that can be read, analysed, and processed for use in business operations. Businesses must correctly pre-process their data since the variety of inputs they utilise to gather raw data might have an impact on the data's quality. Pre-processing data is crucial since raw data may be formatted inconsistently or incompletely. Pre-processing raw data effectively can increase its accuracy, which can raise project quality and reliability.

In this we have two types of analysis

- Train data
- Test data

Train data

The training dataset, which is used to train or fit the machine learning model, is the largest (in terms of size) subset of the original dataset. In order for the ML algorithms to learn how to make predictions for the given task, training data is first supplied into them.

Test data

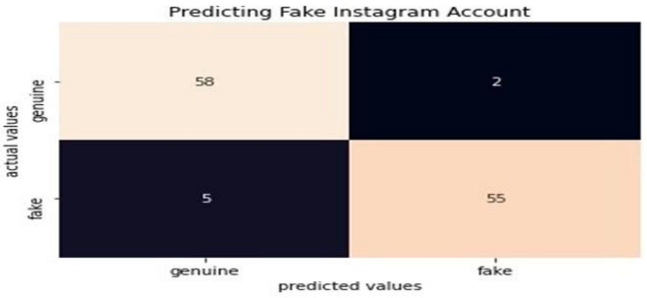
Once the model has been trained using the training dataset, it is time to test it using the test dataset. This dataset assesses the model's performance and guarantees that it can generalise well to new or unexplored datasets. The test dataset is a different subset of the original data from the training dataset.

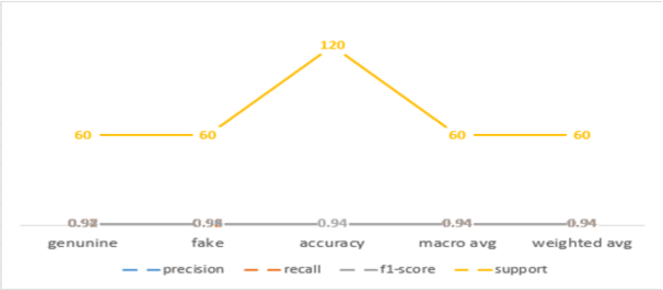
Prediction:

When predicting the likelihood of a specific result, such as whether or not a customer would churn in 30 days, the term "prediction" refers to the output of an algorithm after it has been trained on historical data and applied to new data. For every record in the new data, the algorithm will produce probable values for an unknown variable, enabling the model builder to determine what that value will most likely be.The term "prediction" itself might be deceptive. When you use machine learning to choose the next best step in a marketing campaign, for example, you are effectively anticipating a future outcome.

Yet, sometimes the "prediction" is about something that has already happened, like whether a transaction was fraudulent or not. In such situation, the transaction is already complete, but you're attempting to determine whether or not it was valid so that you may decide what course of action to follow. Based on historical data, machine learning model predictions enable businesses to make extremely precise assumptions about the most likely outcomes of a question. These assumptions can be made about a variety of topics, including the likelihood of customer churn, potential fraudulent activity, and more. They give the company knowledge that has a real economic impact. For instance, if a model indicates a customer is going to leave, the company can reach out to them with targeted messaging to stop the loss of that customer.

VI. RESULTS





VII. CONCLUSION

In this paper, we propose techniques to natural language processing and machine learning algorithms. It is straightforward to spot fake social networking site profiles using these techniques. In this study, we used the dataset from Facebook to identify the fake profiles.. When predicting the likelihood of a specific result, such as whether or not a customer would churn in 30 days, the term "prediction" refers to the output of an algorithm after it has been trained on historical data and applied to new data. For every record in the new data, the algorithm will produce probable values for an unknown variable, enabling the model builder to determine what that value will most likely be.The dataset is analysed using NLP pre-processing methods, and the profiles are then categorised using machine learning algorithms like SVM and Nave Bayes. The detection accuracy rate of the paper was improved by these learning strategies.

VIII. REFERENCES

[1]. Romanov, Aleksei, Alexander Semenov, Oleksiy Mazhelis, and Jari Veijalainen. "Detection of fake profiles in social media-Literature review." In International Conference on Web

Information Systems and Technologies, vol. 2, pp. 363-369. SCITEPRESS, 2018.

[2]. Adikari, Shalinda, and Kaushik Dutta. "Identifying fake profilesin linkedin." arXiv preprint arXiv:2006.01381 (2020).

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

[4]. Elovici, Yuval, F. I. R. E. Michael, and Gilad Katz. "Method for detecting spammers and fake profiles in social networks." U.S. Patent 9,659,185, issued May 23, 2019

[5]. Elyusufi, Y. and Elyusufi, Z., 2019, October. Social networks fake profiles detection using machine learning algorithms. In The Proceedings of the Third International Conference on Smart City Applications (pp. 30-40). Springer, Cham.

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

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

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

[9]. Ojo, Adebola K. "Improved model for detecting fake profiles in online social network: A case study of twitter." Journal of Advances in Mathematics and Computer Science (2019): 1-17.

Cite this article as :

Dr. P. Shanthakumar, S. Jeyasri Pooja, R.Jenifer, "Fake Profile Identification in Online Social Networks Using Machine Learning", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 2, pp. 679-684, March-April 2023. Available at doi : https://doi.org/10.32628/IJSRSET2310292

Journal URL : https://ijsrset.com/IJSRSET2310292