Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 2

Fake Accounts Detection in Social Media Using Machine Learning Techniques

Anwesa Acharya
Department of Computur science Engineering.
CMR Univercity,Bangalore,
Karnataka, India
anwesaacharya03@gmail.com

Madhav Kumar
Department of Electrical Engineering
National Institute of Technology
Meghalaya, India
Madhavkumar523@gmail.com

S Saravana Kumar
Department of Computur science Engineering
CMR Univercity,Bangalore,
Karnataka, India
saravankumarmithun@gmail.com

***Abstract*—: Social networking sites like Facebook, Instagram, and Twitter are now incredibly popular. Online social networks have transformed the way people communicate with their friends and family. Using these platforms, they reveal personal details and social connections. Because of how appealing they are, millions of people worldwide regularly log into social networking sites. Because of their popularity, scammers can sign up for accounts on popular websites. Attackers and imposters are drawn to social networking sites due to the rapid growth of these platforms and the massive amount of personal data of their subscribers, which can be used for identity theft, fake news dissemination, and other malicious purposes. However, researchers have begun looking into effective techniques to identify suspicious or fraudulent accounts by analyzing account characteristics and employing classification algorithms. However, using standalone classification algorithms does not always yield satisfactory results, and some of the exploited features of the account have a negative contribution to the results or have no impact. This paper introduces a method for identifying fake profiles on social media platforms using machine learning. In order to identify the imposter accounts, the proposed method employs supervised learning strategies like artificial neural networks and support vector machines. Two datasets culled from the social media platforms provide empirical evidence for the effectiveness of the proposed method. The outcomes prove that the proposed method can successfully identify fake accounts. The paper also covers the difficulties of spotting fake profiles on social media and points the way for future studies.**

Keywords*— *social media, Machine Learning, Fake Accounts Detection, Instagram

I. INTRODUCTION

Social media is an online platform that lets users publish and share content in the form of posts, images, videos, and other types of media. It is a potent tool that makes it possible for individuals to connect and communicate with one another, exchange thoughts and opinions, and develop relationships. With more than 3 billion users worldwide, social media has firmly established itself as a part of daily life. Social media has completely changed the way we communicate, whether it's used for networking, marketing, entertainment, or just to stay in touch. Users of social networking websites can share information and daily activities, which draws many users to these sites. Figure 1 depicts data on social media site usage across the entire world [1-3].

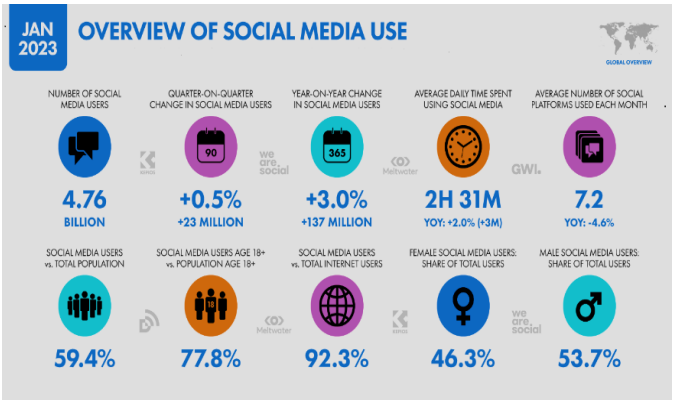

Figure 1. Social media site usage across the entire world

Instagram is one of the most frequently used social networking platforms. From 2013 to 2021, Instagram's monthly active users, as shown in Figure 2. Instagram users can add friends and share a range of content, including social, political, business, and personal information. Additionally, they can exchange photos, videos, travelogues, and other daily activities. Though not everyone uses these websites maliciously. As a result, they make fictitious accounts on social networking sites. False accounts lack a real identity. Attacker, in its simplest form, is the person who makes false accounts. To create a fake account, the attacker uses false information or statistics about a real person. With the help of these fake accounts, the attacker spread incorrect information that has an impact on other users. One of the main problems facing social networking sites is how to protect such sensitive user data [4-6].

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 2

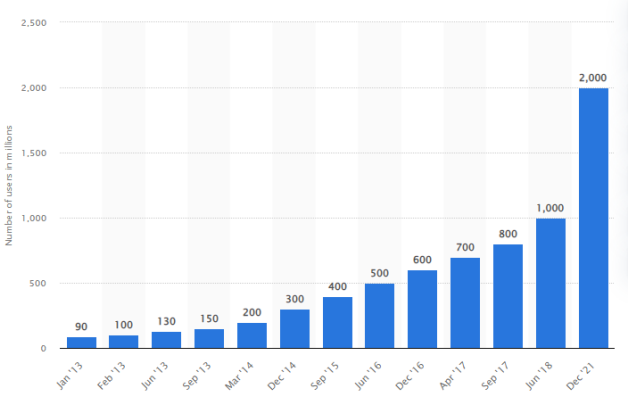

Figure 2. Number of monthly active users on Instagram

Social networking sites have many issues, including the issue of fake accounts, which can result in a number of issues. It has a variety of effects on social networking site users. Multiple fake accounts are a problem for online social networks. There aren't many ways to identify fake Instagram accounts. Even currently used methods are not very accurate. With support vector machines, which have the ability to learn and solve problems, this proposed work has a weighted feature set. These methods produce incredibly precise results while solving problems in real time [7-8].

This paper includes;

- To learn about the various data classification strategies implemented by machine learning.
- The objective is to investigate potential indicators of fake accounts.
- The goal is to determine the necessary and best methods of achieving the desired outcomes.
- The proposed method for identifying fake accounts must be put into practice.
- To determine the outcomes.

II. Clasification Techniques

Classification is a data mining technique used to assign a set of items to specific groups. The end goal of classification is an exact determination of the target class for each data point. The process of categorization has two stages. Finding out which classification algorithm was used to examine the training data is the first step. The second stage is a classification, wherein the reliability of the information is determined using test data. The output of a classification is a prediction based on the input. Classification algorithms using the training dataset determine the item's classification class. There is a wide selection of methods for categorizing data. The two most effective methods of classification are support vector machines (SVM) and neural networks.

A. Neural Networks

Neural Networks or Artificial Neural Networks (ANN) are a set of algorithms designed to recognize patterns. They are used to solve complex mathematical problems by recognizing patterns within the given data. Neural Networks are designed to mimic the behavior of a biological neuron. The neurons are connected in layers and each neuron is responsible for a specific task. Network has hundreds, thousands, or even millions of artificial neurons called units. Units arranged in a series of layers- Input layer, output layer, hidden layer as shown in Figure 3. Input layer accepts the information from the outside, and processing of that input is done by the hidden layer. The hidden layer plays an important role in producing output. The output layer is used provide the output to the user. The weights and biases of the neurons are adjusted to optimize the results.

- **Input layer** - receives a various form of information from the outside.
- **Hidden layer** – actual processing is done by hidden layer.
- **Output layer**-provides the output.

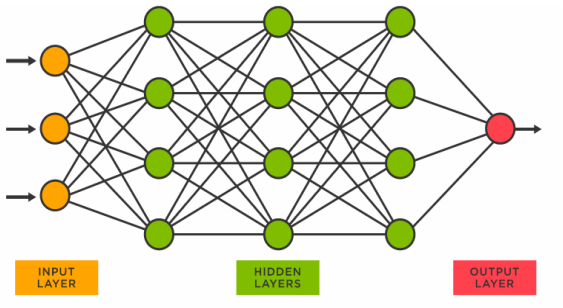

Figure 3. Artificial Neural Networks (ANN) structure

B. Support Vector Machines (SVM)

Support vector machines (SVMs) are a class of supervised learning algorithm used in machine learning and data mining. SVMs are effective and flexible learning algorithms used for classification, regression, and outliers' detection issues. Due to their versatility and ability to handle high-dimensional data, SVMs have risen in popularity over the past decade. In this piece, I'll go over how the SVM algorithm works and where you can put it to use. To classify data into two groups, support vector machines look for a line, or "hyperplane," in a high-dimensional space. The "support vectors" are the points that are closest to the hyperplane and lie on either side of it. Next, we equalize the distance between the hyperplane and the support vectors of each group. The SVM algorithm employs a kernel function to map the data points into a higher-dimensional space, where they can be separated by a hyperplane, if they are not linearly separable. The kernel function and the optimization algorithm form the backbone of the SVM algorithm. The data points are projected into a higher-dimensional space using the kernel function, and the optimal hyperplane separating the points is determined using an optimization algorithm. The concept of "maximal margin," or the greatest possible separation between the two

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 2

classes' nearest points, forms the basis of the optimization algorithm. Finding the hyperplane that maximizes the margin while being equally distant from the support vectors of both classes is the goal of the optimization algorithm. Both classification and regression issues are amenable to the SVM algorithm. The SVM algorithm classifies new data points into one of two groups based on which side of the hyperplane they fall on in classification problems. By summing up the squared differences between the data points and the hyperplane, the SVM algorithm determines which hyperplane best solves the regression problem. When compared to other machine learning algorithms, the SVM algorithm has a number of benefits. The SVM algorithm's strength lies in its ability to handle high-dimensional data, which consists of a great number of features or variables. In addition to being able to handle non-linear data that cannot be partitioned by a linear hyperplane, the SVM algorithm is also resistant to outliers. The SVM algorithm has dual-purpose applicability, being applicable to both classification and regression tasks. In addition to its use in text classification and image recognition, the SVM algorithm also finds use in financial forecasting and medical diagnosis. By analyzing the text and assigning it to one or more categories, SVM algorithms facilitate text classification. SVM algorithms are used in image recognition to determine what an image is of. Financial forecasting makes use of SVM algorithms to make predictions about stock prices based on past data. Using patient data, SVM algorithms classify diseases for medical diagnosis.

Algorithm: SVM

- **Collect data from social media accounts:** Collect data from a variety of sources such as Twitter, Facebook, Instagram, and other social media platforms.
- **Pre-process the data:** Pre-process the data by removing any irrelevant or redundant information, removing stop words, and normalizing the data.
- **Feature extraction:** Extract features such as user name, profile picture, number of posts, number of followers, and other important features that may help distinguish between real and fake accounts.
- **Build a model:** Build a machine learning model using Support Vector Machines (SVM).
- **Training and Testing:** Train the model using the training set and test the model using the test set.
- **Evaluation:** Evaluate the performance of the model using metrics such as accuracy, precision, recall, and F1 score.
- **Deployment:** Deploy the model to be used in real-time to detect fake accounts.

III. Fake Accounts Detection using SVM

A. *Evaluation Parameters*

- **Precision:** The ability to correctly identify real accounts as real accounts and fake accounts as fake accounts.

$$\text{Precision} = TP / (TP + FP)$$

- **Recall:** The ability to correctly identify both real and fake accounts.

$$\text{Recall} = TP / (TP+FN)$$

- **F1 Score:** The symbiotic average of recall and accuracy. It is used to assess a model's overall accuracy.
- **Accuracy:** The proportion of correctly classified instances over the total number of instances.
- **True Positive Rate:** The ratio of correctly predicted positives among all actual positives.

$$\text{True Positive Rate (TPR)} = TP/(TP+FN)$$

- False Positive Rate: The ratio of incorrectly predicted positives among all actual negatives.

$$\text{False Positive Rate (FPR)} = FP/(FP+TN)$$

- **AUC:** The ROC curve's area under the curve indicates how well the device is performing. It is a metric for evaluating the precision of the classification algorithm.
- **Training and Test Error:** The difference between the training error and the test error is used to measure the generalization of the model.
- **Time Complexity:** The time taken to train the model and make predictions on new data.
- **Confusion Matrix -** One way to evaluate the efficacy of a classifier is with the help of a "confusion matrix." You can learn more about the strengths and weaknesses of your classification model by computing a confusion matrix.

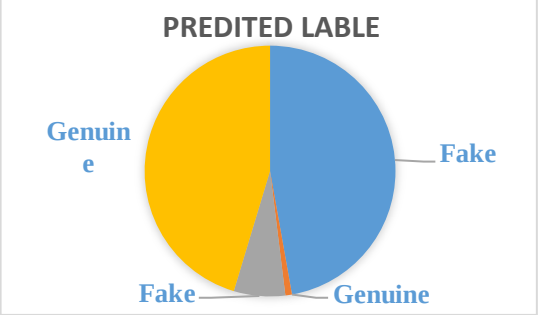

Figure 4. Confusion Matrix

Efficiency/Accuracy = Number of predictions/Total

Number of Predictions Percent Error = (1-Accuracy) *100

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 2

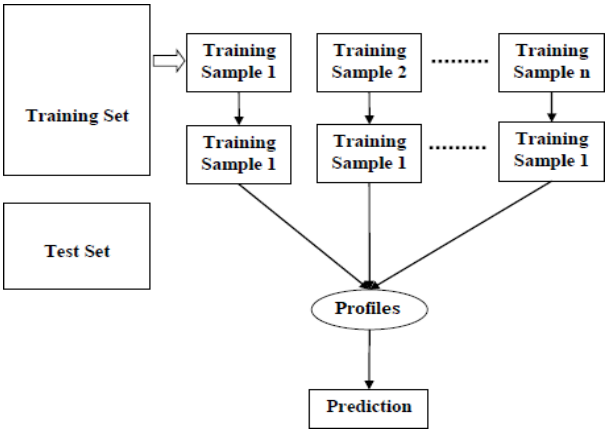

Figure 5. Random Forest model

Table-I. Classification Report

	precision	recall	F1 score	Support
Fake	0.88	0.96	0.95	266
Genuine	0.95	0.85	0.96	297
Avg/ Total	0.90	0.91	0.91	565

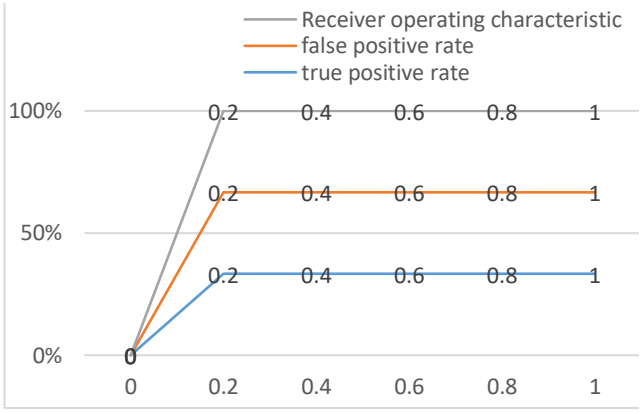

Figure 6. ROC Curve

Data classification efficiency for the Random Forest Classifier is 96%. The training dataset contains 80% of the data, while the test dataset contains 20%.

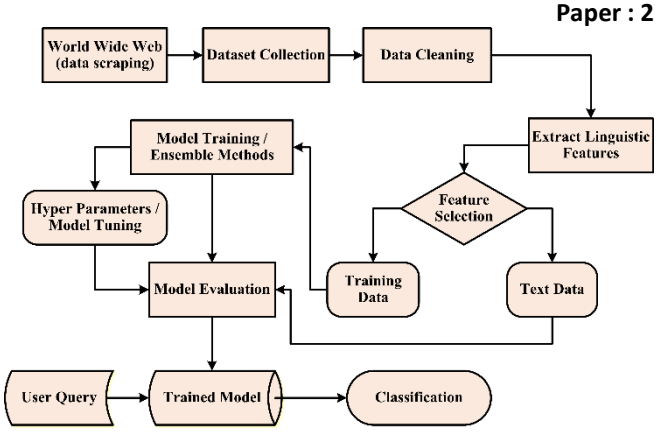

Figure 7. Flowchart for training algorithms and classification

IV. Results And Analysis

A. *Random Forest*

As a supervised learning algorithm, random forest can be applied to both classification and regression tasks. However, its primary application is in solving classification issues. Since trees are the building blocks of forests, it stands to reason that healthier forests have more trees. Similarly, the random forest algorithm constructs decision trees from data subsamples, collects predictions from each tree, and then uses a voting mechanism to determine which prediction is most accurate. Because it averages the results from multiple decision trees, this ensemble method is superior to using a single decision tree.

- The following steps will help us comprehend how the Random Forest algorithm functions:
- The first stage involves picking arbitrary subsets of a larger dataset.
- After that, this algorithm will make a decision tree for each sample as the second step. Then it will collect the outcome of every decision tree's prediction.
- The third step is that, as expected, voting will take place in all of the predicted outcomes.
- Fourth, take the prediction with the most votes and use that one.

Table-II Data sheet required for classification.

SL No.	Attribute	Description
1	Profile ID	Profile id of account holder
2	Profile name	Name of account holder
3	Status count	No of tweets made by account of followers for account
4	Followers count	How many followers are there
5	Friends count	No of friends for account
6	Location	Location of account holder

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 2

7	Created date	Which date account created

The complete process of identifying a fake profile on a social networking site.

1. To begin with, we pick all of the features that the classification algorithm will use. It's important to take precautions when selecting features, such as picking features that don't rely on others and picking features that can boost the classification's efficiency.

2. To train a classification algorithm, it is necessary to have a dataset of already-distinguished fake and real profiles, after the appropriate selection of attributes. Barracuda Labs is an independent firm that focuses on providing protection, networking, and data storage via network appliances and cloud computing. We created the real profile dataset, and they provided the fake profile dataset.

3. Extracting the attributes chosen in Step 1 from the profiles (fake and genuine) is Step 3. Companies in the social networking space interested in adopting our scheme can easily extract the necessary features from their existing databases without resorting to the scraping process. Given the lack of a publicly available social network dataset for the study of identifying fake profiles, we decided to apply to have the profiles scraped.

4. The dataset of phony and genuine profiles is then prepared (4). To create a training and testing set from this data, we use 80% of the real profiles and 20% of the fake profiles. Using 922 profiles from the training dataset and 240 profiles from the testing dataset, we determine the effectiveness of the classification algorithm.

5. Next, the training dataset is fed into the classification algorithm, followed by the testing dataset. It takes in information from the training algorithm and is then expected to accurately predict class levels on the test dataset.

6. Sixth, we leave it up to the trained classifier to decide what the levels should be after we have removed them from the testing dataset. Number of accurate predictions as a percentage of total predictions represents the classifier's efficacy. We have used three different classification algorithms and compared their performance.

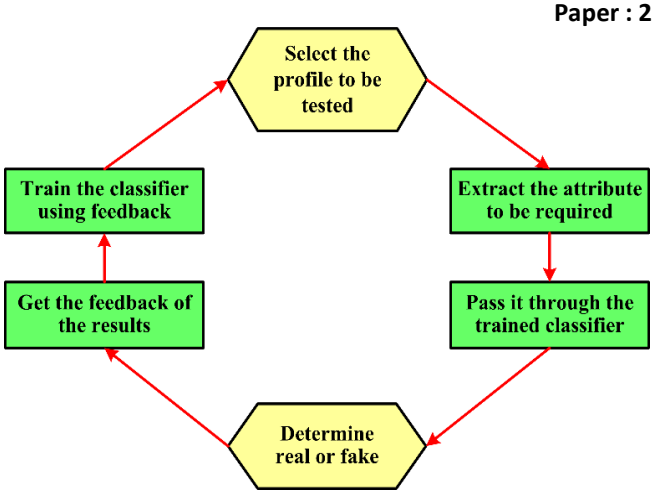

Figure 8. Architecture of the system

Framework:

The steps that must be taken to continuously detect fake profiles using active learning from the feedback of the result given by the classification algorithm are depicted in Figure 8 of the proposed framework. Companies in the social networking space can easily adopt this framework.

- The first step in detection is choosing which profile to analyse.
- Selecting the profile is followed by deciding which attributes to use as features in the classification algorithm.
- A trained classifier receives the extracted attributes.
- At regular intervals, the classifier receives updated training information in the form of new training data.
- The classifier decides if the profile is real or not.
- Since the classifier's categorization of the profile might not be perfect, it receives the results' criticism.
- This is repeated, and as more data is added to the training set, the classifier gets better at identifying fake profiles.

System Proposed:

This subsequent project's domain of application was "Community Detection." Understanding the structure of complex networks and ultimately extracting useful information from them requires the use of community detection. As part of this project, we developed a framework for identifying fake profiles by means of machine learning algorithms, making it possible for people's online social lives to be safer.

- The first step in classification is deciding which profile to categorize.
- Selecting a profile is the first step in extracting features that can be used for classification.
- Afterwards, the features are fed into a trained

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 2

classifier.

- ❖ The classifier is constantly being fine-tuned by being fed fresh data.
- ❖ After that, Classifier decides if the profile is real or not.
- ❖ The classifier's output is checked, and the results are fed back into the classifier as reinforcement.
- ❖ Increasing the amount of training data improves the classifier's ability to identify fake profiles.

Advantages of the Proposed System

The social networking sites improve our interpersonal lives, but they also bring with them a host of problems. Privacy concerns, cyberbullying, misuse, trolls, etc., are all factors to consider. Fake profiles are commonly used in these activities. To protect people's online relationships, we developed a system to identify fake profiles using machine learning algorithms.

V. Conclusion

The detection and classification of fake accounts on social media platforms is greatly aided by the use of machine learning techniques such as support vector machines (SVMs). SVMs can recognize data patterns and reliably categorize fake accounts. SVMs are helpful because they can recognize patterns in data that would be invisible to the naked eye. It's also possible to train SVM models to identify fake accounts across multiple social media sites. In general, machine learning methods, such as support vector machines (SVMs), can be an effective method for uncovering fake profiles on social media. Protecting against fraud and other malicious activity requires the ability to accurately identify patterns in data. In addition, a more secure social media ecosystem can result from the use of machine learning techniques for the detection of fake accounts. SVMs are likely to become more widely used to detect fake social media accounts as the prevalence of machine learning techniques rises.

References

[1] G. Stringhini, “Detecting Spammers on Social Networks,” ACSAC, pp. 1–9, 2010.

[2] I. Bara, C. J. Fung, and T. Dinh, “Enhancing Twitter Spam Accounts Discovery Using Cross-Account Pattern Mining,” IEEE, 2015.

[3] M. Secchiero, “FakeBook : Detecting Fake Profiles in On-line Social Networks,” IEEE, 2012.

[4] Cao X, David MF, Theodore H (2015) Detecting clusters of fake accounts in online social networks. In: 8th ACM workshop on artificial intelligence and security, pp 91–101

[5] Rao, K. Sreenivasa, N. Swapna, and P. Praveen Kumar. "Educational data mining for student placement prediction using machine learning algorithms." Int. J. Eng. Technol. Sci 7.1.2 (2018): 43-46.

[6] Granik M, Mesyura V (2017) Fake news detection using Naive Bayes classifer. In: 2017 IEEE frst Ukraine conference on electrical and computer engineering (UKRCON), pp 900–903.

[7] J. R. Douceur, “The sybil attack,” in International workshop on peerto-peer systems. Springer, 2002, pp. 251–260.

[8] N. Singh, T. Sharma, A. Thakral and T. Choudhury, "Detection of Fake Profile in Online Social Networks Using Machine Learning," 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris, 2018, pp. 231-234.