FAKE ACCOUNTS DETECTION ON SOCIAL MEDIA USING MACHINE LEARNING AND DEEP LEARNING

[1]Dr. G. Harinatha Reddy, [2]C. Vinisha, [3]M. Vamsi, [4]P. Saileela, [5]P. Sivarjuna

[1]Professor & Head of the Department, [2,3,4,5]Students
Electronics and Communication Engineering
N.B.K.R Institute of Science and Technology, Tirupati District,
Andhra Pradesh, India

***Abstract*: Online social networks (OSNs) have grown in popularity and are now more closely associated with people's social activities than ever before. They use OSNs to communicate with one another, exchange news, plan activities, and even operate their own online businesses. In order to steal personal information, spread malicious activities, and share false information, attackers and imposters have been drawn to OSNs because of their explosive growth and the vast quantity of personal data they collect from their users. On the other hand, academics have begun to look into effective methods for spotting suspicious activity and bogus accounts using account features and classification algorithms. However, some of the characteristics of the account that are exploited have an adverse effect on the results or have no effect at all. Additionally, using independent classification algorithms does not always produce satisfactory results. Four feature selection and dimension reduction techniques were used to create the decision tree in this paper, which is suggested to provide effective detection for fake Instagram accounts. To determine whether the target account was genuine or fake, four machine learning classification algorithms—Decision Tree, Random Forest, Logistic Regression, and CNN—were used. High-end machine learning algorithm CNN is a specific type of network design for deep learning algorithms that is employed for tasks requiring the processing of numerical data as well as dataset recognition.**

***Keywords*: Decision Tree, Random Forest, Logistic Regression and CNN (Convolutional Neural Network)**

1. INTRODUCTION

Over the past few years, online social networks (OSNs) like Facebook, Twitter, LinkedIn, and Google+ have grown in popularity. OSNs are used by people to communicate with one another, exchange information, plan events, and even operate their own online businesses. Non-profit organizations spent about 2.53 million dollars between 2014 and 2018 sponsoring political advertisements on Facebook. OSNs are susceptible to Sybil attacks because of their open nature and the enormous quantity of personal information that their subscribers provide. Facebook discovered misuse in 2012, including the publication of false news, hate speech, sensational and polarizing content, among other things. Attackers adopt the idea that OSN user accounts are "keys to walled gardens," so they pose as someone else by using images and profiles that are either stolen secretly from real people or created artificially in order to spread false information and steal personal data. Imposters are the common name for these false identities. Such fake accounts hurt users in both situations, and their motivations are never positive ones because they frequently flood users with spam or steal personal information. Researchers work to develop automated detection tools because personally detecting fake accounts would be time-consuming and expensive. The results of the researchers' efforts may enable an OSN operator to identify fake accounts quickly and accurately, which would enhance the user experience by reducing the amount of irritating spam and other offensive content. The OSN operator can also make its user data appear more reliable and make it possible for outside parties to evaluate its user accounts. The maintenance and provision of information security and privacy, two of the main demands of social network members, boosts the credibility of the network and, as a result, its income. Consequently, automated Sybil detection does not always produce accurate results that are useful. In this study, a hybrid classification algorithm has been used, which uses fewer features but can still correctly classify about 98% of the accounts in our training dataset. The neural network (NN) classification algorithm has been run on the decision values obtained from the support vector machine (SVM). As shown in, also verified the detection capabilities of our classifiers using two additional sets of genuine and fake accounts that were unrelated to the initial training dataset. It gives a summary of the study done on the Twitter network and earlier studies on fake profile detection. In, it is shown how the data was pre-processed and how the results were used to categorize the accounts into fake accounts and genuine accounts. The overall accuracy rates have been examined and evaluated in relation to all other applied techniques.

2. LITERATURE SURVEY

Facebook political advertising is the most recent in a long line of advancements in campaign strategy, and it has been widely used in elections all over the world. We [1] argue that existing measures provide little insight into current campaign trends, offering analytical, methodological, and normative issues for academics and electoral authorities alike. Large-scale peer-to-peer systems face security risks from unreliable or malicious remote computing components. In order to counter these dangers, many of these systems employ redundancy. However, the redundancy can be undermined if a single flawed entity can assume several [2] identities and control a sizable chunk of the system. This paper discusses numerous anomaly types and their novel [3] categorization according to distinct traits. This paper discusses a variety of approaches for preventing and identifying anomalies, as well as the underlying presumptions and causes of such anomalies. The study offers a discussion of several data mining techniques for finding

abnormalities. The objective of the study was to [4] ascertain how much perceived value, service quality, and social variables influenced users' inclinations to stick around for the social media-based online brand community of a major automaker.

3. METHODOLOGY

a. Over view of the proposed system

The dataset used is a collection of both real and fake accounts. The algorithms use various features like profile picture, user name, full name, full name = user name, bio, external URL, private or public, posts, followers, follows to detect whether an account is fake or real..

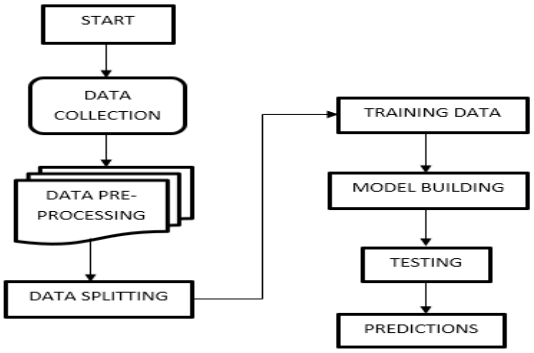

Fig1: Flow Chart

b. Algorithms

1. Logistic Regression:

When the objective (dependent variable) is a categorical variable, logistic regression is used. For binary classification problems, one of the most used machine learning algorithms is logistic regression.

The purpose of logistic regression is to assess the likelihood of events, including identifying a relationship between certain variables and specific outcomes.

2. Decision Tree Classifier:

It has a tree-like structure, with internal nodes standing in for dataset attributes, branches for decision rules, and leaf nodes for the classification outcomes.

3. Random Forest Classifier:

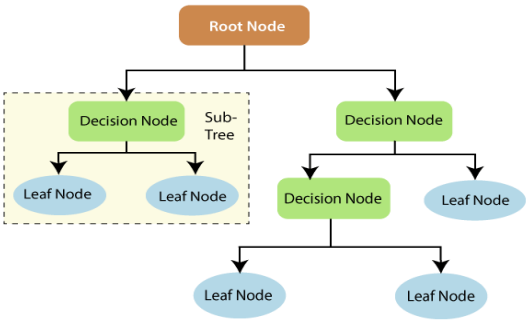

Fig 2: Random Forest Classifier

In order to increase the projected accuracy of the input dataset, the Random Forest classifier averages the results from multiple decision trees applied to various subsets of the input dataset.

4. Convolutional Neural Network:

A common type of artificial neural network used for object and picture recognition and classification is the CNN. As a result, Deep Learning uses a CNN to identify items in a picture

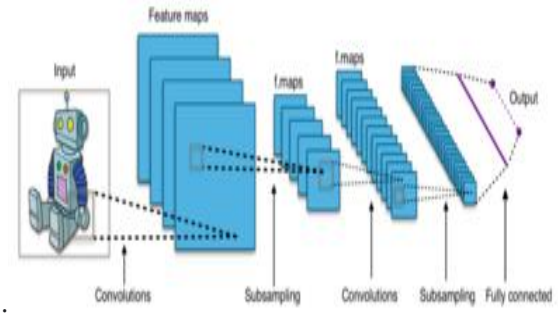

Fig3: Convolutional Neural Network

c. UML Diagrams:

Unified Modeling Language is referred to as UML. The discipline of object-oriented software engineering uses the universal modelling language, or UML.

- Use case diagram
- Class Diagram
- Sequence Diagram
- Collaboration Diagram
- Activity Diagram
- Deployment Diagram
- Component Diagram
- ER Diagram
- DFD Diagram

d. Frame work:

Flask:

Python-based Flask is a microweb framework. Due to the fact that it doesn't require any specific tools or libraries, it is categorized as a microframework. It lacks any components where pre-existing third-party libraries already provide common functions, such as a database abstraction layer, form validation, or other components. But, Flask allows for extensions that may be used to add application functionalities just like they were built into the core of Flask. There are extensions for object-relational mappers, form validation, management of uploads, numerous open authentication protocols, and a number of widely used framework-related tools. A lightweight and adaptable Python web framework called Flask makes it simple for programmers to create web apps. Based on the Werkzeug WSGI toolkit and the Jinja2 template engine, Armin Ronacher developed it.

The simplicity of Flask is one of its primary characteristics. Even for developers who are new to web development, Flask is simple to understand and use. With its straightforward and user-friendly API, developers can create web applications quickly and without needless complication.

The adaptability of Flask is another important characteristic. Flask is a versatile web development tool that can be used for everything from straightforward online applications to intricate web services. Moreover, Flask offers a large selection of third-party libraries and extensions, making it simple to upgrade your application's features as necessary.

4. RESULTS

The accuracies obtained by the different algorithms are:

Logistic Regression - 89.95%

Decision tree Classifier - 88.51%

Random Forest Classifier - 91.38%

Convolutional Neural Network – 82.35%

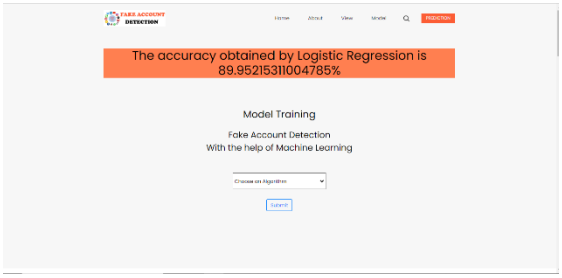

Fig 4: Model Selection

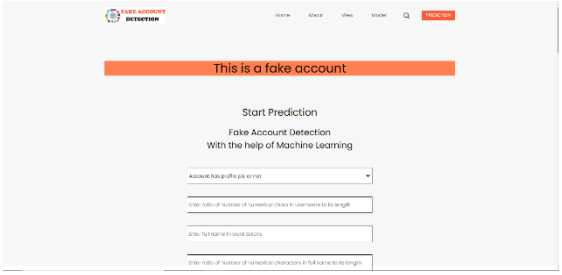

Fig 5: Prediction of Dataset

5. CONCLUSION & FUTURE SCOPE

In the end, this paper concludes that among the four algorithms Random Forest Classifier gives more accuracy because it can perform both regression and classification tasks. Therefore, the model will successfully be able to distinguish between a fake account and a genuine account.

These four algorithms can be used for other social networking platforms and other algorithms may be used to increase the accuracy.

REFERENCES:

[1] (2018) Political advertising spending on Facebook between 2014 and 2018. Internet draft.[Online].Available: https://www.statista.com/statistics/891327/political-advertising spending-face book-by-sponsor-category/
[2] J. R. Douceur, "The Sybil attack," in International workshop on peer-to-peer systems. Springer, 2002, pp. 251–260.
[3] (2012) Cbc.facebook shares drop on news of fake accounts. Internet draft. [Online]. Available: http://www.cbc.ca/news/technology/facebook-shares-drop-on news-of-fake-accounts-1.1177067
[4] R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," Egyptian informatics journal, vol. 17, no. 2, pp. 199–216, 2016.
[5] L. M. Potgieter and R. Naidoo, "Factors explaining user loyalty in a social media-based brand community," South African Journal of Information Management, vol. 19, no. 1, pp. 1–9, 2017.
[6] (2018) Quarterly earning reports. Internet draft. [Online]. Available: https://investor.fb.com/home/default.aspx
[7] (2018) Statista.twitter: number of monthly active users 2010-2018. Internet draft. [Online]. Available: https://www.statista.com/statistics/282087/number-of-monthly active-twitter-users/
[8] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, "Thwarting fake accounts by predicting their victims," in Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015, pp. 81–89.
[9] (2018) Facebook publishes enforcement numbers for the first time. Internet draft. [Online]. Available: https://newsroom.fb.com/news/2018/05/enforcement-numbers/
[10] (2013) Banque populaire dis-moi combien damis tu as sur facebook, je te dirai si ta banque va taccorder un prłt. Internet draft. [Online]. Available: http://bigbrowser.blog.lemonde.fr/2013/09/19/popularitedis-moi-combien-damis-tu-as-sur-facebook-je-te-dirai-si-ta-banqueva-taccorder-un-pret/
[11] S.-T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," in Proceedings of the 2010 New Security Paradigms Workshop. ACM, 2010, pp. 61–72.
[12] S. Fong, Y. Zhuang, and J. He, "Not every friend on a social network can be trusted: Classifying imposters using decision trees," in Future Generation Communication Technology (FGCT), 2012 International Conference on. IEEE, 2012, pp. 58–63.