iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** VII **Month of publication:** July 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.36637

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VII July 2021- Available at www.ijraset.com*

# Twitter Bots Detection Using Machine Learning Techniques

Deekshith S G [1], Harish N [2], Manoj M B [3], Vaishaka K R[4], Prof. Manasa C[5]
[1, 2, 3, 4]*Student's, Department of CSE, Bangalore Institute of Technology, Bengaluru*
[5]*Assistant Professor, Department of CSE, Bangalore Institute of Technology, Bengaluru*

***Abstract:*** ***The social network, a crucial part of our life is plagued by online impersonation and fake accounts. Fake profiles are mostly used by the intruders to carry out malicious activities such as harming person , identity theft and privacy intrusion in Online Social Network(OSN). Hence identifying an account is genuine or fake is one of the critical problem in OSN .In this paper we proposed many classification algorithm like Support Vector Machine algorithm ,KNN, and Random Forest algorithm. It also studies the comparison of classification methods on Spam User datasetwhich is used to select the best.***
***Keywords: Machine learning, twitter detection, Support Vector Machine (SVM), KNN, Random Forest.***

## I. INTRODUCTION

In today's Modern society, social media plays a vital role in everyone's life. The main advantage of online social media is that we can connect to people easily and communicate with them in a better way. On the other hand, they suffer from expanding the number of fake accounts that has been created. Fake accounts means that the accounts that do not belong to real humans. Detection of malicious account is significant. The methods based on machine learning techniques were used to detect fake accounts that could mislead people. In this project we will overcome this problem. So Supervised machine learning techniques can be used to identify fake identities.

## II. AIM AND OBJECTIVES

*A.* The main aim of this project is to find the fake accounts in Twitter and make comfortable for the legitimate users.
*B.* To develop and implement machine-learning model which is used to detect the identities is fake or not.
*C.* To pre-process and extract useful features from data.
*D.* To give a framework with which the automatic detection of fake identities can be done so that the social life of people becomes secured and using this automatic detection technique.
*E.* To evaluate model-performance and improve it.

## III. DRAWBACKS OR LIMITATIONS

Twitter has the spam problem like other social networking sites, some twitter users only tweet their products, blog or
Website links, some users send the spam messages or they spam you by tweeting the spam tweets. Twitter has limited message size of 140 characters per tweet, it can include a message or link on your website as it is free and free for the advertisements, you have to face the problem with bunch of posters like the other social networking. Twitter also faces the overloading problem means due to the large numbers of users and it gets crashed.

## IV. PROPOSED SYSTEM

Machine Learning techniques can be used to detect fake identities in the official dataset for tweets in twitter. This project proposes the detection process starts with the selection of the profile that needs to be tested. After selection of the profile the suitable attributes and the features are selected on which the classification algorithm is being implemented, the features such as, name postdate, user index, retweet_count, location, comment_count, like_count, post content are used. The attributes extracted is passed to the trained classifier. The classifier is being trained regularly as new training data set is fed into the classifier. The classifier determines whether the profile is fake or real and some features are used to determine the account is fake or not. In addition, So that we could have the best accuracy for prediction's

1) The detection process starts with the selection of the profile that needs to be tested.
2) After the selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented.
3) The attributes extracted is passed to the trained classifier. The classifier gets trained regularly as new training data is feed into the classifier.
4) The classifier determines whether the profile is fake or genuine.
5) The classifier may not be 100% accurate in classifying the profile so the feedback of the result is given back to the classifier.
6) This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake profiles.

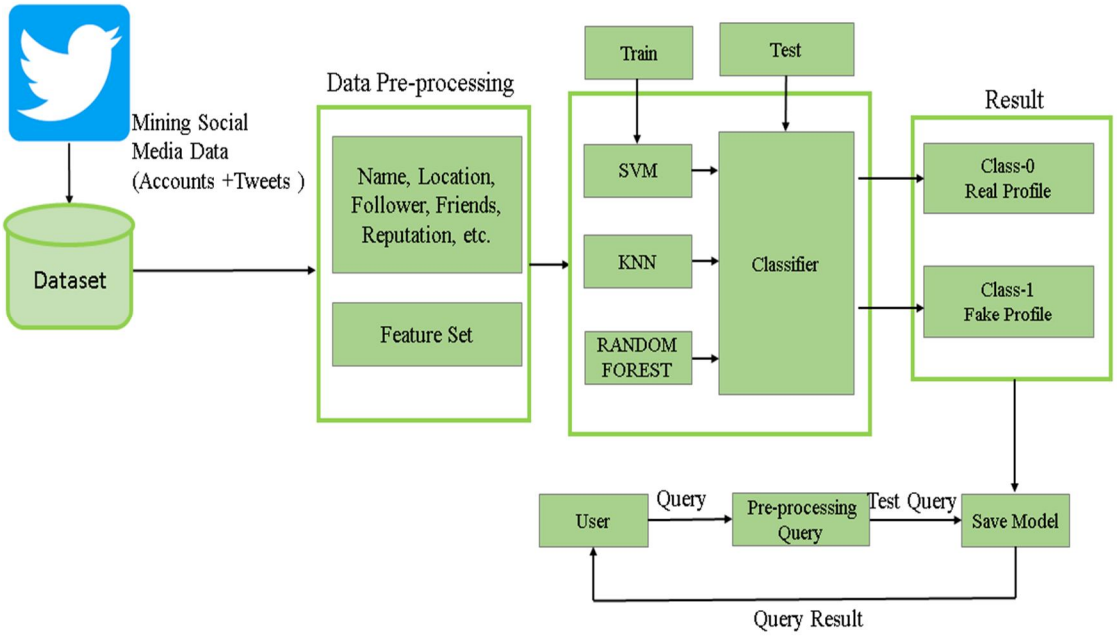



Fig 1. Architecture of Proposed System

## V. LITERATURE SURVEYS

### A. *Detecting Fake Followers in Twitter: A Machine Learning Approach*

This paper was published in the year 2017 by Ashraf Khalil proposed a system for detecting fake accounts in twitter labelled collection of users, preclassified as fake or genuine. They identified number of characteristics that distinguish fake and genuine followers such as number of tweets and number of followers. Then, they used these characteristics as attributes to machine learning algorithms to classify users as fake or genuine.

### B. *Machine Learning Implementation for Identifying Fake Accounts in Social Network*

This Paper published in 2018 by Rohit Raturi for identifying the accounts are real or not using SVM**.** Social Networking is the main era of data transmission as well as data creation in a large scale and the reason why big data is created is very much known. Social networking is the main platform where tons of data is being created and by 2025 even Google data centres can't handle that kind of huge volume. They are using Machine Learning technique to implement for better prediction on identifying the fake account based on their posts and status on their social networking walls block the fake and unwanted information circulating over the network for the peace and security.

### C. *Detecting Fake Accounts on Twitter Social media using machine learning algorithms.*

This paper was published in 2020 by Dr.K.Sreenivasa Rao ,Dr.G.Sreeram. proposed many classification algorithms like Support Vector Machine algorithm and deep neural network. The classifier is being trained regularly as new training data set is feed into the classifier. The classifier determines whether the profile is fake or real. The classifier may not be 100 % accurate in classifying the profile so the feedback obtained from the result is being given back to the classifier.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VII July 2021- Available at www.ijraset.com*

## VI. METHODOLOGY

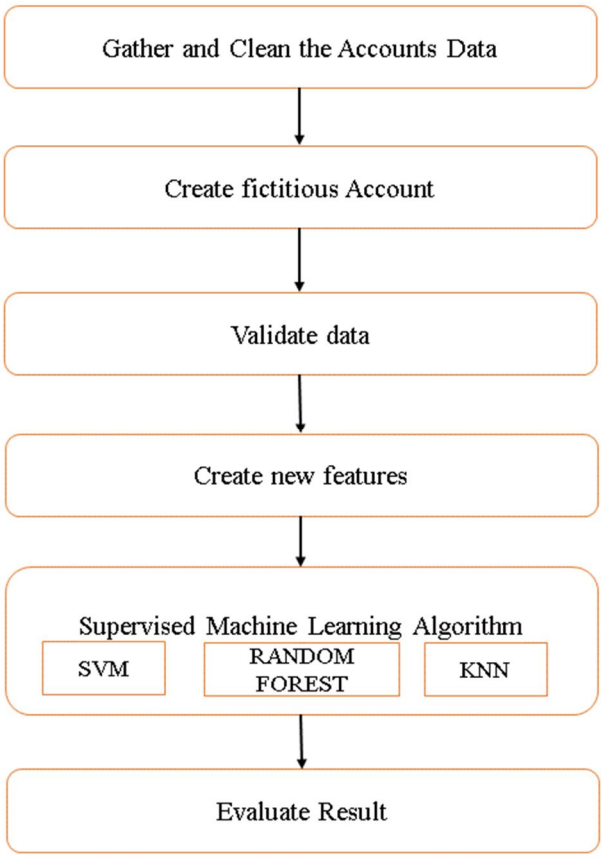



Fig 2. Proposed Methodology

The Figure 2 shows the Proposed Methodology of this project. This begins with Data collection. It is collected from various social media networks .Then creates non-relational databases. Then cleaning process is started after that the data is stored in relational databases. Then train the dataset using supervised machine learning algorithms. Cross validation and resampling methods are used in machine learning to detect fake identities. The input traffic data is used for twitter dataset with some features. The training dataset contains data preprocessing which includes two steps: Feature Extraction and Machine Learning techniques. After using these two steps it is arranged in the model, which is used for selecting number of features. After applying the Support Vector machine for classifying the data and training the model. Finally the results are visualized and evaluated.
The different ways in which an algorithm can model a problem is based on its interaction with the experience or environment for the model preparation process that helps in choosing the most appropriate algorithm for the given input data in order to get the best result.

### *A. Support Vector Machine*

Support Vector Machine is a binary classification algorithm that finds the maximum separation hyper plane between two classes. It is a supervised learning algorithm that gives enough training examples, divides two classes fairly well and classifies new examples. It offers a principle approach to machine learning problems because of their mathematical foundation in statistical learning theory. SVM construct their solution, as a weighted sum of SVs, which are only a subset of the training input .It is effective in cases where number of dimensions is greater than the number of samples given.

### *B. Random Forest*

Random Forest is versatile method performing both classification and regression tasks. It has nearly same hyper parameters as a decision tree or a bagging classifier. It creates many variations of trees .The best outcome will be used to predict identity deception .Each outcomes from the classifier represents different section of a tree.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VII July 2021- Available at www.ijraset.com*

### *C. K-NEAREST Neighbors*

K Nearest Neighbor Classifier Algorithm This is very popular algorithm for classification of data. This algorithm is used for categorize dataset samples base on nearest training samples. To classify the test tweet, KNN algorithm identifies, k closest samples that are similar to test sample. The k nearest neighbors are identified by similarities of data sample. The data sample similarities are computed with some set of similarity measures. Euclidean distance measure is one of familiar similarity computing approach. The distance between two data samples can be found using Euclidean distance formula. The performance of classification model is improved using cross validation technique. The cross-validation approach is used to validate the classification model performance and accuracy. After k nearest neighbor's is found.

Features Extracted

| S.NO | FEATURES |
|---|---|
| 1 | Number of friends |
| 2 | Number of |
| 3 | Followers |
| 4 | Favorite Count |
| 5 | Languages |
| 7 | Sex code |
| 8 | Listed Count |
| 9 | Status Count |
| 10 | Reputation |
| 11 | Average Hash Tag |
| 12 | Location |
| 13 | Average Followers Count |
| 14 | Average Favorite Count |
| 15 | Average Age Count |
| 16 | Account Created Time |
| 17 | Account Status |

## VII. RESULTS

### *A. Evaluation Results*

*1) Confusion Matrix:* Confusion Matrix is a technique for summarizing the performance of a classification algorithm. Calculating a confusion matrix can give you a better idea of what your classification model is getting right and what types of errors it is making.

TPR- True Positive Rate TPR=TP/(TP+FN)
FPR- False Positive Rate FPR=FP/(FP+TN)
TNR- True Negative Rate TNR=TN/(FP+TN)
FNR- False Negative Rate FNR=1-TPR

*2) Recall:* How many of the true positives were recalled (found), i.e. how many of the correct hits were also found.
Recall = TP / (TP+FN)

*3) Precision:* Precision is how many of the returned hits weretrue positive i.e. how many of the found were correct hits.
Precision = TP / (TP + FP)

*4) F1 score:* F1 score is a measure of a test's accuracy. It considers both the precision p and the recall r of the test to compute the score.

*5) ROC Curve:* The Receiver Operating Characteristic is the plot of TPR versus FPR. ROC can be used to compare the performances of different classifiers.

Table shows the results of applying all 13 extracted features on the Test Set 1 and Test Set 2 using three algorithms of Random Forest, KNN and Support Vector Machine.

**KNN** **SVM** **RANDOM FOREST**

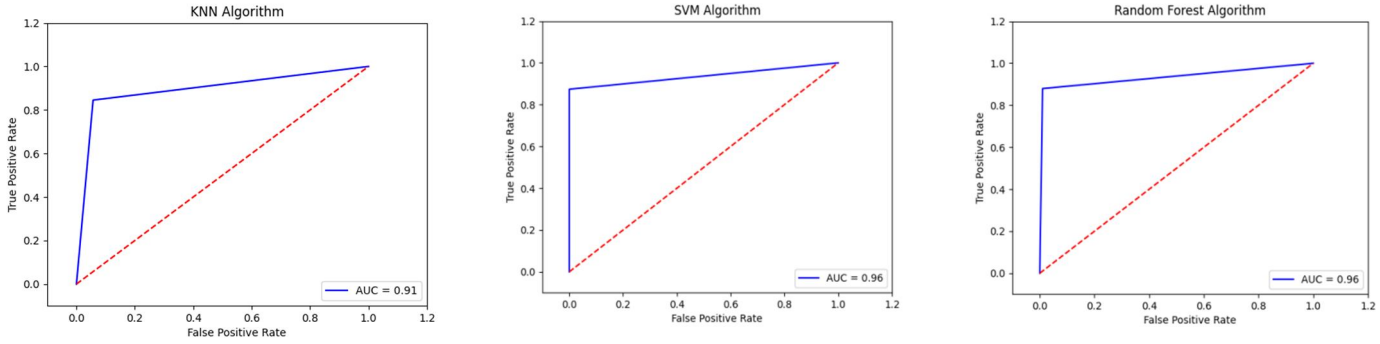



Fig 3 :ROC Curve

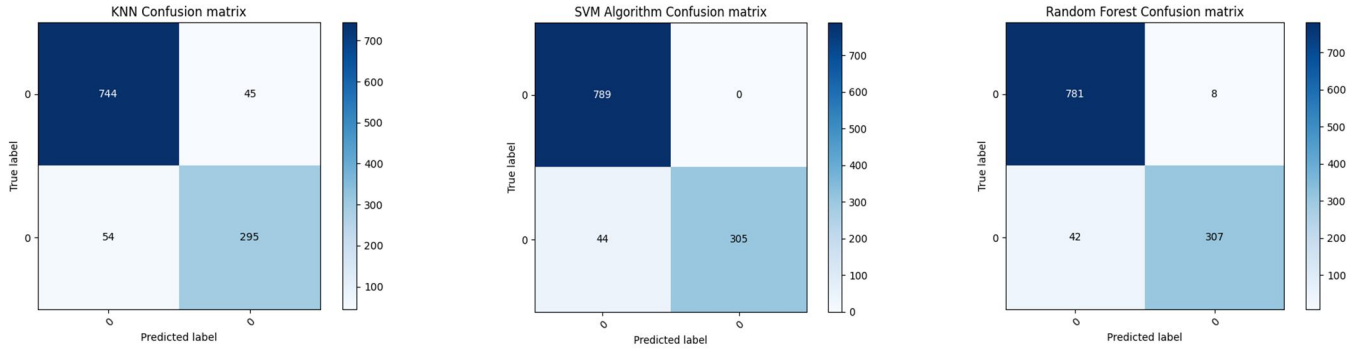



Fig 4 :Confusion Matrix

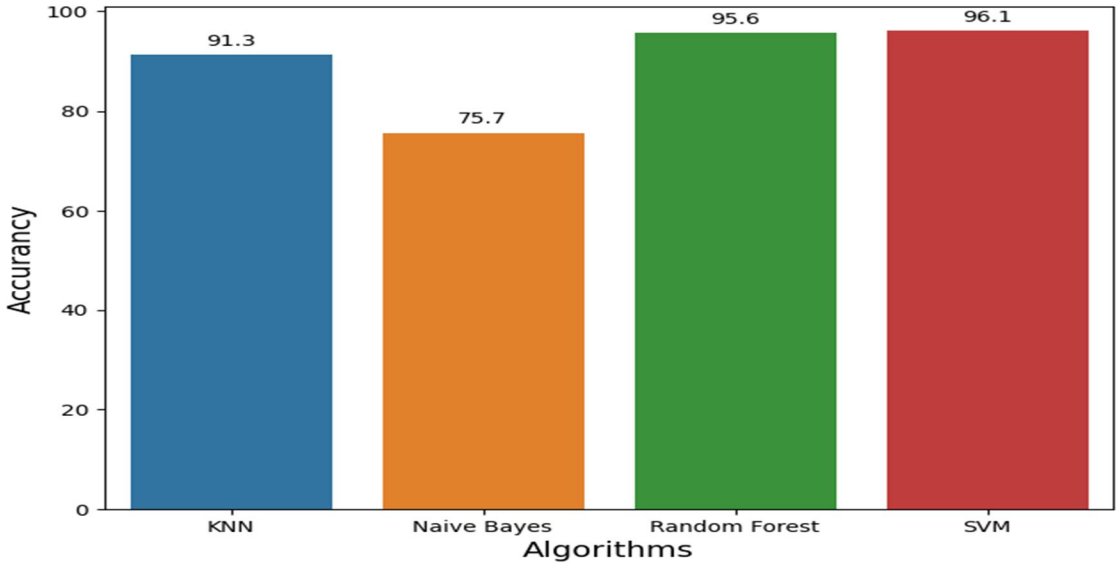



Fig 5 :Bar Chart

| Dataset | Machine learning algorithm | Accuracy% | F-Measure% | MCC% |
|---|---|---|---|---|
| Test Set 1 | Random Forest | 95.6 | 94.7 | 95.47 |
| | KNN | 91.3 | 91.04 | 90.31 |
| | SVM | 96.1 | 96 | 96.01 |
| Test Set 2 | Random Forest | 94 | 93.9 | 93.8 |
| | KNN | 90.1 | 89.2 | 89.9 |
| | SVM | 97.5 | 97.6 | 95.13 |

Classification performance using all 46 extracted features on Test Set 1 and Test Set 2

## VIII. FUTURE SCOPE

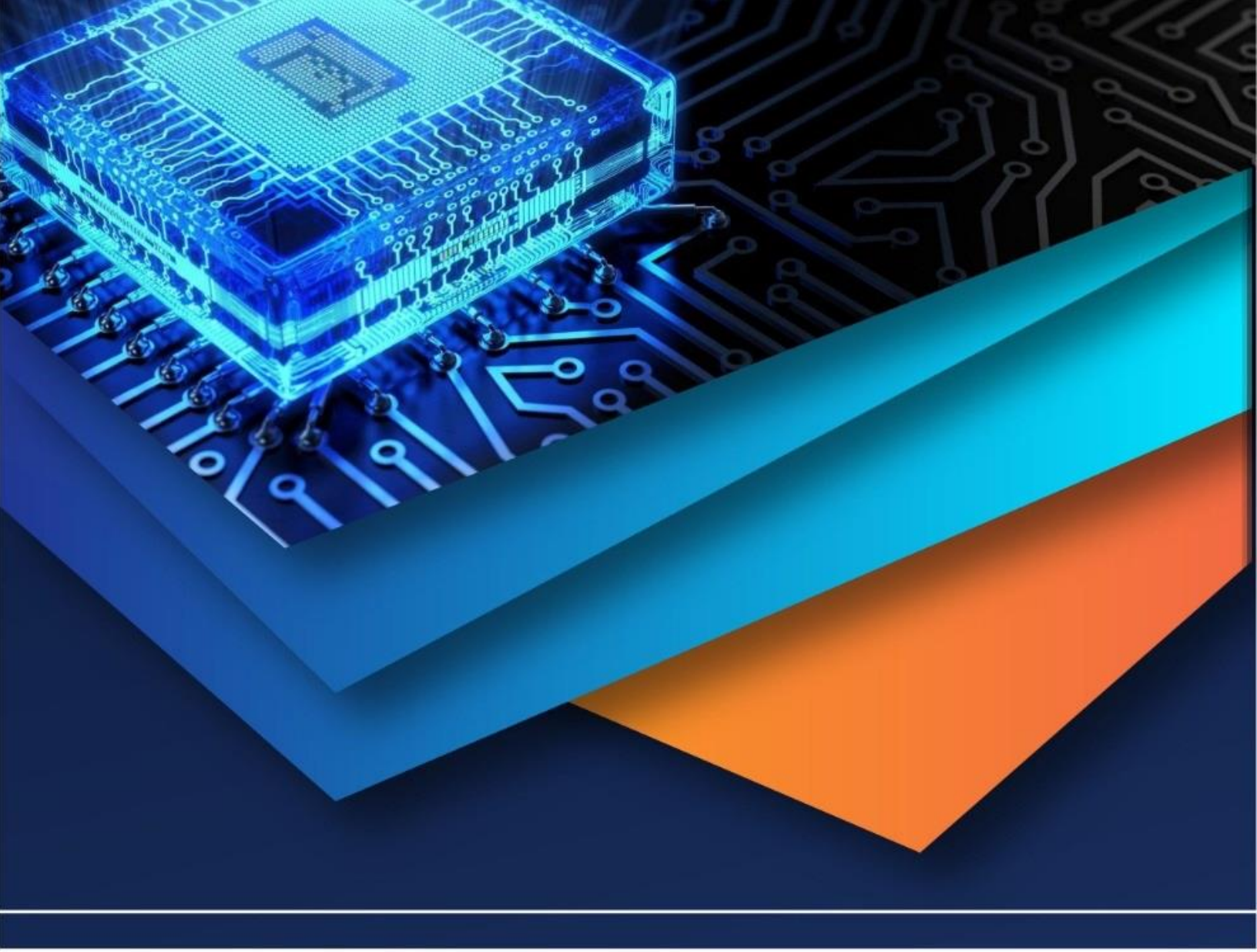
Method, the user friend network structure was analysed and the fake users were predicted by computing similarity and the classifier algorithms. In this method, fake accounts must work in the network so that it will be possible to recognize them as legitimate or fake ones, by analysing their friend's networks. This is a weakness of the proposed method. In future researches, a new method will be presented; which can recognize the legitimate or fake account before any activity of the user in the network or at the time of registration.

## IX. CONCLUSION

In this project, We intend to give a framework, which collects data from Twitter using Twitter API and from every tweet, we extract features that we need to feed our classifiers, that binary classification through the SVM is more efficient than through any other classifier. In the future, we wish to classify profiles by analysing the behaviour of the user by his tweets find out a pattern and classify.

## REFERENCES

[1] Ashraf Khalil, Hassan Hajjdiab, and Nabeel Al-Qirim, "Detecting Fake Followers in Twitter: A Machine Learning Approach," in International Journal of Machine Learning and Computing, December 2017,
[2] Sarah Khaled,Hoda M. O. Mokhtar, Neamat El-Tazi "Detecting Fake Accounts on Social Media," in Conference Paper · December 2018.
[3] Myo Myo Swe, Nyein Nyein Myo , "Fake Accounts Detection on Twitter Using Blacklist," in IEEE,June 2018
[4] Rohit Raturi, "Machine Learning Implementation for Identifying Fake Accounts in Social Network.," International Journal of Pure and Applied Mathematics and Volume 118 No. 20 2018, 4785-4797
[5] Cody Buntain, Jennifer Golbeck "Automatically Identifying Fake News in Popular Twitter Threads," in arXiv:1705.01613v2 [cs.SI] 30 May 2018
[6] S. P. Maniraj, Harie Krishnan G, Surya T, Pranav R, "Fake Account Detection using Machine Learning and Data Science," International Journal of Innovative Technology and Exploring Engineering ISSN: 2278-3075, Volume-9 Issue-1, November, 2019.
[7] Miss. Richa Ramesh Sharma, Prof. Yogesh S. Patil, Prof. Dinesh D. Patil "Twitter Spam Detection by Using Machine Learning Frameworks" International Journal of Innovative Research in Science, Engineering and Technology Vol. 8, Issue 5, May 2019
[8] Noha Y. Hassan,Wael H. Gomaa,Ghada A. Khoriba,Mohammed H. Haggag, "Credibility Detection in Twitter Using Word N-gram Analysis and Supervised Machine Learning Techniques," in INASS October 26, 2019. Revised: December 3, 2019
[9] Faiza Masood, GhanaAmmad ,Ahmad Almogren, "Spammer Detection and Fake User Identification on Social Networks," Digital Object Identifier 10.1109/ACCESS.2019.2918196



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY