**Fake Profiles Detection**

*A*

*Project Report*

*Submitted in partial fulfilment of the Requirements* *for the award of the Degree of*

**BACHELOR OFENGINEERING**

IN

**INFORMATION TECHNOLOGY**

**By**

**M. Charishma(1602-19-737-008)**

**M. Pranay Kumar Reddy(1602-19-737-027)**

**N. Rachel Reddy(1602-19-737-030)**

A picture containing diagram

Description automatically generated

**Department of Information Technology**

# **Vasavi College of Engineering (Autonomous)**

***ACCREDITED BY NAAC WITH 'A++' GRADE***

**(Affiliated to Osmania University)**

**Ibrahimbagh, Hyderabad-31**

**2021-22**

# **Vasavi College of Engineering (Autonomous)**

***ACCREDITED BY NAAC WITH 'A++' GRADE***

# **(Affiliated to Osmania University)**

# **Hyderabad-500 031**

**Department of Information Technology**

A picture containing diagram

Description automatically generated

**DECLARATION BY THE CANDIDATES**

We, **M. Charishma Reddy** , **M. Pranay Kumar Reddy**, **N. Rachel Reddy** bearing hall ticket number, **1602-19-737-008**, **1602-18-737-027**, **1602-18-737-030**, hereby declare that the project report entitled “**Fake Profiles Detection**” under the guidance of **Ms.L.Divya**, Assistant Professor, Department of Information Technology, Vasavi College of Engineering, Hyderabad, is submitted in partial fulfilment of the requirement of Mini project of V semester of **Bachelor of Engineering in Information Technology.**

This is a record of bonafide work carried out by us and the results embodied in this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

**M. Charishma Reddy**, (1602-19-737-008)

**M. Pranay Kumar Reddy**, (1602-19-737-027)

**N. Rachel Reddy**, (1602-19-737-030)

**Vasavi College of Engineering (Autonomous)**

***ACCREDITED BY NAAC WITH 'A++' GRADE***

**(Affiliated to Osmania University)**

**Hyderabad-500031**

A close-up of a sandwich

Description automatically generated with low confidence**Department of Information Technology**

**BONAFIDE CERTIFICATE**

This is to certify that the project entitled “**Fake Profiles Detection**” being submitted by **M. Charishma Reddy , M. Pranay Kumar Reddy, N. Rachel Reddy** bearing **1602-19-737-008**, **1602-19-737-027, 1602-19-737-030**, in partial fulfillment of the requirements for the completion of **Mini Project** of Bachelor of Engineering in Information Technology is a record of bonafide work carried out by them under my guidance.

# **ACKNOWLEDGEMENT**

I extend my sincere thanks to **Dr. S. V. Ramana**, Principal, Vasavi College of Engineering for his encouragement.

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them.

It is with utmost pleasure that we avail this opportunity to express our heartfelt gratitude to **Ms. L.Divya (Asst. Prof, IT),** our internal guide, under whose guidance we have finished this project successfully. Her constant guidance and willingness to share her vast knowledge made us understand this project and its manifestations in great depths and helped us to complete the work.

Finally, yet importantly, we would like to express our heartfelt thanks to our respected **Dr. K. Ram Mohan Rao (Prof. & HOD, IT)** who was very helpful in providing resources for the project.

We would like to thank all teaching and non teaching members of the Department of Information Technology, Vasavi College of Engineering for their generous help in various ways for the completion of this project.

**M.Charishma Reddy (1602-19-737-008)**

**M.Pranay Kumar Reddy (1602-19-737-027)**

**N.Rachel Reddy (1602-19-737-030)**

**Table of Contents:**

1.Abstract …6

2.Introduction …7

3.Literature Survey …8

4.Existing Method/System

4.1 Drawbacks …11

5.System Requirements and Specifications …12

6.Proposed Method/System …13

6.1Architecture …14

7.Implementation and Testing

7.1 Screenshots and Test cases …16

8.Results …17

9.Conclusion and Future Scope …19

10.References …20

**ABSTRACT**

In these modern days the usage of social media is at its peaks. The main negativity in social media is due to fake profiles, in this project we aim to identify those fake accounts.

The main motivation to the project comes from the people who struggle because of the abuses they face in social media platforms. These abuses and trolling are done by fake users.

We are trying to tackle this problem by using Machine Learning Algorithms.

**INTRODUCTION**

Many researchers around the world are working to find a feasible solution to the problem of online impersonation and the use of spam users. In this project, we intend to give a framework using machine learning techniques with which the detection of spam users can be done so that the social life of people can become a little more secure.

There were multiple instances wherein I read a review online for a movie or a restaurant which was not as suggested. These reviews are usually done by anonymous fake users reviewing places to promote it. This is a simple example that I have come across but there are similar issues where spam users spread false content online. This may also lead to harassment of a real user or try to retrieve account information of real users. These instances have been increasing day by day and thus require a solution.

**LITERATURE SURVEY**

With the widespread of Online Social Networks(OSNs), the privacy of the users involved in such services is becoming a major concern. Several researchers already proposed solutions to mitigate the privacy threat for those people having profiles in OSNs (which, for example, count more than 800 million for Facebook, one of the most popular OSN). As an example of such privacy-threat mitigation solutions, in [1] the authors proposed the concept of Virtual Private Social Network (VPSN). VPSN basically reflects the concept of Virtual Private Network (known in computer networks) within OSNs: only friends within the VPSN are able to see the real information of a person. Other people in the OSN, as well as the OSN manager, do not have the means to access the same information. Most of the work in the literature aimed at protecting the information the OSN is aware of—to be accessed only by the authorised people in an authorised way. For example, in [2] the authors show how an adversary might get access to the information that the victim shares in the profile, against the victim’s wishes. While the problem of protecting the privacy of the information that a real person put on the OSN has been at least already considered, we believe that too little attention has been put in protecting the privacy of the people that might not even use a specific OSN. In fact, an adversary willing to get private information of a victim might run a “social engineering” type of attack. As an example, one might create the profile of the victim, and then try to get private information of the victim, while interacting with the victim’s real friends connected to the fake profile. We refer to this malicious behaviour as a Fake Profile Attack (FPA). In [3], the authors first demonstrated the feasibility of mounting identity threat attacks on OSN with two variants: single OSN and cross-sites OSNs. In the first case, the victim already has a profile in the OSN where the adversary will create the clone profile. In cross-site OSNs, the victim does not have a profile in the same OSN where the attack is run, but the profile of the victim exists in other OSNs. In [4], the authors present a detection framework based on profiles similarities: attribute and friends network similarity. In [4], Facebook is considered to be the OSN where the adversary runs the attack. A similar approach was used in [5], considering Twitter as the target OSN. We underline that the current solutions for detecting leverage the assumption that a profile of the victim is available in some 9 OSN, which might not always be the case. Furthermore, if the OSN in which the attack is run and the one considered as a reference for similarity are not of the same type, we expect the performances of the detection solutions to be lower, compared to the case when considering, for example, the reference profile being the same OSN as the cloned one. In [4], authors already pointed out that their approach (measuring similarities) is very specific to the existence of an original profile where the victim already has a presence in. In fact, since there is no pre-existing profile, the similarity measurements and other techniques proposed so far for the detection of cannot be applied to FPA. Recently, another issue has been introduced, it concerns multiple identities in OSNs [6]. It proposes a framework for grouping similar identities which refer to the same person. We focus our study on characterising the behaviour of users, based on dynamic structural information of the OSN of the user. While static aspects of OSNs have been widely considered, less interest has been put so far in dynamic features. However, some investigation has already been made. For example, in [16] authors propose a way to evaluate the global structure of a large scale network by analysing microscopic behaviour of nodes in an OSN. Their model observes the edge-by-edge evolution of the graph by adopting the maximum-likelihood principle. Given a new node arrival in the graph, the creation of new edges is affected by the degree and age of the node. In [7], the authors get a macroscopic view of OSNs graph evolution. It studies OSN growth by evaluating the evolution of three types of groups: singletons, giant components, and the middle region. Other researchers [8] considered and combined two important features of OSNs: service recommendation and friendship prediction. The work shows a correlation between user-service interactions (interests networks) and the link between users (friendship network). However, none of these work leveraged dynamic features of OSNs for privacy purposes.

**4.EXISTING METHOD/SYSTEM:**

There is no proper application/algorithm which detects the fake profiles yet. There is a lot of research going on in this area.

We all know that the claim of Twitter is that it has only <5% of spam/bot users, which is evidently not true. And many discussions are happening on this issue.

4.1 DRAWBACKS:

Any user does not label himself as spam. So identifying spam users is purely based on human intuition which always may not be true.

**5**.**SYSTEM REQUIREMENTS**

**AND SPECIFICATIONS**

Operating System: Windows or Mac

Programming Language: Python

Web Development: Flask

Libraries used:

Numpy

Pandas

Matplotlib

Sklearn

**6. PROPOSED METHOD/ SYSTEM**

The proposed framework in Fig. 1 shows the sequence of processes that need to be followed for continued detection of fake profiles with active learning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by social networking companies.

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) (detailed discussed in chapter 5) is selected on which the classification algorithm is implemented.

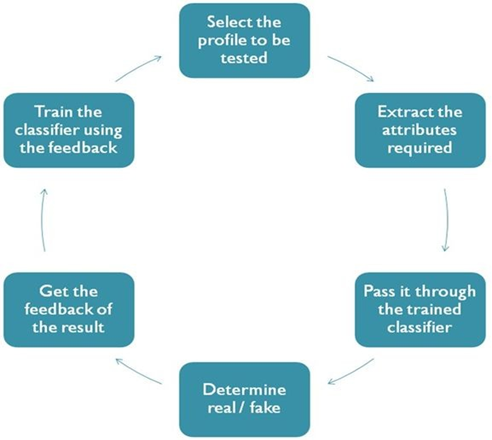
3. The attributes extracted are passed to the trained classifier. The classifier gets trained regularly as new training data is fed into the classifier.

4. The classifier determines whether the profile is spam or real.

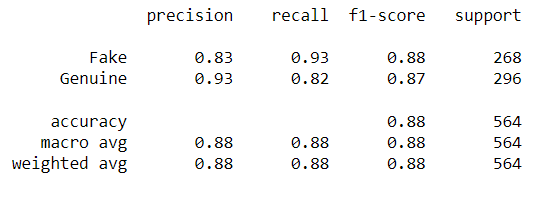
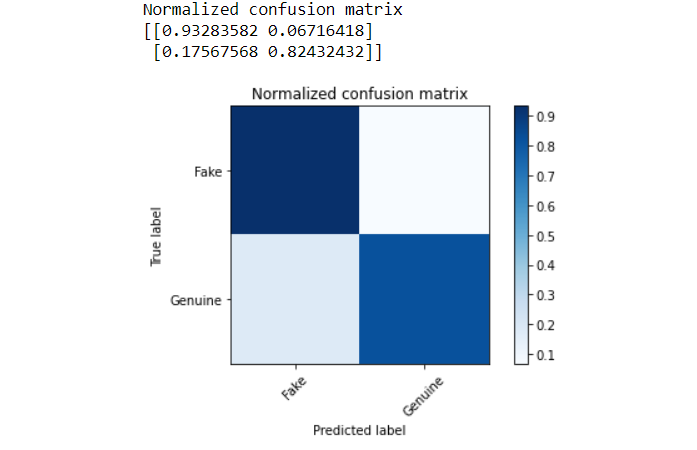
5. The classifier may not be 100% accurate in classifying the profile so; the feedback of the result is given back to the classifier. For example, if the profile is identified as spam, social networking sites can send a notification to the profile to submit identification. If the valid identification is given, feedback is sent to the classifier that the profile was not fake.

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.

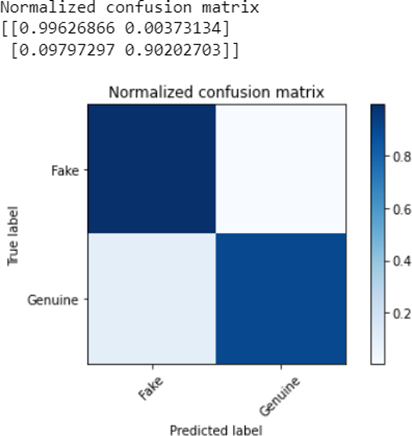
**6.1 PROPOSED ARCHITECTURE**

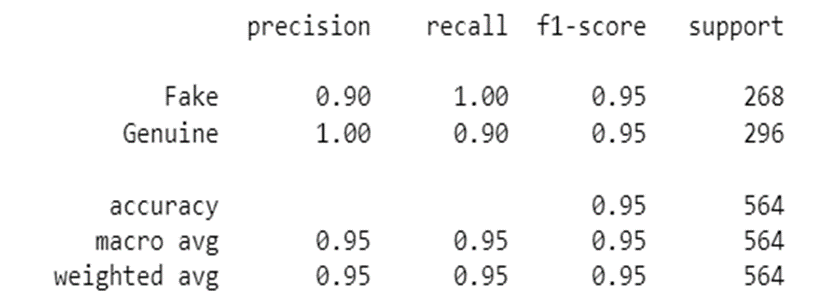


**IMPLEMENTATION AND TESTING:** Support Vector Machine:

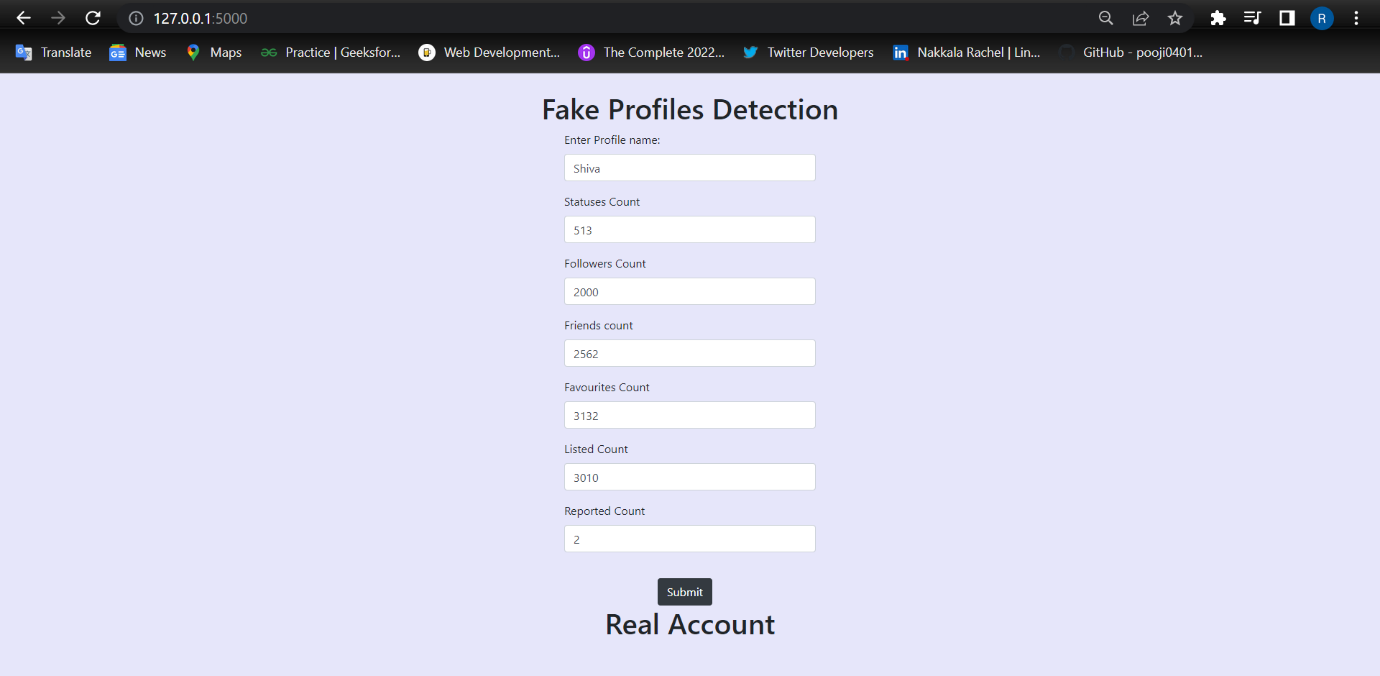


Random Forest:



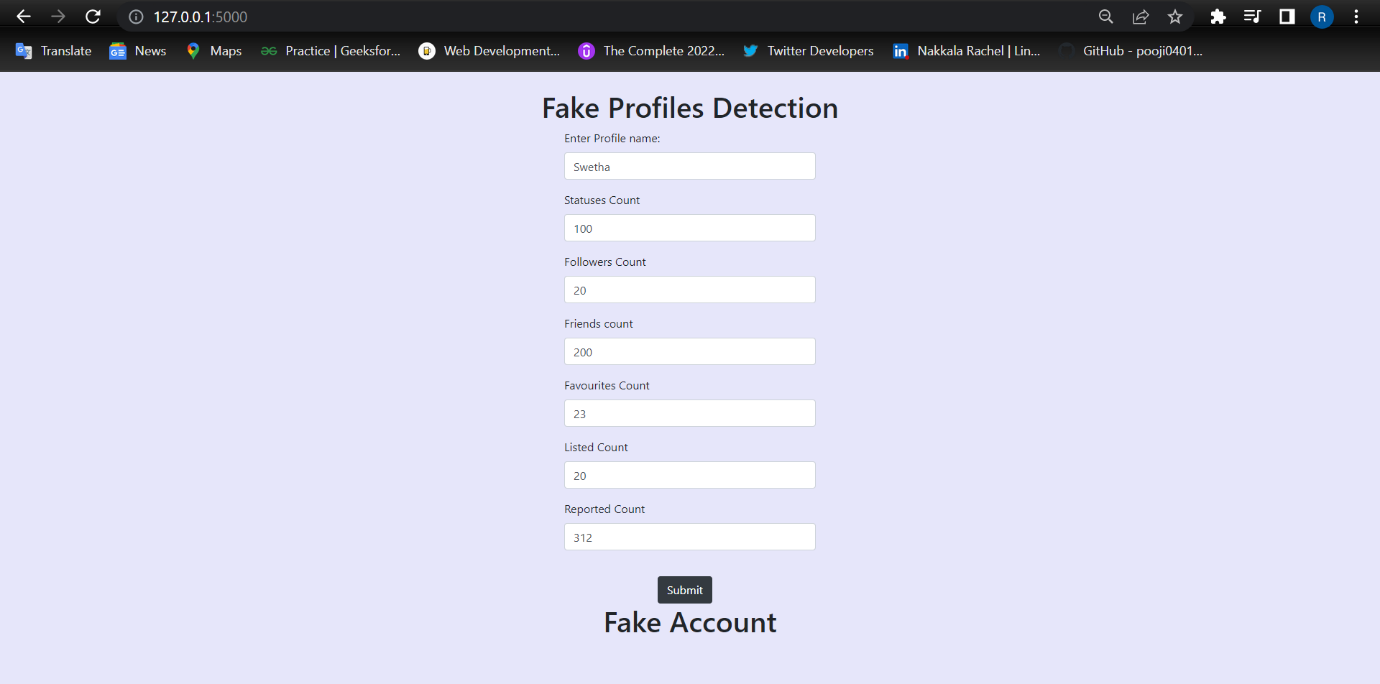


**RESULTS:**



In the above result, the followers count is 2000 and the friends count is 2562. From this we can say that he has almost 80% of his friends are following him back, so there are less chances that this is a fake account. The number of members listed him is far greater than the number of people reported him.

Hence the result is displayed as real account.



In this result, the followers count is 20 and friends count is 200. Here, only 10% of her friends are following her back which is a very low number. And there are chances that the account is created very recently, and this scenario took place.

Coming to the listed and reported count, reported count is far greater than the listed count which makes the account suspicious.

Hence the account is termed as Fake.

**CONCLUSION AND FUTURE WORK:**

In this application the datasets are taken from kaggle. We have extracted a few features and applied Support Vector Machine and Random Forest Algorithms. Random Forest algorithm gave more accuracy(90%).

In future we would like to take twitter data and extract more features, which would be more helpful/reliable.

**REFERENCES:**

1. Romanov, A., Semenov, A., Veijalainen, J.: Revealing fake profiles in social networks by longitudinal data analysis. In: 13th International Conference on Web Information Systems and Technologies, January 2017
2. . Nazir, A., Raza, S., Chuah, C.-N., Schipper, B.: Ghostbusting Facebook: detecting and characterizing phantom profiles in online social gaming applications. In: Proceedings of the 3rd Conference on Online Social Networks, WOSN 2010. USENIX Association, Berkeley, CA, USA, p. 1 (2010)
3. Adikari, S., Dutta, K.: Identifying fake profiles in Linkedin. Presented at the Pacific Asia Conference on Information Systems PACIS 2014 Proceedings (2014)
4. Stringhini, G., Kruegel, C., Vigna, G.: Detecting spammers on social networks. In: Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC 2010, pp. 1–9 (2010
5. . Ameena, A., Reeba, R.: Survey on different classification techniques for detection of fake profiles in social networks. Int. J. Sci. Technol. Manage. 04(01), (2015)