FAKE ACCOUNT CONTROL OVER SOCIAL MEDIA NETWORKS USING SUPERVISED MACHINE LEARNING ALGORITHMS

Dr. D.J Samatha Naidu Principal,Annamacharya PG College Of Computer Studies ,rajampet.
U. RAMARAJU, Student 4th Semester MCA,Annamacharya PG College Of Computer Studies,Rajampet.

ABSTRACT

- *Online Social Network (OSN) is a network hub where people with similar interests or real world relationships interact.*
- *Launch Fake profile is the creation of profile in the name of a person or a company which does not really exist in social media, to carry out malicious activities.*
- *Fake profiles are detected based on set of rules that can effectively classify fake and genuine profile.*
- *Using Artificial Neural Networks we are identifying whether given account details are from genuine or fake users.*
- *ANN algorithm will be trained with all previous users fake and genuine account data and then whenever we gave new test data then that ANN train model will be applied on new test data to identify whether given new account details are from genuine or fake users.*

Keyword: - Tungsten inert gas (TIG), 316 Stainless steel, penetration, Tensile strength.

1. INTRODUCTION

In 2017 Facebook reached a total population of 2.46 billion users making it the most popular choice of social media. Social media networks make revenues from the data provided by users. The average user does not know that their rights are given up the moment they use the social media network's service. Social media companies have a lot to gain at the expense of the user. Every time a user shares a new location, new photos, likes, dislikes, and tag other users in content posted, Facebook makes revenue via advertisements and data. More specifically, the average American user generates about $26.76 per quarter. That number adds up quickly when millions of users are involved. In today's digital age, the ever-increasing dependency on computer technology has left the average citizen vulnerable to crimes such as data breaches and possible identity theft. These attacks can occur without notice and often without notification to the victims of a data breach. At this time, there is little incentive for social networks to improve their data security. These breaches often target social media networks such as Facebook and Twitter.

RELATED WORK

- Sybil rank was designed in late 2012, to efficiently identify fake profiles through a ranking graph-based system[5]. The algorithm uses a seed selection method combined with early terminated random walks to propagate trust [5]. Its computational cost is measured in O (nlogn). Profiles are ranked according to the number of interactions, tags, wall posts, and friends over time. Profiles that have a high rank are considered to be real with fake profiles having a low rank in the system. Unfortunately, this technique was found to be mostly unreliable because it failed to take into account the possibility that real profiles can be ranked low and fake profiles can be ranked high. Sarode and Mishra proposed a different approach which is a sequence of steps to detect fake profiles [6]. They used the Facebook graph API tool to gain access to numerous profiles and wrote a script to extract the viewed information. Later on, this extracted information forms the attributes the classifier will use in their algorithm. First, the data is in JSON format, which is further parsed to a structured format (CSV) that is easier readable by machine learning techniques.

EXISTING WORK

In Existing system is similarity of attribute values from original and cloned profiles and the second method is based on the network relationships. A person who doubts that his profile has been cloned will be chosen as a victim A classification method for detecting fake accounts on Twitter. They have collected some effective features for the detection process from different research and have filtered and weighted them in first stage Malicious users create fake profiles to phish login information from unsuspecting users. A fake profile will send friend requests to many users with public profiles. These counterfeit profiles bait unsuspecting users with pictures of people that are considered attractive. Once the user accepts the request, the owner of the phony profile will spam friend requests to anyone this user is a friend. The fake profile's contents typically have links that lead to an external website where the damage happens. An unaware curious user clicking the bad link will damage their computer. The cost can be as simple as catching a virus to as bad as installing a rootkit turning the computer into a zombie. While Facebook has a rigorous screening to keep these fake accounts out, it only takes one fake profile to damage the computers of many.

PROPOSED WORK

To develop machine learning algorithms in predicting and detecting Fake profiles in Twitter. Fake profiles on set of rules that can effectively classify fake and genuine profiles. In our solution, we use machine learning, namely an artificial neural network to determine what are the chances that a friend request is authentic or not. Each equation at each neuron (node) is put through a Sigmoid function to keep the results between the interval of 0.0 and 1.0. At the output end, this could easily be multiplied by 100 to give us the possible percentage that it is a malicious request. Our solution would be only one deep neural network, meaning it only has a single hidden layer. Each input neuron would be a different, previously chosen feature of each profile converted into a numerical value (e.g., gender as a binary number, female 0 and male 1) and if needed, divided by an arbitrary number (e.g., age is always divided by 100) to minimize one feature having more influence on the result than the other. The neurons represent nodes.

4. SOFTWARE AND HARDWARE SPECIFICATIONS

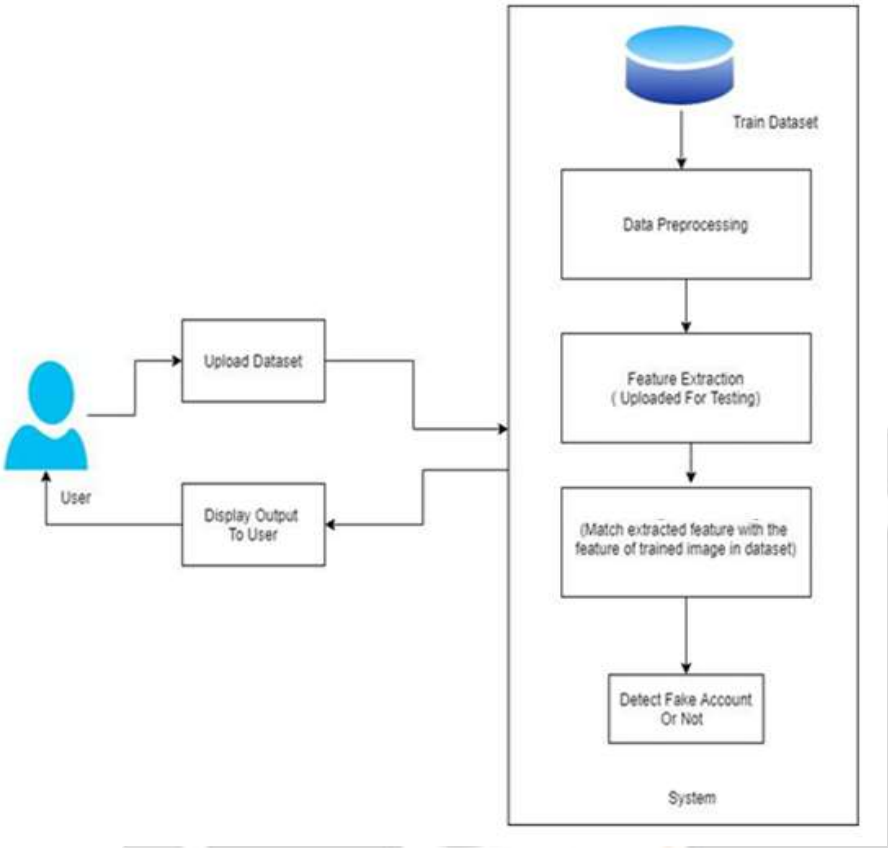
4.1 SOFTWARE REQUIREMENTS

Operating System	:	Windows 7/8/10
Coding Language	:	Python
Server	:	Wamp Server
Database	:	MYSQL

4.2 HARDWARE REQUIREMENTS

System	:	Pentium IV 2.4 GHz or More
Hard Disk	:	250 GB
RAM	:	4

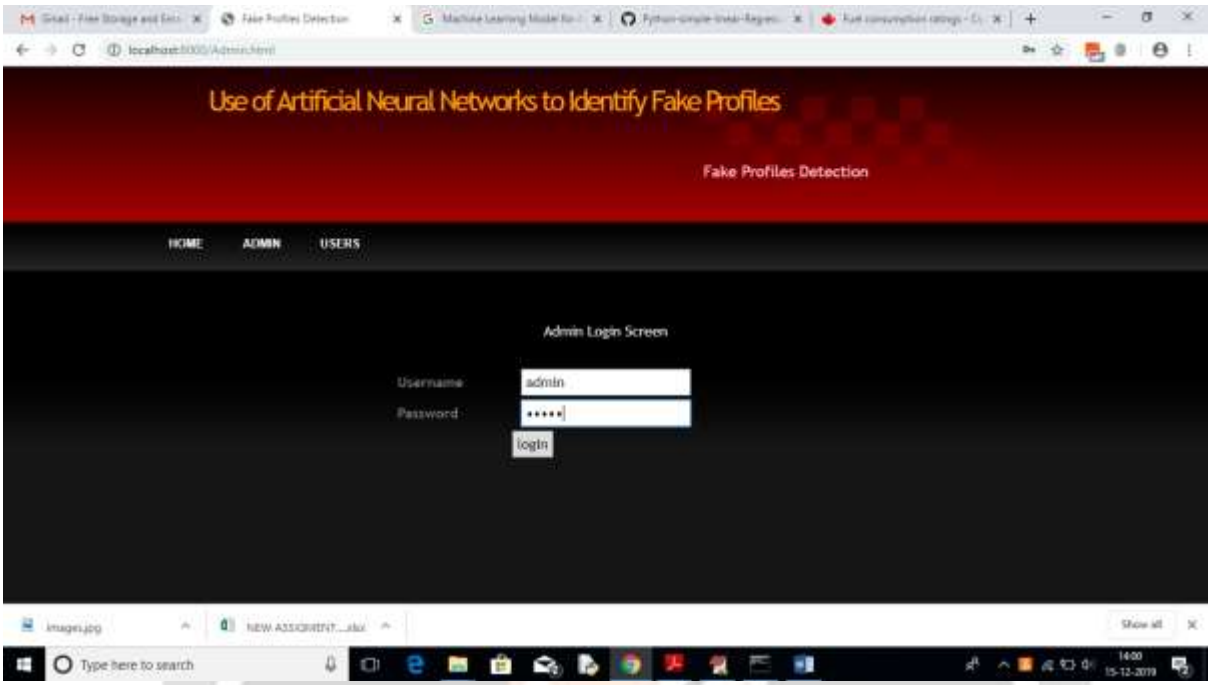
SYSTEM ARCHITECTURE:



9. SAMPLE SCREENS

Deploy this application on DJANGO server and then run in browser enter URL as 'http://localhost:8000/index.html' to get below screen

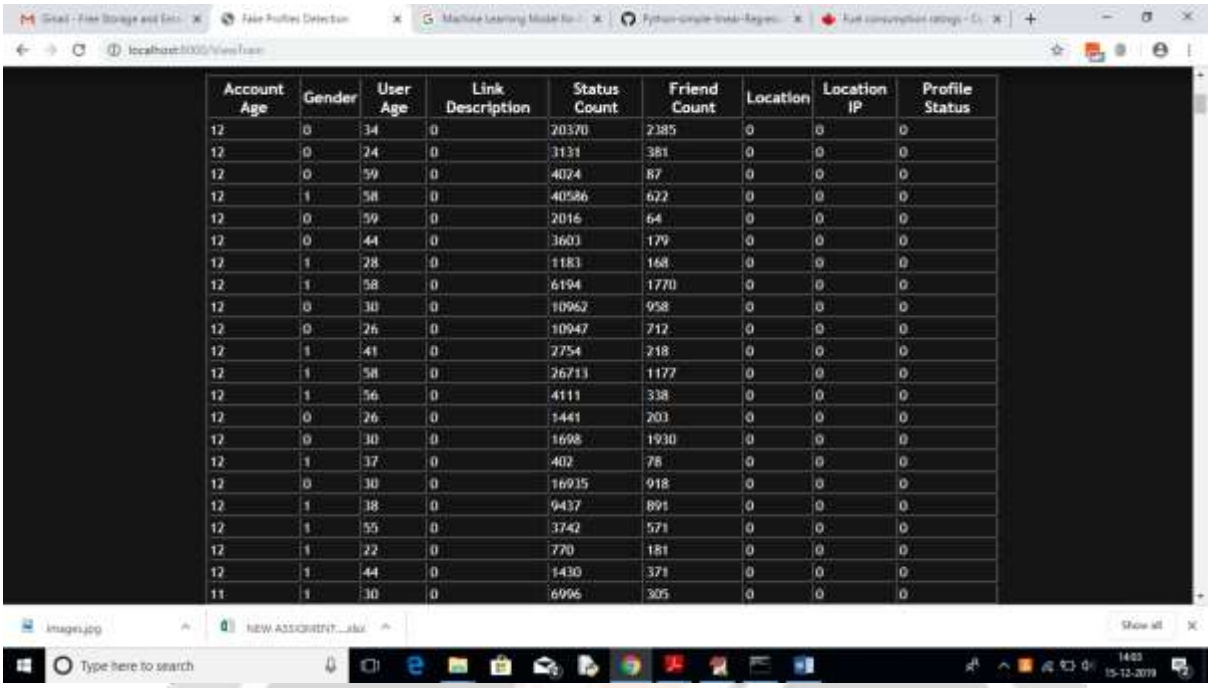
Screen 1: In above screen click on 'ADMIN' link to get below login screen



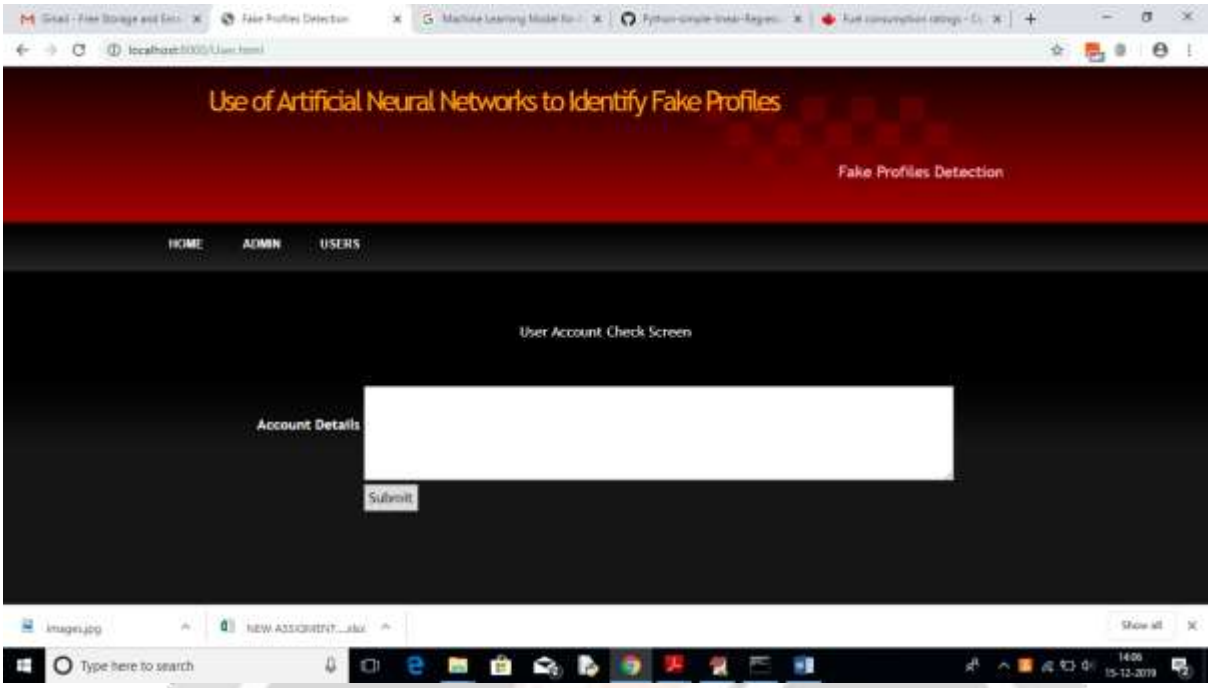
Screen 2:In above screen enter admin and admin as username and password to login as admin. After login will get below screen

Screen 3: In above screen click on 'Generate ANN Train Model' to generate training model on dataset. After clicking on that link you can see server console to check ANN processing details with accuracy.

Screen 3: In above screen click on 'Generate ANN Train Model' to generate training model on dataset. After clicking on that link you can see server console to check ANN processing details with accuracy

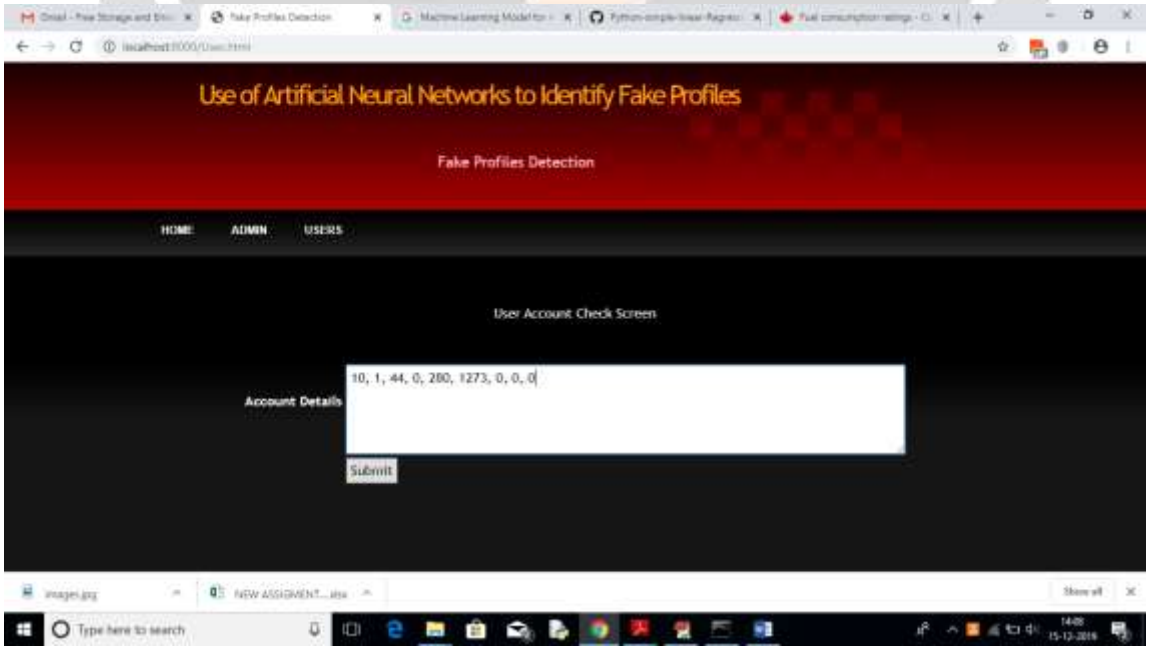


Account Age	Gender	User Age	Link Description	Status Count	Friend Count	Location	Location IP	Profile Status
12	0	34	0	20370	2385	0	0	0
12	0	24	0	3131	381	0	0	0
12	0	59	0	4024	87	0	0	0
12	1	58	0	40586	622	0	0	0
12	0	59	0	2016	64	0	0	0
12	0	44	0	3603	179	0	0	0
12	1	28	0	1183	168	0	0	0
12	1	58	0	6194	1770	0	0	0
12	0	30	0	10962	958	0	0	0
12	0	26	0	10947	712	0	0	0
12	1	41	0	2754	218	0	0	0
12	1	58	0	26713	1177	0	0	0
12	1	56	0	4111	338	0	0	0
12	0	26	0	1441	203	0	0	0
12	0	30	0	1698	1930	0	0	0
12	1	37	0	402	78	0	0	0
12	0	30	0	16935	918	0	0	0
12	1	38	0	9437	891	0	0	0
12	1	55	0	3742	571	0	0	0
12	1	22	0	770	181	0	0	0
12	1	44	0	1430	371	0	0	0
11	1	30	0	6996	305	0	0	0



Screen 7: In above screen enter some test account details to get prediction/identification from ANN. You can use below records to check

10, 1, 44, 0, 280, 1273, 0, 0
10, 0, 54, 0, 5237, 241, 0, 0
7, 0, 42, 1, 57, 631, 1, 1
7, 1, 56, 1, 66, 623, 1, 1



Screen 8: For above input will get below resul

10. CONCLUSION AND FUTURE SCOPE

We have given a framework using which we can identify fake profiles in any online social network by using ANN Algorithm with a very high efficiency as high as around 95%.

Fake profile Identification can be improved by applying ANN techniques and Neural Networks to process the posts and the profiles. In the future, we wish to classify profiles by taking profile pictures as one of the features.

In this Project, we use machine learning, namely an artificial neural network to determine what are the chances that a friend request is authentic are or not. Each equation at each neuron (node) is put through a Sigmoid function. We use a training data set by Facebook or other social networks. This would allow the presented deep learning algorithm to learn the patterns of bot behavior by backpropagation, minimizing the final cost function and adjusting each neuron's weight and bias. In this paper, we outline the classes and libraries involved. We also discuss the sigmoid function and how are the weights determined and used. We also consider the parameters of the social network page which are the most important to our solution.

10.2. FUTURE SCOPE

Each input neuron would be a different, previously chosen feature of each profile converted into a numerical value (e.g., gender as a binary number, female 0 and male 1) and if needed, divided by an arbitrary number (e.g., age is always divided by 100) to minimize one feature having more influence on the result than the other. The neurons represent nodes. Each node would be responsible for exactly one decision-making process

11. REFERENCES

[1] https://www.statista.com/topics/1164/social-networks/
[2] https://www.cnbc.com/2018/01/31/facebook-earnings-q4-2017- arpu.html
[3] https://www.cnet.com/news/facebook-breach-affected-50-millionpeople/
[4] https://www.facebook.com/policy.php
[5] Qiang Cao, Michael Sirivianos, Xiaowei Yang, and Tiago Pregueiro. 2012. Aiding the detection of fake accounts in large scale social online services. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (NSDI'12). USENIX Association, Berkeley, CA, USA, 15-15.
[6] Akshay J. Sarode and Arun Mishra. 2015. Audit and Analysis of Impostors: An experimental approach to detect fake profile in an online social network. In Proceedings of the Sixth International Conference on Computer and Communication Technology 2015 (ICCCT '15). ACM, New York, NY, USA, 1-8. DOI: https://doi.org/10.1145/2818567.2818568
[7] Devakunchari Ramalingam, Valliyammai Chinnaiah. Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, Volume 65, 2018, Pages 165-177, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2017.05.020.
[8] https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime
[9] pages.cs.wisc.edu/~bolo/shipyard/neural/local.html
[10] https://stackoverflow.com/