Vol 12, Issue 07, July/2021
ISSN NO:0377-9254

Fake Profile Identification in Online Social Networks Using ANN

AVULA MANOHAR [1], DR. S NAVEEN KUMAR [2]

[1]PG Scholar, Dept of MCA, Audisankara College of Engineering and **Technology (AUTONOMOUS), Gudur, AP, India.**

[2]Associate Professor, Dept of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

Abstract_ There is a notable make bigger in applied sciences these days.. Mobiles are turning into smart. Technology is related with on line social networks which has emerge as a section in each one's existence in making new pals and retaining buddies, their hobbies are regarded easier. But this amplify in networking on line make many troubles like faking their profile. — In this paper, we use computing device learning, particularly an synthetic neural community to determine what are the possibilities that Facebook buddy request is genuine or not. We additionally define the training and libraries involved. Furthermore, we talk about the sigmoid feature and how the weights are decided and used. Finally, we reflect on consideration on the parameters of the social community web page which are utmost necessary in the furnished solution.

1. INTRODUCTION

In 2017 Facebook reached a complete populace of 2.46 billion customers making it the most famous preference of social media [1]. Social media networks make revenues from the information supplied by means of users. The common consumer does now not recognize that their rights are given up the second they use the social media network's service. Social media corporations have a lot to obtain at the price of the user. Every time a person shares a new location, new photos, likes, dislikes, and tag different customers in content material posted, Facebook makes income by using classified ads and data. More specifically, the common American consumer generates about $26.76 per quarter [2]. That variety provides up rapidly when thousands and thousands of customers are involved. In trendy digital age, the ever-increasing dependency on pc technological know-how has left the common citizen prone to crimes such as statistics breaches and feasible identification theft. These assaults can show up barring observe and frequently besides notification to the victims of a facts breach. At this time, there is little incentive for social networks to enhance their statistics security. These breaches regularly goal social media networks such as Facebook and Twitter. They can additionally goal banks and different monetary institutions. There looks to be a newsworthy difficulty involving social media networks getting hacked each day. Recently, Facebook had a facts breach which affected about 50 million customers [3]. Facebook affords a set of in reality described provisions that

provide an explanation for what they do with the user's information [4]. The coverage does very little to forestall the consistent exploitation of protection and privacy. Fake profiles appear to slip via Facebook's built-in protection features. The different risks of non-public records being received for fraudulent functions is the presence of bots and pretend profiles. Bots are applications that can accumulate records about the person except the consumer even knowing. This manner is regarded as internet scraping. What is worse, is that this motion is legal. Bots can be hidden or come in the shape of a faux pal request on a social community web page to obtain get entry to to personal information. The answer introduced in this paper intends to focal point on the risks of a bot in the shape of a pretend profile on your social media. This answer would come in the structure of an algorithm. The language that we selected to use is Python. The algorithm would be capable to decide if a present day buddy request that a person receives on line is an proper individual or if it is a bot or it is a faux buddy request fishing for information. Our algorithm would work with the assist of the social media companies, as we would want a education dataset from them to instruct our mannequin and later confirm if the profiles are pretend or not. The algorithm should even work as a ordinary layer on the user's net browser as a browser plug-in.

2. LITERAURE SURVEY

Accounts in online social media have heaps of input data like name, sexual orientation, companions, devotees, preferences, area numbers. Half part of this input data are both of public and private. We have to use input that are public to know profiles which are phony for interpersonal organization as data from private is unavailable. In any case, on the off chance that our proposed plan is utilized by the interpersonal interaction organizations itself, at that point they can utilize the private data of the users to know not from abusing from security issues. Considered data is highlights for profiles to classify of phony and genuine profiles.

For detecting fake profiles we followed these steps:

1. Functions are to be selected after choice of attributes, the ataset of profiles which are already classified as fake or real are wanted for the schooling motive of the classification algorithm. We have used a publicly available dataset of 1337 fake customers and 1481 actual users which includes numerous attributes consisting of call, status count, number of friends, fans depend, favourites, languages regarded and so forth.

2. The selected attributes are extracted from profile for the purpose of type.

3. After this the dataset of fake and actual seasoned files are prepared. From this dataset, 80% of both seasoned files (authentic and pretend) are used to prepare a schooling dataset and 20% of both profiles are used to put together a testing dataset.

4. The schooling dataset is then fed to the classification set of rules. It learns from the education dataset and is predicted to offer correct elegance labels for the testing dataset.

5. The labels from the testing dataset are eliminated and are left for determination by the educated classifier.

6. The result of classification algorithm is shown in 4.4. we've got used two classification algorithms and have compared the efficiency of these algorithms. 7. The proposed structure in the figure 1 shows the succession of procedures that should be pursued for persistent location of phony profiles with dynamic gaining from the input of the outcome given by the arrangement calculation.

3. PROPOSED SYSTEM

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. We utilize Microsoft Excel to store old and new fake data profiles. The algorithm then stores the data in a data frame. This collection of data will be divided into a training set and a testing set. We would need a data set from the social media sites to train our model.

For the training set, the features that we use to determine a fake profile are Account age, Gender, User age, Link in the description, Number of messages sent out, Number of friend requests sent out, Entered location, Location by IP, Fake or Not. Each of these parameters is tested and assigned a value. For example, for the gender parameter if the profile can be determined to be a female or male a value of (1) is assigned to the training set for Gender. The same process is applied to other parameters. We also use the country of origin as a factor We then determine the Number of messages sent out parameter by dividing the number of messages sent by the age of the account. We then determine the Number of friend requests sent out parameter by dividing the Number of friend computing and used primarily for multi-dimensional matrix multiplication as we are dealing with a large amount of numbers that are very dependent on each other.

3.1 IMPLEMENTATIONS

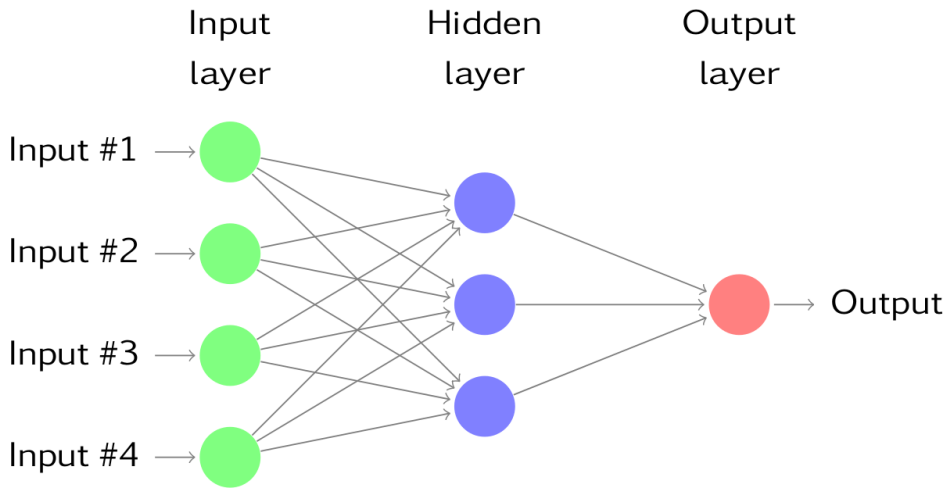
ANN algorithms Details

To demonstrate how to build a ANN neural network based image classifier, we shall build a 6 layer neural network that will identify and separate one image from other. This

network that we shall build is a very small network that we can run on a CPU as well. Traditional neural networks that are very good at doing image classification have many more parameters and take a lot of time if trained on normal CPU. However, our objective is to show how to build a real-world convolutional neural network using TENSORFLOW.

Neural Networks are essentially mathematical models to solve an optimization problem. They are made of neurons, the basic computation unit of neural networks. A neuron takes an input (say x), do some computation on it (say: multiply it with a variable w and adds another variable b) to produce a value (say; z= wx + b). This value is passed to a non-linear function called activation function (f) to produce the final output (activation) of a neuron. There are many kinds of activation functions. One of the popular activation function is Sigmoid. The neuron which uses sigmoid function as an activation function will be called sigmoid neuron. Depending on the activation functions, neurons are named and there are many kinds of them like RELU, TanH.

If you stack neurons in a single line, it's called a layer; which is the next building block of neural networks. See below image with layers



To predict image class multiple layers operate on each other to get best match layer and this process continues till no more improvement left.

Module Details:

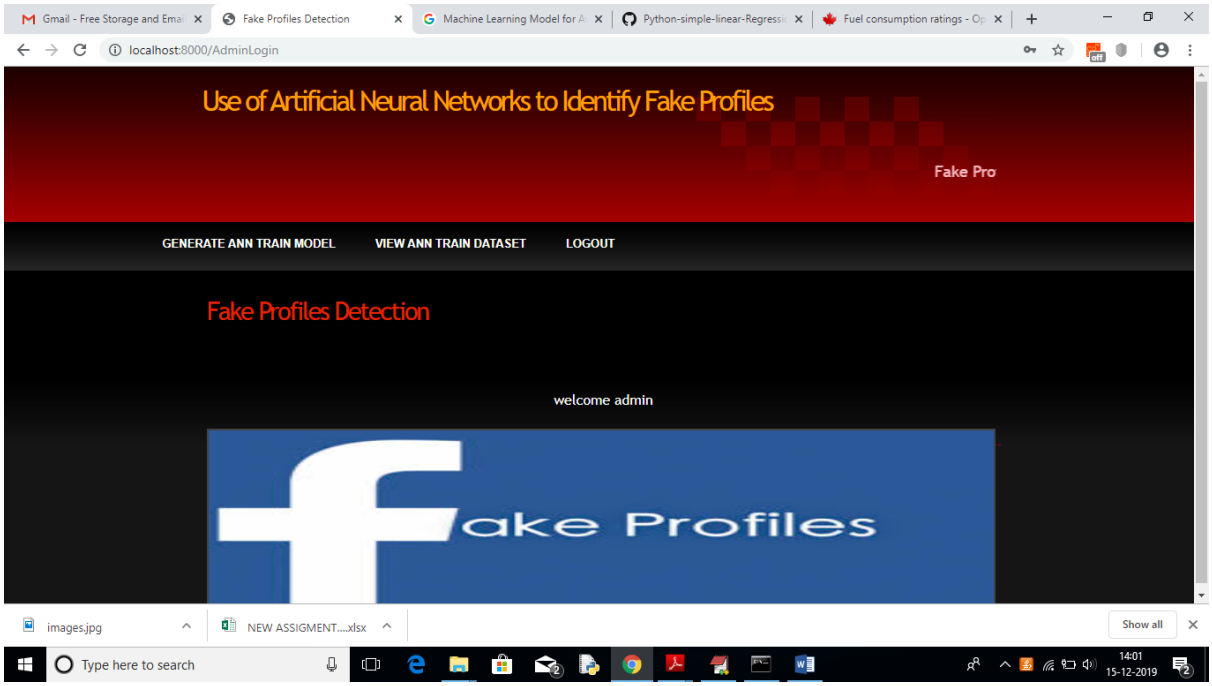
Admin Module: Admin will login to application by using username as 'admin' and password as 'admin' and then perform below actions.

a) Generate ANN Train Model: Admin will upload profile dataset to ANN algorithm to build train model. This train model can be used to predict fake or genuine account by taking new account test data.

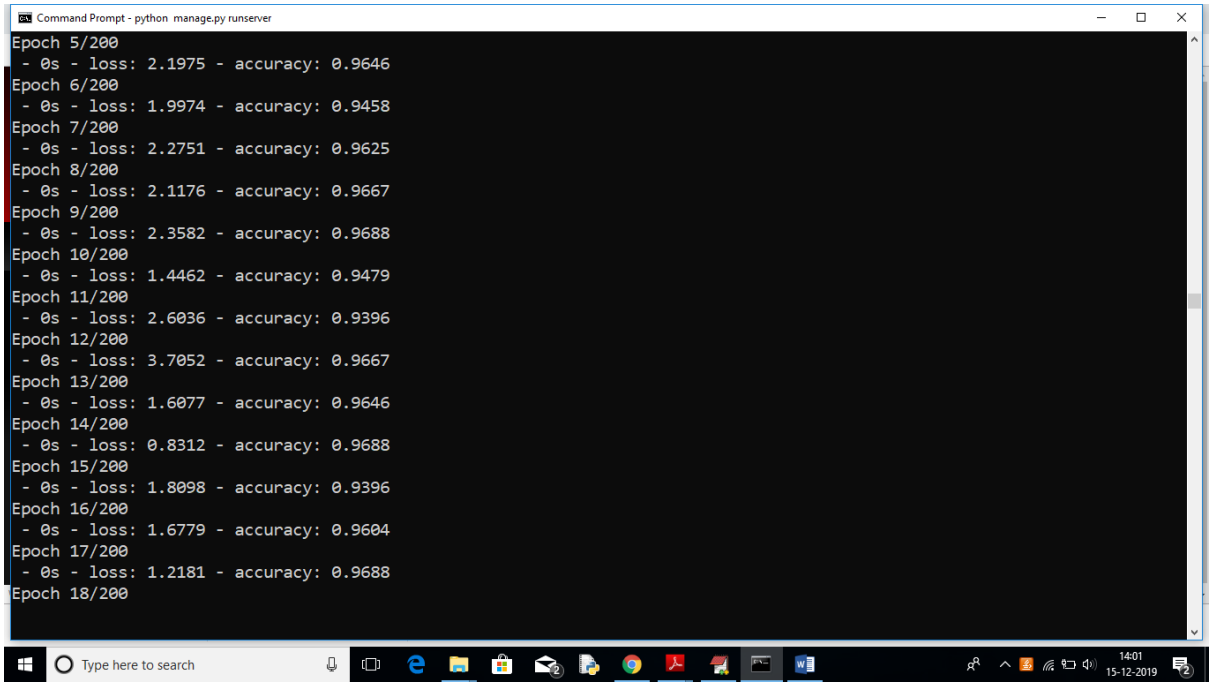
b) View ANN Train Dataset: Using this module admin can view all dataset used to train ANN model.

User Module: Any user can use this application and enter test data of new account and call ANN algorithm. ANN algorithm will take new test data and applied train model to predict whether given test data contains fake or genuine details.

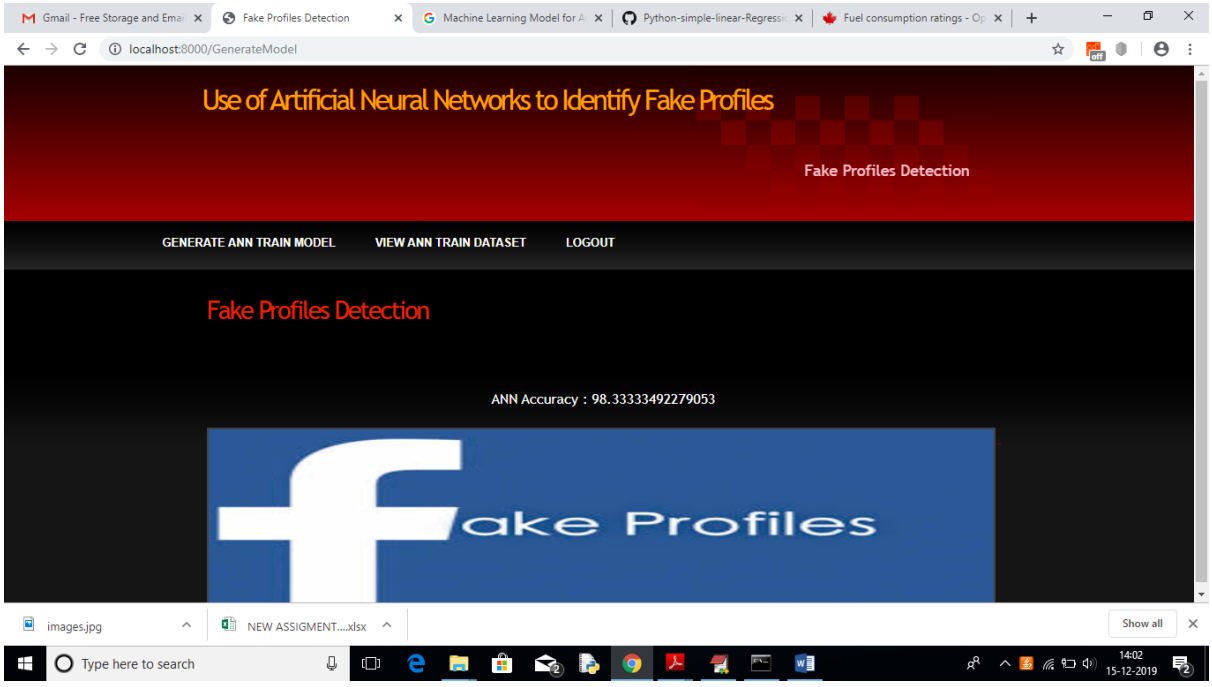
4. RESULTS AND DISCUSSIONS



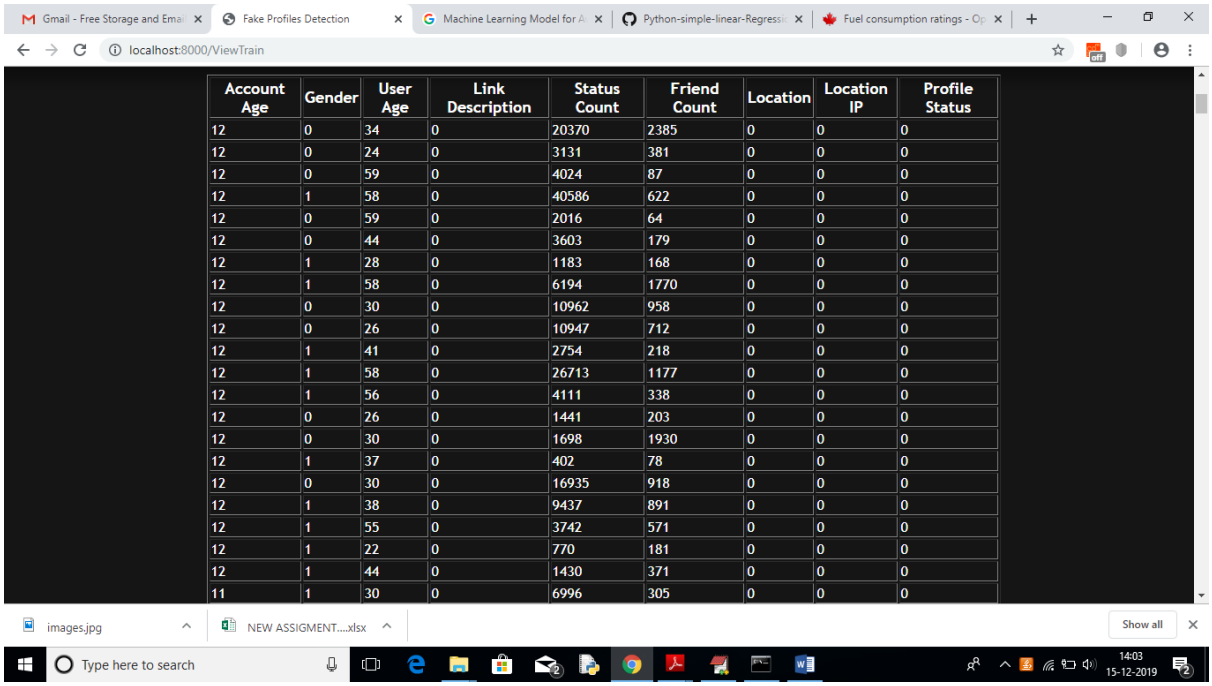
In above screen click on 'Generate ANN Train Model' to generate training model on dataset. After clicking on that link you can see server console to check ANN processing details with accuracy



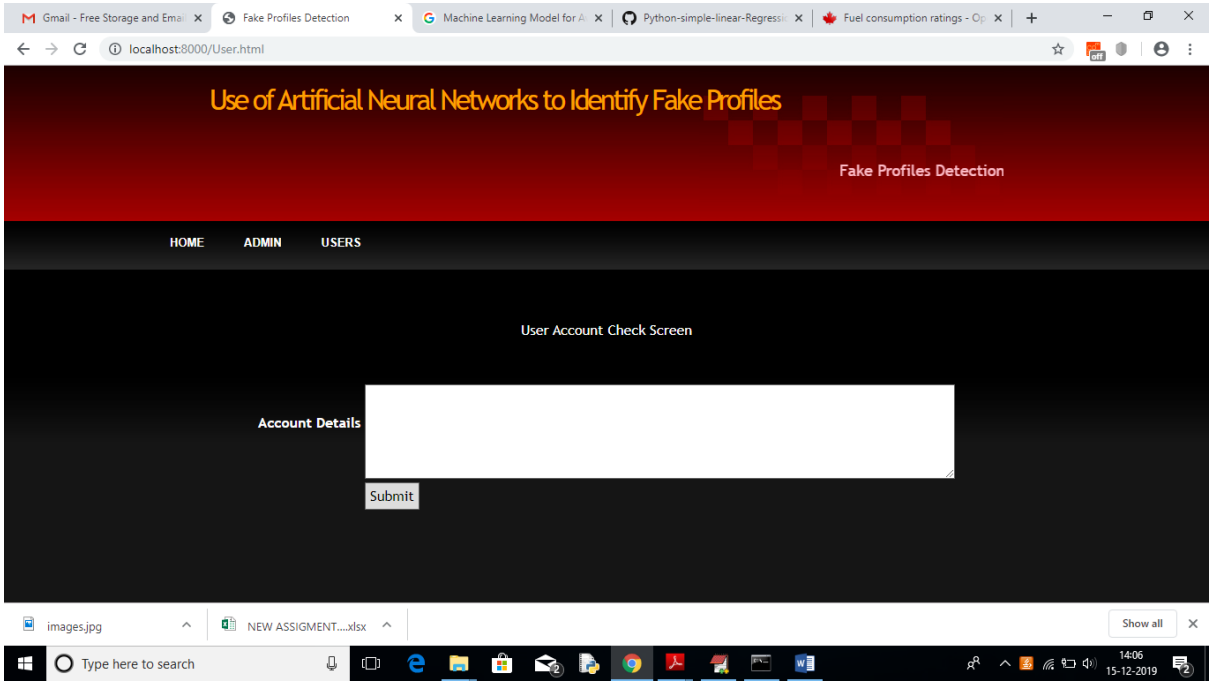
In above black console we can see all ANN details.



In above screen we can see ANN got 98% accuracy to train all Facebook profile. Now click on 'View Ann Train Dataset' link to view all dataset details

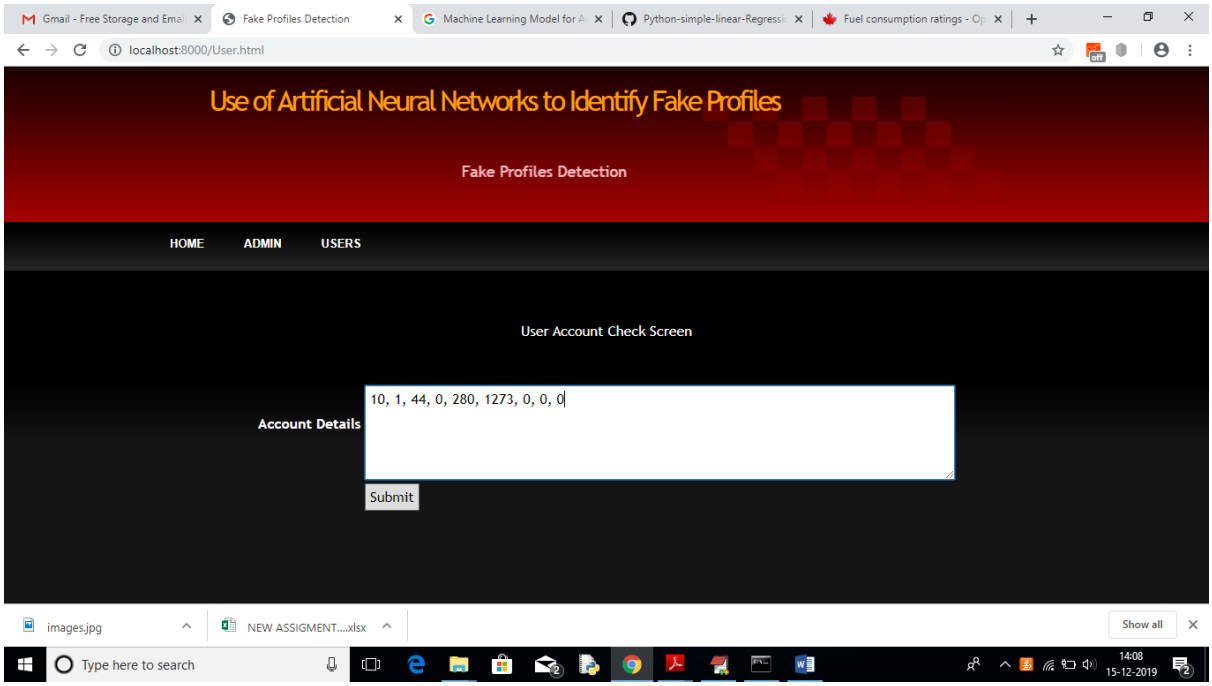


In above screen we can see all train data and scroll down to view all records. Now ANN train model is ready and you can logout and click on 'User' link to get below screen.

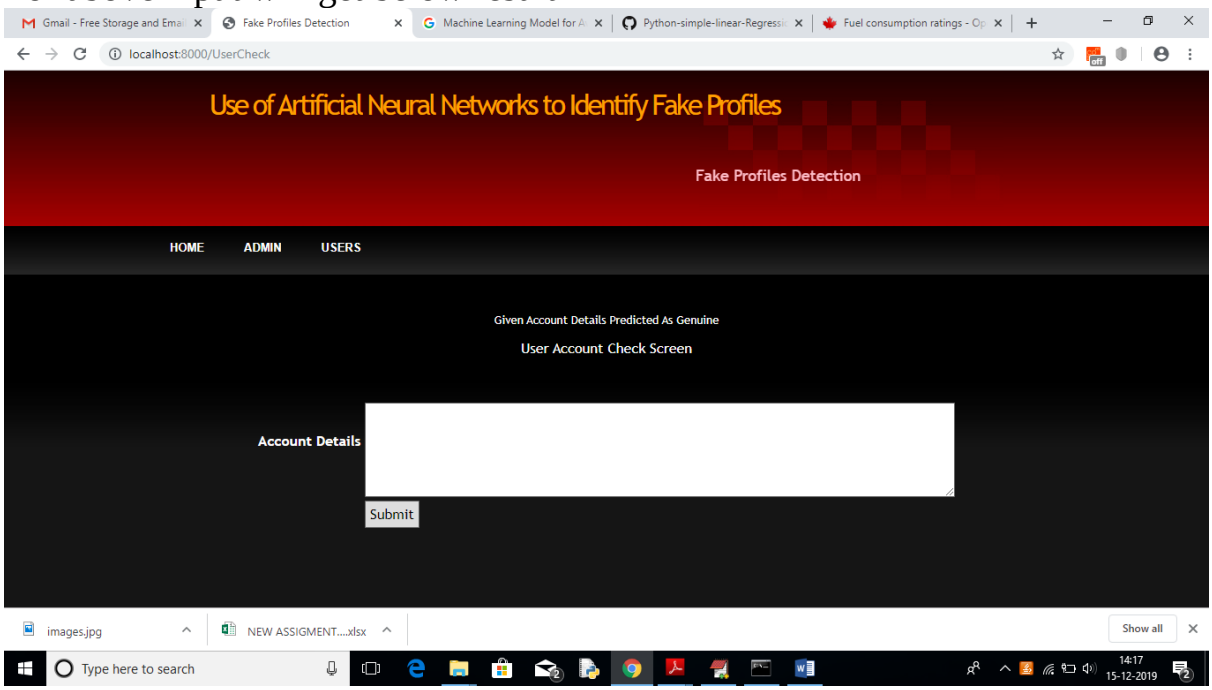


In above screen enter some test account details to get prediction/identification from ANN. You can use below records to check

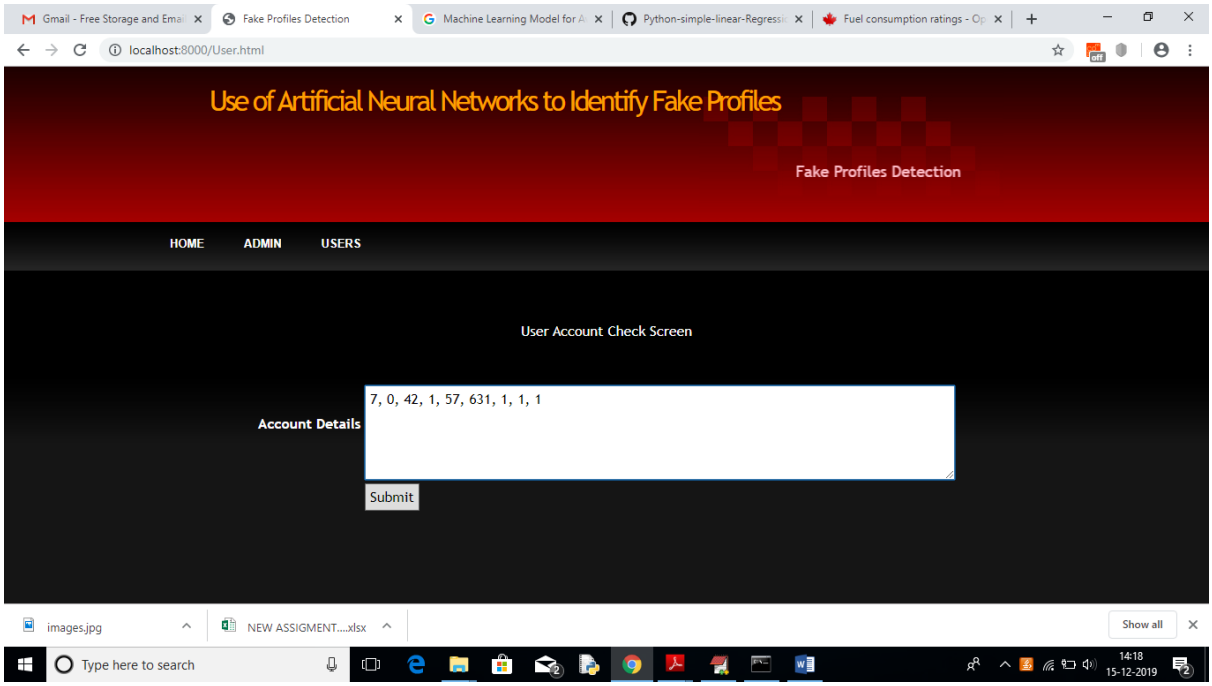
10, 1, 44, 0, 280, 1273, 0, 0
10, 0, 54, 0, 5237, 241, 0, 0
7, 0, 42, 1, 57, 631, 1, 1
7, 1, 56, 1, 66, 623, 1, 1



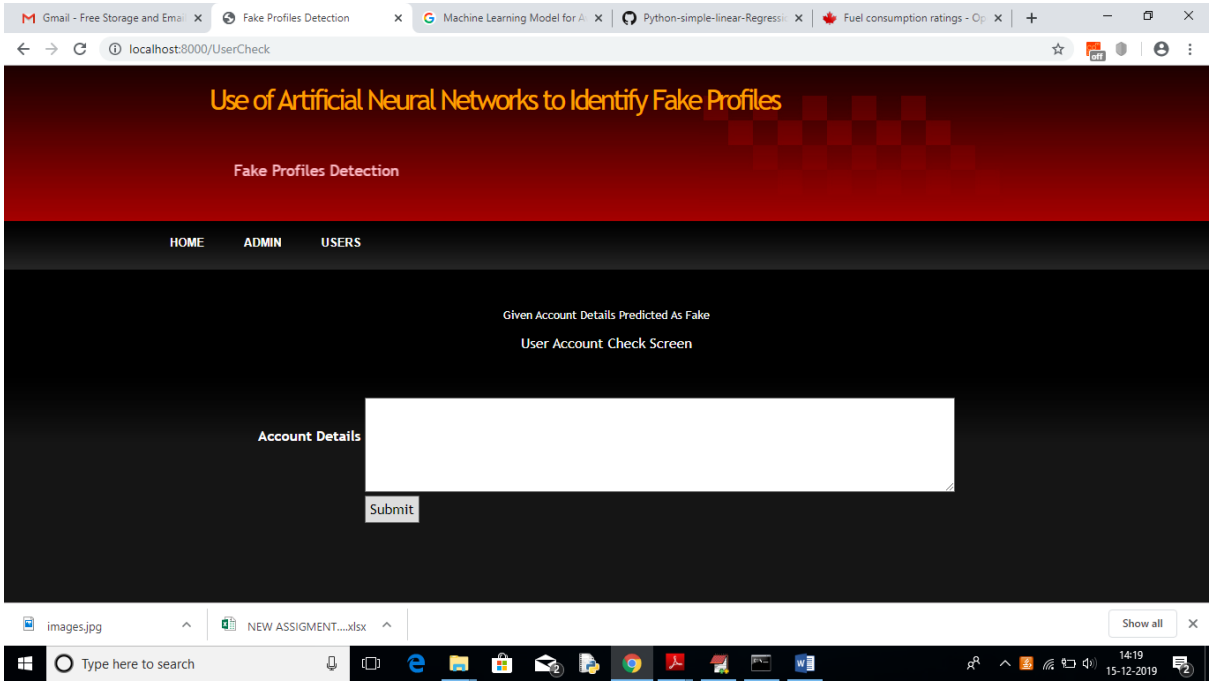
For above input will get below result



In above screen we can see the result predicted as genuine account



For above account details we got below result



In above screen we got result as fake for given account data

5. CONCLUSION

In this paper, we use desktop learning, particularly an synthetic neural community to decide what are the possibilities that a buddy request is actual are or not. Each equation at every neuron (node) is put via a Sigmoid function. We use a education records set by using Facebook or different social networks. This would enable the introduced deep gaining

knowledge of algorithm to research the patterns of bot conduct with the aid of backpropagation, minimizing the last value feature and adjusting every neuron's weight and bias. In this paper, we define the lessons and libraries involved. We additionally talk about the sigmoid characteristic and how are the weights decided and used. We additionally think about the parameters of the social community web page which are the most necessary to our solution..

6.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/questions/40758562/can-anyone-explain-mestandardscaler

[11] https://pandas.pydata.org

[12] https://www.tutorialspoint.com/python_pandas/index.htm

[13] http://www.numpy.org

[14] https://www.mathworks.com/products/matlab.html

[15] http://www.deeplearning.net/software/theano/

[16] https://scikit-learn.org/stable/

[17] https://keras.io

[18] https://www.tensorflow.org

Author's Profile:

AVULA MANOHAR has Pursuing his MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, affiliated to JNTUA in 2021. Andhra Pradesh, India.

DR. NAVEEN KUMAR. S has received him M.Tech degree in CSE from Sri Venkateswara University in 2014, Tirupati and PhD in CSE from Annamalai University in 2019 respectively. He is dedicated to teaching field from the last 2 years. He has guided P.G and U.G students. Him research areas included Artificial Intelligence, Network Security and Machine Learning. At present he is working as Associate Professor in Audisankara College of Engineering and Technology, Gudur, Nellore(Dt), Andhra Pradesh, India.