International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 9 ǁ September 2022 ǁ PP. 122-129

Fake Profile Identification in Large Scale Online Networks Using Ann

Dr. S Naveen Kumar[1], Sk. Kousar[2]

[1]Associate Professor, Dept. of CSE, Audisankara College of Engineering andTechnology (AUTONOMOUS), Gudur, AP, India,
[2] PG Scholar, Dept of MCA, Audisankara College of Engineering andTechnology(AUTONOMOUS), Gudur, AP, India.

Abstract
These days, applied sciences have undergone a noticeable expansion. Smart phones are evolving. Online social networks are linked to technology and have become an integral partof everyone's life, making it simpler for them to maintain friendships and make new ones, as well as pursue their hobbies. However, this increase in online networking creates problems like people fabricating their profiles. In this study, we employ computer learning, in particular a synthetic neural network, to assess the likelihood that a Facebook friend request is real or not. We also outline the associated training and libraries. We also discuss the sigmoid feature and how the weights are chosen and applied. Finally, we analyse the social community website parameters that are absolutely essential to the provided solution.

Date of Submission: 25-08-2022 Date of acceptance: 09-09-2022

I. INTRODUCTION

Facebook became the most well-known social media platform in 2017 after reaching a total population of 2.46 billion users [1]. Users' information is used by social media networks to generate cash. The average customer is increasingly unaware that when they utilise the service of a social media network, their rights are forfeited. At the expense of the user, social media companies have a lot to gain. Facebook generates revenue utilising classified advertisements and user data for each time someone publishes a new location, new photo, their likes and dislikes, and tags other users in uploaded content. The average American consumer produces roughly $26.76 every quarter, to be more precise [2]. When tens of thousands of customers are engaged, that variation quickly runs out. In the modern digital age, the growing reliance on computer technology has made the average person more vulnerable to crimes like data breachesand potential identity theft. These assaults may occur without being seen and usually without warning to the victims of a data breach. Social networks now have little need to improve the security of their statistics. Social media platforms like Facebook and Twitter are frequently the target of these attacks. Banks and other financial institutions are another possible target. Social media networks getting hacked seems to be a newsworthy problem every day. A recent data breach at Facebook affected roughly 50 million users [3]. Facebook provides a variety of actual mentioned features that Give a justification for how they utilize the user's data [4]. The coverage does absolutely little to stop the ongoing abuse of privacy and protection. The built- in security measures on Facebook seem to allow fake profiles to go through.

The existence of bots and fake profiles is one of the several concerns associated with non- public records being used for fraudulent purposes. Bots are programmes that can gather information on a person without the user even being aware of it. This practice is known as web scraping. [5] Even worse, this motion is legitimate. On a social network website, bots can be disguised or appear as a fake friend request to get access to personal data. The solution offered in this essay focuses on the dangers of a bot that appears as a fake profile on your social network. This response would have an algorithmic framework. We decided to utilize Python as our language. The system would be able to determine if a modern friend request received online is coming from a legitimate person, a machine, or a fake buddy request that is gathering information. As we would need a training dataset from the social media firms to educate our mannequin and afterwards verify whether the accounts are fake or real, our algorithm would function with their assistance [6]. The method should even function as a standard layer and browserplug-in on the user's web browser.

II. LITERATURE SURVEY

[8] Accounts in online social media have heaps of input data like name, sexual orientation,

companions, devotees, preferences, and area numbers. Half part of this input data are both ofpublic and private. We have to use inputs that are public to know profiles which are phonyfor 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 abusingfrom 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 dataset 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.

III. PROPOSED SYSTEM

To identify whether a friend request is genuine or not, we leverage machine learning in our approach, namely an artificial neural network. To keep both old and new phone data profiles, we use Microsoft Excel. The data is subsequently kept by the algorithm in a data frame. A training set and a testing set will be created from this data collection. To train our model, we would want a collection of data from the social media platforms. The attributes we use for the training set for determining if a profile is false are the following: Account age, Gender, User age, Link in the description, Number of messages exchanged, Number of friend requests sent, Entered location, Location by IP, and Fake or Not. Each of these variables is evaluated before being given a value. For the gender parameter, for instance, a value of (1) is assigned to the training set for Gender if it can be identified whether the profile is a female or a man. Other metrics are subjected to the same procedure. 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 dependenton each other.

IV. IMPLEMENTATIONS

The ANN algorithms We will construct a 6-layer neural network that will distinguish between one image and another in order to show how to construct an ANN-based imageclassifier. This We are going to construct a very modest network that we can also run on a CPU. Traditional neural networks that are excellent at classifying images have many more parameters and need a lot of training time on a standard CPU. However, our goal is to demonstrate how to use TENSORFLOW to create a convolutional neural network in the real world. In essence, neural networks are mathematical models that may be used to address optimization issues. Neurons, the fundamental computational component of neural networks, make them up. A neuron processes an input (let's say x) and outputs a value (let's say z= wx + b) by multiplying it by a variable (let's say w) and adding another variable (let's say b). To create the final output (activation) of a neuron, this value is transferred to a non-linear function called the activation function (f). The many activationfunctions are varied. Sigmoid is a well-liked activation function. The term "sigmoidneuron" refers to a neuron that utilises the sigmoid function as an activation function. There are several other types of neurons, including RELU and TanH, that have names based on their activation roles.

The next building component of neural networks is a layer, which is formed by stacking neurons in a single line. View the layered picture below.

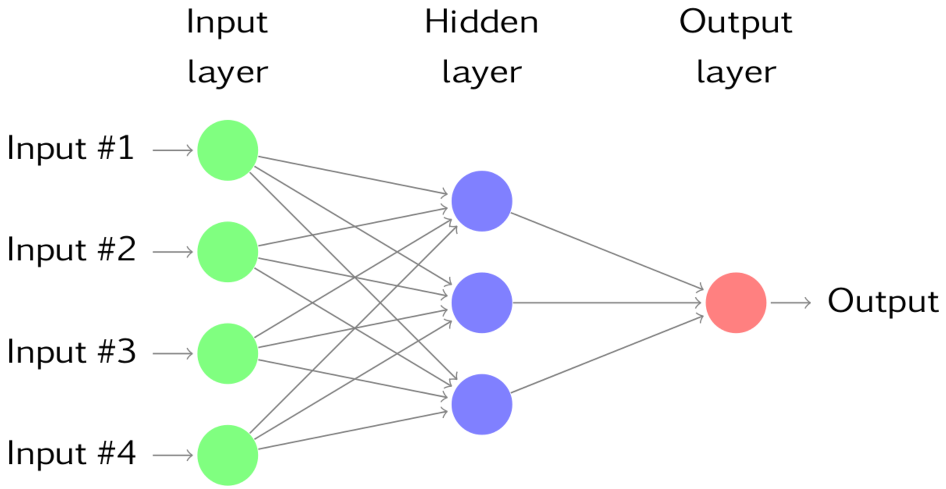


Fig. 1: Convolutional Neural Network

Multiple layers work together to find the best match layer when predicting the picture class and this process is repeated until there is no more room for improvement.

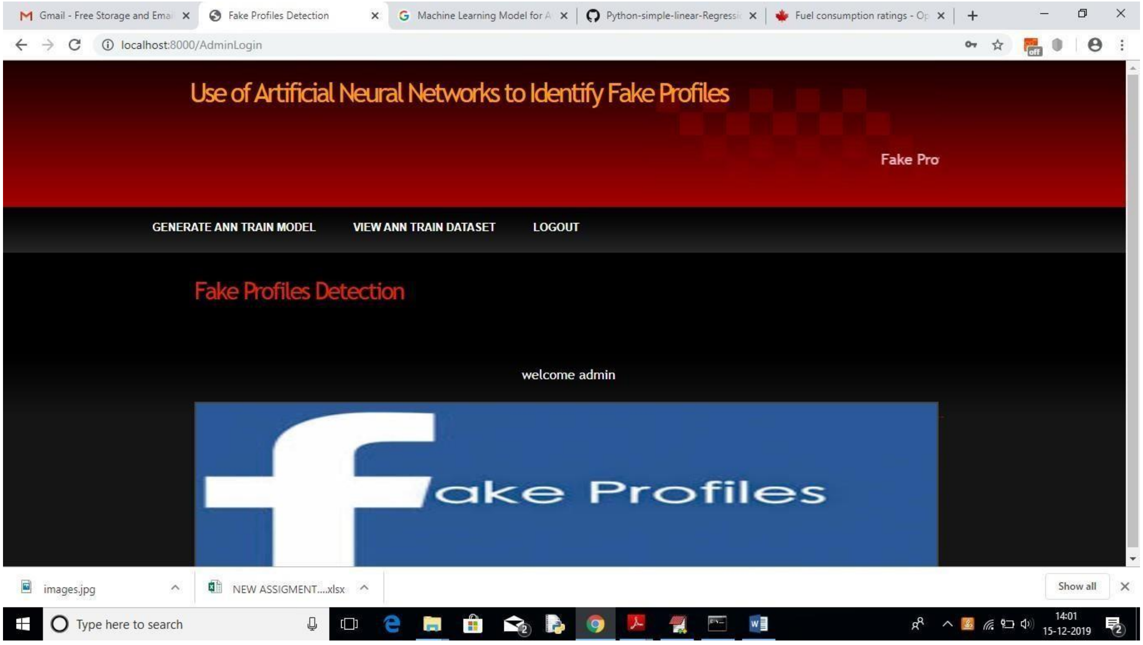
Module specifics:
The administrator will log in to the programme using the credentials "admin" and "admin" andthen take the following actions.

a) Create an ANN train model by uploading the profile dataset to the ANN algorithm. By usingdata from new account testing, this train model may be used to determine if an accountis phoney or real.

b) Access the ANN Train Dataset: The admin may view all the datasets used to train the ANNmodel by using this module.

Any user may access this programme, enter test data for a new account, and invoke the ANN algorithm. To determine if the provided test data contains bogus or real information, the ANNalgorithm will use new test data and a trained model.

V. RESULTS AND DISCUSSIONS

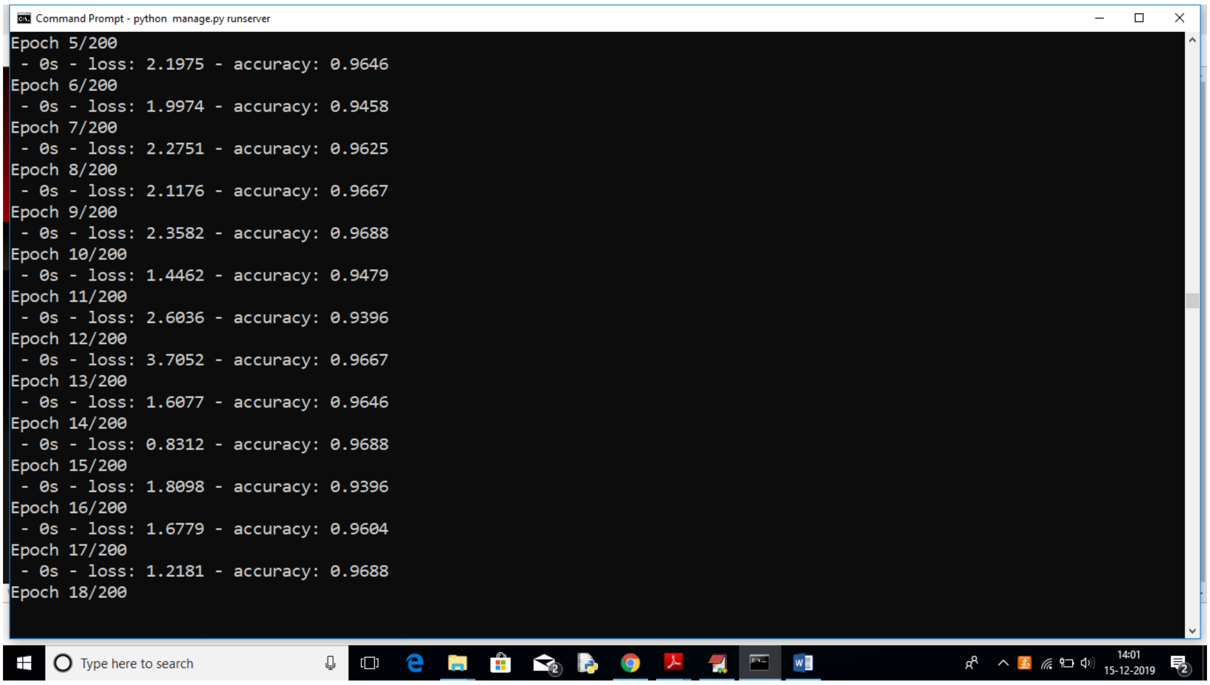

Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

welcome admin

Fig. 2: **Generation of ANN Train Model**

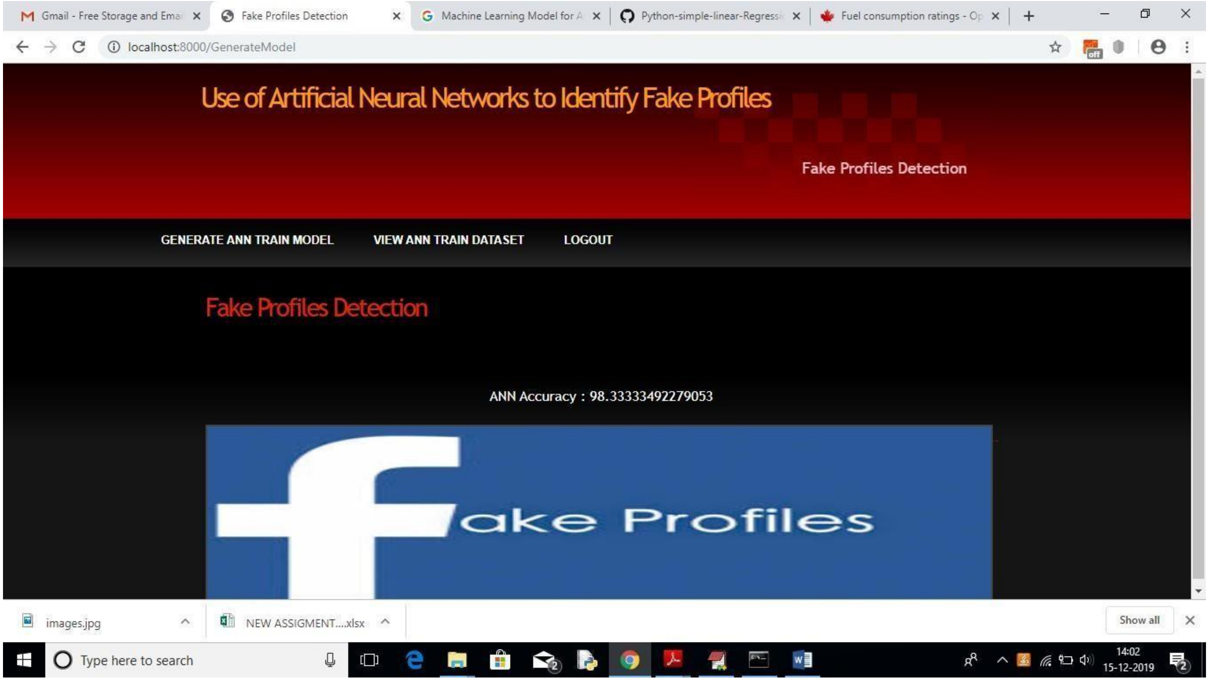
In above screen click on ‘Generate ANN Train Model’ to generate training model on dataset. After clicking on that link you can see server console to check ANN processing details with accuracy



```
Epoch 5/200
 - 0s - loss: 2.1975 - accuracy: 0.9646
Epoch 6/200
 - 0s - loss: 1.9974 - accuracy: 0.9458
Epoch 7/200
 - 0s - loss: 2.2751 - accuracy: 0.9625
Epoch 8/200
 - 0s - loss: 2.1176 - accuracy: 0.9667
Epoch 9/200
 - 0s - loss: 2.3582 - accuracy: 0.9688
Epoch 10/200
 - 0s - loss: 1.4462 - accuracy: 0.9479
Epoch 11/200
 - 0s - loss: 2.6036 - accuracy: 0.9396
Epoch 12/200
 - 0s - loss: 3.7052 - accuracy: 0.9667
Epoch 13/200
 - 0s - loss: 1.6077 - accuracy: 0.9646
Epoch 14/200
 - 0s - loss: 0.8312 - accuracy: 0.9688
Epoch 15/200
 - 0s - loss: 1.8098 - accuracy: 0.9396
Epoch 16/200
 - 0s - loss: 1.6779 - accuracy: 0.9604
Epoch 17/200
 - 0s - loss: 1.2181 - accuracy: 0.9688
Epoch 18/200
```

Fig. 3: **Consolidated Details of ANN**

In above black console we can see all ANN details.



Use of Artificial Neural Networks to Identify Fake Profiles

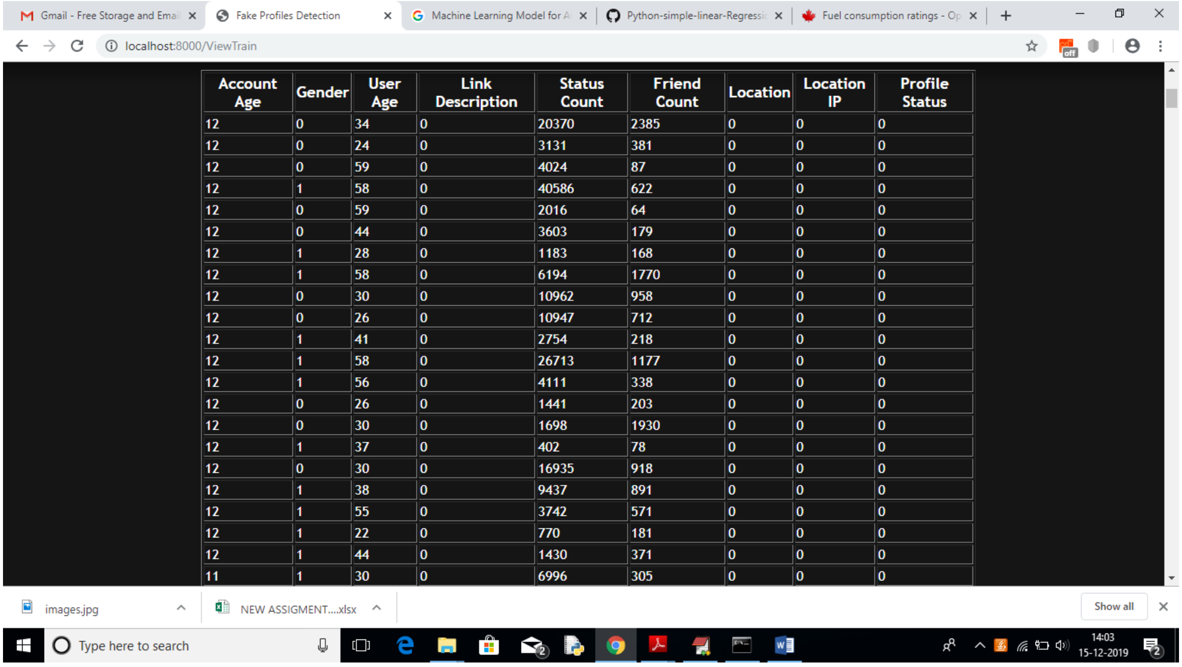
Fake Profiles Detection

Fake Profiles Detection

ANN Accuracy : 98.33333492279053

Fig. 4: **Accuracy for Trained ANN**

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



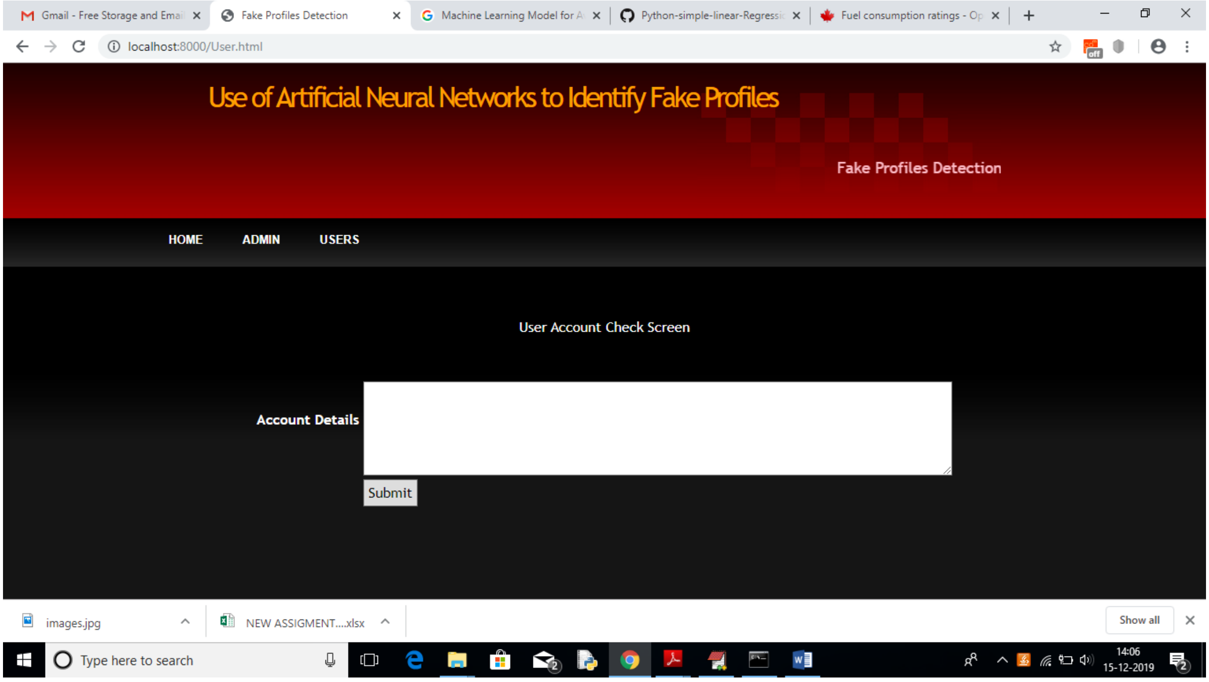
localhost:8000/ViewTrain

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

Gmail - Free Storage and Emai
Fake Profiles Detection
Machine Learning Model for A
Python-simple-linear-Regressi
Fuel consumption ratings - Op
images.jpg
NEW ASSIGMENT....xlsx
Show all
Type here to search
14:03
15-12-2019

Fig. 5: **Status Count for ANN models**

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



localhost:8000/User.html

Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

HOME ADMIN USERS

User Account Check Screen

Account Details

Submit

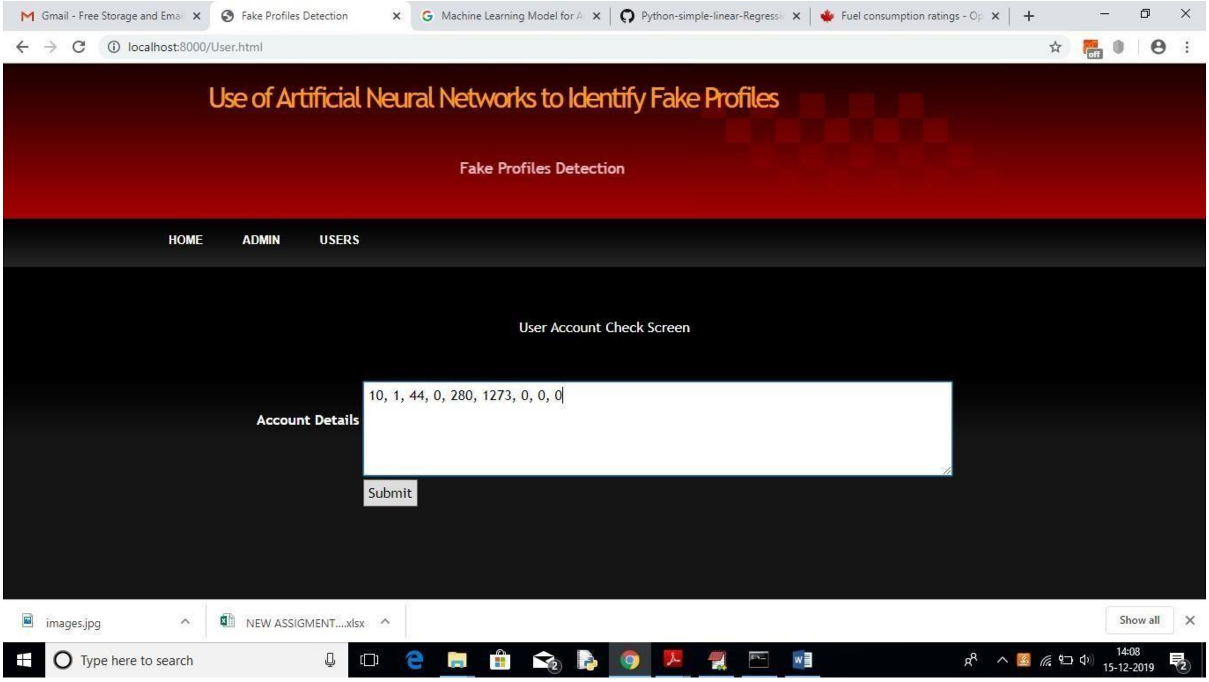
Gmail - Free Storage and Emai
Fake Profiles Detection
Machine Learning Model for A
Python-simple-linear-Regressi
Fuel consumption ratings - Op
images.jpg
NEW ASSIGMENT....xlsx
Show all
Type here to search
14:06
15-12-2019

Fig. 6: User Account Check 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



Use of Artificial Neural Networks to Identify Fake Profiles

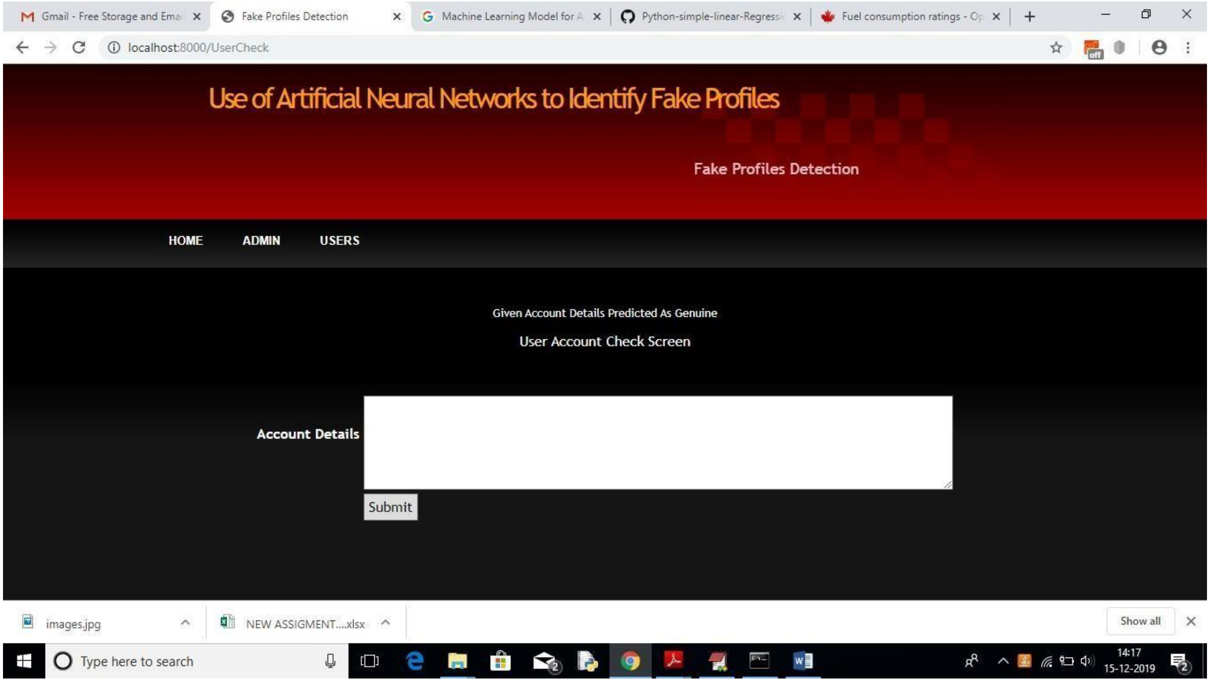
Fake Profiles Detection

User Account Check Screen

Account Details: 10, 1, 44, 0, 280, 1273, 0, 0, 0

Fig. 7: Identifying Fake Profiles using Address

For above input will get below result



Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

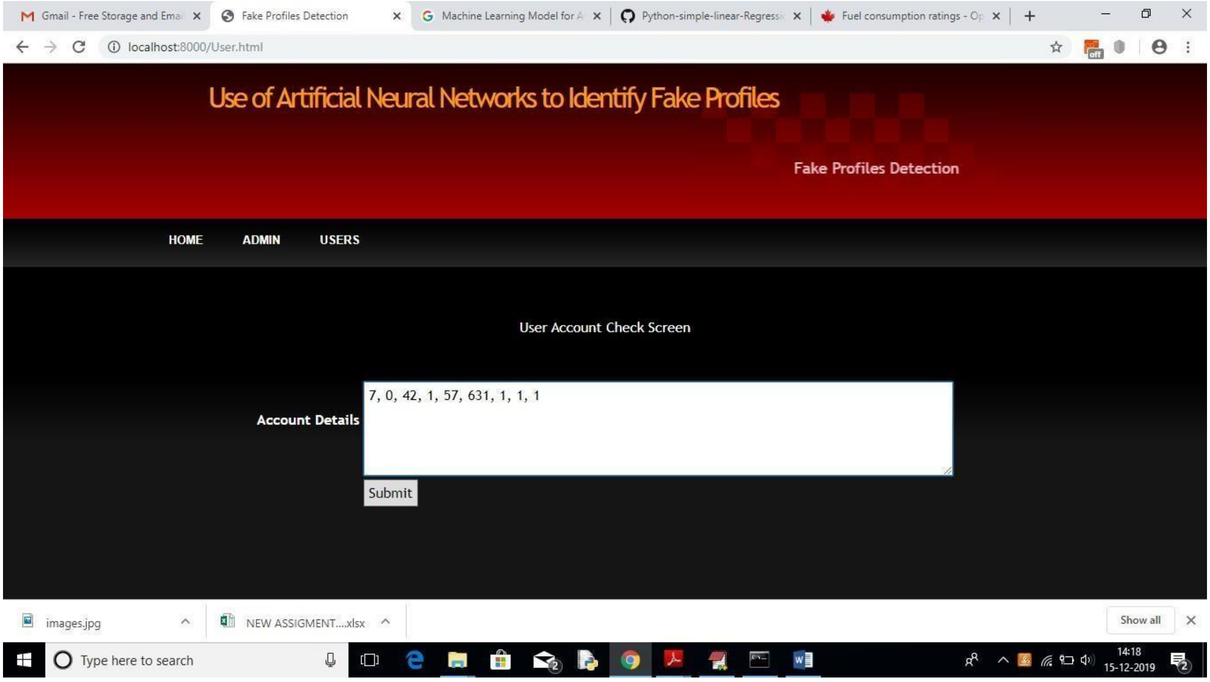
Given Account Details Predicted As Genuine

User Account Check Screen

Account Details

Fig. 8: **Results Prediction for Genuine Accounts**

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


Gmail - Free Storage and Emai
Fake Profiles Detection
Machine Learning Model for A
Python-simple-linear-Regressi
Fuel consumption ratings - Op
localhost:8000/User.html
Use of Artificial Neural Networks to Identify Fake Profiles
Fake Profiles Detection
HOME
ADMIN
USERS
images.jpg
NEW ASSIGMENT....xlsx
Show all
Type here to search
14:18
15-12-2019

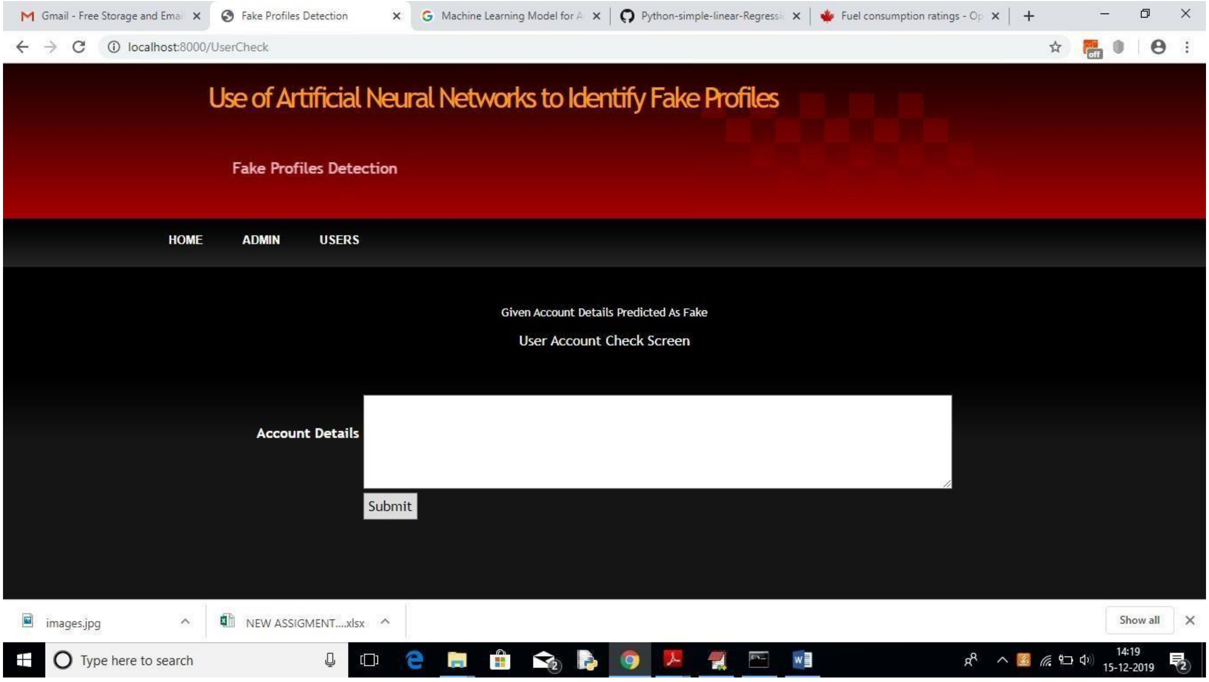
User Account Check Screen

Account Details: 7, 0, 42, 1, 57, 631, 1, 1, 1

Submit

Fig. 9: **User Address Verifying**

For above account details we got below result


Gmail - Free Storage and Emai
Fake Profiles Detection
Machine Learning Model for A
Python-simple-linear-Regressi
Fuel consumption ratings - Op
localhost:8000/UserCheck
Use of Artificial Neural Networks to Identify Fake Profiles
Fake Profiles Detection
HOME
ADMIN
USERS
images.jpg
NEW ASSIGMENT....xlsx
Show all
Type here to search
14:19
15-12-2019

Given Account Details Predicted As Fake

User Account Check Screen

Account Details

Submit

Fig. 10: **Fake Results Identification**

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

VI. CONCLUSION

In this paper, we use desktop learning, particularly a 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 an 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.

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 9thUSENIX 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 techniquesin 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:

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 last2 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, Tirupati(Dt), Andhra Pradesh, India.

SHIAK KOUSAR has Pursuing his MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, affiliated to JNTUAin 2022. Andhra Pradesh, India.