JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

A NOVEL ARTIFICIAL NEURAL NETWORKS AND FCNN ALGORITHMS FOR IDENTIFICATIONS OF FAKE PROFILES ON CLOUD NETWORK

Dr Raghavender K V, Assoc Prof CSE department

G NARAYANAMMA INSTITUTE OF TECHNOLOGY AND SCIENCE

SHAIKPET HYDERABAD

drkvraghavender@gmail.com

ABSTRACT

Now a days it is very difficult to identify the fake profiles in online networks and all the primitive methods are not completely success in identifying the fake or phony profiles. Hence this motivated me to develop thus proposed work by utilizing Artificial Neural Networks (ANN) module from deep learning to recognize whether given record subtleties are from certified or counterfeit clients. This ANN will be calculated based on past history of clients with the varying record information from certain point. This ANN calculation will be prepared with all past clients fake profile data and veritable record information and afterward at whatever point we gave new test information then that ANN train model will be applied on new test information to distinguish whether given new record subtleties are from real or fake clients. Online interpersonal organizations, such as facebook or twitter contains client's complete information and some malignant clients will hack informal organization data set to take or penetrate client's data. In order to ensure security of client's information, we are using ANN model to identify fake profiles from online social networks.

Key Words:

Artificial Neural Network, Deep Learning, Fake Profiles, Malignant Clients, Facebook, Twitter, Online Interpersonal Organization.

1. INTRODUCTION

In 2017 Facebook arrived at a complete populace of 2.46 billion clients settling on it the most well-known decision of online media [1]. Online social

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

networks make incomes from the information given by clients. The normal client doesn't realize that their privileges are surrendered the second they utilize the web-based media networks administration. Online media organizations have a great deal to acquire to the detriment of the client. Each time a client shares another area, new photographs, likes, aversions, and label different clients in content posted. Facebook makes income by means of ads and information. All the more explicitly, the normal American client produces about $26.76 per quarter [2]. That number adds up rapidly when a great many clients are involved.

In todays advanced age, the always expanding reliance on PC innovation has left the normal resident powerless against violations, for example, information breaks and conceivable wholesale fraud. These assaults can happen without notice and frequently without notice to the survivors of an information break. As of now, there is minimal motivating force for informal communities to further develop their information security. These breaks regularly target web-based media organizations like Facebook and Twitter. They can likewise target banks and other monetary establishments.

In todays advanced age, the always expanding reliance on PC innovation has left the normal resident powerless against violations, for example, information breaks and conceivable wholesale fraud. These assaults can happen without notice and frequently without notice to the survivors of an information break. As of now, there is minimal motivating force for informal communities to further develop their information security. These breaks regularly target web-based media organizations like Facebook and Twitter. They can likewise target banks and other monetary establishments. There is by all accounts a newsworthy issue including online media networks getting hacked each day. As of late, Facebook had an information break which influenced around 50 million clients [3]. Facebook gives a bunch of unmistakably characterized arrangements that clarify how they manage the user’s information [4].

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

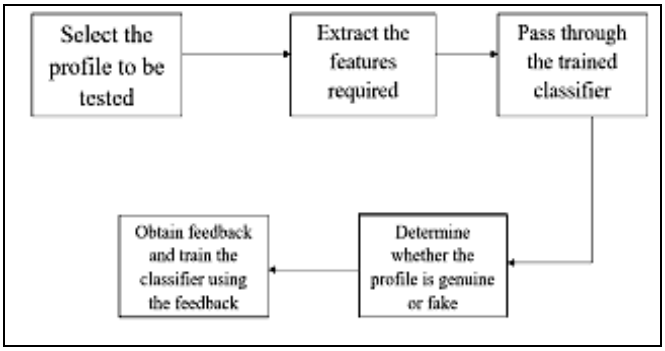


Figure 1. Represent the Flow of Fake Profile Prediction

The approach does very little to forestall the consistent double-dealing of safety and security. Counterfeit profiles appear to fall through Facebook's worked in security highlights. A different risk of individual information being acquired for deceitful intentions is the presence of bots and phony profiles. Bots are programs that can accumulate data about the client without the client in any event, knowing. This interaction is known as web scratching. What is more awful, is that this activity is lawful. Bots can be covered up or come as a phony companion demand on an interpersonal organization site to access private data. The arrangement introduced in this paper expects to zero in on the risks of a bot as a phony profile on your web-based media. This arrangement would come as a calculation. The language that we decided to utilize is Python and by using python programming language and utilizing all the libraries we are going to show the performance of our proposed method in efficient way.

2. LITERATURE SURVEY

Literature survey is that the most vital step in the software development process. Before developing the new application or model, it's necessary to work out the time factor, economy, and company strength. Once all these factors are confirmed and got approval then we can start building the application.

1) Counterfeit Profile Identification in Online Social Networks

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Sk.Shama, K.Siva Nandini, There is a gigantic expansion in innovations nowadays.. Mobiles are becoming brilliant. Innovation is related with online informal organizations which have turned into a section in each one's life in making new companions and keeping companions, their inclinations are known simpler. Yet, this expansion in systems administration online make numerous issues like faking their profiles, online pantomime having become increasingly more in present days. Clients are taken care of with more pointless information during riding which are posted by counterfeit clients. Explores have seen that 20% to 40% profiles in web-based informal communities like facebook are phony profiles. Hence this location of phony profiles in web-based informal communities results into arrangement utilizing systems.

2) Utilization of Artificial Neural Networks to Identify Fake Profiles
Gergo Hajdu and Yaclaudes Minos In this paper, we use AI, specifically a counterfeit neural organization to figure out what are the possibilities that Facebook companion demand is valid or not. We likewise layout the classes and libraries included. Besides, we talk about the sigmoid capacity and how the still up in the air and utilized. At long last, we consider the boundaries of the interpersonal organization page which are most extreme significant in the gave solution. The different risks of individual information being acquired for false reasons for existing is the presence of bots and phony profiles. Bots are programs that can accumulate data about the client without the client in any event, knowing. This cycle is known as web scratching. What is more terrible is that this activity is lawful. Bots can be covered up or come as a phony companion demand on an interpersonal organization site to access private information. The arrangement introduced in this paper expects to zero in on the risks of a bot as a phony profile on your online media. This arrangement would come as a calculation. The language that we decided to utilize is Python. The calculation would have the option to decide whether a current companion demand that a client gets online is a real individual or on the other hand in case it is a bot or it is a phony companion demand looking for data. Our calculation would work with the assistance of the online media organizations, as we would require a preparation dataset from them to prepare our model and later check if the profiles are phony or not. The calculation could even function as a customary layer on the user’s internet browser as a program module.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

3) Recognition of phony cash note utilizing convolutional neural networks(2016). Navya Krishna.G and Naga Sri Ram.B Records in internet based web-based media have loads of info information like name, sexual direction, colleagues, enthusiasts, inclinations, region numbers. Half piece of this information are both of public and private. We need to utilize input that is public to know profiles which are fake for relational association as information from private is inaccessible. Regardless, if our proposed plan is used by the relational cooperation associations itself, by then they can use the private information of the clients to know not from mishandling from security issues. Considered information is features for profiles to characterize of fake and veritable profiles. For distinguishing counterfeit profiles we followed these means: 1. Capacities are to be chosen after selection of characteristics, the at a bunch of profiles which are now delegated phony or genuine are needed for the tutoring rationale of the order calculation. We have utilized a freely accessible dataset of 1337 phony clients and 1481 genuine clients which incorporate various qualities comprising of call, status count, number of companions, fans depend, top picks, dialects respected, etc. 2. The tutoring dataset is then taken care of to the arrangement set of rules. It gains from the training dataset and is anticipated to offer right tastefulness marks for the testing dataset. 5. The marks from the testing dataset are killed and are left for assurance by the informed classifier. 6.

3. EXISTING SYSTEM

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.

LIMITATIONS OF EXISTING SYSTEM

The following are the main limitations of the existing system. They are as follows:

1) The fake profile’s contents typically have links that lead to an external website where the damage happens.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

2) 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.

3) While Facebook has a rigorous screening to keep these fake accounts out, it only takes one fake profile to damage the computers of many.

4) Sometimes the fake profile not only grab the users information but also create damage for the personal computers.

4. PROPOSED METHODOLOGY

In our proposed work, we use AI with CNN model in order to find out the fake profiles who try to create malware attempt on genuine user records. In general we try to use MS-Excel to store old and new phony information profiles. Initially we try to calculate the information in starting point and then try to find out the outline information about all users at that point. Now we try to do assortment of information based on user information partitioned into a preparation set and a testing set. For partition of information we require some information collected from online social media to prepare our current model. In our current model we try to assume the fake profiles are gathered from a online social network such as facebook or twitter and we try to concentrate on a phony profile like Account age, Gender, User age, Link in the portrayal, Number of messages conveyed, Number of companion demands conveyed, Entered area, Location by IP, Fake or Not. Each and every field has some importance and we try to figure out information from any filed. For instance, for the sexual orientation boundary if the profile not really set in stone to be a female or male a worth of (1) is relegated to the preparation set for Gender. A similar cycle is applied to different boundaries. We likewise utilize the nation of beginning as a factor

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

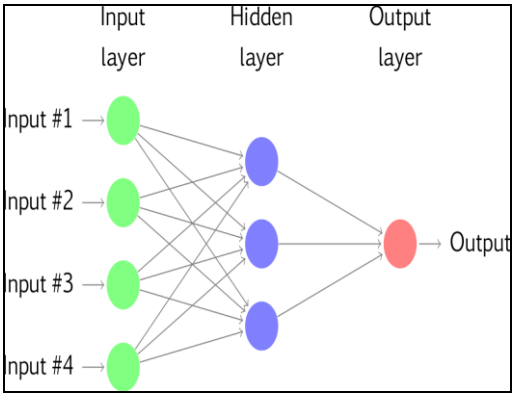


Figure 2. Represent the Architecture flow of CNN

From the above figure 2, we can clearly identify there are three layers present in neural network such as: Input Layer, Hidden Layer and Output Layer.

Initially the data or input is collected from input layer and the input will be undergo several pre-processing stages and then enter into hidden layer. In this current model, the input is nothing but several clients profiles are collected and examined to identify the fake profiles and normal profiles. Once the profile is loaded as input now we need to enter into hidden layer. In the hidden layer we can see all the mathematical processing and problem formulation steps. At this stage we try to apply calculations for identifying the fake profiles based on some features. In this stage we will take some features and match the features with previous genuine profiles to identify the similarity of fake and normal profiles.

Now the hidden layer will process the input and then processed information is send as outcome for the end user. This outcome can be displayed on output layer and this will give clear idea about the output.

In order to train the current ANN model, we use the following details or features which are collected from real time social network such as facebook.

1) Account_Age,
2) Gender,
3) User_Age,

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

4) Link_Desc,
5) Status_Count,
6) Friend_Count,
7) Location,
8) Location_IP, and
9) Status

Normally for every fake user, they will have some intention like send friend requests to normal users to gain illegal access of genuine profiles. So they try to hack the genuine users profile data and collect as much of information they can.Based on some continuous observations of fake profiles, we shortlisted some attributes which are used to find out whether profile is genuine or fake. This facebook profile data we downloaded from Facebook website and using this data to train ANN model. Below are some values from profile dataset.

Account_Age, Gender, User_Age, Link_Desc, Status_Count, Friend_Count, Location, Location_IP, Status

10, 1, 22, 0, 1073, 237, 0, 0, 0
10, 0, 33, 0, 127, 152, 0, 0, 0
10, 1, 46, 0, 1601, 405, 0, 0, 0
10, 0, 25, 0, 704, 380, 0, 0, 0
7, 1, 34, 1, 64, 721, 1, 1, 1
7, 1, 30, 1, 69, 587, 1, 1, 1
7, 1, 36, 1, 61, 782, 1, 1, 1
7, 1, 52, 1, 96, 827, 1, 1, 1

The above dataset contains nearly 9 columns and each and every column name has its own importance and for easy reference they kept in bold. The corresponding values are separated by using comma between each and every value.Here the features what we consider for fake profile identification are holding numerical values, because ANN model will not accept strings as matching parameters.In some cases if there is any string value present in input dataset,those string values are mapped with numerical values by replacing with either zero or one.For example if we take gender as one feature,the gender filed contains two

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

possibilities either male or female. So we convert gender values to 0 or 1, if male value is 1 and if female value is 0. In above dataset last column give us information of fake or genuine account if last column contains value 0 then account is genuine otherwise fake. All fake account will have less number of posts as their main intention is to send friend requests not posts, so by analyzing this features Facebook mark that record with value 1 which means it's a fake account. We are using above dataset to train ANN model and this dataset saved inside code 'dataset' folder. After building train model we input test data with account details and ANN will give result as fake or genuine. Below are some values from test data

Account_Age, Gender, User_Age, Link_Desc, Status_Count, Friend_Count, Location, Location_IP

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

In above test data STATUS column and its value is there and ANN will predict status and give us result whether above test data is fake or genuine. In output we can see result of above test data.

ANN ALGORITHM

To demonstrate how to build a ANN neural network based image classifier, we try to construct a 6 layer neural network to identify and separate each and every profile with one another. As this current model we are going to build on small dataset ,there is no need to worry about the memory , we can use direct CPU memory to store and access the network rather than use GPU. 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.

In this proposed work our main objective is to build a CNN using TENSORFLOW.In general the CNN models are purely mathematical models to

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

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

$z = wx + b$

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. These all we can clearly seen in figure 2.

5. IMPLEMENTATION STAGE

Implementation is a stage where the theoretical design is converted into programmatically manner. Here we try to divide the application into number of modules and then coded for deployement.Here we used python as programming language with tensorflow to show the performance of our current application. The proposed application is mainly divided into 2 modules. They are as follows:

1) Admin Module

2) User Module

5.1 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:

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Using this module admin can view all dataset used to train ANN model.

5.2 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. Here the user module is one which is mainly used to show the similarity between normal profile and fake profile.

6. EXPERIMENTAL RESULTS

In order to show the performance of our proposed application, we try to deploy the current application using Python as programming language. First we will import all the necessary libraries and then load the input dataset to find out the desired output

IMPORT LIBRARIES

```
from django.shortcuts import render
from django.template import RequestContext
from django.contrib import messages
from django.http import HttpResponse
import pandas as pd
from sklearn.model_selection import train_test_split
from keras.models import Sequential
from keras.layers.core import Dense,Activation,Dropout
from keras.callbacks import EarlyStopping
from sklearn.preprocessing import OneHotEncoder
from keras.optimizers import Adam
```

In the above window we can clearly see there are several libraries and packages used to prove the current objective. Hence we try to load all those necessary libraries and import them into our application.

DATA SET PRE-PROCESSING

```
def importdata():
    balance_data = pd.read_csv
('C:/FakeProfile/Profile/dataset/dataset.txt')
    balance_data = balance_data.abs()
    rows = balance_data.shape[0]  # gives number of row count
    cols = balance_data.shape[1]  # gives number of col count
    return balance_data

def splitdataset(balance_data):
    X = balance_data.values[:, 0:8]
    y_ = balance_data.values[:, 8]
    y_ = y_.reshape(-1, 1)
    encoder = OneHotEncoder(sparse=False)
    Y = encoder.fit_transform(y_)
    print(Y)
    train_x, test_x, train_y, test_y = train_test_split(X, Y,
test_size=0.2)
    return train_x, test_x, train_y, test_y
```

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

In the above window we can clearly see the dataset is loaded and it is pre-processed and converted into test and train folders. Once the pre-processing step is completed next we can able to test the model on sample user profiles and check how efficiently the current model is able to identify fake profile or not.

APPLY ANN MODEL

```
def GenerateModel(request):
    global model
    data = importdata()
    train_x, test_x, train_y, test_y = splitdataset(data)
    model = Sequential()
    model.add(Dense(200, input_shape=(8,), activation='relu',
name='fc1'))
    model.add(Dense(200, activation='relu', name='fc2'))
    model.add(Dense(2, activation='softmax', name='output'))
    optimizer = Adam(lr=0.001)
    model.compile(optimizer, loss='categorical_crossentropy',
metrics=['accuracy'])
    print('CNN Neural Network Model Summary: ')
    print(model.summary())
    model.fit(train_x, train_y, verbose=2, batch_size=5, epochs=
200)
    results = model.evaluate(test_x, test_y)
    ann_acc = results[1] * 100
    context= {'data':'ANN Accuracy : '+str(ann_acc)}
    return render(request, 'AdminScreen.html', context)
```

From the above window we can clearly see the ANN model is defined for the proposed module. Here we try to apply ANN model to check the efficiency of our current application in order to check whether user profile is genuine or fake.

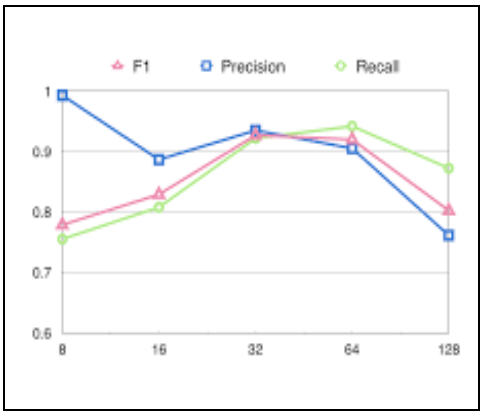
PREDICT THE OUTCOME

```
test = test.values[:, 0:8]
predict = model.predict_classes(test)
print(predict[0])
msg = ''
if str(predict[0]) == '0':
   msg = "Given Account Details Predicted As Genuine"
if str(predict[0]) == '1':
   msg = "Given Account Details Predicted As Fake"
context= {'data':msg}
return render(request, 'User.html', context)
```

From the above window we can clearly test condition is verified on 9 attributes which are applied to check whether given profile is genuine or fake. Here we can able to see two cases for prediction, one is fake profile prediction and other one is normal profile.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

GROWTH GRAPH



From the above window we can clearly identify the following growth factors such as Precision,F1 Score, Recall for the given dataset by using ANN model.

7. CONCLUSION

In this proposed work, we for the first time developed a novel methodology of finding the most accurate analysis of fake profile prediction in online social networks. In general, till now there is no accurate method which can able to find out the fake profiles very accurately and efficiently from online social networks and hence a lot of valuable users are lost their sensitive information illegally. Hence this motivated me to do this proposed work by taking Artificial Neural Network (ANN) model and then try to find out the fake profiles very accurately and efficiently. By conducting various experiments on our proposed model by taking some sample dataset, our comparative results clearly state that our proposed ANN model achieves high level of accuracy in order to predict the fake profiles.

REFERENCES

1) Sai Pooja, G., Rajarajeswari, P., Yamini Radha, V ., Na vya Krishna.G., Naga Sri Ram.B., Recognition of phony cash note utilizing convolutional neural networks(2016). Global Journal of Innovative Technology and Exploring Engineering, 58-63,8(5).

2) Mohammed Ali Al-Garadi,Mohammad Rashid Hussain, Henry Friday Nweke, Ihsanali,Ghulammujtaba1,Harunachiro Ma,Hasanalikhattak,Andabdullahgani "Predicti-Ngcyber Bullying On Social Networks.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

3) Yadongzhou,Daewookkim,Junjiezhang,(Member,Ieee),Lili Liu1, Huanjin3, "(IEEE)ProGuard: Detecting Malicious Accounts in SocialNetwork-Based Online Promotions".

4) Mauro Conti University of Padua, Radha Poovendran University of Washington, Marco Secchiero University of Padua,"FakeBook: Detecting Fake Profiles in, ACM/IEEE International Conference on Advances in Social Networks Analysis and Mining.

5) ni .N., Smruthi.M.,"A Hybrid Scheme for Detecting FakeAccounts in Facebook" ISSN: 2277-3878, (IJRTE)International Journal of Recent Technology and Engineering (2019) , Issue-5S3, Volume-7.

6) NarsimhaGugulothu,JayadevGyani, Srinivas Rao Pulluri "A Comprehensive Model for Detecting Fake Profiles in Online Social Networks(2016)".

7) Dr.Narsimha.G, Dr.JayadevGyani, P. Srinivas Rao ,"Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP(2018)", International Journal of Applied Engineering Research ISSN 0973-4562, Number 6, Volume 13.

8) Reddy, A. V. N., &Phanikrishna, C. Form following based information extraction and article acknowledgment utilizing profound learning neural networks(2016). Paper introduced at the Proceedings on second International Conference on Next Generation Computing Technologies in 2016, NGCT 2016, 352-354. doi:10.1109/NGCT.2016.7877440.

9) V. Rama Krishna,& K.Kanaka Durga. Programmed location of ill-conceived sites with common clustering.(2016) International Journal of Electrical and Computer Engineering, 6(3), 995-1001. doi:10.11591/ijece.v6i3.9878

10) D.Rajeswara Rao & V.Pellakuri. Preparing and improvement of counterfeit neural organization models: Single layer feedforward and multi-facet feedforward neural network(2016). Diary of Theoretical and Applied Information Technology, 150-156,84(2).

11) Challa, N.,. Pasupuleti, S. K, & Chandra, J. V. A pragmatic way to deal with E-mail spam channels to shield information from cutting edge tenacious threat.(2016) Paper introduced at the Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2016, doi:10.1109/ICCPCT.2016.7530239.