International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Use of Artificial Neural Networks to Identify Fake Profiles

T Sarada [1],Maggidi Meghana[2], Medipally Sriya[3],Deva Vineeth[4], Gasiganti Sarayu[5]
[2,3,4,5] UG Scholars, Department of CSE, **AVN Institute of Engineering and Technology,**Hyderabad, Telangana, India.
[1] Assistant Professor, Department of CSE, **AVN Institute of Engineering and Technology**, Hyderabad, Telangana, India.

Abstract
In this project, we use machine learning, namely an artificial neural network to determine what are the chances that Facebook friend request is authentic or not. We also outline the classes and libraries involved. Furthermore, we discuss the sigmoid function and how the weights are determined and used. Finally, we consider the parameters of the social network page which are utmost important in the provided solution. The other dangers of personal data being obtained for fraudulent purposes is the presence of bots and fake profiles. Bots are programs that can gather information about the user without the user even knowing. This process is known as web scraping. What is worse, is that this action is legal. Bots can be hidden or come in the form of a fake friend request on a social network site to gain access to private information

Intoduction

In 2017 Facebook reached a total population of 2.46 billion users making it the most popular choice of social media [1]. 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 [2]. 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. They can also target banks and other financial institutions.

This chapter provides the details of the project's need based survey, system requirements, Hardware Requirements, Software Requirements, and System Requirements.

Project Overview :-

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

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.

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 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

Advantages :-

- Vote Trust uses a voting based system that pulls user activities to find fake profiles using trust-based vote assignment and global votes total. It is considered as the first line of defense due to limitations which include real

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

accounts that were already compromised being sold

Modules of the Application:

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.

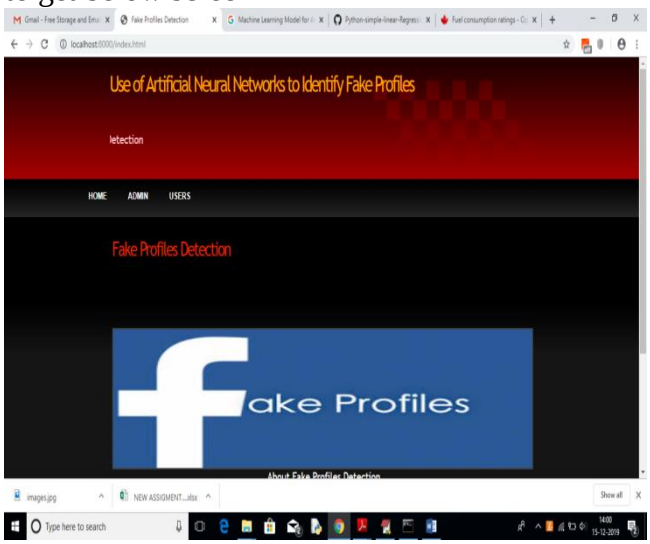
OBJECTIVES OF THE PROJECT:

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.

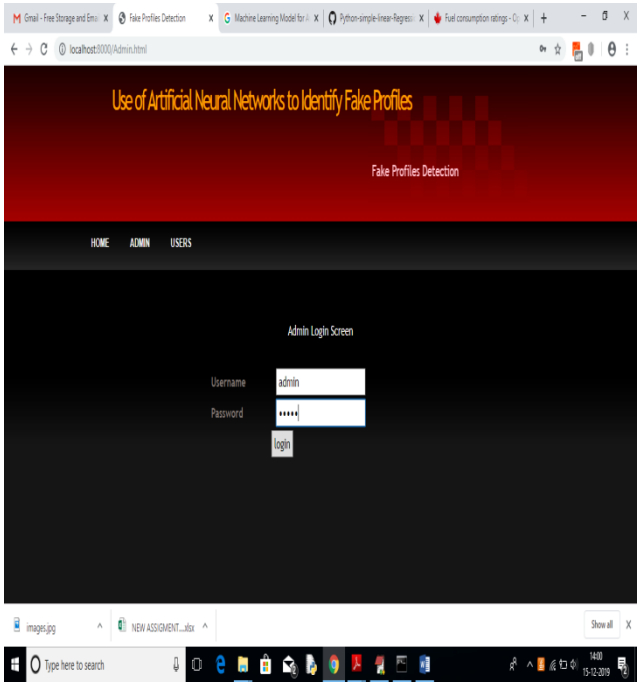
Results

User Login Screen:

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



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

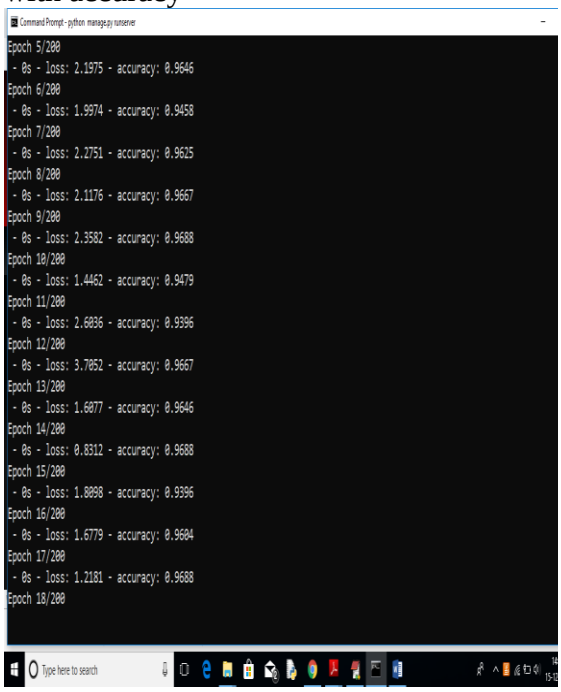


In above screen enter admin and admin as username and password

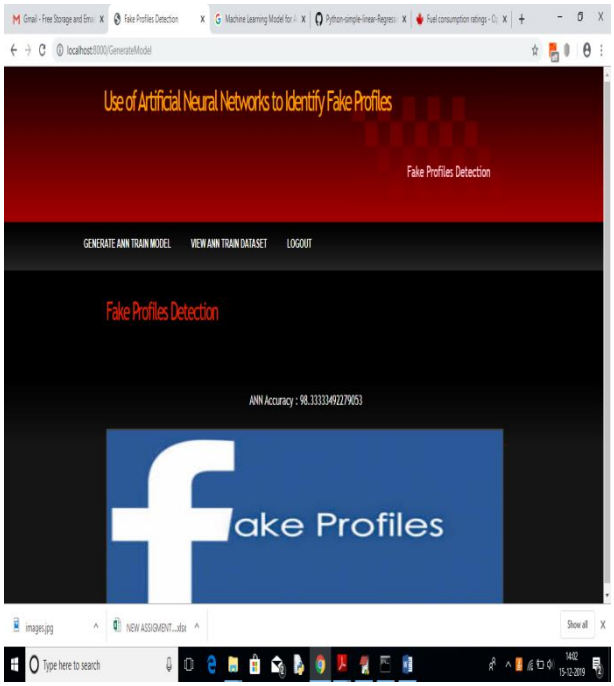
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

to login as admin. After login will get below screen

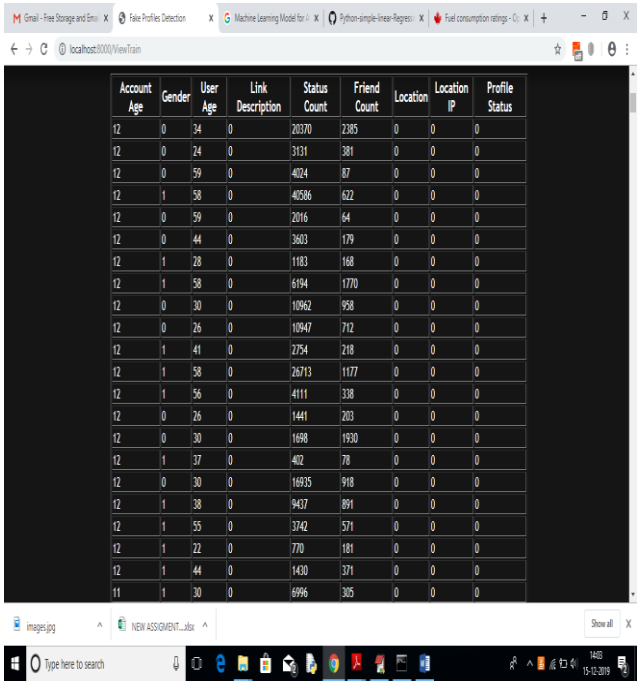
In above screen click on 'Generate ANN Train Model' to generate training model on dataset. After clicking on that link you can see server console to check ANN processing details with accuracy



In above black console we can see all ANN details.



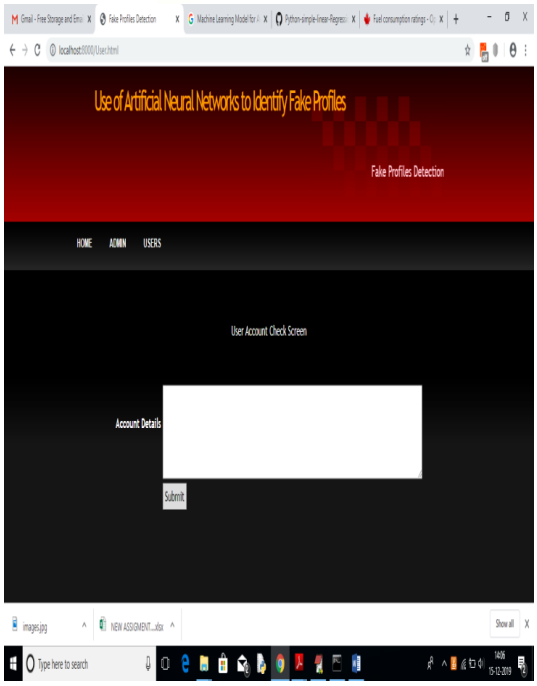
In above screen we can see ANN got 98% accuracy to train all Facebook profile. Now click on 'View Ann Train Dataset' link to view all dataset details



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

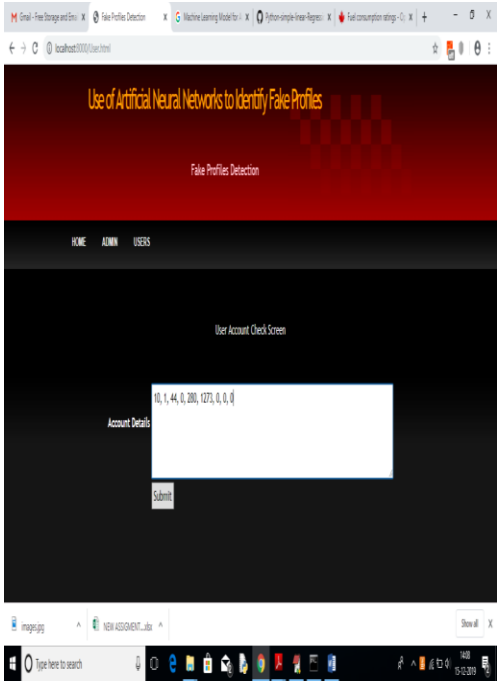
In above screen we can see all train data and scroll down to view all records. Now ANN train model is ready and you can logout and click on 'User' link to get below screen.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

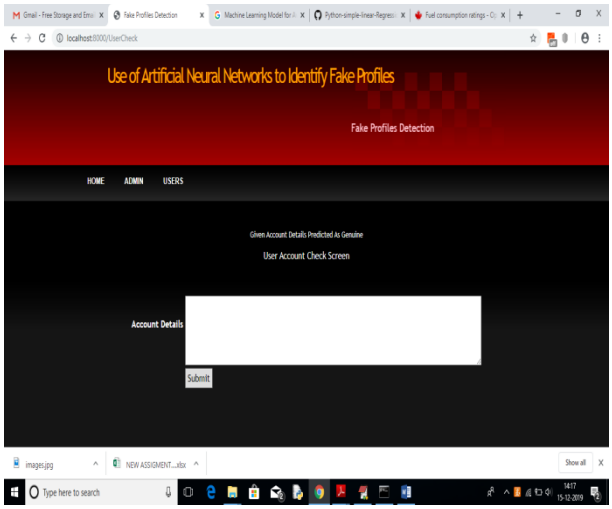


In above screen enter some test account details to get prediction/identification from ANN. You can use below records to check

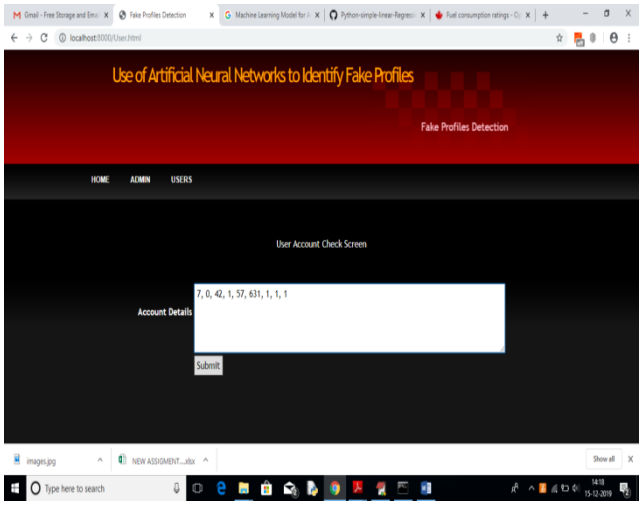
10, 1, 44, 0, 280, 1273, 0, 0
10, 0, 54, 0, 5237, 241, 0, 0
7, 0, 42, 1, 57, 631, 1, 1
7, 1, 56, 1, 66, 623, 1, 1



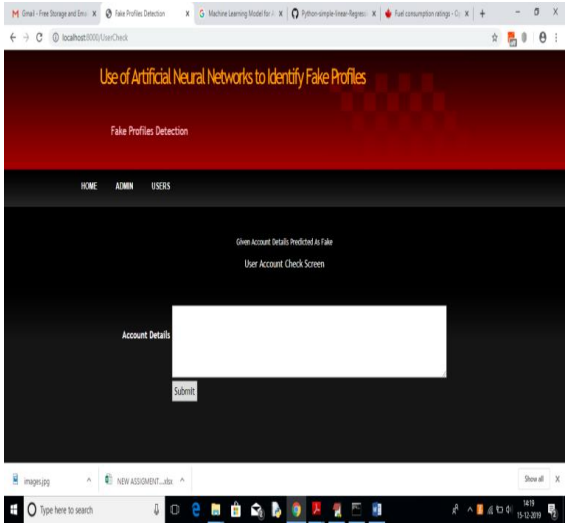
For above input will get below result



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

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

fake for given account data

RESULTS AND CHALLENGES

RESULTS

The current android application is developed using Xml, Java, SQL with Firebase connectivity. It can be used by every individual who are in a need of fulfilling their household services.

At the time of submission of my application was capable of doing the following:

- Displaying thehome screen with different fragments.
- Authentication of user by using login screen using Firebase.
- Home screen to display based on user or service provider.
- After successful login of user, they can choose the service and book a slot of their particular service provider from the displayed list.
- Add, update, view, delete the user details.
- After successful login of service provider, they can view all the bookings that are booked by the users and can attend them one by one.
- Service provider can also set his preferences to not available, if he's too busy or many users had already booked him.
- Service provider has the ability to change their particular radius of location for servicing.
- He can set up to 10 km radius.
- Logout and end the session.

Challenges

Understanding the connections of SQLite Database is a tricky part and confusing when dealing with multiple tables within a database.

Making exact orientation API design levels was a difficult task as there are many types of devices like desktop, tablet, mobile with varying screen size andresolutions.

Implementing synchronization with Firebasewas a challenging task.

Learning different technologies and frameworks with little guidance.

CONCLUSION

Conclusion

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 back propagation, minimizing the final cost function and adjusting each neuron's weight and bias.

Scope for futurework

- 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

BIBLIOGRAPHY

[1]. Code snippets for any errors http://stackoverflow.com/Android Development Guide https://www.udemy.com/androidXml and Layout Guide
[2].https://www.androidhive.com/Connecting to Firebase Docs
[3]. https://firebase.google.com Software Testing
[4].http://en.wikipedia.org/wiki/Software_testingManual Testinghttp://en.wikipedia.org/wiki/Manual_testing
[5]. Performance Testing http://en.wikipedia.org/wiki/Software_performance_testing
[6].https://www.statista.com/topics/1164/social-networks/
[7].https://www.cnbc.com/2018/01/31/facebook-earnings-q4-2017-arpu.html
[8].https://www.cnet.com/news/facebook-breach-affected-50-millionpeople/
[9]. https://www.facebook.com/policy.php
[10]. Qiang Cao, Michael Sirivianos, Xiaowei Yang, and Tiago Pregueiro. 2012. Aiding the detectionof
[11]. 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

.