International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Attempt at Detecting Fake Profiles Using Neural Networks

Mr.M.Amareswara Kumar[1], G.Manjulatha[2],A.Srivalli[3],M.Shabhirun[4],B.Ramani[5],C.Bhavani[6]

[1]Assistant Professor, Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal

[2,3,4,5,6]*Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal*

DOI: https://doi.org/10.55248/gengpi.2023.4.4.35591

ABSTRACT

Here, we use machine learning, in the form of an artificial neural network, to calculate the probability that a user's friend request on Face book is genuine/real or not. The relevant libraries and classes are also described. Further, we talk about the sigmoid function and how the weights are calculated and applied. In the end, we think about the most crucial aspects of the social network page to consider while implementing the proposed solution.

Keywords: Neural Network,Social network analysis,Data Preprocessing.

I. INTRODUCTION

With 2.46 billion active users as of 2017, Facebook is clearly the most popular social media platform. The information shared by its users is the source of income for social media platforms. When people sign up for a social media account, they don't realize that they're giving up certain legal protections. The social media giants stand to earn significantly, but this comes at the price of the user.Facebook generates income from adverts and user data every each time a person publishes information about their location, uploads a picture, expresses an,opinion about a post, or tags other users in a post user. When you consider millions of users, that sum soon grows. The victims of a data breach may not even be aware that they were attacked[16]. Right now, there is nothing driving social media platforms to beef up their data protection measures. These hacks often affect popular social media websites like Facebook and Twitter. Every day, there's a new story about a social media platform that's been hacked. About 50 million individuals had their information compromised recently on Facebook[12].

Facebook has a series of spelled-out policies that detail how the company handles userinformation . The policy doesn't do anything to stop the persistent breaching of security and privacy. Unfortunately, it seems that Facebook's anti-fake profile measures often fail to catch the fake accounts that are created. The proliferation of bots and phony accounts also increases the risk of personal data being collected for illicit reasons. The term "web scraping" describes this action[17]. To make matters worse, this is well within the law. To steal personal information, bots might lurk undetected or pose as a friend request on social networking sites.

This paper's proposed solution is meant to draw attention to the threats posed by a bot in the guise of a false social media presence. This answer would be expressed in the form of an algorithm. Python is the programming language of choice for us[18].

As soon as a user receives a friend request online, the algorithm would be able to tell whether it was sent by a real person, a bot, or a phony account trying to steal their personal information[13]. Our algorithm relies on the cooperation of the social media platforms, since we require a training dataset provided by them in order to properly calibrate our model and then test it to see whether the profiles are genuine[11]. The algorithm may also function in the conventional sense as a browser add-on for the user's web browser.

II. RELATED WORK

"Audit and Analysis of Imposters: A Novel Strategy for Identifying Fake Profiles in Social Networks."

Nowadays, everyone's social life revolves on their many online social networks (OSN). The way we communicate with one another has been revolutionized by these platforms. It is simpler to meet new people, maintain relationships with those you already have, and stay abreast of their latest exploits. However, along with their meteoric rise, issues like bogus profiles and online impersonation have multiplied in number as well. The fact that anybody may create a fake profile and pose as someone else poses a threat on the OSN[15].

In this work, we provide an experimental framework that makes fraudulent profile identification in a friend list possible, however it is only applicable to the social networking site Facebook.

"An in-depth look at the methods used to spot fake profiles on the web's largest social networks"

Present day, the Internet's most widely used and rapidly spreading applications are online social networks.

Because of these incentives, fraudulent actors have begun preying on those who utilize social networks[16].

If you want to do the most damage on a social network, create a false profile and use it to spread fake news or other malicious content. As soon as a phony profile is created, the user has to be alerted, but this crime needs to be uncovered far before that happens. The identification of false profiles has been the subject of several algorithms and methodologies, many of which make advantage of the massive amount of unstructured data produced by social networks[14].

This research provides an overview of the current and most recent technological progress on detecting bogus profiles.

III. METHODOLOGY

To assess the legitimacy of a friend request, we use machine learning, in the form of a synthetic neural network. An associated sigmoid function is applied to each equation at each neuron (node) to ensure that the node-level solutions remain within the range [0.0, 1.0].

Multiplying this by 100 at the output end would give us the likely percentage that this is a malicious request. When it comes to our proposed approach, we'll just be using a single deep neural network, which will have only one hidden layer. Each input neuron would be a different feature of each profile that was selected in advance and converted into a numerical value (for example, gender as a binary number, female 0 and male 1) and, if necessary, divided by an arbitrary number (for example, age is always divided by 100) to reduce the impact of any one feature. Nodes are represented by the neurons. In this setup, each node would be in charge of making a single choice. Each factor contributes its own unique importance and perspective to the equation. The calculated result would be a % estimate of how likely it is that the friend request is not from a genuine person. The used neural network is shown in Fig. 1.

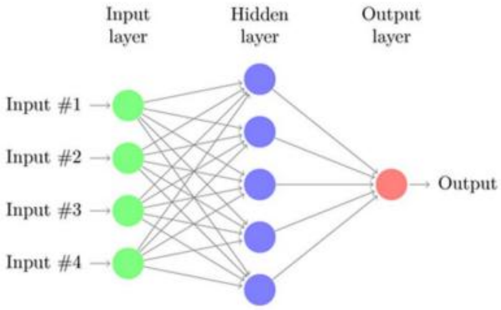


Fig.1:Neural Network

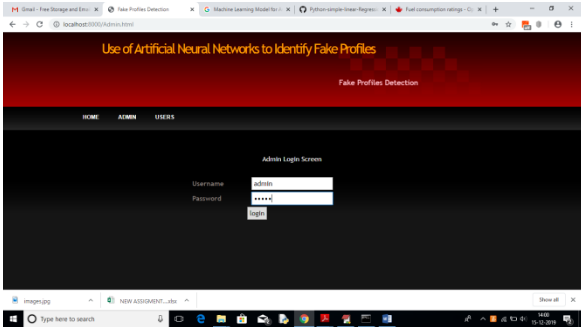
We need a training set, which may come from Facebook or another social media network site, or even simply web scraping if we locate enough phony accounts.

Our deep learning system may then learn the bot's behavior patterns through back propagation by minimizing the final cost function and fine-tuning the weights and biases of each neuron.

This article provides an overview of the related classes and libraries.

IV. RESULT AND DISCUSSION

In this study, we employ Artificial Neural Networks to determine whether the provided account data belong to real people or bots. The ANN algorithm will be trained using both real and fraudulent account data from prior users, and then the ANN train model will be used to fresh test data to determine whether the data represents real or fake accounts.


Gmail - Free Storage and Ema
Fake Profiles Detection
Machine Learning Model for A
Python-simple-linear-Regress
Fuel consumption ratings - O
localhost:8000/Admin.html
HOME
ADMIN
USERS
login
images.jpg
NEW ASSIGMENT....xlsx
Show all
Type here to search
14:00
15-12-2019

Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

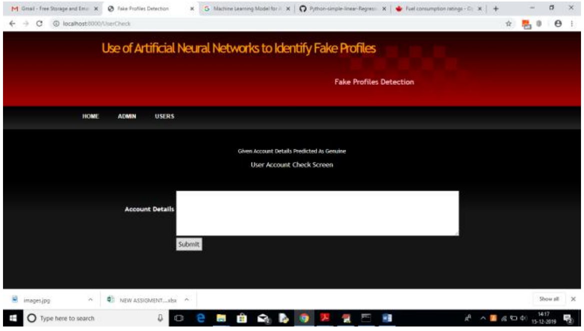
Admin Login Screen

Username admin

Password •••••

Fig.2: AdminPage

Enter your username and password to access the admin panel, and then use the ANN algorithm to train the dataset. The whole ANN profile is shown on the rear control panel. Evidently,ANN was able to train every Facebook profile to an accuracy of 98%



Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

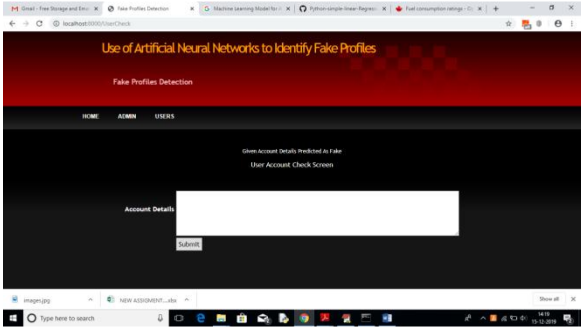
Given Account Details Predicted As Genuine

User Account Check Screen

Account Details:

Fig.3: Sample 1 Data To Test Geniune Or Fake

There is evidence to suggest this is a legitimate narrative. InFig. 3. sample 1 data result is genuine.



Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

Given Account Details Predicted As Fake

User Account Check Screen

Account Details:

Fig.4: Sample 2 Data To Test Geniune or Fake

It's likely that this account is a hoax. In Fig.4 sample 2 data result is fake

V. CONCLUSION

Whether you get a friend request and you're not sure if it's real or not, run it through a neural network. For each neuron (node), the equations are Sigmoid-transformed.

The data used for training comes from Facebook or another social network. The described deep learning method might then use back propagation to learn the patterns of bot behaviour by optimizing the final cost function and fine-tuning the weights and biases of each neuron. This article provides an overview of the related classes and libraries. We also talk about the sigmoid function and how the weights are calculated and applied for it. Important to our solution are the characteristics of the social media page itself, which we take into account.

VI. 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, ValliyammaiChinnaiah. 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] Karukula, Nageswara Reddy, and Sunar Mohammed Farooq. "A route map for detecting Sybil attacks in urban vehicular networks." *Journal of Information, Knowledge, and Research in Computer Engineering* 2.2 (2013): 540-544.

[12] Mahammad, Farooq Sunar, and V. Madhu Viswanatham. "Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach." *The Journal of Supercomputing* 76.4 (2020): 2275-2288.

[13] Farooq, Sunar Mohammed, and K. NageswaraReddy. "Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications." (2015).

[14]Sathish, A., et al. "A Technique to Reduce Data-Bus Coupling Transitions in DSM Technology." *i-Manager's Journal on Software Engineering* 4.2 (2009): 67.

[15]Mallikarjuna Rao, Y., M. V. Subramanyam, and K. Satya Prasad. "Cluster- based mobility management algorithms for wireless mesh networks." International Journal of Communication Systems 31.11 (2018): e3595.

[16]Subramanyam, M. V., and K. Satya Prasad. "Delay efficient algorithm for adhoc wireless networks." Information Technology Journal 5.5 (2006): 976-981.

[17]https://ijrar.org/papers/IJRAR19J2281.pdf

[18]https://www.ijrpr.com/uploads/V1ISSUE1/IJRPR0012.pdf

[19] Mahammad, Farooq Sunar, et al. "Prediction Of Covid-19 Infection Based on Lifestyle Habits Employing Random Forest Algorithm." *JOURNAL OF ALGEBRAIC STATISTICS* 13.3 (2022): 40-45.

[20]https://ejmcm.com/article_9974_b564072310db5c6f9d1f5b39221afc09.pdf