Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

USE OF ARTIFICIAL NEURAL NETWORKS TO IDENTIFY FAKE PROFILES

[1]PATAN SHAIKSHAVALI KHAN, [2]SABOLU PAVAN KALYAN, [3]BOYA RAJASHEKAR, [4]M SUDHARSHAN REDDY, [5]B HARISH KUMAR REDDY
[1234]B.Tech Student, [5] Assistant Professor
Department of CSE
Dr. K. V. Subba Reddy Institute Of Technology, Kurnool.

Abstract:
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.

I. INTRODUCTION

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.

There seems to be a newsworthy issue involving social media networks getting hacked every day. Recently, Facebook had a data breach which affected about 50 million users [3]. Facebook provides a set of clearly defined provisions that explain what they do with the user's data [4]. The policy does very little to prevent the constant exploitation of security and privacy. Fake profiles seem to slip through Facebook's built-in security features.

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.

The solution presented in this paper intends to focus on the dangers of a bot in the form of a fake profile on your social media. This solution would come in the form of an algorithm. The language that we chose to use is Python. The algorithm would be able to determine if a current friend request that a user gets online is an actual person or if it is a bot or it is a fake friend request fishing for information. Our algorithm would work with the help of the social media companies, as we would need a training dataset from them to train our model and later verify if the profiles are fake or not. The algorithm could even work as a traditional layer on the user's web browser as a browser plug-in.

II. LITERATURE SURVEY

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.

Users increasingly rely on the trustworthiness of the information exposed on Online Social Networks (OSNs). In addition, OSN providers base their business models on the marketability of this information. However, OSNs suffer from abuse in the form of the creation of fake accounts, which do not correspond to real humans. Fakes can introduce spam, manipulate online rating, or exploit knowledge extracted from the network. OSN operators currently expend significant resources to detect, manually verify, and shut down fake accounts. Tuenti, the largest OSN in Spain, dedicates 14 full-time employees in that task alone, incurring a significant monetary cost. Such a task has yet to be successfully automated because of the difficulty in reliably capturing the diverse behavior of fake and real OSN profiles.

We introduce a new tool in the hands of OSN operators, which we call *SybilRank*. It relies on social graph properties to rank users according to their perceived likelihood of being fake (Sybils). SybilRank is computationally efficient and can scale to graphs with hundreds of millions of nodes, as demonstrated by our Hadoop prototype. We deployed SybilRank in Tuenti's operation center. We found that ~90% of the 200K accounts that SybilRank designated as most likely to be fake, actually warranted suspension. On the other hand, with Tuenti's current user-report-based approach only ~5% of the inspected accounts are indeed fake.

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

In the present generation, the social life of every person has become associated with online social networks (OSN). These sites have made drastic changes in the way we socialize. Making friends and keeping in contact with them as well as being updated of their activities, has become easier. But with their rapid growth, problems like fake profiles, online impersonation have also increased. The risk lies in the fact that anybody can create a profile to impersonate a real person

on the OSN. The fake profile could be exploited to build online relationship with a targeted person purely through online interactions with the friends of victim.

In present work, we have proposed experimental framework with which detection of fake profile is feasible within the friend list, however this framework is restricted to a specific online social networking site namely Facebook. This framework extracts data from the friend list and uses it to classify them as real or fake by using unsupervised and supervised machine learning.

III. SYSTEM ANALYSIS AND DESIGN

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.

SYSTM DESIGN

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.

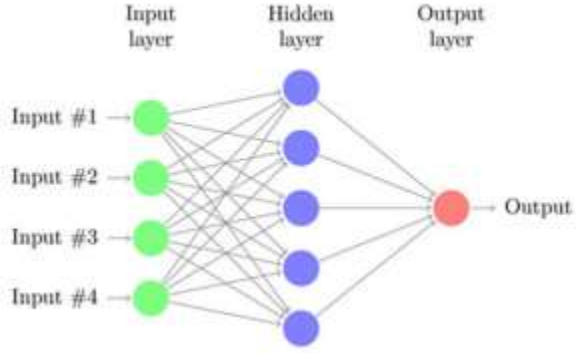
• We utilize Microsoft Excel to store old and new fake data profiles. The algorithm then stores the data in a data frame. This collection of data will be divided into a training set and a testing set. We would need a data set from the social media sites to train our model.

• 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 accounts that were already compromised being sold

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023



IV. IMPLEMENTATION

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.

V. 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.

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