IDENTIFYING FAKE ACCOUNTS ON SOCIAL MEDIA THROUGH ARTIFICIAL NEURAL NETWORKS

[1]Shaik Hussain Bi,[2] A Vinod Kumar,[3]B. Benarji,[4]Soma Pushparaganjali
[1,3]Associate Professor,[2]AssistantProfessor,[4]Student
Department of CSE
G V R & S College of Engineering &Technology, Guntur,AP

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 isthe 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.

DOI Number: 10.48047/nq.2021.19.9.NQ21174 NeuroQuantology 2021; 19(9): 1023-1025

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.

II.LITERATURE SURVEY

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.

III.SYSTEM ANALYSIS

SYSTEM ARCHITECTURE

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 accounts that were already compromised being sold.

IV.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 future work

• 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

Code snippets for any errors
http://stackoverflow.com/
Android Development Guide
https://www.udemy.com/android
Xml and Layout Guide
https://www.androidhive.com/
Connecting to Firebase Docs
https://firebase.google.com
Software
Testinghttp://en.wikipedia.org/wiki/Software_testing

Manual Testing
http://en.wikipedia.org/wiki/Manual_testing
Performance Testing
http://en.wikipedia.org/wiki/Software_performa
nce_testing