International Journal of Research
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Design and Development of Artificial Neural Networks to Identify Fake Profiles

M. Likitha, K. Rahul, A. Prudhvi Sai ,A.Mallikarjuna Reddy
Associate Professor
Department of Computer Science and Engineering
Anurag Group of Institutions, Hyderabad, Telangana, India
Emails: 16h61a0594@cvsr.ac.in, 16h61a05a6@cvsr.ac.in, 16h61a0564@cvsr.ac.in, mallikarjunreddycse@cvsr.ac.in,

Abstract- In this present generation, the social life of everyone has become associated with the online social networks. Making friends and keeping in contact with them and their updates has become easier. But with the rapid growth of these social networking sites, many problems like fake profiles, online impersonation have also grown. An algorithm was used in which the profiles are ranked according to the number of interactions, tags, wall posts, and friends over time. Profiles that have a high rank are considered to be real while profiles having a low rank are considered to be fake. Unfortunately, this technique was found to be unreliable because it failed to take into account the possibility that real profiles can be ranked low and fake profiles can be ranked high. In this project, we use an artificial neural network to determine what are the chances that a friend request is authentic or not. It 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 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 if it is a fake friend request fishing for information. We need a training dataset to train our model and later verify if the profiles are fake or not. Through the use of different libraries, we can easily design and develop an artificial neural network. The language we choose to use is Python. We also consider the parameters of the social networking page which are the most important to our solution. For training set, the features that we use determine a fake profile are Account age, Gender, User age, Number of messages sent out, Number of friend requests sent out. This proposed solution will help in determining whether the profile is genuine or not and gives us an accuracy of 96%.

Keywords – Identify, Profile, Detection.

I. INTRODUCTION

In 2019, Facebook has reached a total population of 2.5 billion users making it the most popular choice of social media. 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. 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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Twitter. They can also target banks and other financial institutions. So to overcome the problem of finding profile is authentic or not we are developing an artificial neural network. This proposed solution will help to identify whether the profile is genuine or fake.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED SYSTEM

2.1 Architecture of the System–

The solution presented in this project 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 needs a training dataset to train our model and later verify if the profiles are fake or not.

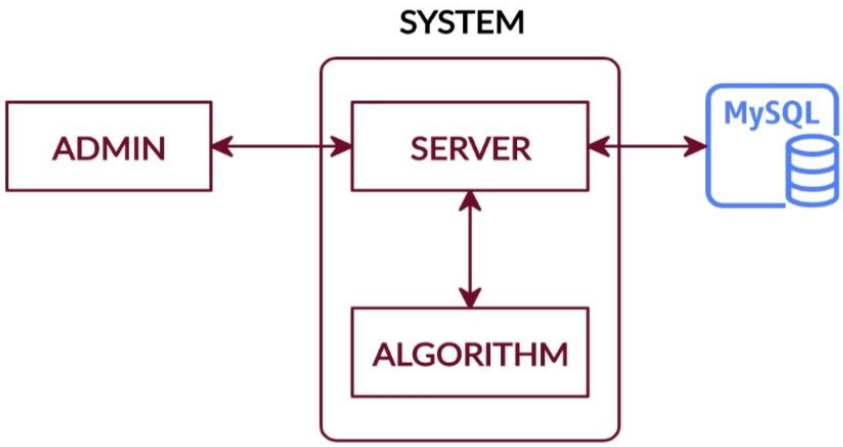

Figure 1. Architecture of the System

2.2. Artificial Neural Network –

In our solution, we use an artificial neural network, to determine what are the chances that a friend request is authentic or not. Each equation at each neuron (node) is put through a Sigmoid function to keep the results between the interval of 0.0 and 1.0. At the output end, this could easily be multiplied by 100 to give us the possible percentage that it is a malicious request. Our solution has a single hidden layer.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

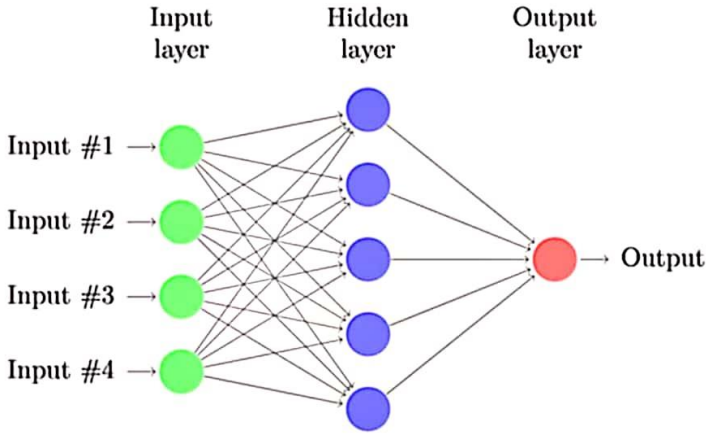

Figure 2. Neural Network Diagram

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.

We would need a training data set which would be provided by Facebook or other social network sites or just web scraping given that we find enough fake profiles. This would allow our algorithm to learn the patterns of bot behavior by backpropagation, minimizing the final cost function and adjusting each neuron's weight and bias, changing the equations. In this proposed system, different libraries are used.

III. Experiment and Result

The test set for this evaluation experiment is randomly selected from the internet. Python, Django and MySQL are the software required to perform the experiment. The PC for experiment is equipped with a platinumIV or higher processor, a minimum RAM of 256MB and a minimum Hard disk of 512MB.

Table -1 Test Cases

Testcase ID	Testcase	Input	Expected Result	Actual Result	Status
1	Login	Invalid Username and password	Invalid	Invalid	PASS
2	Login	Valid Username and password	Valid	Valid	PASS

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

3	Generate training model	Click on the Generate model tab	Training model is generated	Training model generated	PASS
4	View the training dataset	Click on View the training dataset	Training dataset can be viewed	Training dataset can be viewed	PASS
5	Prediction of fake profile	Submit Fake profile detalis	The profile is fake	The profile is fake	PASS
6	Prediction of genuine profile	Submit Genuine account details	The profile is genuine	The profile is genuine	PASS
7	Terminate the process	Click on Logout	-	-	PASS

Figure 3.1 User login screen

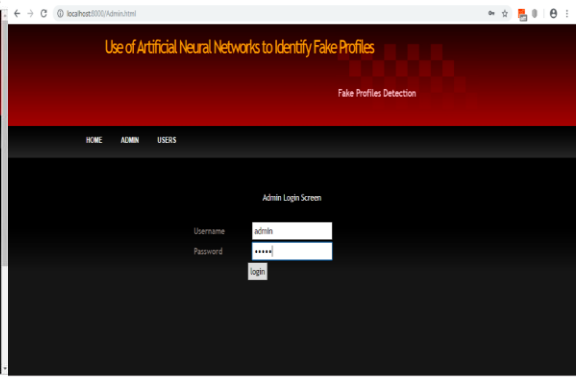

Figure 3.2 Admin login screen

Figure 3.3 Admin page opens

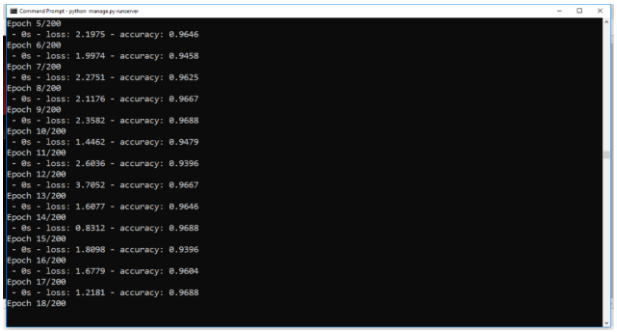

Figure 3.4 Generating a training model

International Journal of Research
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Figure 3.5 Accuracy of ANN(96%)

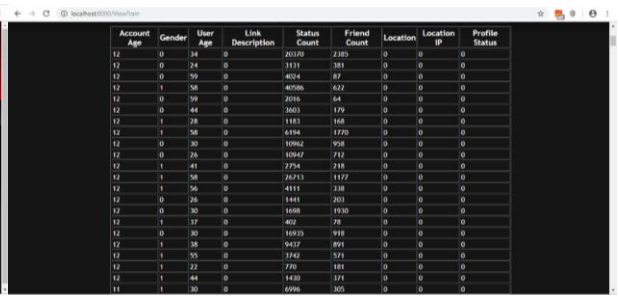

Figure 3.6 View the trained dataset

Figure 3.8 Enter test account details

Figure 3.7 Logout and click on "USER"

Figure 3.9 If the account is genuine

Figure 3.10 If the account is fake

IV.CONCLUSION

We have given a framework using which we can detect fake profiles in any online social network with a very high efficiency as high as around 96%. In this proposed system, we use machine learning, to determine what are the chances that a friend request is authentic 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. In this proposed system, we outline the classes and libraries

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

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.

REFERENCES

[1] Qiang Cao, Michael Srinivas, "Aiding the detection of fake accounts in large scale social online services",2012

[2] Akshay J, Sarode and Arun Mishra, "Audit and Analysis of Impostors:An experimental approach to detect fake profile in online social network",2015

[3] Devakunchi Ramalingam, Valliyammai Chinnaiah, "Fake profile detection techniques in large-scale online social networks".

[4] T. Stein, E. Chen, and K. Mangla. "Facebook immune system",2011.

[5] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. "The socialbot network: when bots socialize for fame and money",2011

[6] C. Wagner, S. Mitter, C. Kornor, and M. Strohmaier. "When social bots attack: Modeling susceptability of users in online social networks", 2012

[7] G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Marakatos, "Detecting social network profile cloning", 2011

[8] A. Wang "Detecting spam bots in online social networking sites: a machine learing approach", 2010

[9] H Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B.Y. Zhao "Detecting and characterizing social spam campaigns", 2010.