BioGecko

Vol 12 Issue 03 2023

ISSN NO: 2230-5807

Use of Artificial Neural Networks to Identify Fake Profiles

Mrs. N. Sujata Kumari[1], G. Manasa[2], K. Advaitha[3], Seema Panda[4]

[1]Assistant Professor, Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India
[2]Computer Science and Engineering, Sridevi Women's Engineering College, B. Tech IV Year, Hyderabad, India
[3]Computer Science and Engineering, Sridevi Women's Engineering College, B. Tech IV Year, Hyderabad, India
[4]Computer Science and Engineering, Sridevi Women's Engineering College, B. Tech IV Year, Hyderabad, India

Abstract

In today's digital life, the dependency of computer technology is increasing day-by-day. So, the main target of hackers are social media networks such as Facebook, Instagram, and twitter. So, this is being a major cyber security problem these days. This intends to build an Artificial Intelligence solution to prevent the dangers of a bot in the form of fake profile on social media. We are using deep learning algorithm which is Artificial Neural Network, so it determines the possibility of social media profile to be fake or genuine. The popularity of social networks has skyrocketed in recent years, with a glut of personal information being posted to sites like Facebook and LinkedIn by users. But this unchecked expansion has opened the door to problems such as false profiles and malicious actors. Fake accounts can be used for malicious purposes such as spreading spam or committing fraud, so it's important to have systems in place that can detect these fraudulent accounts. In this paper, we focus on social networks and analyse methods of detecting fake profiles, comparing them across various applications and measuring performance criteria.

1. INTRODUCTION

In our modern world, social media plays a major role in the everyday lifestyle of many people. Platforms like Facebook and LinkedIn have seen usage rapidly increase over the past few years, with users providing increasing amounts of personal information on their profiles. Unfortunately, this rise in visibility has come with its own issues, namely the proliferation of fake accounts. With the single click of a button, malicious actors can create thousands of fraudulent profiles to further their own goals such as spreading spam or committing fraud. This paper aims to outline existing techniques for detecting fake accounts in social networks, monitoring performance parameters for various applications and drawing comparisons between them. Keeping communications authentic on social networks requires users to authenticate themselves when first establishing relationships. Unfortunately, the profile attacking, which enables adversaries to gather OSN activities. Retrieval and analysis attack targets multimedia information such as images, videos, etc., followed by reverse engineering in order to convince victims into contacting the attacker directly. It's crucial that more effective authentication methods be implemented for online security. In order to ensure the security of social networks, users must authenticate their identities to one another. Currently available methods for this user identification process are not sufficient for 2 preventing fake profile creation, as a single user has the capability to have multiple profiles without any effective identityverifying procedures. This vulnerability means adversaries can create many false profiles and use them to attack social network systems. Profile attacking is done in an attempt to collect information about OSN activities; pull and analysis attacks also aim at multimedia objects such as videos, images, and audio files. Reverse Engineering Attacks (RSE) may occur next - individuals are tricked into contacting hackers without intention or knowledge of doing so.

2. LITERATURE SURVEY

“Facilitating the identification of phony profiles in massive social networks.”

Users have become used to relying on the veracity of data posted on OSNs. Furthermore, OSN providers depend on the commercial value of this data to drive their operations. Unfortunately, OSNs are subject to misuse in the shape of bots and other non-human accounts that pretend to be actual people. False information may introduce spam, alter online rankings, or exploit data mined from the network. Right now, it takes a lot of time and effort on the part of OSN operators to search for verify and delete bogus accounts. The biggest OSN in Spain, Tuenti, spends a lot of money (14 full-time people) on only that one duty. Since properly recording the different behaviors of false and actual OSN profiles is challenging, this process has not been effectively automated. SybilRank is a brand new resource for OSN administrators. To determine which users are more likely to be Sybils (fake accounts), it analyzes their social network attributes. SybilRank is highly computational and, as shown by our Hadoop prototype, can scale to networks with hundreds of millions of nodes. SybilRank is now live in Tuenti's ops hub thanks to our efforts. Ninety percent (90%) of the 200,000 accounts that SybilRank flagged as potentially false were really deserving of punishment. Tuenti's present method relies on user reports, and only around 5% of the accounts they investigate are false.

“Audit & Analysis of Imitators: A Novel Strategy for Identifying Bogus Profiles in Social Networks.”

Online social networks (OSN) have become integral to everyone's social lives in today's world. These platforms have revolutionized our social lives. It's less difficult to meet new people, maintain relationships with those you already have, and stay abreast of what they're up to. However, along with their meteoric rise, issues like bogus profiles and online impersonation have multiplied. The fact that anybody may create a false profile on the OSN poses a threat. Using the victim's acquaintances as a conduit, the phony profile might be used to cultivate an online connection with the target. In this paper, we provide an experimental framework for detecting false profiles inside a friend network; however, this approach is limited to the Facebook social network.

This framework mines your buddy list for information, then utilizes supervised and unsupervised machine learning to determine who among them is genuine and who is phony.

3. METHODOLOGY

In supervised learning, a machine learningtrained by being provided with sample data that has been labelled and classified. The model is tested to determine its accuracy when fed the sample dataset. This approach to teaching machines mirrors the way students learn under the instruction of a teacher. Spam filtering is a great example of supervised learning and two algorithms can be used for this type of learning. Alternatively, unsupervised learning involves instructing a computer in such a manner that it learns without human assistance; an unlabelled dataset is presented and the algorithm must discern structure from these unlabelled pieces of data. Unsupervised tasks require machines 4 to develop new features or artefacts from their input datasets without supervision. TensorFlow is a powerful tool for training, inference, and deep neural networks. The process for utilizing TensorFlow in our use case involves four steps: dataset processing, model development, model evaluation and model assessment. First, we must lay out which features and labels are involved by processing our data set. Then, using the training data, we aim to reduce errors in our model through training. After this, it's time to evaluate the developed model on test data and measure the accuracy achieved. Lastly, when it comes to assessing potential threat actors on social media platforms like Twitter or Reddit, we can differentiate between genuine and false accounts through classification - something that historically has utilized a range of methods to accurately determine who is causing threats online. Vector Machines are a powerful supervised learning tool commonly used in classification tasks for machine learning.

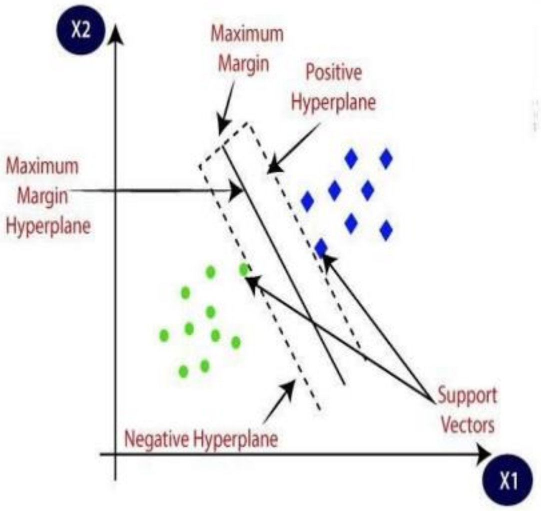


Fig. 1. Tensor Flow Architecture

The SVM algorithm is designed to identify the best decision boundary, known as a hyperplane, that effectively divides an dimensional space into different classes and presents an easy framework for assigning new data points to one of those categories. Support Vector Machines achieve this by finding extreme points or vectors, referred to as support vectors, and using them to determine the optimal hyperplane. For example, the image above demonstrates how two distinct groupings can be classified with a decision boundary or hyperplane.

System Architecture

As Figure 2 displays, the system architecture consists of the following six steps:

a) Collecting Data
b) Pre-processing
c) Feature Reduction
d) Training the Model
e) Applying the Machine Learning Algorithm
f) Evaluating Classification Results into Fake and Real

To complete this process, we first identified elements to be used in the classification algorithm. Then scraped off profiles that are necessary for training and testing purposes as no social network dataset is available for free for identifying fake profiles. From this dataset, 80% were used for constructing a training dataset while 5 20% were allocated to setting up a testing dataset.

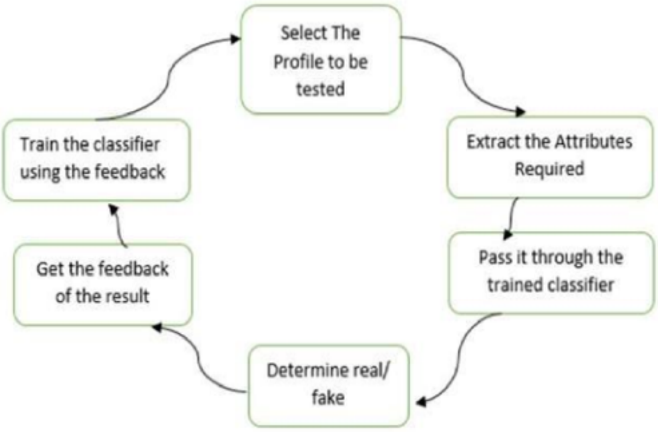

Select The Profile to be tested
Extract the Attributes Required
Pass it through the trained classifier
Determine real/ fake
Get the feedback of the result
Train the classifier using the feedback

Fig. 2. System Architecture

The preparation and testing datasets, containing 922 profiles and 240 profiles respectively, were employed to measure the productivity of arrangement calculation. The arrangement calculation was then fed with the preparation dataset and used to generate accurate classifications for the testing dataset. After the predictions were made, their accuracy was evaluated by comparing them with actual results from the testing dataset. Three order calculation models were used to assess the performance of these predictions, which determined the overall effectiveness of classification for these models.

Algorithm

In this algorithm it is a six-layer Artificial Neural Network (ANN) to separate one image from another. This ANN will be small enough to run on a regular home computer CPU. Traditional neural networks used for image classification typically contain many more parameters and take far longer to train if executed on a traditional CPU. Our goal is to illustrate how to construct a real-world convolutional neural network using TENSORFLOW. However, Neural Networks are mathematical models which compute solutions for optimization problems. At their core, they're made up of neurons - the basic computation elements within neural networks. Neurons calculate an output z by receiving an input x, multiplying it with variable w and then adding variable b. z=wx+b.

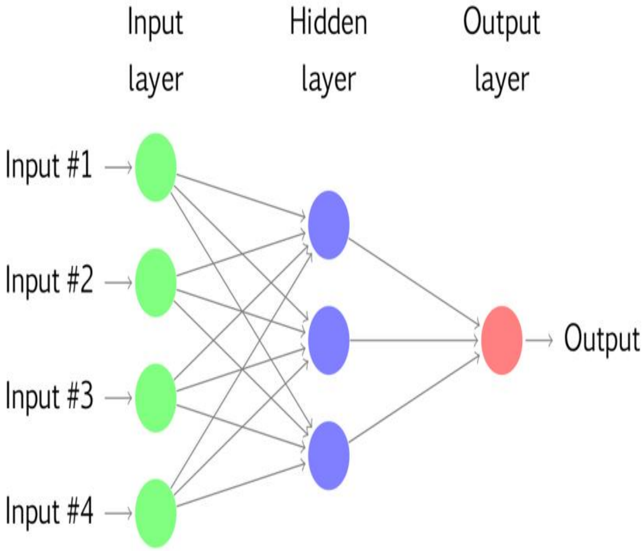
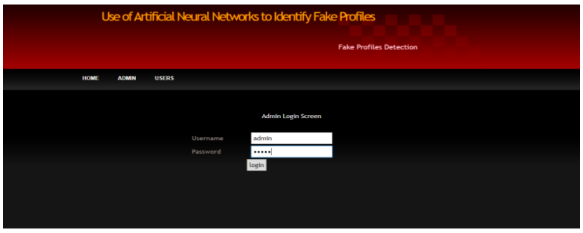


Fig. 3. Algorithm

A key component of neurons (the individual processing units within layers) is the activation function (f). This value is passed to a non-linear function, which then produces the output for that neuron. Popular examples include sigmoid and RELU neurons, though there are other options, such as TanH. A neural network is made up of stacked layers of these neurons. Neural networks can also be modified by changing how these neurons/layers are connected and configuring their respective activation functions.

4. RESULTS

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.


Use of Artificial Neural Networks to Identify Fake Profiles

Fake Profiles Detection

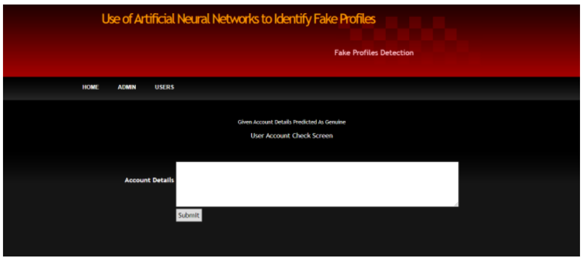
Admin Login Screen

Username: admin

Password: •••••

Fig. 4. Admin Page

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 Face book 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. 5. Checking User Accounts

There is evidence to suggest this is a legitimate narrative. It's likely that this account is a hoax.

5. CONCLUSION

It summarize, the use of machine learning toanalyze the likelihood that a friend request is genuine using an artificial neural network. Each neuron (node equations)'s are sent via a Sigmoid function. Here, we use a Face book- or other social network-provided training data set. Back propagation, minimization of the final cost function, and weight and bias adjustments for each neuronwould then enable the described deep learning algorithm to learn the patterns of bot behavior. Classes and libraries are described in this text. We also go over the sigmoid function and how the weights are calculated and applied. We also take into account the social network page's most crucial settings. Since quantum computers can handle several processes at once, they can provide substantially quicker results, particularly in the realms of R&D. Numerous sectors, such as machine learning, artificial intelligence (AI), health, and cyber security, will reap the rewards of these developments.

6. REFERENCES

1. Kumud Patel; Sudhanshu Agrahari; Saijshree Srivastava "Survey on Fake Profile Detection on Social Sites by Using Machine Learning Algorithm 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) Year: 2020 | Conference Paper | Publisher: IEEE
2. "Keynote Speech 2: Detecting fake news and profiling fake news spreaders and conspiracy propagators" 2021 12th International Conference on Information and Communication Systems (ICICS) Year: 2021 | Conference Paper | Publisher: IEEE
3. Samuel Delgado Muñoz; Edward Paul Guillén Pinto "A dataset for the detection of fake profiles on social networking services" 2020 International Conference on Computational Science and Computational Intelligence (CSCI) Year: 2020 | Conference Paper | Publisher: IEEE
4. Pradeep Kumar Roy; Shivam Chahar "Fake Profile Detection on Social Networking Websites: A Comprehensive Review" IEEE Transactions on Artificial Intelligence Year: 2020 | Volume: 1, Issue:3 | Journal Article | Publisher: IEEE
5. P Sowmya; Madhumita Chatterjee "Detection of Fake and Clone accounts in Twitter using Classification and Distance Measure Algorithms" 2020 International Conference on Communication and Signal Processing (ICCSP) Year: 2020 | Conference Paper | Publisher: IEEE
6. Padmaveni Krishnan. John Aravindhar; Palagati Bhanu Prakash Reddy "Finite Automata for Fake Profile Identification in Online Social Networks" 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) Year: 2020 | Conference Paper | Publisher: IEEE
7. Saeed Abu-Nimeh, T. M. Chen, and O. Alzubi, "Malicious and Spam Posts in Online Social Networks," Computer, vol.44, no.9, IEEE2011, pp.23– 28.