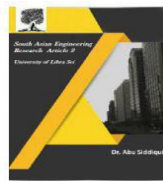




2581-4575



DETECTING FAKE ACCOUNTS ON SOCIAL MEDIA USING ARTIFICIAL NEURAL NETWORKS

¹Dr N SRIKANTH , ²CH SWATHI, ³MAINODDIN TIKOTIKAR, ⁴V SOWMYA

^{1,2,3}ASSISTANT PROFESSOR, BRILLIANT INSTITUTE OF ENGINEERING & TECHNOLOGY, ABDULLAPURMET(V&M) RANGA REDDY DIST-501505

⁴UG SCHOLAR, DEPARTMENT OF CSE, BRILLIANT INSTITUTE OF ENGINEERING & TECHNOLOGY, ABDULLAPURMET(V&M) RANGA REDDY DIST-501505

Abstract:

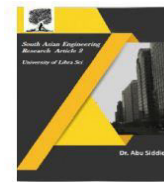
We utilize machine learning, specifically an artificial neural network, to assess the likelihood that a Facebook friend request is genuine. In our discussion, we highlight the relevant classes and libraries that play a crucial role in this process. Additionally, we delve into the sigmoid function, explaining how weights are established and applied. We also examine the social network page parameters, which are critical to our solution.

Beyond this, we must remain vigilant about the risks associated with personal data being exploited for fraudulent activities, especially due to the prevalence of bots and fake profiles. Bots are automated programs capable of collecting user information surreptitiously, a process known as web scraping, and troublingly, this practice is often legal. These bots may operate discreetly, masquerading as fake friend requests on social networking platforms to gain access to private information.

1.INTRODUCTION

In 2017, Facebook reached a staggering 2.46 billion users, solidifying its position as the leading social media platform. Social media networks thrive on the data shared by their users, often without the average person realizing that they forfeit certain rights the moment they sign up for these services. It's a one-sided transaction where social media companies stand to gain significantly from user interactions. Each photo shared, location tagged, and like clicked contributes to Facebook's revenue through advertisements and data collection. To put it in perspective, the average American user generates approximately \$26.76 in revenue quarterly, and when multiplied by millions, the total becomes impressive.

In our digital era, the growing reliance on technology has unfortunately rendered many individuals susceptible to crimes like data breaches and identity theft. These incidents can strike suddenly and often without warning to those affected. Currently, there's minimal motivation for social networks to enhance their data security measures. Breaches frequently target social media giants like Facebook and Twitter but can also extend to banks and other financial institutions..



II. LITERATURE SURVEY

This chapter outlines the findings from the project's needs-based survey, along with the necessary hardware and software specifications, as well as the overall system requirements.

Project Overview :-

- Each input neuron corresponds to a specific feature from each profile, represented as a numerical value. For instance, gender can be encoded as a binary number, with female as 0 and male as 1. If necessary, we can also normalize certain values; for example, age might be divided by 100. This approach ensures that no single feature overly influences the final outcome. Each neuron acts as a distinct node, dedicated to making its own part of the overall decision-making process.

III. SYSTEM ANALYSIS

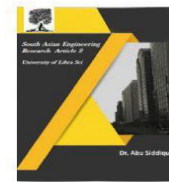
SYSTEM ARCHITECTURE

Existing System :-

- Malicious individuals often set up fake profiles to trick unsuspecting users into revealing their login credentials. These fraudulent accounts send friend requests to many users with public profiles, typically featuring appealing photos to lure victims in. Once a user accepts the request, the person behind the fake profile begins to flood that user's friends with friend requests as well.
- The content of fake profiles usually contains links that direct users to harmful external websites. When an unsuspecting user clicks on one of these dangerous links, they risk compromising their computer. The consequences can range from acquiring a virus to more severe issues, like installing a rootkit that transforms the computer into a bot. While Facebook employs strict measures to filter out these fraudulent accounts, it only takes a single fake profile to potentially jeopardize the computers of numerous users.

Proposed System :-

- In our approach, we leverage machine learning, specifically an artificial neural network, to assess the likelihood that a friend request is genuine.
- We use Microsoft Excel to keep track of both old and new fake data profiles. The algorithm organizes this information into a data frame. We will then split this collection into a training set and a testing set. To effectively train our model, we will need a data set from social media platforms.
- For the training set, we focus on specific features to identify a fake profile: Account Age, Gender, User Age, a Link in the Description, the Number of Messages Sent, the Number of Friend Requests Sent, Entered Location, Location by IP, and whether it's Fake or Not. Each parameter is evaluated and assigned a corresponding value. For instance, if we can determine the gender of a profile as



female or male, it receives a value of (1) in our training set for Gender. We apply this same assessment process to the other parameters as well. Additionally, we factor in the country of origin in our analysis.

Advantages :-

- Vote Trust implements a voting-based mechanism that leverages user activities to identify fake profiles. This approach uses trust-based vote assignment alongside a cumulative tally of global votes. While it serves as a primary defense line, it's important to note its limitations, particularly the risk of compromised real accounts being sold.

IV. Conclusion

We leverage machine learning, specifically through an artificial neural network, to assess the likelihood that a friend request is genuine. Each neuron processes its equation using a Sigmoid function. By utilizing a training dataset from platforms like Facebook or other social networks, our deep learning algorithm can identify patterns indicative of bot behavior. This is achieved through backpropagation, which helps to minimize the final cost function and refine the weights and biases of each neuron.

Scope for future work

- Each input neuron corresponds to a specific feature from each profile, which has been converted into a numerical value—for instance, gender can be represented as a binary number, where female is 0 and male is 1. To ensure that no single feature skews the results, values like age may be divided by a standard figure, such as 100. These neurons act as nodes, with each one tasked with a particular 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 Testing http://en.wikipedia.org/wiki/Software_testing

Manual Testing http://en.wikipedia.org/wiki/Manual_testing

Performance Testing http://en.wikipedia.org/wiki/Software_performance_testing