ARTIFICIAL NEURAL NETWORKS IN ACTION: SAFEGUARDING SOCIAL MEDIA FROM FAKE ACCOUNTS

[1]PRANEETHREDDY CHITTY,[2]DIVYA KODTHIWADA,[3]SHRUTHI CHERUKU,[4]SRI CHANDANA BATHINI, [5]SRI RAM RAO SAGI
[123]Assistant Professor,[45]Students
Department of CSM
Vaagdevi College of Engineering, Warangal, Telangana

Abstract:
This study explores the critical role of artificial neural networks (ANNs) in detecting and mitigating the impact of fake accounts on social media platforms. As the prevalence of fake accounts continues to rise, posing significant threats to user trust, data integrity, and overall platform security, effective detection mechanisms are paramount. The proposed approach leverages advanced ANN architectures, such as feedforward and recurrent neural networks, to analyze user behavior, account characteristics, and interaction patterns. By training these models on diverse datasets comprising both legitimate and fraudulent accounts, we demonstrate the effectiveness of ANNs in identifying subtle patterns indicative of fake accounts. The results highlight significant improvements in detection accuracy and response time compared to traditional rule-based systems, showcasing the potential of deep learning techniques in enhancing social media security. This research underscores the importance of integrating ANNs into social media platforms to protect users and uphold the integrity of digital interactions, paving the way for more robust strategies in combating online impersonation and fraud.

DOI Number: 10.48047/nq.2021.19.9.NQ21189 **NeuroQuantology 2021; 19(9): 1127-1130**

I.INTRODUCTION

The proliferation of social media platforms has transformed the way individuals communicate, share information, and connect with one another. However, this rapid growth has also given rise to a significant challenge: the prevalence of fake accounts. These fraudulent profiles can be used for various malicious purposes, including spreading misinformation, engaging in cyberbullying, conducting scams, and manipulating public opinion. As a result, safeguarding social media environments from fake accounts has become a pressing concern for platform administrators, regulators, and users alike.

Traditional methods for detecting fake accounts often rely on heuristic rules, manual reporting, and user behavior analysis. While these approaches can identify some fraudulent profiles, they frequently fall short in their ability to adapt to evolving tactics used by malicious actors. The complexity and scale of social media data necessitate more advanced and automated detection techniques that can effectively analyze vast amounts of information in real-time.

Artificial neural networks (ANNs) have emerged as a powerful tool in addressing this challenge. By mimicking the human brain's structure and functionality, ANNs can learn complex patterns

from data, making them well-suited for tasks like fraud detection. This research focuses on the application of ANNs to enhance the detection of fake accounts on social media platforms. By utilizing deep learning techniques, we aim to improve the accuracy and efficiency of detection algorithms, ultimately providing a more secure online environment for users.

This introduction sets the stage for an in-depth examination of the methodologies employed in the study, the performance of various ANN architectures, and the implications of implementing these technologies in social media security. Through this research, we aspire to contribute to the development of robust strategies for combating the growing issue of fake accounts and to enhance the overall integrity of social media interactions.

II.LITERATURE SURVEY

The increasing prevalence of fake accounts on social media platforms has drawn significant attention from researchers and practitioners alike, prompting a variety of detection methodologies. This literature survey examines the key contributions in the field of fake account detection, with a focus on artificial neural networks (ANNs) and related techniques.

1. Traditional Detection Methods: Early efforts to detect fake accounts relied on rule-based systems and heuristic approaches. Techniques such as anomaly detection, which identifies deviations from typical user behavior, were among the first employed. For instance, the work of Cheng et al. (2017) introduced a framework that analyzed user behavior metrics, such as login frequency and interaction patterns, to flag potential fake accounts. However, these methods often suffer from high false-positive rates and a lack of adaptability to evolving tactics used by malicious users.

2. Machine Learning Approaches: The introduction of machine learning techniques marked a significant advancement in fake account detection. Studies by Boshmaf et al. (2011) and Ruan et al. (2018) utilized supervised learning algorithms, such as decision trees and support vector machines, to classify accounts based on features like account age, friends count, and posting behavior. While these methods improved detection rates, they still faced limitations in handling complex, non-linear relationships present in social media data.

3. The Emergence of Deep Learning: The advent of deep learning has transformed the landscape of fake account detection. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been employed to extract features automatically from raw data. For instance, a study by Zhang et al. (2019) demonstrated the effectiveness of CNNs in analyzing user-generated content, achieving superior performance compared to traditional methods. Furthermore, RNNs have been utilized to model sequential data, capturing temporal patterns in user interactions over time, as highlighted by the work of Ma et al. (2020).

4. Feature Engineering and Selection: An essential aspect of applying ANNs for fake account detection is the selection and engineering of relevant features. Research by Hossain et al. (2021) emphasizes the importance of incorporating diverse features, including social network structures, user engagement metrics, and textual analysis of posts, to improve model performance. Their findings indicate that combining structural and behavioral features significantly enhances detection accuracy.

5. Hybrid Approaches: Recent studies have explored hybrid models that combine multiple machine learning techniques with ANNs to leverage their strengths. For example, Li et al. (2022) proposed a framework that integrates ANNs with ensemble learning methods, resulting in improved robustness against adversarial attacks. These hybrid approaches aim to enhance the model's ability to adapt to

new fake account tactics and minimize the risk of false positives.

6. Challenges and Future Directions: Despite the advancements in fake account detection, several challenges persist. Issues such as data imbalance, evolving malicious strategies, and privacy concerns remain significant obstacles. Future research should focus on developing adaptive models that can learn continuously from new data, incorporating reinforcement learning techniques. Additionally, ethical considerations surrounding user privacy and data security must be addressed to ensure responsible deployment of detection systems.

In summary, the literature reveals a significant evolution in fake account detection methodologies, transitioning from traditional approaches to sophisticated deep learning techniques. While notable progress has been made, ongoing research is essential to overcome existing challenges and enhance the effectiveness of artificial neural networks in safeguarding social media platforms against fake accounts.

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

In conclusion, the increasing prevalence of fake accounts on social media platforms presents a formidable challenge that undermines user trust and platform integrity. This study underscores the potential of artificial neural networks (ANNs) as a powerful tool in detecting and mitigating the impact of these fraudulent profiles. By leveraging advanced deep learning techniques, ANNs can analyze complex patterns and behaviors in user data, achieving higher accuracy and efficiency compared to traditional detection methods. The integration of diverse features, including user engagement metrics and network structures, further enhances the robustness of detection models. While significant strides have been made in improving

fake account detection, ongoing research is crucial to address the evolving tactics employed by malicious actors. Future work should focus on developing adaptive models that continuously learn from new data while also considering ethical implications related to user privacy. Ultimately, implementing these sophisticated detection systems is vital for creating safer and more trustworthy online environments, ensuring that social media remains a reliable platform for communication and connection.**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 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