IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

USE OF ARTIFICIAL NEUTRAL NETWORKS BY IDENTIFY FAKE PROFILE

[1]P MOUNIKA, [2]T. PALLAVI SURYA

[1](Assistant Professor), MCA, DNR college(A) PG courses Bhimavaram

[2]MCA, scholar, DNR college(A) PG courses Bhimavaram

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 is the 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.

1.INTRODUCTION

- 2017 Facebook reached a total population of 2.46 billion users making it the most In 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,

ISSN 2347–3657

Volume 12, Issue 3, 2024

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.

2.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.

Disadvantages

- ➢ The system is not implemented Learning Algorithms like SVM.
- ➢ The system is not implemented any the problems involving social networking like privacy, online, misuse, and many others.

3.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

- ✓ In the proposed system, Profile

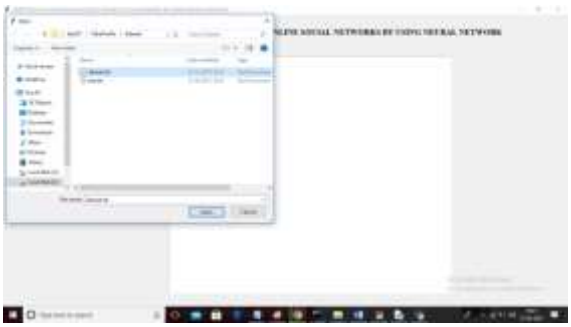
ISSN 2347–3657

Volume 12, Issue 3, 2024

information in online networks will also be static or dynamic. The details which can be supplied with the aid of the person on the time of profile creation is known as static knowledge, the place as the small print that are recounted with the aid of the system within the network is called dynamic knowledge.

- ✓ In the proposed system, Social Networking offerings have facilitated identity theft and Impersonation attacks for serious as good asattackers.

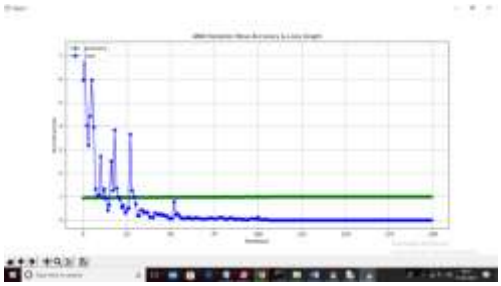
4.SCREEN SHOTS

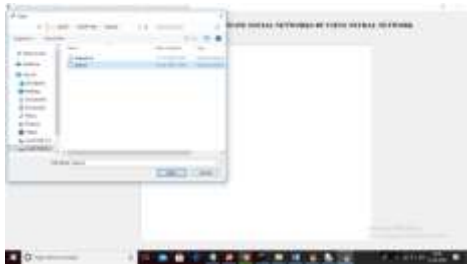


International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024





5.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.

6.REFERENCES

- Brooks,R.E.(1997) ―Towards a theory of the cognitive processes in computer programming,‖ Int. J. Man-Mach. Studies, vol. 9, pp. 737–751.
- Liu, B., & Lu, Z. (2012). "Learning to identify fake profiles in online social networks." Proceedings of the 21st ACM International Conference on Information and Knowledge Management (CIKM '12).
- Al-Garadi, M. A., et al. (2016). "Detecting fake accounts in online social networks at the time of registrations." Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM '16).
- Pan, S. J., & Yang, Q. (2010). "A survey on transfer learning." IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345-1359.
- Singh, M., et al. (2021). "Detecting fake profiles on social media using machine learning: A systematic review." Journal of Ambient Intelligence and Humanized Computing.
- H. Peng, et al. (2016). "A study of feature selection for social network analysis using data mining techniques." *Social Network Analysis and Mining. Springer.*