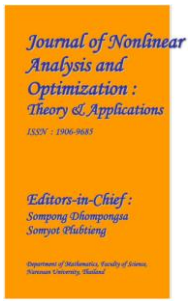
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 12, No. 1, (2021),
ISSN : **1906-9685**



ANN TECHNOLOGY-BASED FAKE OSN PROFILE IDENTIFICATION AND DETECTION

[1]Srilakshmi Darapureddi, [2]Sai Rekha Raghupatruni, [3]Aruna Kumari Aku La, [4]Mandumula Shivani
[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Computer science and Engineering, Rishi MS Institute of Engineering and Technlogy for Women, Kukatpally, Hyderabad.

ABSTRACT
Applied sciences are now expanding quickly. The use of smart phones is growing. Everybody now uses online social networks, which make it simpler to make new friends, stay in touch with old ones, and follow one's passions. However, there are some negative aspects to the growth of internet networking, such as people fabricating profiles. We can determine the authenticity of an account's information by using neural networks. To train an artificial neural network (ANN) algorithm that will be employed whenever fresh test data is provided to distinguish between real and fake user accounts, all previous users' fraudulent and actual account data will be used.

1. INTRODUCTION
Tens of millions of people use the internet for long-distance communication, consuming trillions of minutes of their time in the process. OSN administrations include social networking platforms like Facebook and MySpace, understanding-driven platforms like Twitter and Google Buzz, and social networking platforms used to introduce frameworks like Flicker. Social Networking Sites Online (OSN). Contrary to popular assumption, ensuring OSN privacy and enhancing security is a difficult task with a significant bottleneck. People disclose a staggering amount of information about their personal lives on social media platforms (Sns). We are great targets for special attacks because to our entire or partial exposure to the general public, including the most horrible of them all, ID burglary. It is possible to commit data fraud when an individual takes advantage of a character's abilities for their own personal gain or gain of some other kind. It has been a major problem in the past several years because it has affected a large number of people around the world. Victims of ID theft may be subjected to a wide range of consequences, including loss of time and money, placement in a correctional facility, destruction of their public image, and impairment to their relationships with partners, friends, and family. As of right moment, the vast majority of SNs no longer checks the duties of common users and have privacy and security techniques that are completely insecure. Many of SN's programmers default to a low level of privacy, making it an ideal platform for misrepresentation and abuse. For genuine assailants equivalent to innocents, person-to-person communication contributions have worked in conjunction with data fraud and impersonation attacks. To add insult to injury, customers are expected to have a working knowledge of social networking sites in order to create a profile. Simply keeping an eye on what customers post online might lead to catastrophic failures, and that's before we even consider the possibility that these bills have been compromised. Web-based companies' profiles might be static or dynamic, depending on the company's policy. Static information refers to the specifics that an individual can supply at the time of profile creation, whereas dynamic information refers to the location as the key portion that is specified with the framework's guide inside the company. Segment components and advantages of a person are incorporated into static data, while runtime propensities and region for an individual are stored in dynamic data. Static and dynamic data are used extensively in

http://doi.org/10.36893/JNAO.2021.V12I1.151-156

momentum studies. It's not suited to a large number of informal groups, where just a few static profiles can be observed and dynamic profiles are usually not evident to the organisation. More than one approach has been presented by exceptional experts who are trying to figure out the false characters and harmful content material in web-based informal communities. There were positives and negatives to every interaction. Long-distance interpersonal communication difficulties, such as security, web-based agony, abuse, and savaging, as well as a number of other issues, are addressed. Many of these examples include the use of false information in long-distance interpersonal contact profiles. A misleading profile is a profile that isn't explicitly stated, such as a profile of a person whose qualifications are incorrect. More and more, people are engaging in pernicious and undesired activities as a result of bogus Facebook profiles, which is causing some problems for social local area clients. For social designing, online pantomime to stigmatise a man or woman, advancing and campaigning for a person or a group of people, people create fake profiles. In order to prevent spamming, phishing, etc., Facebook has its own security system. In addition, Facebook Immune framework is a common name for the comparable (FIS). The FIS is no longer prepared to detect more fraudulent Facebook profiles created by customers.

2. LITERAURE SURVEY

A variety of fake report attention approaches rely on the examination of human interpersonal agency profiles, with the goal of defining the characteristics or a combination thereof that aid in identifying the real and the fake records. In specifically, the profiles and posts are mined for information, and then machine learning methods are employed to build a classifier capable of identifying fake data. For example, In online social gaming apps, phantom profiles can be detected and described by Nazir et al. (2010) [1]. Facebook application "Fighters club" is examined in this article, which claims to reward consumers who recommend their friends to join the game. Players are encouraged to fabricate their identities by the game, according to the writers. For the consumer, offering these fake profiles within the game serves as an additional motivational factor.

Fake LinkedIn profiles have been documented by Adikari and Dutta [2]. Fake profiles can be discovered with 84% accuracy and 2.444% false negatives using restricted profile records as input. Applications include neural networks and SVMs as well as principal issue evaluation. In addition to highlighting the number of languages spoken, training, abilities, suggestions, interests, and accolades, these are just a few examples. The characteristics of profiles on strange websites, which are considered to be false, are used as a ground truth.

People, bots, and cyborgs are all included in Chu et al. (2010) [3]'s classification of Twitter money owed (i.e., bots and humans working in concert). An Orthogonal Sparse Bigram (OSB) textual content classifier is used to identify spamming data as a part of the problem formulation.

Social media supporter markets are studied by Stringhini et al. (2013) [4]. They describe the features of Twitter fanatics and the customers of the business sectors. False accounts ("sybils") and compromised accounts, whose vendors don't assume that the list of their followers is growing, are the two main types of bills pursued by the "client," according to the authors. Adherent markets customers may be well-known people or politicians, who want to appear to have a larger fan base, or may be crooks, who want to make their document appear consistently real, so they can spread malware and spam.

A study by Thomas et al. (2013) [5] focuses on the use of black market money due for Twitter spam distribution. Check out Facebook like cultivates by distributing honeypot pages by De Cristofaro et al. (2014) [6]. Based on their like behaviour, Viswanath and colleagues (2014) [7] identify out illegal market Facebook documents. Farooqi et al. (2015) discovered two black hat online industrial centres, My Cheap Jobs and Search Engine Marketing Clerks. Fayazi et al. (2015) believe that on-line review manipulation is possible.

THE SYSTEM THAT IS BEING PROPOSED

To determine whether a friend request is genuine or not, we employ machine learning, specifically an artificial neural network. Microsoft Excel is used to store both old and new phoney data profiles.

http://doi.org/10.36893/JNAO.2021.V12I1.151-156

A data frame is then used to store the results of the algorithm. A training set and a testing set will be created from this data. Our model would have to be trained using data from social media sites.
Training set characteristics include Account age, Gender, User age, Link in the description, Number of messages sent out, Number of friend requests made, Entered location, Location by IP, and Fake or Not. Each of these variables is put through its paces and given a numerical value. A value of (1) is assigned to the training set for Gender if the profile can be identified as female or male. It is possible to use the same method to other variables. In addition, the country of origin is taken into consideration. Using this information, we divide the number of messages sent by the account's age to get the number of messages sent out parameter. Because we are working with a huge number of values that are highly interdependent, we divide the Number of friend requests sent out parameter by the Number of friends. This parameter is then utilised largely for multi-dimensional matrix multiplication.
By employing neural networks, we can determine whether or not an account's information is authentic. Every time we provide fresh test data, this ANN train model is applied to the new test data in order to determine whether or not the account details provided are those of legitimate or bogus users.

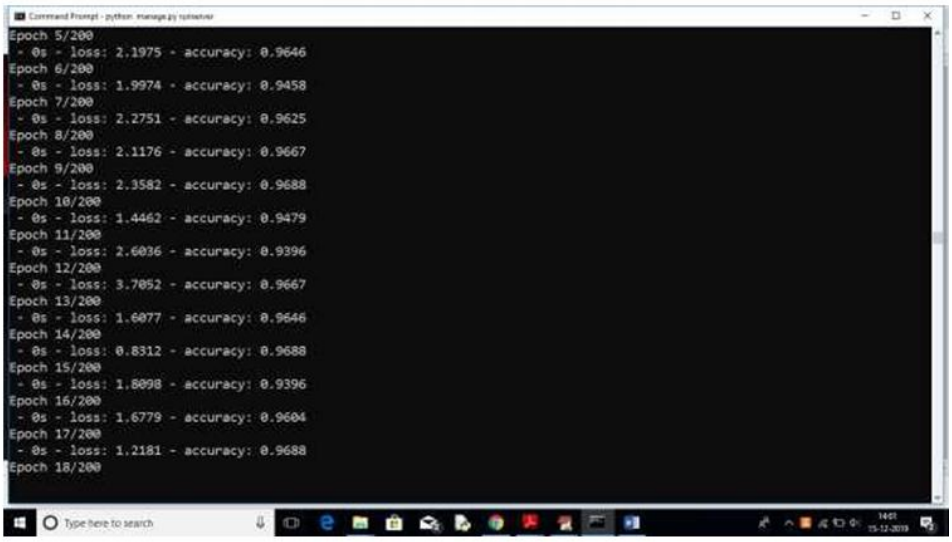
3. MODULE DETAILS:

Admin Module: Admin will login to application by using username as ‘admin’ and password as ‘admin’ and then perform below actions.
a. Generate ANN Train Model: Admin will upload profile dataset to ANN algorithm to build train model. This train model can be used to predict fake or genuine account by taking new account test data. Some unscrupulous individuals will hack into social network databases to steal or breach user information, which is why we utilise the ANN Algorithm to protect user data on sites like Facebook and Twitter.
b. View ANN Train Dataset: Using this module admin can view all dataset used to train ANN model. User Module: Any user can use this application and enter test data of new account and call ANN algorithm. ANN algorithm will take new test data and applied train model to predict whether given test data contains fake or genuine details.

4. RESULTS AND DISCUSSIONS

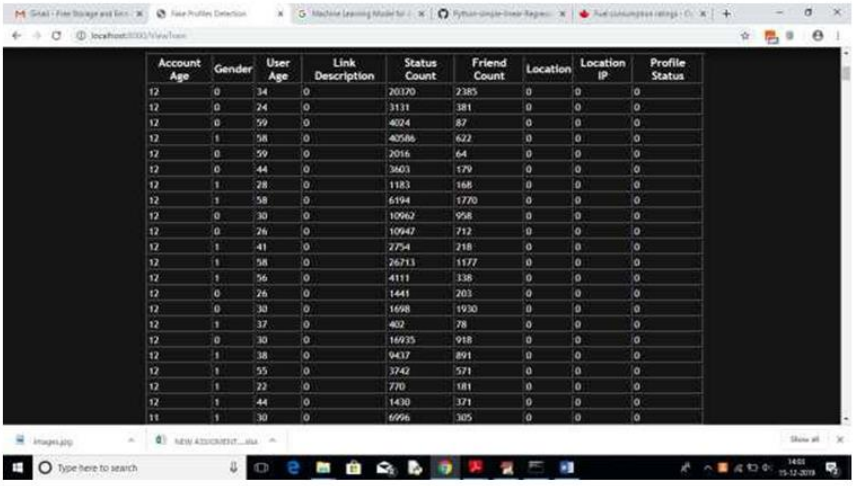
In above screen click on ‘Generate ANN Train Model’ to generate training model on dataset. After clicking on that link you can see server console to check ANN processing details with accuracy

http://doi.org/10.36893/JNAO.2021.V12I1.151-156



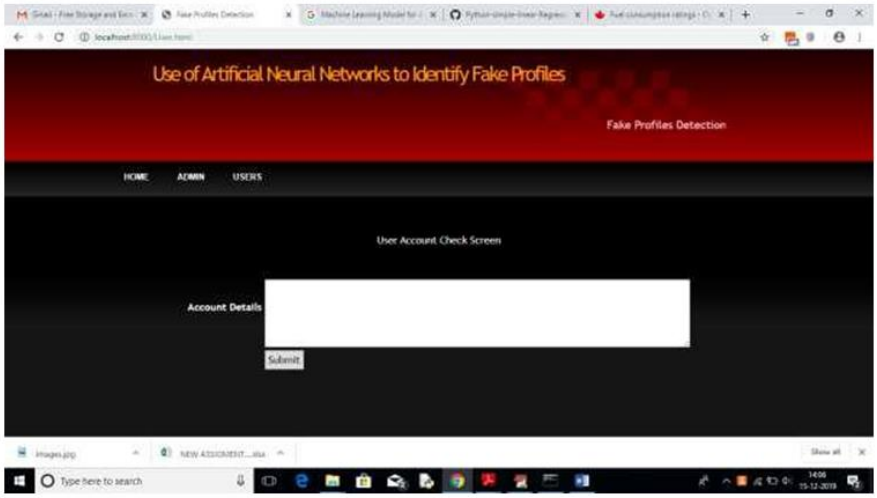
In above black console we can see all ANN details.

In above screen we can see ANN got 98% accuracy to train all Facebook profile. Now click on 'View Ann Train Dataset' link to view all dataset details



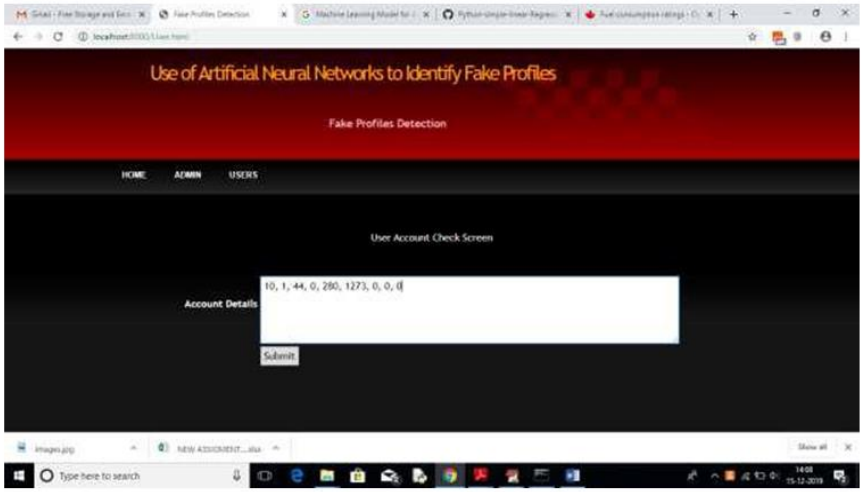
In above screen we can see all train data and scroll down to view all records. Now ANN train model is ready and you can logout and click on 'User' link to get below screen.

http://doi.org/10.36893/JNAO.2021.V12I1.151-156

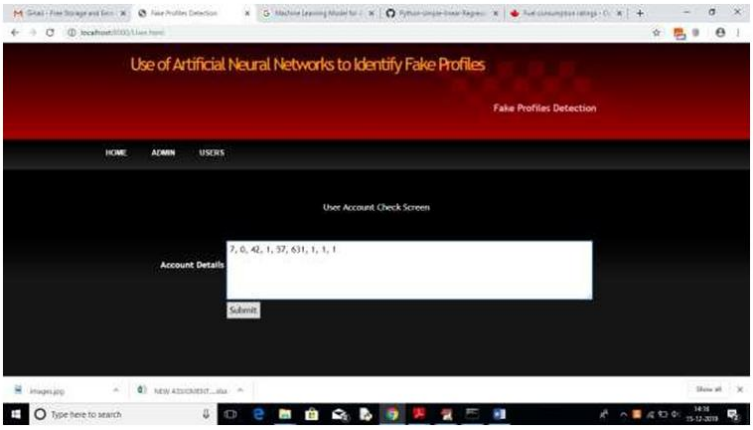


In above screen enter some test account details to get prediction/identification from ANN. You can use below records to check

10, 1, 44, 0, 280, 1273, 0, 0
10, 0, 54, 0, 5237, 241, 0, 0
7, 0, 42, 1, 57, 631, 1, 1
7, 1, 56, 1, 66, 623, 1, 1

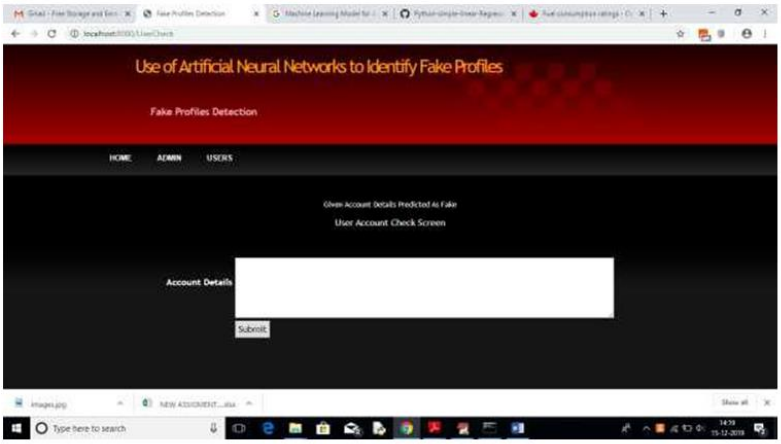


For above input will get below result



For above account details we got below result

http://doi.org/10.36893/JNAO.2021.V12I1.151-156



In above screen we got result as fake for given account data

CONCLUSION

In order to determine whether a friend request is legitimate or not, an artificial neural network (ANN) is utilized in this study. Each equation is subjected to a Sigmoid function at each neuron (node). We get training data from social networks like Facebook. By minimizing the final cost function, adjusting each neuron's weight and bias, and using back propagation, deep learning algorithms like the one depicted below can learn patterns of bad behavior. This document includes descriptions of the classes and libraries involved. Also covered are the sigmoid function and the selection and application of weights. For our solution, we also consider the social media page's most important features.

REFERENCES

1. https://www.statista.com/topics/1164/social-networks/
2. https://www.cnbc.com/2018/01/31/facebook-earnings-q4-2017- arpu.html
3. https://www.cnet.com/news/facebook-breach-affected-50-millionpeople
4. https://www.facebook.com/policy.ph p
5. Qiang Cao, Michael Sirivianos, Xiaowei Yang, and Tiago Pregueiro. 2012. Aiding the detection of fake accounts in large scale social online services. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (NSDI'12). USENIX Association, Berkeley, CA, USA, 15-15.
6. Akshay J. Sarode and Arun Mishra.2015. Audit and Analysis of Impostors: An experimental approach to detect fake profile in an online social network. In Proceedings of the Sixth International Conference on Computer and Communication Technology 2015 (ICCCT '15). ACM, New York, NY, USA, 1-8. DOI: https://doi.org/10.1145/2818567.281856 8
7. Devakunchari Ramalingam, Valliyammai Chinnaiah. Fake profile detection techniques in large-scale_online social networks: A comprehensive review. Computers & Electrical Engineering, Volume 65, 2018, Pages 165-177, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2017.05.020.