DETECTING UNAUTHORIZED OR FRAUD PROFILES USING ARTIFICIAL NEURAL NETWORKS

[1]Mr K.K. SWAMY
Assistant Professor *in Sreyas Institute of Engineering and Technology, JNTUH, India.*
kk.swamy@sreyas.ac.in
[2]Ms. B. MEGHANA REDDY
B.Tech in Sreyas Institute of Engineering and Technology, JNTUH, India.
Meghanabethelli@gmail.com
[3]Mr. K. SAI CHAITANYA
B.Tech in Sreyas Institute of Engineering and Technology, JNTUH, India. saikashetty2001@gmail.com
[4]MS. M. HARINI
B.Tech in Sreyas Institute of Engineering and Technology, JNTUH, India.
medishettyharini@gmail.com
[5]Mr. T. MEHER PRANEETH
B.Tech in Sreyas Institute of Engineering and Technology, JNTUH, India.
Praneethtirunagari@gmail.com

ABSTRACT:

In moment's digital age, the ever- adding reliance on computer technology has left the average citizen vulnerable to crimes similar as data breaches and possible identity theft. These attacks can do without notice and frequently without announcement to the victims of a data breach. At this time, there's little provocation for social networks to ameliorate their data security. These breaches frequently target social media networks similar as Face book, Twitter, Instagram and many other platforms. They can also target banks and other fiscal institutions. Vicious users' produce fake accounts to phish login information from unknowing users. A fake profile will shoot friend requests to numerous users' with public profiles. These fraud account users bait unknowing genuine users with film land of people that are considered seductive. Once the person accepts the request, the fake user of the phony profile will spam friend requests to anyone this person is a friend. Then, by using Artificial Neural Networks (ANN) we're relating whether given account details are from genuine or fake users'. ANN algorithm will be trained with all former users' fake and genuine account data and also whenever we gave a new test data then that ANN train model will be applied on new test data to identify whether given new account details are from genuine or fake accounts. Online social networks similar as Face book or Twitter contain users' details and some vicious users' will hack social network database to steal or transgress genuine user's information, to cover users' data we're using ANN Algorithm. To train ANN algorithm we're using below details from social networks. Age of Account, User gender, Age of user, Profile link description, Usage count, Friends or followers count, Position, Location IP address, Status.

Keywords – Artificial Neural Networks, Data Security, Identify Fake Biographies.

1. INTRODUCTION

Social media is a platform where each person has a profile about themselves which make connections with people, transfer information about them on online.[2] These social media platforms or Networks use different type of technologies which helps users in maintaining their accounts either with permanent or temporary purposes. This type of accounts welcome users with similar hobbies or interests connect easily. These accounts may be anything for example Face book, Twitter, Snap chat, Instagram, Online gaming sites etc. In 2017 Face book has reached a complete population of 2.46 billion users making it the foremost popular choice of social media. Social media networks make revenues from the information provided by users. The information of a user over different social media can be categorized into two types i.e. static and dynamic. The information is considered as static if the information is given while creating an account, for example name to display to other users, date of birth, interests, email id and phone number, etc. After a user created an account the amount the time the person is using the account, the purpose of using an account, number of persons the user is friend with, the type of content the user likes and shares is considered as dynamic information. There are many problems to be considered on social media like privacy breach, bullying with texts and comments, misusing, trolling and may others. These problems will be created by the users whose intention is to phish information from other users either by hacking or asking by blackmailing. The average user doesn't know that their rights are given up the instant they use the social media network's service. Social media companies have tons to realize at the expense of the user. In moment's digital age, the ever-adding reliance on computer technology has left the average citizen vulnerable to crimes similar as data breaches and possible identity theft. These attacks can do without notice and frequently without announcement to the victims of a data breach. Most of the attackers use these profiles to make money by capturing it from unknown genuine users. At this time, there's little incitement for social networks to ameliorate their data security. These breaches frequently target social media networks similar as Face book and Twitter. They can also target banks and other institutions such as business or financial.

2. OBJECTIVE

As the usage of computer technology is being increased day by day, there is no significant security to the user’s data where there are possibilities of data breaches and theft from unauthorized or Fraud profiles and thereby detecting fraud profiles will make users safer to utilize the technology. We use machine learning, namely an artificial neural network to determine what are the chances that social media networks like face book friend request is Authentic or not.

3. LITERATURE SURVEY

It's the most important part of your report as it gives you a direction in the area of your exploration. It helps you set a thing for your analysis- therefore giving you is your problem statement. [1]Neural networks, also known as artificial neural networks (ANNs) or dissembled neural networks (SNNs), are a subset of machine literacy and are at the heart of deep literacy algorithms. Their Name and structure are inspired by the neurons of brain,

mimicking the way that natural neurons gesture to one another. Artificial neural networks (ANNs) are comprised of a knot layers, containing an input sub caste, one or further layers, and a sub caste. Each knot, or artificial neuron, connects to another and has an associated weight and threshold. However, that knot is actuated, transferring data to the coming sub caste of the network, if the connection of any individual knot is above the specified threshold value. Else, no data is passed along to the coming sub caste system of the network.

Profiles in social media platforms have the information of input date like user name, gender orientation, etc. Some part of this input data can be whether the profile can be private or public, whether the information of user can be seen by everyone or only limited people. As the main objective is to determine the fake profiles we approach a procedure.

1. [3]Data sets are to be selected as attributes from the profile.
2. After selection we determine the type of attribute.
3. We prepare a database with the collected attributes and separated them as either fake or genuine.
4. This dataset is then set considered classifying the set of rules. It learns itself from the trained dataset to predict the output to the data we input.
5. This result will be based on Decision tree algorithm.

4. EXISTING SYSTEM

[2]Vicious users produce fake lives to phish login information from unknowing genuine users. A fake profile will shoot friend requests to multitudinous genuine users with public lives. These fake lives bait unknowing genuine users with profile 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 generally have links that lead to an external website where the damage happens. An ignorant 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 root attack turning the computer into unusable form of mode. While Face book has a rigorous netting to keep these fake accounts out, it only takes one fake profile to damage the computers of many. As the current system provides to find these type of profile but can manage only a single type of data set which can't be accurate to find the lives which a cause damage to the unknowing profile.

5. PROPOSED SYSTEM

In our system, we use machine knowledge, known as artificial neural network to determine what the chances that a friend request is suspicious are or not. [4]The algorithms we use are support vector machine and decision tree. We use Microsoft Excel to store old and new fake data lives. The Decision Tree algorithm also stores the data in a data frame. The neural network method we use is considered by which a computer can work with the instructions or algorithms we provide and provides an output based the input it takes. [1]This concept of artificial neural networks helps with a problem by training a network to build a program which can learn in its own way and generate a solution which can be closely related to the certain point of accuracy. We use sigmoid function to determine the output value. Rectified

linear unit and fully controlled layers of artificial neural networks are used as activation functions. [4]This collection of data can be parted into a training set and a testing set. We would need a data set from the social media spots 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 dispatches transferred out, Number of friend requests transferred out, Entered position, Position by IP, Fake or Not. Each of these parameters is tested and assigned a value. For illustration, for the gender parameter if the profile can be determined to be a woman or girl a value of (1) is assigned to the training set for Gender and (0) for man or boy. The same procedure will be applied to other parameters. We can also use the origin state or country as a factor. By this we determine how much number of text or multimedia messages has been sent by the account, how many numbers of friend requests has been sent and received by the account.

6. IMPLEMENTATION

To determine the procedure of building an ANN based image classifier, we have to build an input layer, hidden layer and output layer which can identify and separate the images from one to another. This neural network can be constructed even on small networks. [1]Neural networks are technically a mathematical model which can be used in solving the problem of optimization. The primary computation of neural networks is neurons. Performance includes all those conditioning that take place to covert from old system to new system. The old system consists of manual operations, which is operated in a truly delicate manner from the proposed system. A proper performance is essential to give a reliable system to meet the conditions of the association.

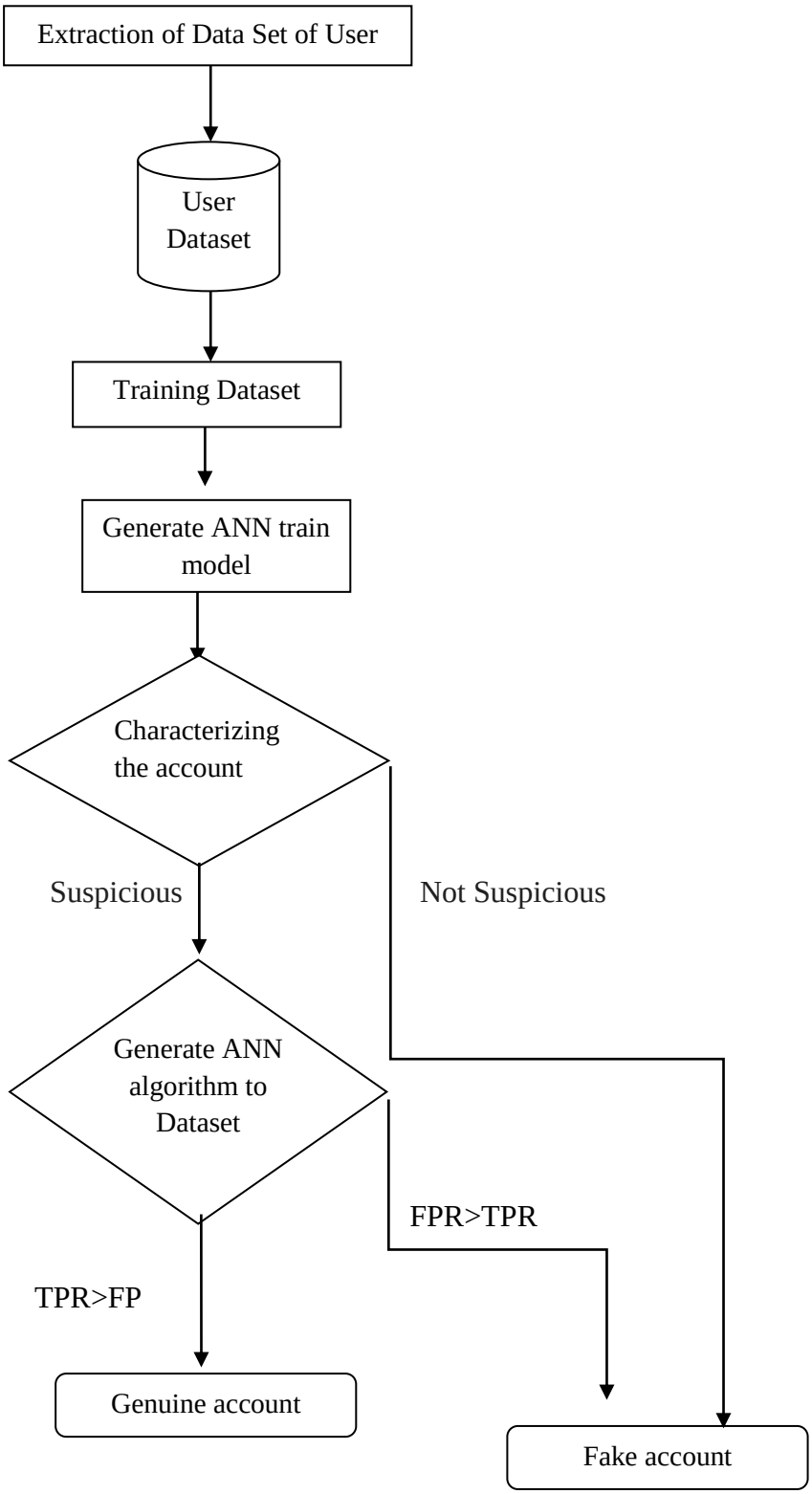
[6]Admin Module Admin will login to operation by using username as ‘admin’ and word as ‘admin’ and also perform below conduct.

1. Firstly collect the required data and preprocess it i.e. introduce a train model. Induce ANN Train Model Admin will upload profile dataset to ANN algorithm to make train model. This training model can be used to predict suspicious or genuine account by taking new test data in to the account.
2. View ANN Train Dataset, [5] Using this module admin can see all the dataset used to train the ANN model.
3. Validation of data is required to find the final output of data i.e. fake or genuine so we create new type of features.
4. After applying neural networks’ algorithm we evaluate the accuracy result by generating the trained model of ANN.
5. In user Module any user can use this operation and enter test data of new account and call ANN algorithm. ANN algorithm will take new test data and applied train model to detect whether given test data contains fake or genuine details.

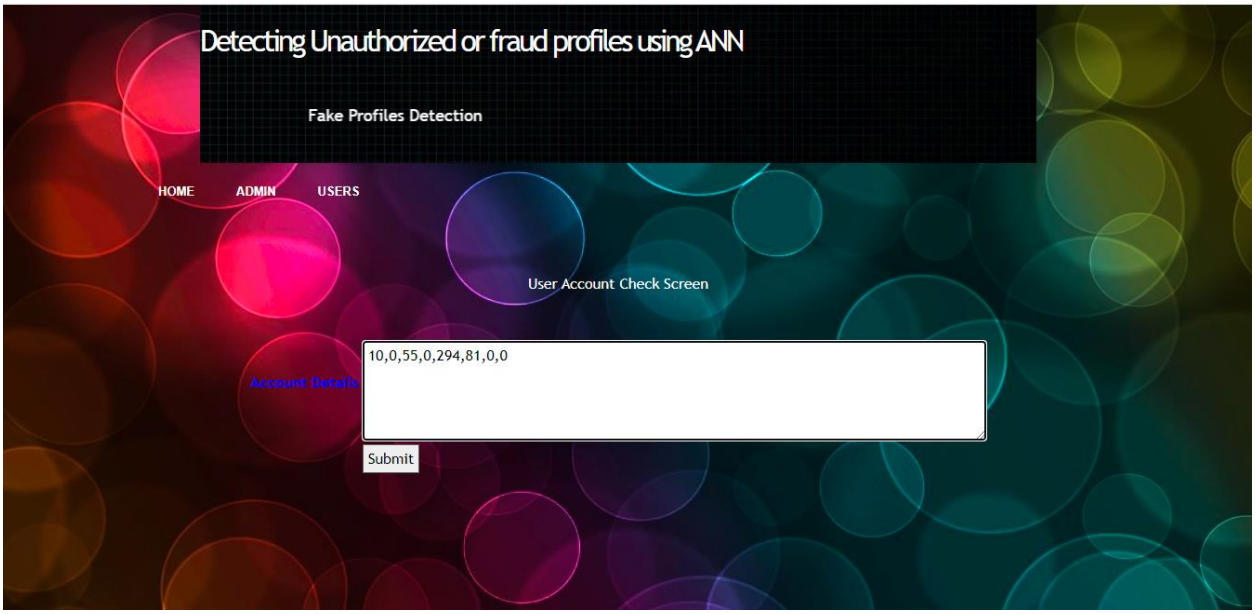
The data set we provide to train, generate and also as an input may have post count, count of the comments, followers counts, the events performed by the user, location of the account, number of posts tagged in, created time of profile and post (if any), and the description of profile. This output is depending upon the true positive rate and false positive rate within the algorithm. If the true positive rate is greater than the false positive rate then the profile is

considered to be genuine else if true positive rate is lesser than false positive rate then the profile will be considered as fake.

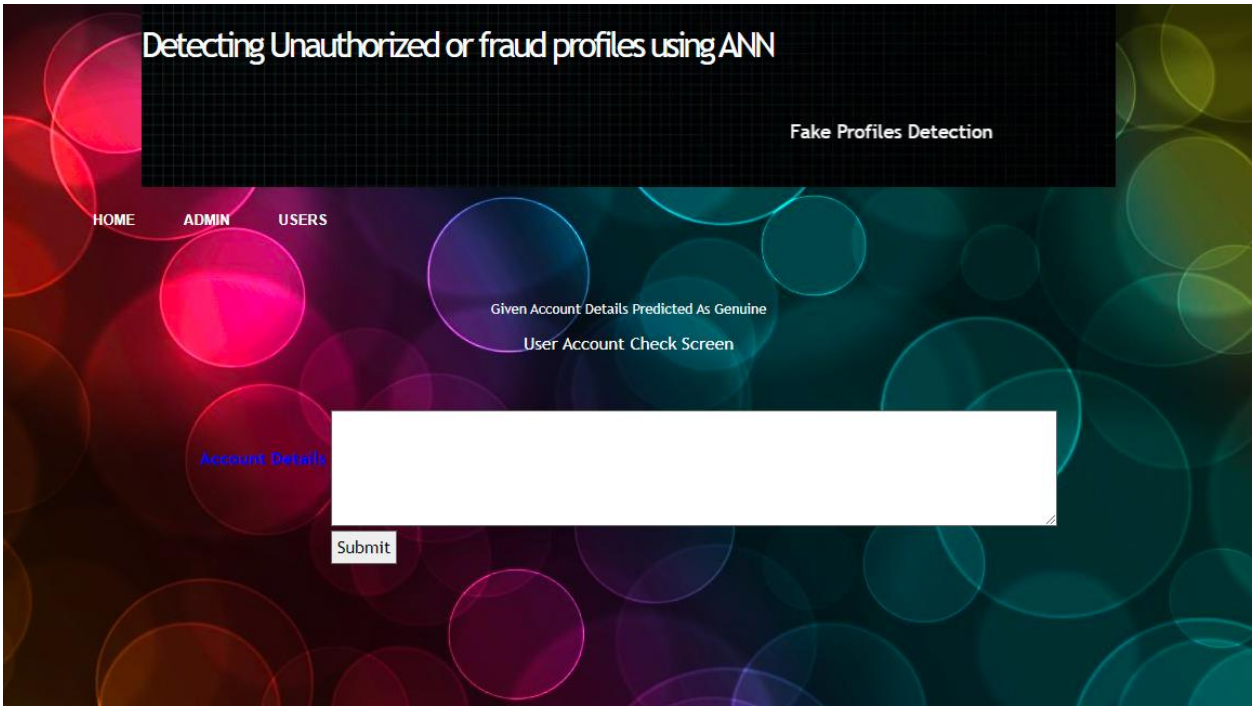
7. ARCHITECTURE



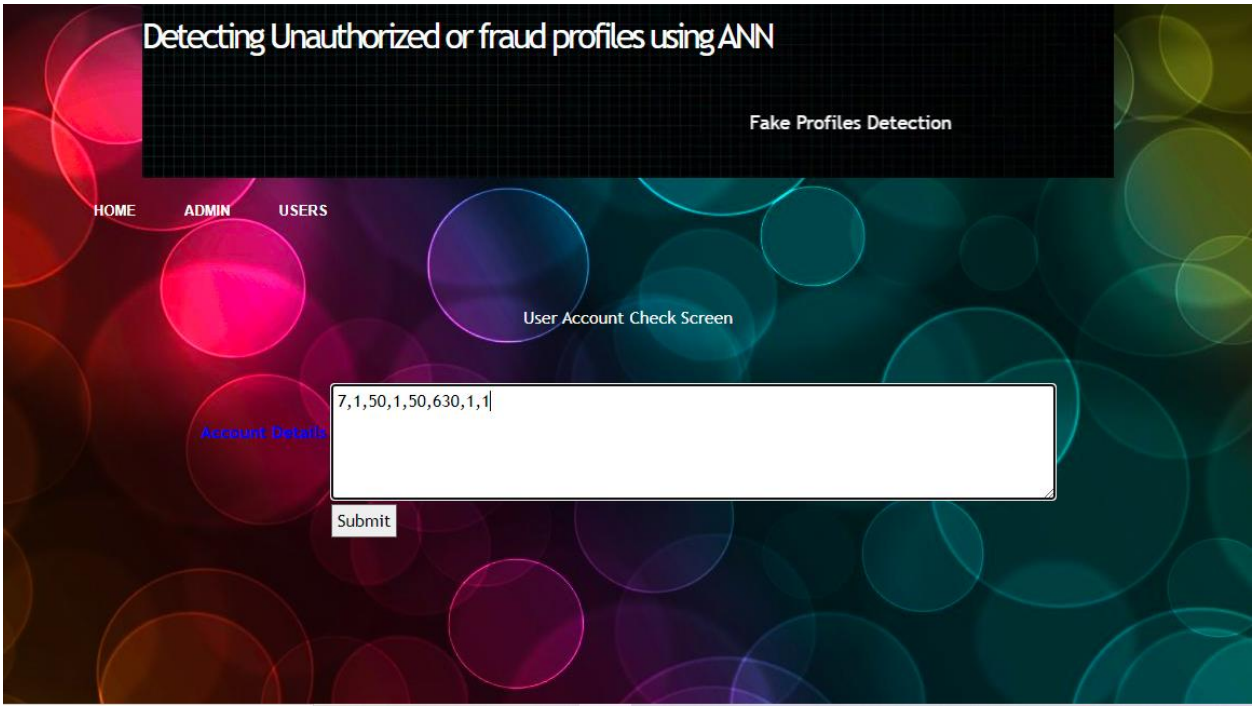
8. RESULTS



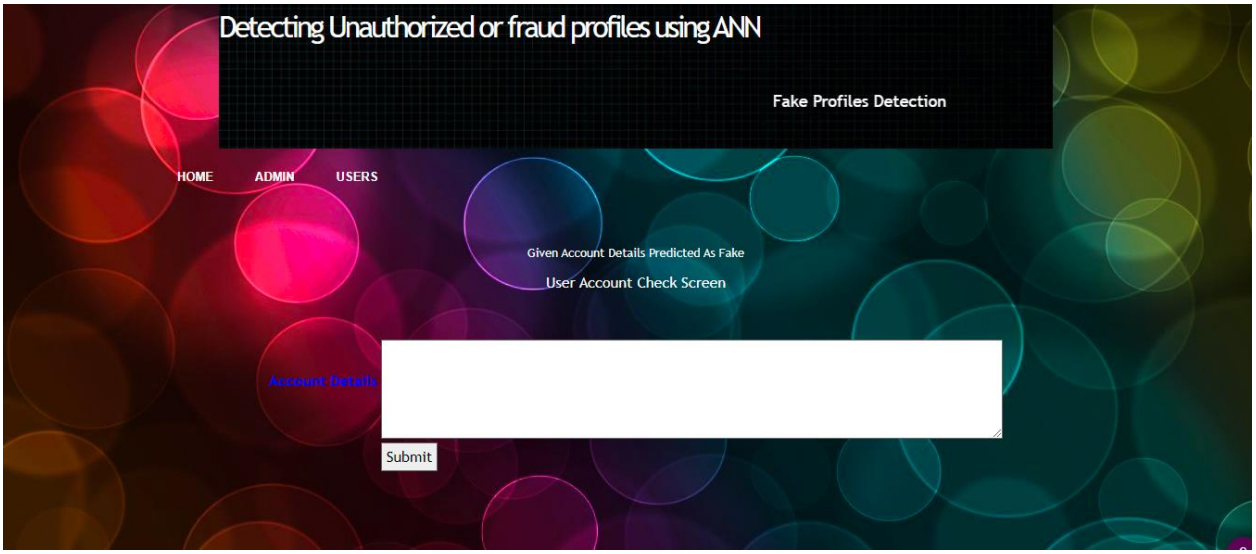
Input a Dataset of a profile, Trained algorithm will now compare given input to previous datasets.



And generates result as genuine based on the algorithm for this profile.



Input a Dataset of another profile and check the details.



Generates result as fake based on the algorithm for this profile.

9. CONCLUSION

Unauthorized or fake profiles are created over different social media platforms for various reasons. We use machine literacy, known as artificial neural network to determine what are the chances that a friend request is authentic are or not. Each equation at each neuron or a knot is put through a sigmoid function. We use a training data set by different social media networks. This would allow the presented Artificial neural networks algorithm to learn the patterns of a profile, provides further accuracy in detecting authentication of a profile by taking each input and training them with preliminarily trained data. Then after a new data is given as input, based on previous data sets the output is provided

10. FUTURE SCOPE

Each neuron input is considered as special, previously chosen feature of every profile changed into a numerical value, for example gender is defined with a binary number, like female is represented with 0 and male is represented with 1 and if needed, divided by an arbitrary number to minimize one feature having more influence on the result than the other. The neurons represent nodes. Each node would be liable for exactly one decision-making process. The main problem about social media is a person can create any number of accounts and can span request to breach the data. In order to avoid this we can bring in linking the identity cards like Aadhar etc. By using this type of identity a person can create only one account as it can restrict the user in creating another one.

12. REFERENCES

[1] ARTIFICIAL NEURAL NETWORKS by ROBERT J SCHALKOFF and also WEB TECHNOLOGIES – BLACK BOOK by KOGENT LEARNING SOLUTIONS

[2] Yadongzhou,Daewookkim,Junjiezhang,(Member,Ieee),LiliLiu1, Huanjin3, "(IEEE)ProGuard: Detecting Malicious Accounts in SocialNetwork-Based Online Promotions"

[3] For Datasets, referred Kaggle.

[4] Dr.Narsimha.G, Dr.JayadevGyani, P. Srinivas Rao ,"Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP(2018)", International Journal of Applied Engineering Research.

[5] https://www.pluralsight.com/blog/machine-learning/3-steps-train-machine-learning

[6] https://www.w3schools.com/html/html_responsive.asp