Spammer Detection and Fake User Identification on Social Network

Tanuja[1], Supritha P C[2], Tanzima Banu[3], Yashaswini R P[4], Vidya K[5]

Assistant Professor, Dept. of CS&E, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India [1]

B E Scholar, Dept. of CS&E, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India [2]

B E Scholar, Dept. of CS&E, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India [3]

B E Scholar, Dept. of CS&E, BGS Institute of Technology, B G Nagar, Mandya, Karnataka, India [4]

B E Scholar, Dept. of CS&E, BGS Institute of Technology, BG Nagar, Mandya, Karnataka, India [5]

ABSTRACT: Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter, Facebook, Snapchat, Flicker, etc have a tremendous impact and occasionally undesirable repercussions for daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amount of irrelevant and deleterious information. In this paper exclusive use of social media also makes it a popular platform for malicious users, known as social spammers, to normal users with unwanted content. One effective way for social spammer detection is to build a classifier based on content and social network information. We present a general optimization framework to collectively use content and network information for social spammer detection, and provide the solution for efficient online processing.

KEYWORDS: Spammer, malicious and general optimization framework

I. INTRODUCTION

Social media is one of the preferred means of communication. At a social media site, a user is usually identified by a profile. It typically contains a picture and name possibly an address and birth date. Identity alluded to in the profile created and controls the profile. If this is not the case, somebody is using somebody else identity. This is called a false identity. In this paper, we are going to identify the fake profile on social media. Online social networks simply called OSN's like facebook, Instagram; twitter allows the account holder to create their identity profile to update their activities to the public, in personal profile to talk with their friends, family, and colleagues. Also, these networks are used for business promotions and communications.

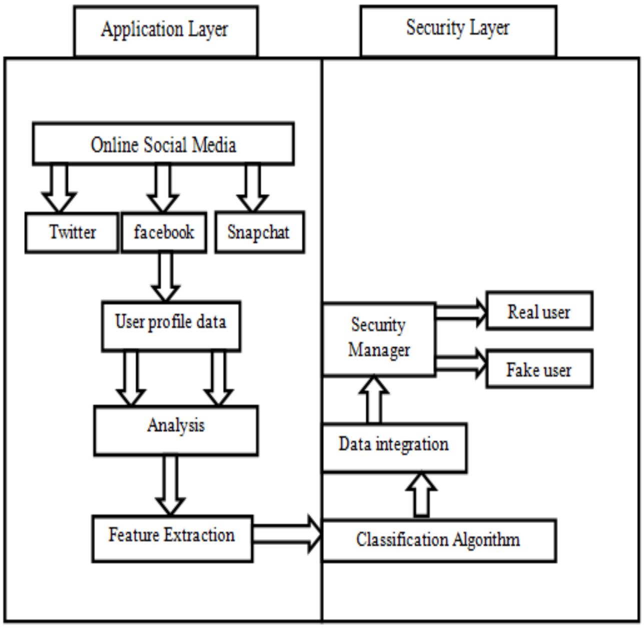
II. EXISTING SYSTEM

So far, the research community has paid little attention to OSN apps specifically. Most research related to spam and malware on Social has focused on detecting malicious posts and social spam campaigns. The existing system works concentrated only on classifying individual URLs or posts as spam, but not focused on identifying malicious applications that are the main source of spam on Social. The existing system works focused on accounts created by spammers instead of malicious applications. The existing system provided only a high-level overview of threats to the Social graph and do not provide any analysis of the system.

III. PROPOSED SYSTEM

Classification is a machine learning technique that assigns class labels to different groups. Classification is the most frequently used data mining function with a predominance of the implementation of and Support Vector Machines. The analysis of social media data improves the spam detection by improving the performance of social media user management tasks. The main application of data mining in the field of social media is predictive analysis. Spam can be predicted if the user's history is analyzed. Predictive analysis is a data mining technique applied to electronic spam records to effectively predict the spam at a very early stage. After identification, social users can avoid spam messages and spammer interaction in the usage of a social network.

IV. SYSTEM ARCHITECTURE



The application layer is used for establishing the process to process communication and user services in a network. Social media is a platform for market research and decision-making process. They create and generate data that enables data analysis to do the analysis.

Social media such as Instagram, Face book, and snap chat they contain fraudulent content it will extract the database and connect multiple applications the user profile data can be analyzed to extract the features of spam contents and obtain the accurate result. To provide security, it needs to secure the layer; the security manager separates the real and fake users. It classifies the supervised and unsupervised data it creates a hyper plane data into classes, data needs to be integrated.

V. METHODS

Back propagation is a supervised learning algorithm, for training Multi-layer Perceptrons (Artificial Neural Networks).While designing a Neural Network, in the beginning; we initialize weights with some random values or any variable for that fact. Now obviously, we are not superhuman. So, it's not necessary that whatever weight values we have selected will be correct, or it fits our model the best. We have selected some weight values in the beginning, but our model output is way different than our actual output i.e. the error value is huge. We need to reduce the error somehow explain the model to change the parameters (weights), such that error becomes minimum.

VI. **PROPOSED ALGORITHM**

In this Paper we are using two functionalities

1. Feature Extraction.
2. Classification Algorithm.

- **Feature Extraction:**

The data set contain the user name random post, historical behavior location identity. For Feature Extraction we are using Back Propagation Algorithm. Back Propagation Algorithm is a supervised Learning Algorithm for training the data set. We analyze the data based on criteria, if data feature matched it captured the features of matched values then the matched values send to the Support Vector Machine algorithm.

- **Classification Algorithm**

Classification of labeled train data set can be done by using SVM Algorithm, it can be used for face , image detection and text etc., Using SVM Algorithm we plot the data item with each value. This data will be used for clustering, it analysis a task of grouping a set of object in such a way that the objects in the same group or more similar to each other.

VII. PSEUDO CODE

The Back propagation algorithm looks for the minimum value of the error function in weight space using a technique called the delta rule or gradient descent. The weights that minimize the error function are then considered to be a solution to the learning problem.

Below are the steps involved in Back propagation:

- Step – 1: Forward Propagation
- Step – 2: Backward Propagation
- Step – 3: Putting all the values together and calculating the updated weight value

VIII. TESTING RESULTS

- **Registration Testing**

TEST N0	TESTING SCENERIO	EXPECTED RESULTS	RESULTS
TC – 01	Clicking submit without entering details	Alert "Please fill all details"	Pass
TC – 02	Clicking submit without entering Username	Alert "Please fill Username"	Pass
TC – 03	Clicking submit without entering password	Alert "Please fill Password"	Pass
TC – 04	Clicking submit without entering email id	Alert "Please fill email id"	Pass
TC – 05	Clicking submit without entering phone number	Alert "Please fill contact number"	Pass
TC – 06	Clicking submit entering confirm password data which is not matching with password data	Alert "Password and Confirm Password do not match"	Pass

- **Login Testing**

TEST NO	TESTING SCENERIO	EXPECTED RESULTS	RESULTS
TC – 07	Clicking submit without entering login details	Alert "Please enter the username and password"	Pass
TC – 08	Clicking submit entering wrong Username and password	Alert "Invalid User"	Pass
TC - 09	Clicking Delete user by admin	Alert "Deleted successfully"	Pass
TC - 10	Clicking View Post by admin	Post data displayed	Pass
TC - 11	Clicking Add post without selecting post details by user	Alert " please select the post"	Pass
TC-12	Clicking Add post with selecting post details by user	Alert " post added"	Pass
TC-13	Clicking View Fake user by user	Fake user details displayed	Pass

IX. CONCLUSION AND FUTURE WORK

In this paper, a Classifier based approach is given to solve the detection of spam messages. A classification model is mainly based on the machine learning algorithm which gives the output in the form of a binary value. Here the feature extraction is an important phase of the project to add more benefits to the system. A performance evaluation is carried out on a large dataset to identify the spammer also system helps to categories the spam and non-spam messages. It may include the implementation of the model in real-time, and assessing the performance. Accordingly, there can be changes made in the definitions of fake and spam content, thus resulting in better recall values for the categories. Following our procedures, steps can be taken to reduce the amount of non-legitimate data online and block the users who spread misinformation in the network.

REFERENCES

[1]Nagaratna Harikant, Suma V, “Risk Analysis in Facebook Based On UserAnomalousBehaviors” ICICCS 2017.

[2] Santa Barbara, Pittsburgh “COMPA: “Detecting Compromised Accounts on Social Networks”.

[3] HongyuGao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao “Detecting and Characterizing Social Spam Campaigns” IMC’10, November 1–3, 2010,

[4] PrateekDewan, PonnurangamKumaraguru, “Towards Automatic Real-Time Identification of Malicious Posts on Facebook” 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST)

[5] Tao Stein, Erdong Chen, Karan Mangla “Facebook Immune System” ACM Jan 1, 2011

[6] M.A. Devmane, Dr.N.K.Rana “Detection and Prevention of Profile Cloning in Online Social Networks” ICRAI E – 2014

[7]Yasmeen Sultana, Prof. B.I.Khodanpur,” Detecting the Malicious Application using FRAppE” ICICCS 2017

[8]Shukla Twinkle Kailas, Design of Machine Learning approach for spam tweet detection,2016

[9] Xiahou, Jiliang Tang, Huan Liu, Online Social Spammer Detection,2014.

[10] Dr. FenzaGiuseppe, Detectionod spam posting accounts o twitter,2018.