INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 2057-5688

DEEP LERNING BASED A FAKE PROFILE IDENTIFICATION USING ANN ALGORITHM

Gopinath[1], G Swarnalatha[2], S Prasad[3], A Sudheer[4]

[2,3,4]Assistant Professor, Department of CSE,Sri Indu College of Engineering & Technology, Hyderabad, Telangana, India.

[1]UG Scholars, Department of CSE, Sri Indu College of Engineering & Technology, Hyderabad, Telangana, India.

ABSTRACT:

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook 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. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased that result in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs). In our project, we performed a review of techniques used for detecting spammers on Twitter. Moreover, a taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also compared based on various features, such as user features, content features, graph

ISSN : 2057-5688

features, structure features, and time features. We are hopeful that the presented study will be a useful resource for researchers to find the highlights of recent developments in Twitter spam detection on a single platform.

Key words: OSN, fake users, ANN, platform.

I INTRODUCTION

Billion users making it the most popular choice of social media. 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, Face book makes revenue via advertisements and data. 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, 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. There seems to be a newsworthy issue involving social media networks getting hacked every day. Recently, Facebook had a data breach which affected about 50 million users. Facebook provides a set of clearly defined provisions that explain what they do with the user's data. The policy does very little to prevent the constant exploitation of security and privacy. Fake profiles seem to slip through Facebook's built-in security features. The other dangers of personal data being obtained for fraudulent purposes are the presence

ISSN : 2057-5688

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. The solution presented in this paper intends to focus on the dangers of a boot in the form of a fake profile on your social media. This solution would come in the form of an algorithm. The language that we chose to use is Python. The algorithm would be able to determine if a current friend request that a user gets online is an actual person or if it is a bot or it is a fake friend request fishing for information. Our algorithm would work with the help of the social media companies, as we would need a training dataset from them to train our model and later verify if the profiles are fake or not. The algorithm could even work as a traditional layer on the user's web browser as a browser plug-in.

2. RELATED STUDY

Sybil rank was designed in late 2012, to efficiently identify fake profiles through a ranking graph-based system. The algorithm uses a seed selection method combined with early terminated random walks to propagate trust. Its computational cost is measured in O (nlogn). Profiles are ranked according to the number of interactions, tags, wall posts, and friends over time. Unfortunately, this technique was found to be mostly unreliable because it failed to take into account the possibility that real profiles can be ranked low and fake profiles can be ranked high. Sarode and Mishra proposed a different approach which is a sequence of steps to detect fake profiles. They used the Facebook graph API tool to gain access to numerous profiles and wrote

ISSN : 2057-5688

a script to extract the viewed information. Later on, this extracted information forms the attributes the classifier will use in their algorithm. First, the data is in JSON format, which is further parsed to a structured format (CSV) that is easier readable by machine learning techniques. These comma separated values will later make the classifier more efficient. The authors tried unsupervised and also supervised machine learning techniques. In this case, supervised machine learning techniques had a higher accuracy rate of almost 98%. For supervised machine learning, they split up the dataset into training and testing sets. They used 80% of the samples to train the classifier and the rest to test it. After the algorithm runs, there is feedback provided to the profile, requiring it to submit identification to prove it is not a fake profile. Profiles are processed on mass to extract features. Resilient Back Propagation algorithm in neural networks algorithm combined with support vector machines is used in the classification of fake profiles. Sybil Frame uses multi-stage level classification. Approaches include content-based and structure based. Content-based approach explores the dataset and extracts information used to calculate prior information about nodes and edges. Structure-based approach correlates nodes using Markov random field and loopy belief propagation which employs previous information. The content-based approach is used in the first stage of Sybil Frame and Structure-based approach is used in the second stage of Sybil Frame technique. Clickstreams are analyzed, and Friend recommendations are examined in stage I. It is considered as the first line of defense due to limitations which include real accounts that were already compromised being sold.

3 METHODOLOGY

ISSN : 2057-5688

In this paper using Artificial Neural Networks we are identifying whether given account details are from genuine or fake users. ANN algorithm will be trained with all previous users fake and genuine account data and then whenever we gave 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 users. Online social networks such as Facebook or Twitter contain users details and some malicious users will hack social network database to steal or breach users information, To protect users data we are using ANN Algorithm. To train ANN algorithm we are using below details from social networks

Account_Age, Gender, User_Age, Link_Desc, Status_Count, Friend_Count, Location, Location_IP, Status. All fake users main intention is to send friend request to normal users to hack their machine or to steal their data and never they will have many number of posts or have many following friends and their account age also will have less number of years. By analysing this feature Facebook will mark whether user profile is fake or genuine. This Facebook profile data we downloaded from Facebook website and using this data to train ANN model. Below are some values from profile dataset.

4 RESULTS EXPLANATION

All fake users main intention is to send friend request to normal users to hack their machine or to steal their data and never they will have many number of posts or have many following friends and their account age also will have less number of years. By analysing this feature Facebook will mark whether user profile is fake or genuine. This Facebook profile data we downloaded from Facebook website and using this

ISSN : 2057-5688

data to train ANN model. Below are some values from profile dataset.

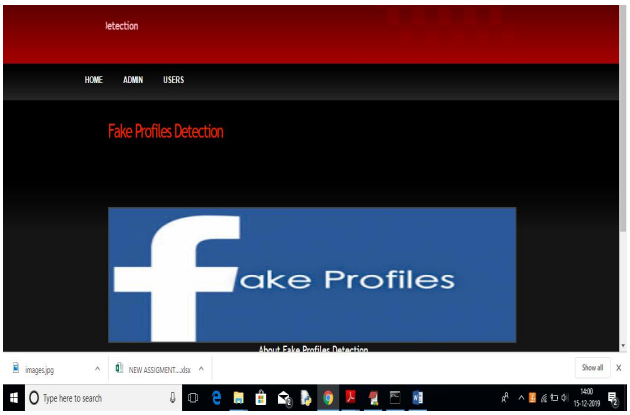

Fig.4.1. Admin Home page.

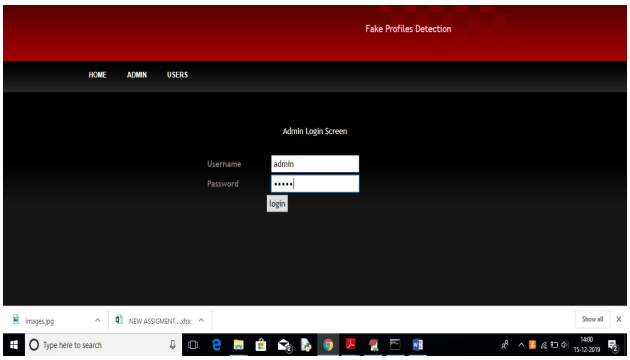

Fig.4.2. Admin login page.

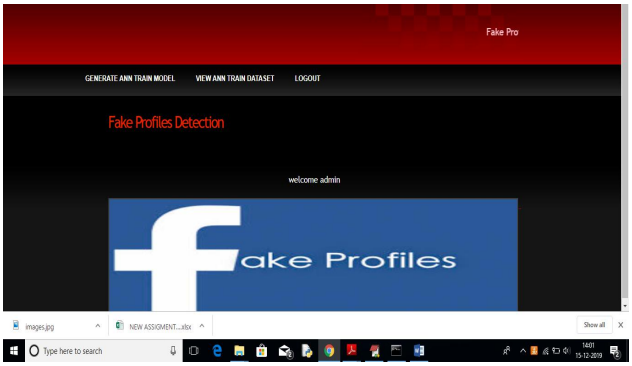

Fig.4.3. Fake profile detected.

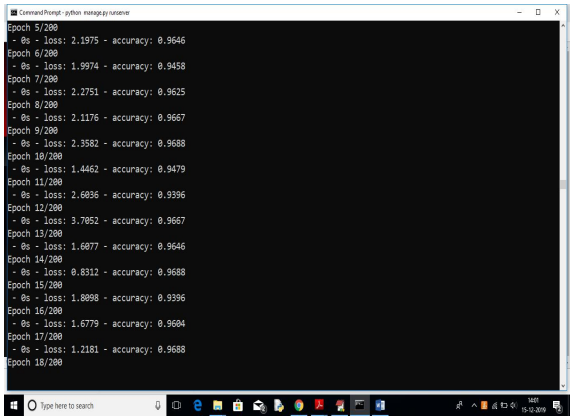

Fig.4.4. OUTPUT of ANN details.

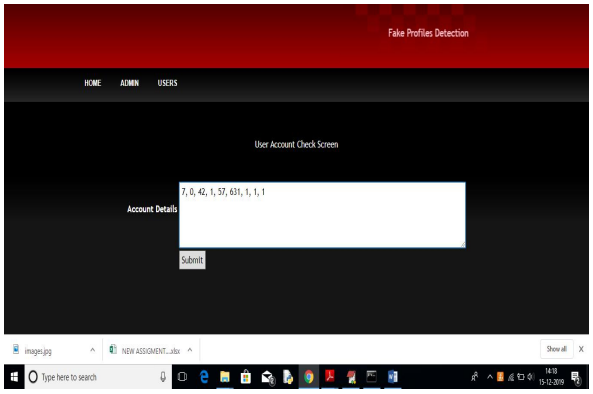

Fig.4.5. User account check screen.

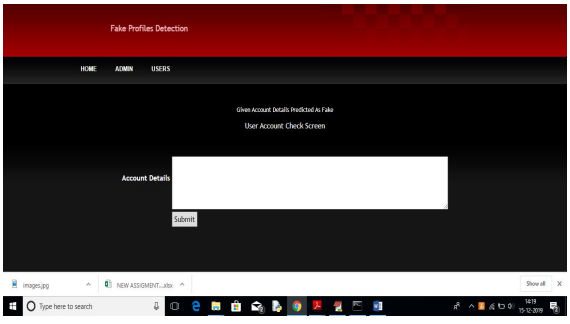

Fig.4.6. OUTPUT screen.

CONCLUSION

In this paper, we use machine learning, namely an artificial neural

ISSN : 2057-5688

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. In this paper, we outline the classes and libraries involved. We also discuss the sigmoid function and how are the weights determined and used. We also consider the parameters of the social network page which are the most important to our solutions.

REFERANCES

[1] B. Erçahin, Ö. Akta³, D. Kilinç, and C. Akyol, "Twitter fake account detection," in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388_392.

[2] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detectingspammers on Twitter," in Proc. Collaboration, Electron. Messaging, Anti- Abuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12.

[3] S. Gharge, and M. Chavan, "An integrated approach for malicious tweets detection using NLP," in Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), Mar. 2017, pp. 435_438.

[4] T. Wu, S. Wen, Y. Xiang, and W. Zhou,"Twitter spam detection: Survey of new approaches and comparative study," Comput. Secur., vol. 76, pp. 265_284, Jul. 2018.

[5] S. J. Soman, "A survey on behaviors exhibited by spammers in popular social media networks," in Proc. Int. Conf. Circuit, Power Comput. Tech- nol. (ICCPCT), Mar. 2016, pp. 1_6.

[6] A. Gupta, H. Lamba, and P. Kumaraguru, "1.00 per RT

ISSN : 2057-5688

#BostonMarathon # prayforboston: Analyzing fake content on Twitter," in Proc. eCrime Researchers Summit (eCRS), 2013, pp. 1_12.

[7] F. Concone, A. De Paola, G. Lo Re, and M. Morana, "Twitter analysis for real-time malware discovery," in Proc. AEIT Int. Annu. Conf., Sep. 2017, pp. 1_6.

[8] N. Eshraqi, M. Jalali, and M. H. Moattar, "Detecting spam tweets in Twitter using a data stream clustering algorithm," in Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK), Nov. 2015, pp. 347_351.

[9] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, "Statistical features-based real-time detection of drifted Twitter spam," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 914_925, Apr. 2017.

[10] C. Buntain and J. Golbeck, "Automatically identifying fake news in popular Twitter threads," in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2017, pp. 208_215.