ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2, 2024

Analyzing and Detecting Money- Laundering Accounts in Online Social Natworks

TALATAM. S V H KRISHNA NAIDU[1], Dr.V.Bhaskara Murthy[2]

[1]MCA Student, B V Raju College, Kovvada, Andhra Pradesh, India.

[2]HOD & Professor, B V Raju College, Kovvada, Andhra Pradesh, India.

Abstract: In seeing the present condition, online social networks are engaging with the majority of the people. From child to adult, all are spending a considerable time on these platforms either by exchanging information or making efficient communication with others. But nowadays, these social networking sites are suffering from a lot of fake accounts in taking advantage of vulnerabilities, either taking the benefits or targeting accounts attempting cybercrimes.

Keywords: Machine learning, fake reviews, online product, E-commerce, Product review monitoring.

I. INTRODUCTION

Online social media is the place each person has a outlook then be able to keep connecting their relations, transfer their updates, join with the people having same likes. Online Social Networks makes use of front end technologies, which permits permanency accounts in accordance with to know each other. Facebook, Twitter are developing along with humans to maintain consultation together with all others. The online accounts welcome people including identical hobbies collectively who makes users easier after perform current friends. Gaming and entertaining web sites which have extra followers unintentionally that means more fan base and supreme ratings. Ratings drives online account holders to understand newer approaches not naturally or manually to compete more with their neighbours. By these analogies , the maximum famous candidate in an election commonly get more number of votes. Happening of fake social media accounts and interests may be known. Instance is fake online account being sold on-line at a online market places for minimum price , brought from collaborative working offerings. More often feasible to have Twitter fans and Facebook media likes in online. Fake user accounts may be created

ISSN2321-2152
www.ijmece .com
Vol 12, Issue.2, 2024

by humans or computers like bots , cyborgs. Cyborg is half bot and half human account. These accounts are usually opened by human, but their actions are made by bots. The another reason for people to create fake profiles for defaming accounts they dislike. This type of users create accounts with the username of the people they hate and post irrelevant stories and snap shots on their accounts to redirect everybody so that they assume that particular person is awful and make their reputation low. Most attackers are in it to make money. They make money by distributing unwanted ads (spam) or capturing accounts they can reuse or resale (phishing). Spammers gather resources to know fake and real users, email ids ,ip locations and computing knowledge power. Every one of these advantages can have a huge expense related with them, and an assault, similar to any business adventure, needs benefit to continue onward. Attackers more often use facebook logins, applications, Events, Group users to gather login credentials, spam users, and ultimately gain profits. They need email records, treats, and a wide scope of IP delivers to go around notoriety based protections. Moreover, they use telephone numbers, taken charge cards, and CAPTCHA arrangements trying to go around validation checks.

II. LITERATURE REVIEW

Opinion Mining by Ontological Spam Detection Duhan and Mittal suggested an article, "Opinion Mining by Ontological Spam Detection," to help us discover. Fake reviews using Naïve Bayes as an algorithm. This device has been introduced as a "Fake Product Review Tracking System" to get fake details inside the website. This device will detect fake reviews by users and block users. To find out if the general description is incorrect or true, we can use some included classes.

If the feedback is from a spammer, then find out the person's IP address to be crossed. If some reviews are from the same IP address, the reviews are considered spam. Account usage is used to evaluate whether reviews are made using the same account. Finding the most effective brand review, i.e. Reviews are about the best brand or not, not about the product. Therefore, it is no longer useful to remember the brand rate when deciding on a product.

The review recognizes the use of negative vocabulary, i.e., faulty phrases. If there are more than 5 negative words, the diagnosis is spam.

Rajashree S et al. [2014] today, the Internet has become an important component, as it provides more convenience to its users. Many social networking sites give users a percentage of their views. People care about politics, social issues, and unique products. Today, it is not uncommon for consumers to review online reviews of this product before buying anything. Multiple sites address these reviews. They provide scores for products and show the distinction between unique products. Some companies create false reviews to influence buyers' behavior and increase their revenue. But how to detect these fake reviews is a difficult plan for consumers. In today's competitive world, any agency needs to maintain its popularity in the market. So everyone needs to understand the corporation's opinion and the employer's manipulation. This article explores unique tactics for identifying manipulated feedback and suggests a brand new technique for selecting these manipulative assessments using the Decision Tree (DT).

Jui-Yu et al. [2013] Identifying tampering with reviews has become one of the top research issues in eCommerce as more and more consumers make their purchasing decisions based primarily on personal impressions from digital communities and e-commerce websites. However, clients should not forget that these personal analytics are more reliable than existing pure classified ads. As a result, some companies create fake personal reviews to influence customer behavior and increase their revenue. But, how to detect fraudulent reviews is a difficult task for consumers. Therefore, this study uses the Decision Tree (DT) to improve the class performance of diagnostic manipulation by introducing the eight capabilities of diagnostic manipulation. Furthermore, we attempt to explore the essential causes of manipulation in identifying criticism using communication assessments and derived technology guides. Finally, a real case of online consumer feedback on smartphones was used to testify to the effectiveness of the proposed procedure.

Benjamin et al. [2007] We deal with the problem of reading some related quotes in the text. For example, such reviews may include food, atmosphere, and service in a restaurant review. We design this project as a two-way scoring issue, which aims to develop a set of numerical scores for each item. We offer an algorithm that mutually learns the character item classification form by modeling dependencies between assigned ranks. This algorithm publishes the predictions of individual classifiers by

analyzing meta-family members in all critiques, including contract and comparison. We prove that our agreement-based pairing model is more expressive than role-playing models. Our experimental effects confirm the model's strength: the algorithm provides substantial construction on each rating and a sophisticated pair rating model.

Ivan Tetovo et al. [2011] Online reviews are often viewed along with the numerical scores provided by the users for a series of services or product items. We suggest a statistical version that can find relevant themes in textual content and extract textual evidence of emotions that helps each of these item ratings, a key issue in summarizing item-based emotions. (Hu and Liu, 2004a). Our version achieves extreme accuracy, without any explicitly categorized information, except for the emotional score provided by that person. The proposed approach is well-known and can be used for distribution in other applications with relevant indicators and sequential information.

Jindal et al. [2007] Finding reviews from product reviews, forum posts, and blogs is an essential research topic with many applications. However, current studies have focused on extracting, classifying, and summarizing these resource studies. One major issue not yet been studied is the reliability of opinion spam or online reviews. In this article, we discuss this issue in product reviews. To our knowledge, no study on this topic has been published yet, although web page spam and unsolicited email have been extensively investigated. We will see that the general definition of spam is very different from web page spam and email spam and therefore requires extraordinary detection strategies. We show that review spam is hugely based on an analysis of 5.8 million reviews and 14 million amazon.com reviewers. This document presents a classification of spam tests and then validates various techniques for detecting spam.

Jindal et al. [2008] The diagnostic test has become a valuable source of criticism about products, presentations, events, people, etc. Recently, many researchers have studied opinion assets such as product reviews, forum posts, and blogs. However, current studies have focused on classifying and summarizing emotions using herbal language processing techniques and statistical mining. One of the major issues that have been overlooked is the reliability of review spam or online reviews. In this article, we explore this

challenge in the context of product reviews, which can generate reviews and be widely used by consumers and product makers. In recent years, many startups are also adding product reviews. So, it's time to look at review spam. To our knowledge, no comment has been posted on this topic yet, although web spam and email spam have been extensively investigated. We will see that opinion spam is quite specific to immovable webmail and email spam, requiring extraordinary detection techniques. Based on an analysis of five, eight million reviews and one pair, 14 million amazon.com reviewers, we show that opinion spam is important in reviews. This document discusses these spam games and offers new techniques for detecting them.

III. METHODOLOGY

In regards to this, an "artificial neural network" system has been introduced as a part of the computer system. It is designed for simulating in a way in which the human brain possesses and analyses information. The inductive research approach can be considered for this type. In viewing the existing process and situations this can be observed through the patterns and system regularities. In taking the technical advantage ANN model need to be used effectively. It can be described as a foundation of artificial intelligence which will solve the problem in proving the difficulty according to human standards. Therefore "artificial neural networks" (ANNs) are introduced as a process of modeling, allowing the human nervous system through learning technique. By depending on the prediction, this detection process is revealing about the "user-level activities' '. User influence is also vital in reporting about the abnormalities. The social influence upon users can be assessed with the two types of factors. One is to find the user's impact upon others, and the other is to give the user importance. The evaluation is also based on the "fine-grained feature'.

IV. PROBLEM STATEMENT

In recent years, online reviews have been instrumental in making purchasing decisions. These reviews can provide users with useful information about products or services. However, to improperly promote or reduce the best products or services, spammers can also be deceived and bring in false reviews. Because of this behavior of spammers, customers lie and make wrong choices. So finding fake reviews (spam) is a big hassle. Review spam refers to the use of excessive and illegal

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2, 2024

techniques, including the growing number of fake reviews, to generate biased positive or negative reviews for a targeted product or service to sell or lower you, respectively. Allows Reviews created for this reason are known as fake spam or fake reviews, and authors responsible for writing such misleading material are spam or fake email reviewers.

V. PROPOSED WORK

Module Details:

1. Upload Social Network Profiles Dataset:

Using this module we will upload dataset to application

2. Preprocess Dataset:

Using this module we will apply processing technique such as removing missing values and then split dataset into train and test where application use 80% dataset to train ANN and 20% dataset to test ANN prediction accuracy

3. Run ANN Algorithm:

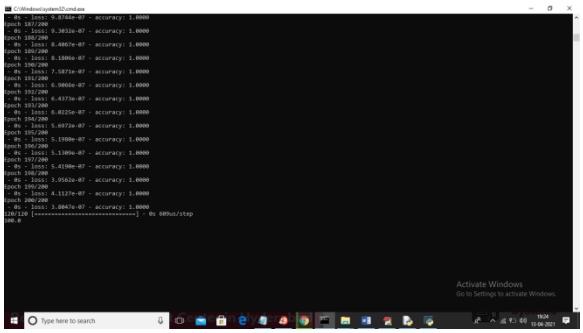
Using this module we will train ANN algorithm with train and test data and then train model will be generated and we can use this train model to predict fake accounts from new dataset.

4. ANN Accuracy & Loss Graph:

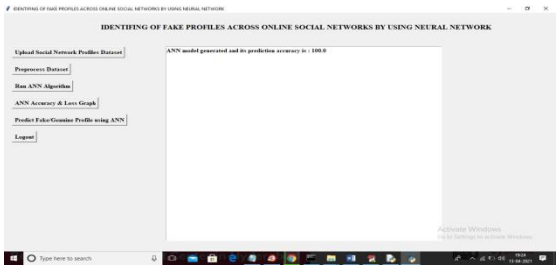
To train ANN model we are taking 200 epoch/iterations and then in graph we will plot accuracy/loss performance of ANN at each epoch/iteration.

5. Predict Fake/Genuine Profile using ANN:

Using this module we will upload new test data and then apply ANN train model to predict whether test data is genuine or fake.



In above screen we can see after 200 epoch ANN got 100% accuracy and in below screen we can see final ANN accuracy

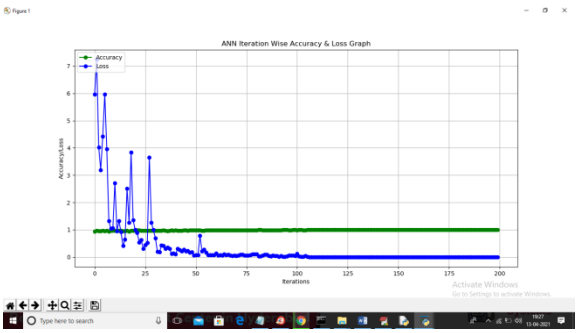


In above screen ANN model generated and now click on 'ANN Accuracy & Loss Graph' button to get below graph

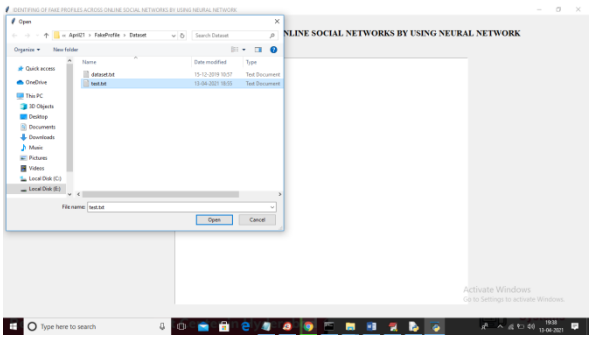
ISSN2321-2152

www.ijmece .com

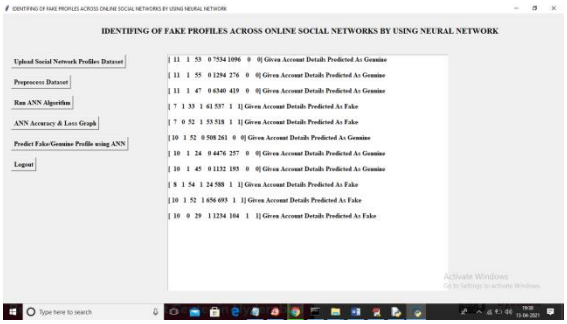
Vol 12, Issue.2, 2024



In above graph x-axis represents epoch and y-axis represents accuracy/loss value and in above graph green line represents accuracy and blue line represents loss value and we can see accuracy was increase from 0.90 to 1 and loss value decrease from 7 to 0.1. Now model is ready and now click on 'Predict Fake/Genuine Profile using ANN' button to upload test data and then ANN will predict below result



In above screen we are selecting and uploading 'test.txt' file and then click on 'Open' button to load test data and to get below prediction result



In above screen in square bracket we can see uploaded test data and after square bracket we can see ANN prediction result as genuine or fake

VI. CONCLUSION

Fake profiles are created in social networks for various reasons by individuals or groups. The results are about detecting the account is fake or genuine by using engineered features and trained using machine learning models like neural networks and random forest. The predictions indicate that the algorithm neural network produced 93% accuracy. In the future, there is a hope that new features make to detect and identify easily like implementing skin detection can be done by using natural language processing techniques more accurate. When Facebook introduces new features then it will be easy to identify fake accounts easily.

REFERENCES

1. Sai Pooja, G., Rajarajeswari, P., Yamini Radha, V ., Navya Krishna.G., Naga Sri

Ram.B., Recognition of fake currency note using convolutional neural networks(2016). International Journal of Innovative Technology and Exploring Engineering, 58-63,8(5).

2. Mohammed Ali Al-Garadi,Mohammad Rashid Hussain, Henry Friday Nweke, Ihsanali,Ghulammujtaba1,Harunachiro Ma,Hasanalikhattak,Andabdullahgani "Predicti-Ngcyber Bullying On Social Networks.

3. Yadongzhou,Daewookkim,Junjiezhang,(Member,Ieee),Lili Liu1, Huanjin3, "(IEEE)ProGuard: Detecting Malicious Accounts in SocialNetwork-Based Online Promotions".

4. Mauro Conti University of Padua, Radha Poovendran University of Washington, Marco Secchiero University of Padua,"FakeBook: Detecting Fake Profiles in On- line Social Networks(2012)", ACM /IEEE International Conference on Advances in Social Networks Analysis and Mining.

5. ni .N., Smruthi.M.,"A Hybrid Scheme for Detecting FakeAccounts in Facebook" ISSN: 2277- 3878, (IJRTE)International Journal of Recent Technology and Engineering (2019) , Issue-5S3, Volume-7.

6. NarsimhaGugulothu,JayadevGyani, Srinivas Rao Pulluri "A Comprehensive Model for Detecting Fake Profiles in Online Social Networks(2016)".

7. 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 ISSN 0973-4562, Number 6, Volume 13.

8. Reddy, A. V. N., &Phanikrishna, C. Contour tracking based knowledge extraction and object recognition using deep learning neural networks(2016). Paper presented at the Proceedings on 2nd International Conference on Next Generation Computing Technologies in 2016, NGCT 2016, 352-354. doi:10.1109/NGCT.2016.7877440.

9. V. Rama Krishna,& K.Kanaka Durga. Automatic detection of illegitimate websites with mutual clustering.(2016) International Journal of Electrical and Computer Engineering, 6(3), 995-1001. doi:10.11591/ijece.v6i3.9878

10. D.Rajeswara Rao & V.Pellakuri. Training and development of artificial neural network models: Single layer feedforward and multi layer feedforward neural network(2016). Journal of Theoretical and Applied Information Technology, 150-156,84(2).

11. Challa, N.,. Pasupuleti, S. K, & Chandra, J. V. A practical approach to E-mail spam filters to protect data from advanced persistent threat.(2016) Paper presented at the Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2016, doi:10.1109/ICCPCT.2016.7530239.