IDENTIFING OF FAKE PROFILES ACROSS ONLINE SOCIAL NETWORKS USING NEURAL NETWORKS

K.Mounika[1], PH.Swarna Rekha[2], Panchalingala Vaishnavi[3], Pesara Navya[4], Patel Uday[5], Kanugula Tarun[6], VadthyaVamshi Kumar[7]

[1]Assistant professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[2]Assistant professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[3,4,5,6,7] IVthBtech Student, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

Abstract:

In today's world, the social media platforms are being used on daily basis and has become an important part of our lives. The number of peoples on social media platforms are incrementing at a greater level for malicious use. On one hand, these social networks provide the advantage of direct connectivity between people, information sharing, ways to create a large audience, etc. on the other hand people also misuse them in many ways. Social networking sites are suffering from people who own bulk of fake accounts to take advantage of vulnerabilities for their immoral benefits such as intriguing targeted accounts to click on malicious links or to attempt any other cybercrimes. These actions motivate researchers to develop a system that can detect fake accounts on these OSNs. Several attempts have been made by the researchers to detect the accounts on social networking sites as fake or real, relying on account's features (user-based, graph-based, content-based, time-based) and various classification algorithms. In order to accomplish the task of detecting, identifying and eliminate the fake accounts we establish a forged human account.

Keywords: Online Social Network, Feature extraction, Spammer, Fake account detection, Data classification.

1.INTRODUCTION

Nowadays social networking sites have become a wide platform for people to keep in touch with each other, to share information, feelings, photos, posts, status, etc. With the help of OSNs like Twitter, Facebook, Instagram, Pinterest, Google+, LinkedIn, etc. people can easily interact with other people residing in any part of the world. One disadvantage of these sites is that most of the users are unaware of identity theft, loss of privacy, fake profiles, malware, etc. Twitter and Facebook are the most prominent OSNs and are continuously being attacked by spammers to steal personal data, spread rumors, and share false news. These spammers sometimes also use automated programs called social bots that can act like humans and contribute to spread nuisance on the internet. Another major problem while using social networking sites is the fake accounts created with different intentions such as to entrap or mislead people or spread malicious activities and because of these reasons it has become very important to develop a mechanism to detect spammers.For the purpose to detect fake accounts on the social media platforms the dataset generated was pre-processed and fake accounts were determined by machine learning algorithms.The classification performances of the algorithms Random Forest, Neural Network and

Support Vector Machines are used for the detection of fake accounts. The accuracy rates of detecting fake accounts using the mentioned algorithms are compared and the algorithm with the best accuracy rate is noted.

2.SURVEY

Fake identities in social media are often used in Advanced Persistent Threat cases, to spread malware or a link to it. They are also used in other malicious activities like junk emails/spams or used to artificially increase the number of users in some applications to promote it.

3.EXISTING SYSTEM

The concern about fake profile is protecting personal data or information from cyber attacks known as phishing attacks. The cyber attackers are often use this in stealing of information. In detecting of passwords, sharing of irrelevant contents, raising

According to an article a gaming application supported by Facebook provides incentives to the user/player of the application who brings more and more peers to play the game. So, in the greed of incentives, people make fake accounts.

•Huge amount of fake accounts may be created by celebrities or politicians, aiming to show off their large fan base or may be created by the cybercriminals so that their account look more real.

•Applications like in an online survey to get better feedback fake accounts are used e.g. for the increment in the rating of a product/application, fake identities are used by the company or the owner.

Disadvantages

1.Resource-intensive: Training a neural network model requires significant computing power and resources, which can be costly.

2.Privacy concerns: The use of neural networks to identify fake profiles may raise privacy concerns, as personal data is used to train the model. It is essential to ensure that user data is handled securely and with consent.

4.PROPOSED SYSTEM

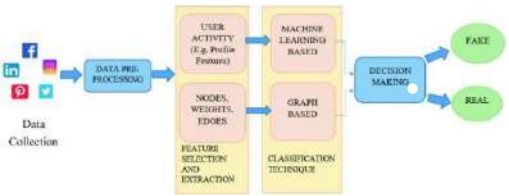
In regards to this, an "artificial neural network" system has been introduced as a part of the computer system. It is designed for simulating in a way in which the human brain possesses and analyses information. The inductive research approach can be considered for this type. In viewing the existing 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’.

Advantages

1.Increased accuracy: Neural networks can identify patterns in large amounts of data, making them effective at identifying fake profiles across multiple online social networks with a high level of accuracy.

2.Automation: Once the model is trained, the process of identifying fake profiles can be automated, saving time and resources.

5.SYSTEM ARCHITECTURE



6. IMPLEMENTATION

MODULES:

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.

7. CONCLUSION

We use machine learning namely an artificial neural network to determine what are the chances that a friend request is authentic are or not.If we look at the system designs, majority of implementations for fake account detection is either graph-based or feature-based and they may use the graph analysis techniques or machine learning techniques to identification of accounts as fake or real.In our proposed framework we use feature-based dataset and selected the features manually. This approach is based upon the user-level activities and the user’s account details.In addition to our satisfying conclusion, we have maintained the highest accuracy in detecting fake accounts by testing and training the dataset.

8. FUTURE SCOPE

The current developed software is installed on the system, i.e. it is a desktop application, and it will be used for some institute. But later it can be updated so that it will be operate as online application. Currently, the system has reached up to some great accuracy level for partial and dense images. It can further be improved to obtain higher accuracy level.It can be automatically updated by the use of the concept of Internet of Things. The future scope of the project can be integrated with the hardware components for example Additionally, an application can be developed to find fake accounts and to maintain a track of online profiles.

9.REFERENCES

Awasthi, S., Shanmugam, R., Jena, S.R. and Srivastava, A., 2020. Review of Techniques to Prevent Fake Accounts on Social Media.

Hajdu, G., Minoso, Y., Lopez, R., Acosta, M. and Elleithy, A., 2019, May. Use of Artificial Neural Networks to Identify Fake Profiles. In *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-4). IEEE.

Kaur, J. and Sabharwal, M., 2018. Spam detection in online social networks using feed forward neural network. In *RSRI conference on recent trends in science and engineering* (Vol. 2, pp. 69-78).

Khaled, S., El-Tazi, N. and Mokhtar, H.M., 2018, December. Detecting fake accounts on social media. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 3672-3681). IEEE.

Meligy, A.M., Ibrahim, H.M. and Torky, M.F., 2017. Identity verification mechanism for detecting fake profiles in online social networks. *Int. J. Comput. Netw. Inf. Secur.(IJCNIS)*, *9*(1), pp.31-39.