FAKE PROFILE DETECTION ON SOCIAL MEDIA

[1]D.Sriya, [2]B.Vyshali, [3]A.Sathwika, [4]A.Rithesh, [5]Dr. R. Jegedeesan, [6]Dr. M Sujatha,[7]K.Sai Veena

IV Year CSE Students[1,2,3,4]Associate Professor[5,6,7]

Jyothishmathi Institute of Technology And Science, Karimnagar, 505 481, Telangana.

ABSTRACT

Everyone's social life has gotten intertwined with online social networks in today's generation. These websites have drastically altered the way we go about our social lives. Making new acquaintances and staying in touch with them has gotten much easier. However, as a result of their quick expansion, several issues such as fraudulent profiles and online impersonation have arisen. There are no practical ways for resolving these issues. Social media is gaining traction in businesses throughout the world, and it has become one of the most widely utilized and popular platforms for digital marketing, as well as for monitoring public trends and better understanding what people want. Fake social profiles are on the rise, spreading fake news and information through this constantly expanding channel. This paper proposes a method for automatically detecting false profiles that is both feasible and efficient. To classify profiles into fake or authentic classifications, this system employs classification techniques such as Artificial Neural Networks. Because this is an automatic detection method, online social networks may readily implement it.

1. INTRODUCTION

Online social networks are rapidly expanding. It is critical for marketing firms that focus on promoting themselves by building a base of followers and fans. Social media platforms such as Facebook and Instagram have grown in popularity and importance in today's world. The use of social media as a communication medium is frequently used to increase popularity and support businesses. Initially, an account's popularity is measured by metrics such as follower count or shared content such as the number of likes, comments, or views. Social media is a fantastic platform for our lives, but there are a number of issues that must be addressed. Concerns about social media, such as confidentiality, online abuse etc.

The increasing usage of social media has turned out to be both a benefit and a liability for society. The use of social media for online fraud and the transmission of false information is rapidly expanding. On social media, fake accounts are the most common source of false information. Businesses that spend a lot of money

on social media influencers need to determine whether the following they've gotten is organic or not. As a result, there is a huge demand for a fake account detection tool that can accurately determine whether or not an account is fraudulent. We employ classification algorithms in machine learning to detect fake accounts in this paper. Finding a fake account is mostly determined by characteristics such as interaction rate and fraudulent activity.

2. LITERATURE REVIEW

Detecting false identities on social media has become a time-consuming task for many online social networking services, including Face book and Instagram. Machine learning is generally used to detect bogus accounts. Methods for detecting phony accounts that were previously employed have proven ineffective. Multiple techniques were employed in [1] for detection, including decision trees, logistic regression, and support vector machine algorithms. The fact that the decision tree algorithm only incorporates data sets for a single feature rather than several features is a serious flaw. As a result, subsequent models reduced the number of features, as seen in [2], which used features such as matching the user's age to their registered email address and location. These tactics became ineffective as the technology for creating fraudulent accounts improved.

The advancement in the creation of fake accounts rendered these methods ineffective in detecting it. As a result, service providers modified their algorithms to predict fake accounts, as seen in [3], which used the METIS clustering algorithm. This algorithm takes the data and clusters it into different groups, making it easier to distinguish between fake and real accounts. In [4], the Nave Bayes algorithm is used.

The probability for the used features was calculated and entered into the naive Bayes formula, and the computed value was compared to a reference value. If the computed value is less than the reference value, the account is considered fake.

3. METHODOLOGY

The proposed system includes a variety of deep learning tasks, and the architecture is as follows. The proposed system collects preprocessed datasets and provides it to a algorithm such as ANN for detecting fraudulent profiles on any social networking site and then evaluates the accuracy of the deep learning algorithm for the given dataset.

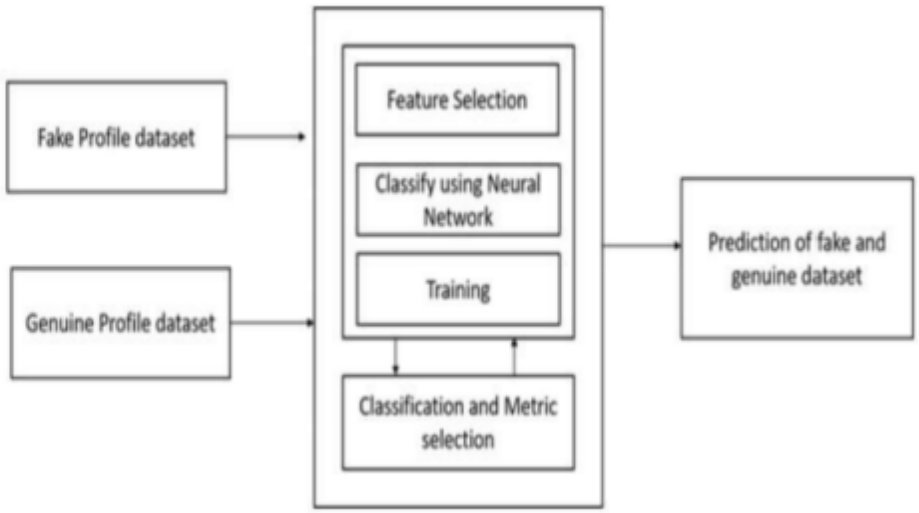

Fig 1: Architecture of Proposed System

The various methods in which an algorithm might model a problem are dependent on its interaction with experience or environment throughout the model preparation process, which aids in selecting the most suited algorithm for the given input data in order to achieve the best outcome.

A neural network is a network or circuit of neurons, or, more recently, an artificial neural network made up of artificial neurons or nodes. In the case of artificial neurons, a neural network (NN) is an interconnected group of natural or artificial neurons that uses a mathematical model for information. Neural networks are a subset of deep learning, which is a type of machine learning in which algorithms are stimulated by a structure similar to the human brain. The NN receives the input data, trains themselves to recognize patterns in the data, and then predicts the output for a comparable set of data. It is the functional component of deep learning that mimics how humans solve issues with their brains.

4. IMPLEMENTATION

1. Gather data and prepare it for analysis.

2. Create fictitious accounts.

3. Validation of data to distinguish between bogus and real.

4. Innovate with new features.

5. Use neural networks techniques.

6. Evaluate the accuracy, recall, and other parameters' findings.

As a result, these methods are used to detect unauthentic profiles.

Dataset:

We required a dataset comprising both fake and real profiles. Number of friends, followers, and status count are some of the attributes to include in the dataset. Datasets are created by combining training and testing data. The training dataset is used to train classification algorithms, and the testing dataset is used to determine the algorithm's efficiency. More than 80% of the accounts in the dataset are used to train the data, while 20% are utilized to test the data.

5. EXPERIMENTATION

In a social network, each profile (or account) has a wealth of information such as gender, number of friends, number of comments, education, work, and so on. Some of this material is private, while others is open to the public. Because private information isn't available, we've relied solely on publicly available data to identify fraudulent profiles on social media. However, if our proposed system is implemented by the social networking businesses themselves, they will be able to use the profiles' private information for detection without infringing any privacy concerns. For the classification of unauthentic and authentic profiles, we used this information as profile traits. The following are the methods we took to identify fake profiles.

1. First, all of the features on which the classification method will be applied are chosen. When selecting features, extreme caution should be exercised, as features that are not dependent on other features should be avoided, and features that can improve the classification's efficiency should be picked.

2. Following the right selection of attributes, the dataset of previously recognized false and real profiles is required for the classification algorithm's training purposes. We created two datasets: one with real profiles and one with phony profiles.

3. From the profiles, the qualities chosen in step 1 must be extracted (fake and genuine). Companies that wish to implement our scheme don't have to go through the scrapping process; they can simply extract the functionality.

4. The dataset of fake and actual profiles is then created. 80 percent of both profiles (actual and false) are utilized to create a training dataset, and 20% of both profiles are used to create a testing dataset from this dataset. Using the training dataset, we determine the classification algorithm's efficiency.

5. The training dataset is fed to the classification algorithm after the training and testing datasets have been prepared. It is meant to learn from the training procedure and provide accurate class levels for the testing dataset.

6. The labels from the training dataset are removed, and the trained classifier is left to decide. Our model will be assessed using the test data once it has been trained from the training data.

7. At the time of testing, the remaining 20% of data is delivered, which the model has never seen before; the model will predict a value, which we will compare to the actual output and compute accuracy.

6. RESULTS

We used Keras with TensorFlow backend to implement the Multi-Layer Perceptron model. The output obtained from the neural network is a single value which we pass through the sigmoid non-linearity to squish it in the range [0, 1] The sigmoid function is defined by the output from the neural network gives the probability (positive). At the prediction step, we round off the probability values to class labels 0 (negative) and 1 (positive).We ran our model up to 20 epochs after which it began to over fit. Thus identifying the profile is real or fake.

Based on the user input the classifier takes the inputs and show the results if the profile is fake or not. If prediction value is 0 then Profile is real otherwise it is Fake classifier is trained regularly as new data is fed into the classifier. After creating the models using the training datasets, we apply the models on unseen data, i.e., and the test dataset. We create the confusion matrix based on these and calculate various performance parameters.

A confusion matrix is a summary of prediction outcomes on a classification problem. The number of accurate and incorrect predictions are summarized with depend values and damaged down by each elegance. that is the key to the confusion matrix. The confusion matrix suggests the methods in which your classification model is confused while it makes predictions. It gives us perception now not only into the mistakes being made by a classifier but extra importantly the forms of mistakes which can be being made.

7. CONCLUSION

Individuals or groups create fake profiles in social media for a variety of purposes. The results are based on leveraging artificial features and machine learning models such as neural networks and random forests to recognize whether an account is fake or authentic. The algorithm neural network delivered 93 percent accuracy, according to the predictions. In the future, it is hoped that additional features would make it easier to detect and identify things, such as skin detection, which can be done more accurately utilizing natural language processing techniques. When Facebook provides new features, it will become much easier to spot fraudulent accounts.

8. FUTURE WORK

The main issue is that a person can have many Facebook accounts, giving the advantage when it comes to creating fake profiles and accounts on social media sites. The goal is to use an Aadhar card number when creating an account so that we can limit the number of accounts created and eliminate the possibility of fraudulent profiles at any time.

REFERENCES

[1]Nazir, Atif, Saqib Raza, Chen-Nee Chuah, Burkhard Schipper, and C. A. Davis. “Ghostbusting Facebook: Detecting and Characterizing Phantom Profiles in Online Social Gaming Applications.” In WOSN. 2010.

[2] Adikari, Shalinda, and Kaushik Dutta. “Identifying Fake Profiles in LinkedIn.” In PACIS, p. 278. 2014.

[3] Chu, Zi, Steven Gianvecchio, Haining Wang, and Sushil Jajodia. “Who is tweeting on Twitter: human, bot, or cyborg?.” In Proceedings of the 26th annual computer security applications conference, pp. 21- 30. ACM, 2010.

[4] Stringhini, Gianluca, Gang Wang, Manuel Egele, Christopher Kruegel, Giovanni Vigna, Haitao Zheng, and Ben Y. Zhao. “Follow the green: growth and dynamics in twitter follower markets.” In Proceedings of the 2013 conference on Internet measurement conference, pp. 163-176. ACM, 2013.

[5] Thomas, Kurt, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. “Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse.” In Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13), pp. 195-210. 2013.

[6] Farooqi, Gohar Irfan, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohamed Ali Kaafar, M. Zubair Shafiq, and Fareed Zaffar. “Characterizing Seller-Driven Black-Hat marketplaces.” arXiv preprint arXiv: 1505.01637 (2015).

[7] Viswanath, Bimal, M. Ahmad Bashir, Mark Crovella, Saikat Guha, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. “Towards detecting anomalous user behavior in online social networks.” In 23rd {USENIX} Security Symposium ({USENIX} Security 14), pp. 223-238. 2014.

[8]. Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.D.Baswaraj, J.Greeda 2019 “Improved Migration Performance In Virtualized Cloud Datacenters” International Journal of Scientific & Technology Research. Volume 8, Issue 09,page no.1515-1518 September 2019. (Scopus indexed)

[9].Annadi Jahnavi, Hanumandla Bhavana, Dr. R. Jegadeesan “An Implementation of Detecting Password Pattern In Dictionary Attack” International Journal of Advanced Science and technology. ISSN 2005-42386, Page no: 84-92 July,2019(Indexed by Scopus, Elsevier).

[10].Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.C.N.Ravi, J.Greeda2019 “A Secure Transaction Authentication Scheme using Blockchain based on IOT” International Journal of Scientific & Technology Research. VOLUME 8, ISSUE 10,Page no:2217-2221 OCTOBER 2019. ISSN 2277-8616 (Scopus indexed)

[11].Dr R Jegadeesan, Dr.C.N.Ravi, Dr.A.Nirmal Kumar 2020 “Automatic Rice Quality Detection Using Morphological and Edge Detection Techniques” ICCCE 2020 3rd International Conference on Communications and cyber Physical Engineering, Metadata of the chapter that will be visualized in Springer Link. Volume, issue, May.2020 Page No.233-242, Springer conference.