Proceedings of the International Conference on Sustainable Computing and Smart Systems (ICSCSS 2023)
IEEE Xplore Part Number: CFP23DJ3-ART; ISBN: 979-8-3503-3360-2

2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS) | 979-8-3503-3360-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCSS57650.2023.10169168

Fake Profile Detection on Social Networking Websites using Machine Learning

Dr. M. Sirish Kumar[1], Dr Jasmine Sabeena[2], Konduru Manasa Veena[3], Kummari Pavan[4], Malepati Sukavya[5], Kundavaram Sravanthi[6]
1Associate Professor, School of Computing, Mohan Babu University, Tirupati, India
2Associate Professor, Dept. of CSE, S V College of Engineering, Tirupati, India
[3,4,5,6]Sree Vidyanikethan Engineering College, Tirupati, India
drmsk2102@gmail.com, jasmine539@gmail.com, manasakonduru11@gmail.com, kumaryashwanth94975@gmail.com,ksravanteepandu@gmail.com

***Abstract*—These days, social media has a significant impact on everyone's life. Most people frequently utilize social media platforms. Each of these social media platforms offers benefits and drawbacks, as well as security risks for our information. To determine who poses threats on these platforms, it is necessary to distinguish between the real and fake social media profiles. There are traditionally used various methods for identifying fake social media accounts. But these platforms need to be better at identifying phoney accounts. The accuracy rate of identifying fake accounts utilising timestamp data types is improved in this proposed work employing high gradient boosting algorithms and Natural Language Processing. In order to investigate the relationship between various machine learning methods and multi-features in time series, this study employs a variety of machine learning techniques.**

Keywords: **Fake profiles, Machine learning methods, Natural Language Processing (NLP), Timestamp, Extreme Gradient Boosting algorithm**

I. INTRODUCTION

A website known as a "social networking site" is one where users may connect with friends, make updates, and find new people who have similar interests. Each user has a profile on the website.Users can communicate with one another using Web 2.0 technologies in these online social networks [1]. The utilisation of social networking sites is expanding quickly and affecting how individuals interact with one another. Online communities bring together people with like interests and make it easy for users to find new friends. The main benefit of internet social networking is that it allows user to easily connect with people and communicate better. This has provided new avenues for potential attacks such as fake identities, disinformation, and more [3]. Researchers are working to determine the impact these online social networks have on people. There is much more to media than just how many people use it. This suggests that the number of fake accounts has grown throughout the past years [4].

ISPs of social networks have a hard time locating these fraudulent accounts. The need to identify these fake accounts is due to the inundation of disinformation, advertisements and more on social media [5].

The datasets were taken and trained for the identification of fake users from the social media networks using machine learning algorithms.

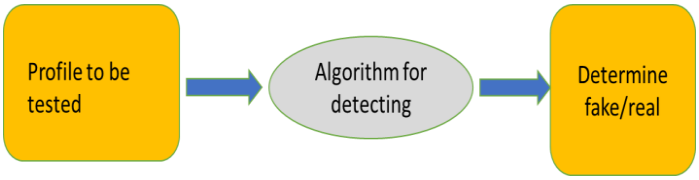

Figure 1: Detection process

II. SYSTEM DESIGN

A. *System architecture*

Figure below depicts the proposed system.

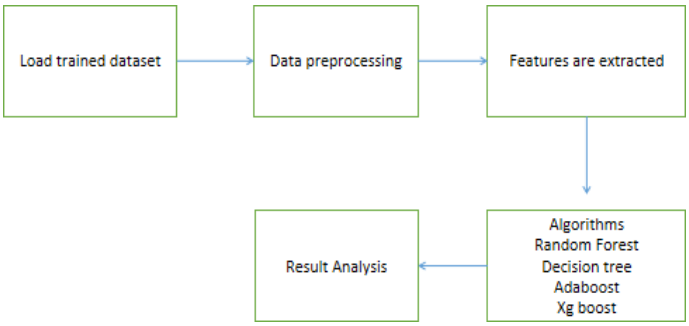

Figure 2: Proposed system

B. *Raw data*

Real users and fake user records are where the raw data is obtained from, which contains 3474 users and 3351 fake users. This data is collected from previous years.

C. *Uploading the data:* A dataset is a collection of instances, and typically need a number of datasets for different tasks when utilising machine learning techniques.[17].

- Training Dataset: A dataset that the machine learning system uses to train the model.
- Testing Dataset: A dataset not used to train the model butinstead to test its accuracy and it can be known as the validation dataset.

D. *Data Preprocessing:* Identifying fake accounts is crucial first step. This stage involves getting the data ready for use in the detection procedure [17]. Prior to giving the data into the model, it is essential to preprocess it, because the valuable information that can be gleaned from it directly affects how well the model learns.

E. *Model Algorithms:*

The following machine learning algorithms are utilised to find profiles:

Random Forest

To enhance the prediction accuracy of datasets, classifiers called random forests use different decision trees on specific subsets of the input data [18]. Rather than relying only on one of the decision trees, Random Forest extrapolates predictions from each Decision Tree and bases them on a majority of votes. First, N decision trees are linked to form a random forest. Predictions are then made for each tree generated in the first stage.

Decision Tree:

It is a graphical representation for locating each potential answer to a question or choice based on predetermined criteria. To forecast the class of the incoming dataset, a decision tree [19] method proceeds upward from the root node. Comparing the values of the record (actual dataset) attribute with those of the root attribute, this algorithm follows the branch and moves on to the next node. The algorithm checks the attribute value with the other subnodes before moving on to the next node.

AdaBoost:

By integrating numerous weak learners into one strong learner, AdaBoost is implemented. AdaBoost's weak learners [20] construct a single split decision tree known as the decision stump by taking into account a single input feature. As the initial decision stump is being drawn out, each observation is given equal weight. As the first decision stump's results are analysed, any observations that were incorrectly categorised are given heavier weights. A new decision stump is created by considering the higher-weight observations to be more significant. Once more, misclassified observations are assigned a higher weight, and this process is repeated until all observations belong to the correct class.

XG boost algorithm:

An enhanced gradient boosting technique is XGBoost [21]. This algorithm's primary goal is to make computations faster and more effective. Because to its sequential data analysis, the Gradient Descent Boosting approach computes the output more slowly. Hence, XGBoost is utilised to enhance or greatly enhance the model's performance. The focus of XGBoost is on model effectiveness and computing speed. The inputs are taken, and the trained dataset is loaded and for every occurrence in the trained data with regard to every feature of the classifier is trained, and the accuracy of the data is predicted.

Pros of XG boost algorithm:

1. Multiple weaker models from trained data can be combined to form stronger model to further accurate results.
2. It can handle huge amount of data to grow parallel trees for individual features.
3. It can handle huge data with missing data also, in order to reduce normalization.

F. *Evaluation method:*

Extreme Gradient Boosting Algorithm, which is a variant of Gradient Boosting Algorithm, is the algorithm utilised to carry out this work.

Assume that the input and target, X and Y respectively, have N samples each. Learning the f(x) function, which converts the input characteristics X into the desired variables y, is what should be aimed to be done. The total number of trees is what is boosted.

The difference between the expected and actual variables is the loss function.

$$L(f) = \sum_{i=1}^{N} L(y_i, f(x_i))$$

The loss function is minimised with respect to f.

$$\hat{f}_0(x) = \underset{f}{argmin}\, L(f) = \underset{f}{argmin} \sum_{i=1}^{N} L(y_i, f(x_i))$$

If the gradient boosting approach is in M stages, the algorithm can add some additional estimators as h_m.

$$\hat{y}_i = F_{m+1}(x_i) = F_m(x_i) + h_m(x_i)$$

The gradient similarly for M trees:

$$f_m(x) = f_{m-1}(x) + \left(\underset{h_m \epsilon H}{argmin} \left[\sum_{i=1}^{N} L(y_i, f_{m-1}(x_i) + h_m(x_i)) \right] \right)(x)$$

The current solution is,

$$f_m = f_{m-1} - \rho_m g_m$$

III. EXPERIMENTAL ANALYSIS AND RESULTS

A. Comparative Analysis:

Existing System:

1. Because of privacy issues, some of the social media datasets are very limited and a lot of details are not made public.

2. Naive Bayes algorithm having less accuracy.

3. There are no features to identify the exact time when the event occurred.

The Random forest method is the one that is most frequently used in fraudulent account detection. A few drawbacks of the technique include its inability to effectively handle category variables with many levels. Additionally, the algorithm's time effectiveness declines as the number of trees rises.

Proposed System:

In that it mainly utilises decision trees, the gradient boosting approach is comparable to the random forest algorithm. Utilising fresh methods to find them, the method of identifying phoney accounts is modified. Spam comments, engagement rates, and fake behavior are some of the strategies used. The gradient boosting method uses these inputs in order to create decision trees which are subsequently used by the gradient boosting process. Even when some inputs are missing, this method is still generating a result. Therefore, this algorithm is the main justification for its use. These methods are very precise in their results. XGBoost and GBM performed extremely well in comparison to the earlier study. Even with the default values of, it significantly outperforms the accuracy of false account identification.

Experimental Analysis:

The trained dataset is given into various algorithms and the accuracy of every algorithm is analysed to find the best fit algorithm for classifying the profiles as either real or fake. Out of the four algorithms used the XgBoost algorithm and Decision tree algorithms achieved atmost same accuracy but when the datasets are trained again, the accuracy of XgBoost algorithm increases every time it is trained. The given inputs social network profiles are run on the Extreme Gradient Boosting algorithm and these inputs are computed sequentially to produce the results. By the parallel processing of the decision trees, the profile is determined as either real or fake.

The graph below gives the model accuracy of XgBoost algorithm, Adaboost algorithm, Decision tree algorithm, and Random Forest algorithm. From the graph below, it can be seen that XgBoost algorithm gives more accuracy.

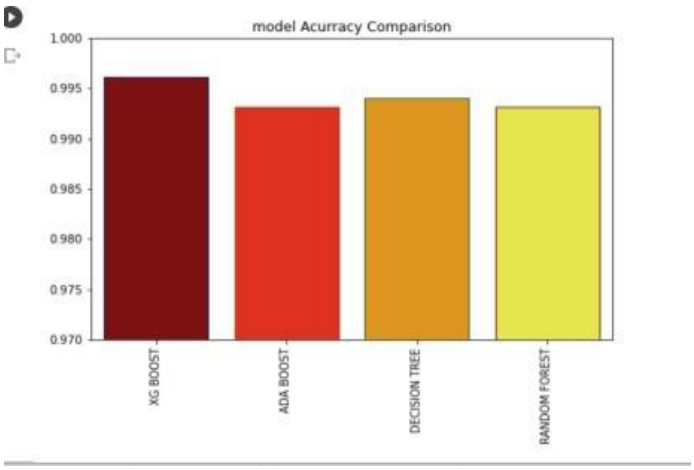

Figure 3 : Model Accuracy Comparison

B. Experimental result:

When the XgBoost algorithm is executed, the model test accuracy, precision, and recall are given.

Table 1: Model Comparison

Index	Model Test Accuracy	Model precision	Model Recall
0	0.9629	0.950641658	0.973710819

The graph given below gives model test accuracy, model precision, and model Recall.

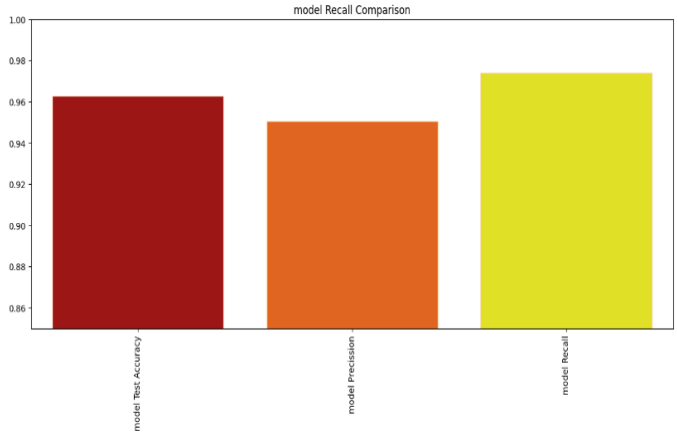

Figure 4 : Model Recall Comparison

IV. CONCLUSION

In this study, real and fake user datasets are used to identify real profiles. The characteristics are extracted using machine learning techniques such random forest, decision tree, adaboost, and XgBoost, with XgBoost algorithm providing the best accuracy to distinguish between real and fraudulent users on social networking website

REFERENCES

[1] E. Karunakar, V. D. R. Pavani, T. N. I. Priya, M. V. Sri, and K. Tiruvalluru, "Ensemble fake profile detection using machine learning (ML)," *J. Inf. Comput. Sci.*, vol. 10, pp. 1071–1077, 2020.

[2] P. Wanda and H. J. Jie, "Deep profile: utilising dynamic search to identify phoney profiles in online social networks CNN" J. Inf. Secur. Appl., vol. 52, pp. 1–13, 2020.

[3] P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter SMS spam," *Future Gener. Comput. Syst.*, vol. 102, pp. 524–533, 2020.

[4] R. Kaur, S. Singh, and H. Kumar, "A modern overview of several countermeasures for the rise of spam and compromised accounts in online social networks," *J. Netw. Comput. Appl.*, vol. 112, pp. 53–88, 2018.

[5] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, "Automatically dismantling online dating fraud," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1128–1137, 2020.

[6] M. U. S. Khan, M. Ali, A. Abbas, S. U. Khan, and A. Y. Zomaya, "Segregating spammers and unsolicited bloggers from genuine experts on twitter," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 551–560, Jul./Aug. 2018.

[7] V. Balakrishnan, S. Khan, and H. R. Arabnia, "Improving cyberbullying detection using twitter users' psychological features and machine learning," *Comput. Secur.*, vol. 90, 2020, Art. no. 101710.

[8] Georgios Kontaxis, I. Polakis, S. Ioannidis and E. P. Markatos, "Detecting social network profile cloning," *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, Seattle, WA, USA, 2011, pp. 295-300, doi: 10.1109/PERCOMW.2011.5766886.

[9] Monther Aldwairi, and Ali Alwahedi, "Detecting Fake News in Social Media Networks", Procedia Computer Science, Volume 141, 2018, Pages 215-222; https://doi.org/10.1016/j.procs.2018.10.171

[10] Buket Erşahin, Özlem Aktaş, D. Kılınç and C. Akyol, "Twitter fake account detection," *2017 International Conference on Computer Science and Engineering (UBMK)*, Antalya, Turkey, 2017, pp. 388-392, doi: 10.1109/UBMK.2017.8093420.

[11] Kumud Patel, Saijshree Srivastava, and Sudhanshu Agrahari, "Survey on Fake Profile Detection on Social Sites by Using Machine Learning Algorithm," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, 2020, pp. 1236-1240, doi: 10.1109/ICRITO48877.2020.9197935.

[12] Alexey D.Frunze and Aleksey A. Frolov, "Methods for Detecting Fake Accounts on the Social Network VK," *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, St. Petersburg, Moscow, Russia, 2021, pp. 342-346, doi: 10.1109/ElConRus51938.2021.9396670.

[13] M. BalaAnand, S. Sankari, R. Sowmipriya, and S. Sivaranjani, "Recognising fraudulent users on social networks through their nonverbal cues," *Int. J. Technol. Eng. Syst.*, vol. 7, no. 2, pp. 157–161, 2015.

[14] A. M. Meligy, H. M. Ibrahim, and M. F. Torky, "Identifier checker tool for online social networks to identify false profiles," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 1, pp. 31–39, 2017.

[15] M. Fire, A. Elyashar, and Y. Elovici, "Friend or enemy? identification of fake profiles in internet social *Social networks",Social Netw. Anal. Mining*, vol. 4, no. 1, 2014, Art. no. 194.

[16] Egele, G. Stringhini, C. Kruegel, and G. Vigna, "IEEE Trans. Dependable Secure Comput., "For detecting compromised accounts on social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 4, pp. 447–460, Jul./Aug. 2017.

[17] K. Chakraborty, S. Bhattacharyya, and R. Bag, "A survey of sentiment analysis from social media data," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 2, pp. 450–464, Apr. 2020.

[18] S. Lee and J. Kim, "WarningBird: IEEE Trans. Dependable Secure Comput., "A near real-time detection method for suspicious URLs in twitter stream," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 3, pp. 183–195, May/Jun. 2013.

[19] H. Drucker, D. Wu, and V. N. Vapnik, "In order to classify spam, support vector machines," *IEEE Trans. Neural Net.*, vol. 10, no. 5, pp. 1048–1054, Sep. 1999.

[20] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, "Real-time drifted Twitter spam detection using statistical features," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 914–925, Apr. 2016.

[21] C. Chen *et al.*, "Streaming spam tweets detection using machine learning: performance evaluation," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 3, pp. 65–76, Sep. 2015.