iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59294

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Use of Machine Learning to Identify Fake Profiles

Dr. G. Ravi Kumar[1], T. Tanujha[2], K.Harshitha[3]
[1]*Associate Professor,* [2,3]*UG Student, Department of CSE, CMR College of Engineering & Technology, Hyderabad, Telangana*

Abstract: ***These days, social media plays a big role in our everyday lives. Presently, over 50% of the global population actively utilizes social media sites. The prevalence of fraudulent accounts on social platforms is a serious problem that has been brought about by their ever-growing popularity. The goal of these fictitious accounts is to mimic or deceive other people. They are now a simple means of deceiving consumers into purchasing phony goods and services. Additionally, billions of people's personal information is in jeopardy. It is now crucial to identify and disable the phony accounts before any damage is done because of these dangers. Thanks to machine learning, it's now simple to identify millions of these accounts automatically. Users fabricate profiles to disseminate false information, including hate speech, rumors, texts from bullied individuals, and more. Researchers used deep learning and machine learning models to propose some strategies to mitigate this problem, yet a large number of phony accounts remain. These phony accounts are unacceptable for a respectable social networking site, nevertheless. This article provides an overview of the latest developments in social networking fake account identification***
Keywords: Fake Profiles, Fabricate, Personal attacks, Machine learning, Feature extraction, ML Applications..

I. INTRODUCTION

A social networking site is an online community where users may create profiles, stay in touch with friends, meet new people, and share information. These social media platforms are expanding swiftly and altering the relationships between people. People who share similar interests are brought together in the online community, which promotes user friendships. Social ramifications In the modern era, everyone's social life is connected to online social networks. These locations have significantly changed how we live in society. It's easier to stay in touch with new pals and updates. Digital social networks impact research, learning, community organizing, employment, businesses, etc. They allow the users to add friends and share various kinds of information such as personal, social, economic, educational, political, business, etc.

Moreover, they can also share photos, videos, and other day-to-day interactions. However, some people don’t use these sites with good objectives. Therefore, they create fake accounts on social sites. Fake accounts do not have any real identity so we can call them an Attacker. These attacker uses incorrect information or statistics about some real-world person to create a fake account. Using these fake accounts, attackers spread fake information that affects other users. Protecting such sensitive data of users is one of the major challenges of social sites. Some techniques in the field of machine learning have been developed to detect fake accounts in social networking sites such as decision classifier default methods like KNN classifier, SVM classifier, and Naive Bayes classification. In recent research, it has been found that these techniques make available enhanced results to detect fake accounts. Based on a variety of account features, KNN and SVM can identify phony accounts on social networking sites and can handle vast amounts of random data. Based on Bayes' theory is the Naive Bayes classifier. It foretells the likelihood that a specific variable is a member of a specified class.

II. RELATED WORK

In the quest for innovation and efficiency, modern projects frequently rely on existing solutions as fundamental building blocks for development. This approach not only recognizes the expertise and advancements of those who came before us but also nurtures a collaborative ecosystem where ideas can evolve and confront new challenges. In our project, we wholeheartedly embrace this ethos, conscientiously integrating elements from existing solutions to enrich our endeavor. These existing solutions serve as guiding lights, offering insights and frameworks that shape the direction of our project.

1) Use Fake Account Detection in Twitter Based on Minimum Weighted Feature Set. Here they effectively detected the fake accounts on the Twitter social network with the help of a minimum set of attributes that were possible. The proposed method consists of two main steps, the first step is to determine the main factors that will show impact and influence the correct detection of fake accounts, and the second step is to apply a classification algorithm that uses the required and sufficient factors in step one on twitter accounts to identify the fake accounts.

They aimed to propose the minimum set of attributes that can detect fake users with the highest accuracy. Many users have always opted for a data set that consists of a large no of attributes. On these attributes, by applying or performing an extensive analysis it is revealed that most of them are not used by the users and it may predict results wrong. They have conducted numerous tests to determine the ideal minimal feature set for identifying fraudulent Twitter accounts. Our goal is to identify the smallest, best set of features is dependent on the laborious process of gathering, processing, and evaluating these features; as a result, determining the smallest set that yields the highest level of accuracy is seen to be one of the most efficient methods for identifying fraudulent accounts. The set of features with the fewest features that yield the highest accuracy percentage is considered the best set of features. Measures that are specifically designed to assess accuracy include precision and recall.

2) Deep neural networks for detecting fake profiles in social media. A deep neural network (DNN) method for identifying phony profiles in social networks is proposed in this paper. The DNN model is intended to learn intricate characteristics and patterns that differentiate between the two types of profiles. It is trained using a sizable dataset of actual and fictitious profiles. Furthermore, by using 16 features derived from content-based and profile-based features, the deep convolution neural network method for detecting fake accounts on social networks is proposed. Additionally, the study looks for the lowest set of profile information required to recognize phony Facebook profiles. The outcomes showed that the suggested technique could identify phony profiles with 99.4% accuracy, which is comparable to the results obtained using larger data sets and more detailed profile information.
3) Fake profile detection using XG Boost.XG Boost, a random forest approach, and observable features from a multilayered neural network with a profile-focused focus were used to generate this model. The features that were collected and retrieved from a CSV file could be easily interpreted by the model. In the end, whether or not a profile is authentic will be determined by the model's testing, training, and analysis. Because Google provides free GPU usage, researchers chose Google Collab to build models. With a 12-gigabyte (GB) capacity, the Google Collab NVIDIA Tesla K80 GPU can run continuously for 12 hours. This technique is effective in identifying false profiles. After training, this model may have a greater accuracy rate than previous similar studies. The XG boost, the stochastic forest, and the LSTM neural network, additional methods are offered in addition to the model.

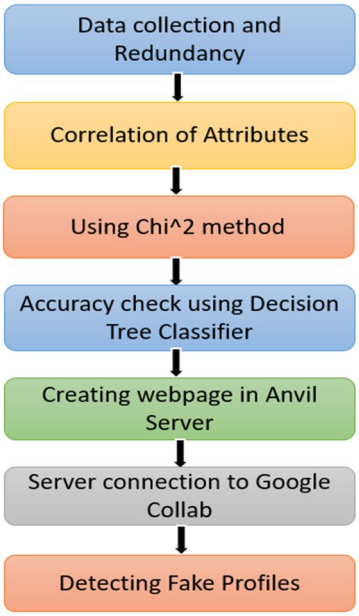
III. METHODS AND EXPERIMENTAL DETAILS

To build the model few environments were required such as Google Collab, anvil interface, and Google Collab with pre-installed libraries such as Seaborn, numpy, pandas, etc,... The algorithm that is implemented is a decision tree classifier and the code is written in Python language in Google Collab. The data which was given to the algorithm is given in the CSV format.

1) *Data Collection And Redundancy:* The data is collected from the Instagram platform and data redundancy is done to remove the missing and repeated values. The data that were collected are the attributes that give us information regarding the account holder.
2) *Data Storing:* The data is stored in the form of attributes in a CSV file with a .csv extension so that it makes it easy to manage the data.
3) *Correlation of Attributes:* The correlation of the attributes is calculated so that we can improve accuracy in identifying fake profiles in social media accounts.
4) *Attributes Selection:* From the correlation values, a few attributes are chosen by applying the chi-square attribute selection method. We choose attributes with high 3 correlation values by implementing the chi-square attribute selection method.
5) *Algorithm:* Decision tree classifier algorithm is used in this prediction model. The procedure in a decision tree begins at the root node to forecast the class of the given dataset. This algorithm follows the branch and advances to the next node by comparing the values of the root attribute with the record (actual dataset) attribute. The method proceeds to the next node by comparing its attribute value with those of the other sub-nodes once more. It keeps doing this till it gets to the tree's leaf node. The default method gini index is used.
6) *Gini Index:* When building a decision tree using the CART (Classification and Regression Tree) technique, the Gini index is a measure of purity or impurity.It is better to choose an attribute with a low Gini index over one with a high index. The CART algorithm only produces binary splits, and it does so by utilizing the Gini index. The formula follows.

Gini Index= $1- \sum_j P_j^2$

7) *Web Application:* Web application is created in anvil works. A complete server-side Python environment that allows us to import any packages we want is provided by Anvil's Server Modules. Anvil also allows us to connect to the code which is written in Google Colab directly without any other environments.



Flowchart-1

IV. RESULT AND DISCUSSION

By using the Decision Tree Classifier we obtained an accuracy of 0.96 and a precision of 0.97 as we considered attributes that we selected by using the chi-square test for feature selection which made it easy to decrease the number of features and increase the accuracy and precision metrics in finding fake profiles on Social media.

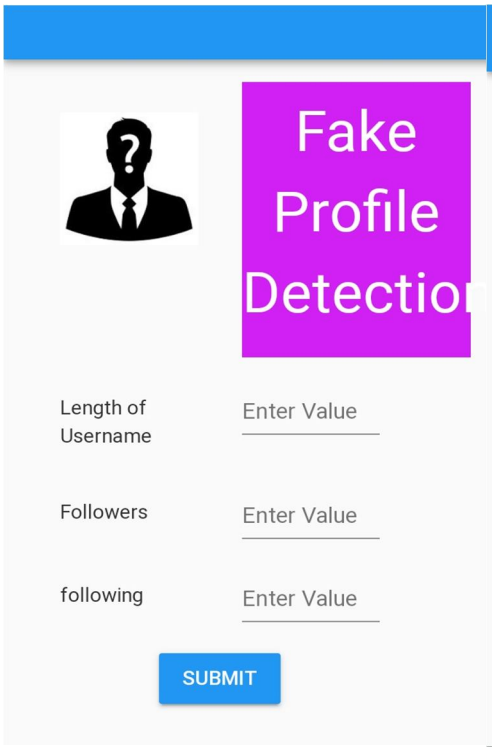


Fig.1 Result

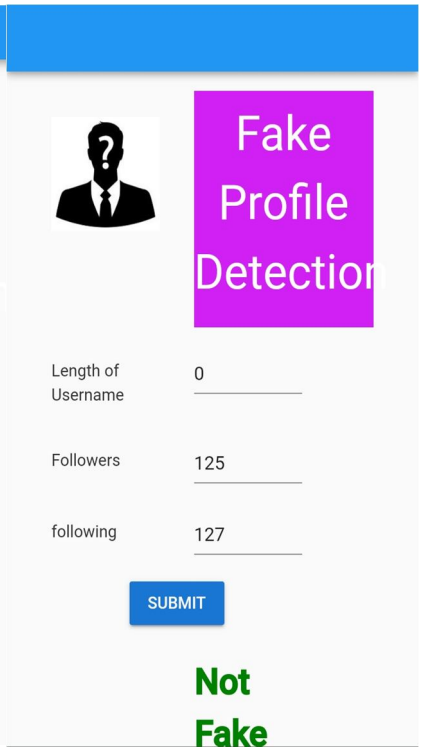


Fig.2 Result

S.No	Algorithm	Accuracy	Precision
1	Decision tree classification	0.96	0.97
2	SVM	0.89	0.79
3	KNN	0.91	0.92
4	Naïve bayes classifier	0.91	0.89

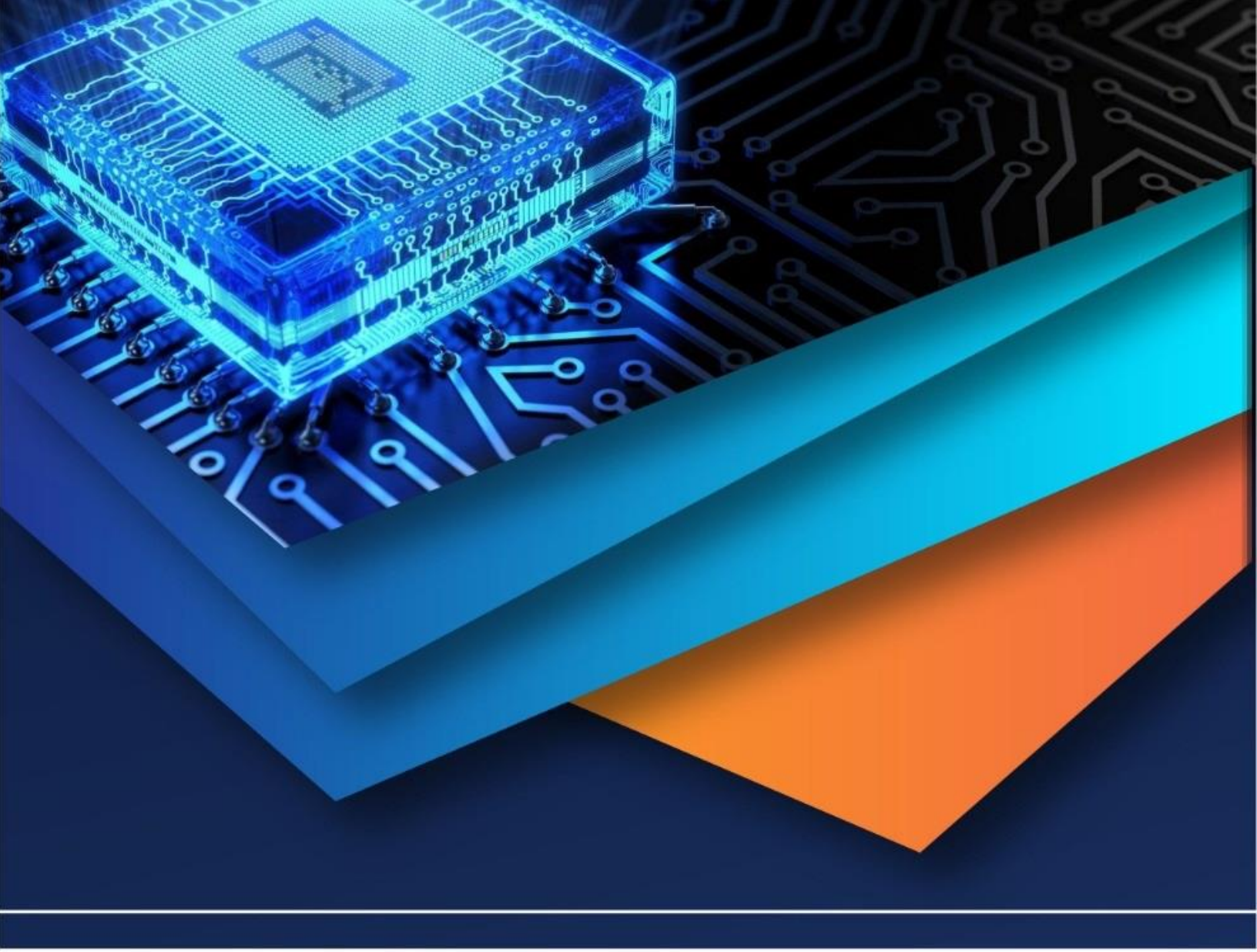
Table.1 Metrics

V. CONCLUSION

Based on our research, a significant problem plaguing social media platforms is the growing quantity of phony accounts on them. In order to solve this issue, we have developed a machine learning model that can quickly identify fake accounts, they can be eliminated before they endanger people seriously. In this study, a machine learning has been proposed while taking into consideration the shortcomings of the present approaches. The employed model examines the data linked to the accounts in order to establish a connection between it and the veracity of the account. We employed learning curves in addition to the model's accuracy to depict the model's performance using the decision classifier approach, which has high accuracy. The model performed well on both the training and testing sets. Only the data supplied for Instagram profiles has been used so far for testing and training, but by providing an effective dataset for them, we may eventually train the model to recognize phony accounts on other well-known platforms like Facebook, LinkedIn, Twitter, and many more.

REFERENCES

[1] M. A. Wani, N. Agarwal, S. Jabin, and S. Z. Hussain, “Analyzing real and fake users in Facebook network based on emotions,” in Proc. IEEE 11th Int. Conf. Commun. Syst. Netw., 2019, pp. 110–117.
[2] P. Galán-García, J. G. de la Puerta, C. L. Gómez, I. Santos, and P. G. Bringas, “Supervised machine learning for the detection of troll profiles in twitter social network:
[3] 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.
[4] S. R. Sahoo and B. Gupta, “Real-time detection of fake account in twitter using machine-learning approach,” in Advances in Computational Intelligence and Communication.
[5] P. Wanda and H. J. Jie, “Deepprofile: Finding fake profile in online social network using dynamic CNN,” J. Inf. Secur. Appl., vol. 52, pp. 1–13, 2020.
[6] J. Yadav, D. Kumar, and D. Chauhan, “Cyberbullying Detection using Pre-Trained BERT Model,” 2020, doi: 10.1109/ICESC48915.2020.9155700.
[7] M. Dadvar and K. Eckert, “Cyberbullying Detection in Social Networks Using Deep Learning Based Models; A Reproducibility Study,” arXiv. 2018.
[8] H. Hazimeh, E. Mugellini, and O. A. Khaled, “Reliable user profile analytics and discovery on social networks,” in Proc. 8th Int. Conf. Softw. Comput. Appl., 2019, pp. 496–500.
[9] J. Kaubiyal and A. K. Jain, “A feature based approach to detect fake profiles in twitter,” in Proc. 3rd Int. Conf. Big Data Int. Things, 2019, pp. 135–139.
[10] 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.
[11] A. Makkar and N. Kumar, “An efficient deep learning-based scheme for web spam detection in IoT environment,” Future Gener. Comput. Syst., vol. 108, pp. 467–487, 2020.
[12] M. Badar, M. Haris, and A. Fatima, “Application of deep learning for retinal image analysis: A review,” Comput. Sci. Rev., vol. 35, pp. 1–18, 2020.
[13] R. Jain, N. Jain, A. Aggarwal, and D. J. Hemanth, “Convolutional neural network based Alzheimer’s disease classification from magnetic resonance brain images,”Cogn. Syst. Res., vol. 57, pp. 147–159, 2019.
[14] M. Vardhana, N. Arunkumar, S. Lasrado, E. Abdulhay, and G. RamirezGonzalez, “Convolutional neural network for bio-medical image segmentation with hardware acceleration,” Cogn. Syst. Res., vol. 50, pp. 10–14, 2018.
[15] E. Daskalakis, M. Tzelepi, and A. Tefas, “Learning deep spatiotemporal features for video captioning,” Pattern Recognit. Lett., vol. 116, pp. 143– 149, 2018.
[16] M. Nabati and A. Behrad, “Video captioning using boosted and parallel long short-term memory networks,” Comput. Vis. Image Understanding, vol. 190, 2020, Art. no. 102840.
[17] M. Nabati and A. Behrad, “Multi-sentence video captioning using content-oriented beam searching and multi-stage refining algorithm,” Inf. Process. Manage., vol. 57, no. 6, 2020, Art. no. 102302.
[18] H. Xiao and J. Shi, “Video captioning with text-based dynamic attention and step-by-step learning,” Pattern Recognit. Lett., vol. 133, pp. 305–312, 2020.
[19] M. M. Swe and N. N. Myo, “Fake accounts detection on twitter using blacklist,” in Proc. IEEE/ACIS 17th Int. Conf. Comput. Inf. Sci., 2018, pp. 562–566.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY