IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

Machine Learning -Based Detection of Counterfeit Accounts in Social Media Outlets

Archana.B[1], Ayishafebin[2], Divyadharshini.P[3], Nandhini.K[4], Manisha.A[5]

Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT: Online social networks have permeated our social lives in the current generation. User trust, platform integrity, and online safety. Detecting these accounts manually is challenging and time-consuming, necessitating the development of automated methods. In this study, we propose a machine learning-based approach for the detection of counterfeit accounts in social media outlets. Our method involves the collection of a diverse dataset comprising both genuine and counterfeit accounts, encompassing various features such as profile information, posting behavior, and interaction patterns. Leveraging these features, we employ advanced machine learning algorithms for model training, including supervised learning techniques such as logistic regression, random forests, and neural networks, as well as unsupervised learning methods like clustering.

KEYWORDS: Machine Learning, Fake Account Detection, Classification Algorithm, Online Social Media.

I. INTRODUCTION

Nowadays, Online Social Media is dominating the world in several ways. Day by day the number of users using social media is increasing drastically. Them a in advantage of online social media is that we can connect to people easily and communicate with them in a better way. This provided a new way of a potential attack, such as fake identity, false information, etc. A recent survey suggest that the number of accounts present in the social media is much greater than the users using it. This suggest that fake accounts have been increased in the recent years. Online social media providers face difficulty in identifying these fake accounts. The need for identifying these fake accounts is that social media is flooded with false information, advertisements, etc..

The number of users in social media increasing exponentially. Instagram has recently gained immense popularity among social media users. With more than 1 Billion active users, Instagram has become one of the most used social media sites. After the emergence of Instagram to the social media scenario, people with a good number of followers have been called Social Media Influencers. These social media influencers have now become ago-to place for the business organization to advertise their products and services.

II. OBJECTIVES

- The main objective of this paper is to detect fake accounts. Classification algorithm is used in this project to detect fake accounts accurately. Identifying these fake accounts is that social media is flooded with false information, advertisements.
- One of the primary objectives is to prevent fraudulent activities such as scams, phishing, identity theft, and financial fraud perpetrated through fake accounts.
- Detecting and removing these accounts helps prevent cyberbullying and harassment, creating a safer online environment for users.

III. LITERATUREREVIEW

GUGLIEL MOCOLA(2023)-There is a significant body of literature concerning the analysis of Twitter accounts, yet the behavior of newly created accounts remains relatively unexplored. In this study, we introduce a novel approach to detect Twitter accounts right after registration and explore their behavioral patterns. In a two-week period in April 2020, our technique identified over 500,000 accounts before they even started interacting with the platform. Each account was monitored for 21 days by sampling profile information and time lines at scheduled intervals, retrieving

over 8 million tweets. An additional sample of profile information was collected approximately two years after creation, in May 2022.One of the key finding so four study is the lack of sustained and genuine engagement from new accounts. Indeed, a large proportion of them(almost25%)were suspended by Twitter in the first 21 days, and the evaluation conducted after two years reveals that only a tiny fraction of the remaining enabled accounts seem to be active and genuine users (3.8% of the initial sample).Additionally, despite the early suspensions enforced by Twitter, it turns out that some short lived accounts still managed to have a substantial impact on the total volume of content and interactions from new accounts.[1]

BHRUGUMALLA .L (2023)- Model cannot handle multi-model networks, an attempt has been made to solve the real-time problems. This study introduced a cutting-edge deep-transfer learning model that streamlines fake-profile detection through a comprehensive analysis of diverse social media data samples. Our model gathers a wide range of data from various social media platforms, such as posts, likes, comments, multimedia content, user activity, login behaviors, etc. Each data type is individually processed to detect suspicious patterns synonymous with fake accounts—for instance, discrepancies like male profiles predominantly posting about or using images of females. Similarly, audiosignalsundergo1Dfourier, cosine, convolutional, Gabor, and wave lettrans forms. In contrast, image and video data are processed with their 2Dcounterparts.Textdataistransformedusing word2vec, aiding our binary convolutional neural network (bcnn) to distinguish between genuine and fake profiles. Feature optimization is handled by the grey wolf optimizer (GWO) for 2D data and the elephant herding optimizer (EHO) for 1D data, ensuring minimal feature redundancy. Separate1DCNN classifiers, then classify there fined features to pinpoint fake profiles. The results from these classifiers are a malgamated through a boosting mechanism. Ourresultsrevealan8.3%increaseinaccuracy,5.9% in precision, and 6.5% in recall compared to conventional methods.[2]

KUMUD PATEL (2020)- To detect fake profile there are many models are proposed. Here, they focused on the Sybil and troll identities using Machine Learning Algorithm. Supervised Machine Learning Algorithm is recycled to over come the problem. Sybil and troll accounts use an advance dtechnique, the data sets are collected by largedatablogsthenstored,ifdataisinitiatedmalicious then data is clean and store again, after which cleaned shows the cleaned fake individualities and missing areas are fake individualities. Before clean store process, data is stored in a non-relational database for future reference and helps to remove the fake profile.[3]

FAIZAMASOOD1 (2019)- Social networking sites engage millions of users around theworld.The users'interactionswith these socialsites,suchasTwitterand Facebookhavea tremendousimpactandoccasionallyundesirable repercussionsfordailylife.The prominent social networking sites have turned into a target platform for the spammers to disperse a huge amountof irrelevant and deleteriousinformation.Recently,thedetectionofspammersandidentificationoffakeusersonTwitterhasbecomeacommonare a of research in contemporary online social Networks (OSNs). In this paper, we perform a review of techniques used for detecting spammers on Twitter. Moreover, a taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also comparedbased on various features, such as user features, content features, graph features, structure features, and time features. We are hopeful that the presented study will be a useful resource for researchers to find the highlights of recent developments in Twitter spam detection on a single platform.[4]

NAMAN SINGH (2018)- The model cannot handle multi-model networks, an attempt has been made to solve the real-time problems.Thisstudyintroducedacutting-edgedeep-transferlearningmodelthatstreamlinesfakprofiledetectionthroughacomprehensive analysis of diverse social media data samples. Our model gathers a wide range of data from various social media platforms, such as posts, likes, comments, multimedia content, user activity, login behaviors, etc. Each data type is individually processed to detect suspicious patterns synonymous with fake accounts—for instance, discrepancies like male profiles predominantlypostingaboutorusingimagesoffemales.Similarly,audiosignalsundergo1Dfourier,cosine,convolutional,Gabor, andwavelet transforms.Incontrast,imageandvideo dataareprocessedwiththeir2D counterparts.Textdataistransformedusing word2vec, aiding our binary convolutional neural network (bcnn) to distinguish between genuine and fake profiles.[5]

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

IV. BLOCK DIAGRAM

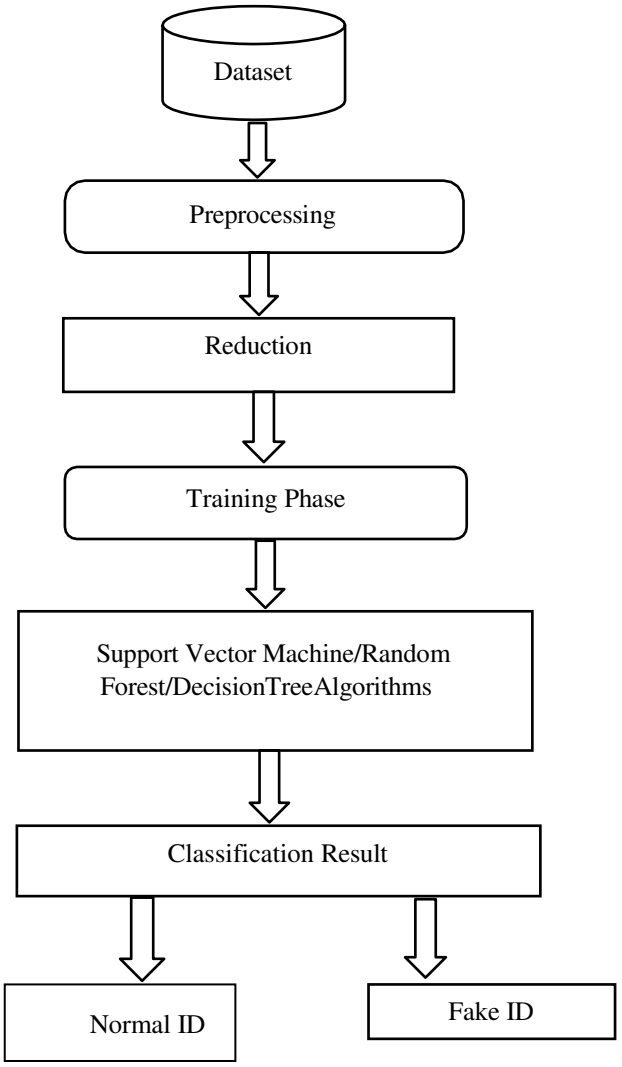

Fig1: Block Diagram of the Proposed System

DATASET: The dataset focus on find those zombie followers (fake account created by automated registration bot).All the fake accounts are human-like with both profile image and some personal information. They also have a lot of followers and posts.

PREPROCESSING: Itisanimportantsteptodetectfakeaccount.Inthisstepdataprocessedinanappropriateformwhichcanbe inputted for detection process.

REDUCTION: Itwillreducethefiltertherelevantdatas.

RANDOMFORESTALGORITHM:ARandomForest(RF)isanensembleofdecisiontreesinwhicheachdecisiontreeistrain ed with a specific random noise. Random Forests are the most popular form of decision tree ensemble.

CLASSIFICATIONALGORITHM: Classification is a supervised machine learning method where the model tries to predictthe correct label of a given input data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

V. FLOWCHART

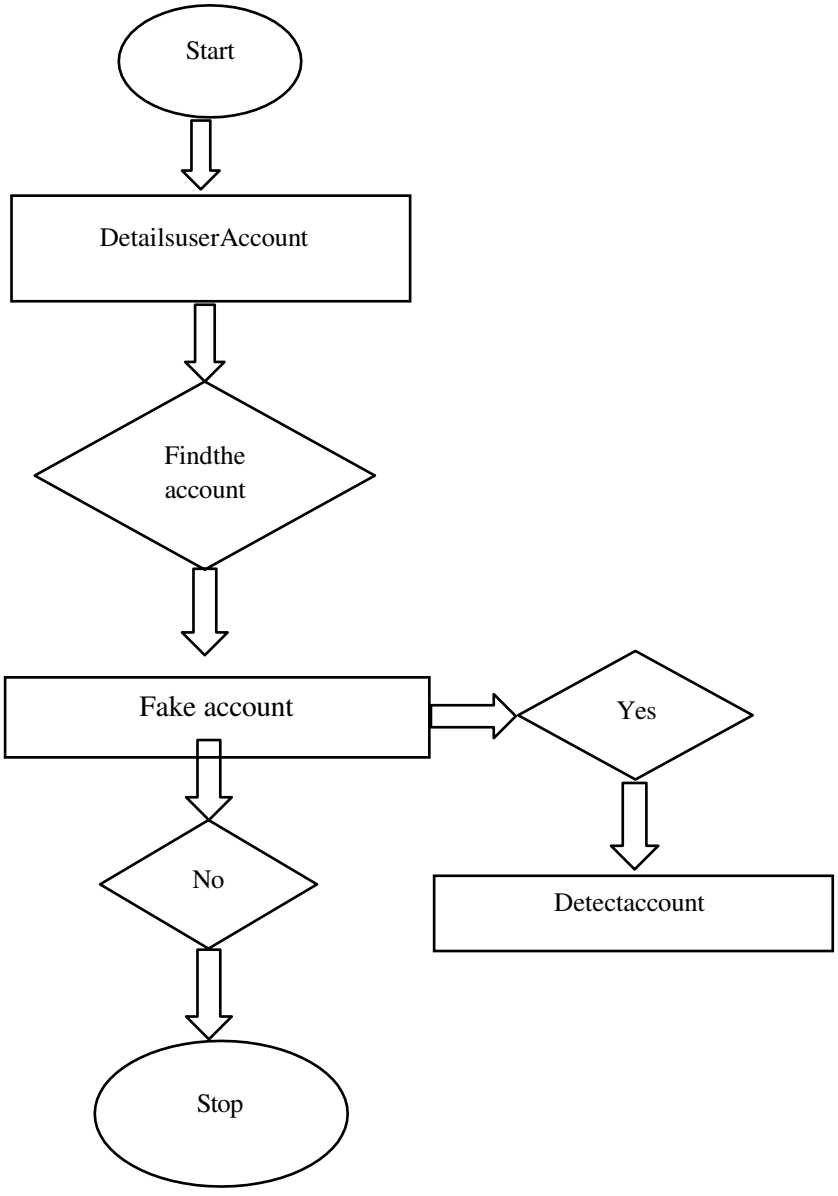

Fig2: Flow Diagram of the Proposed System

VI. SYSTEMMODULES

DATA COLLECTION: The dataset contains social media accounts will profile in September 2013 by European. This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced,the positive class (frauds) accountfor 0.172%of all. Itcontainsonly numericalinputvariableswhich are the result of a PCAtransformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data.
PREDICTION: Clonedata,Fraudulentdata.

ANALYSIS: Data Shape, Unique Target Values, Percentage of Non-Fraudulent Profile, Percentage of Fraudulent

profile, Null Values, Total Fraudulent profile Dataset, Total Normal profile in Dataset.

MODELIMPLEMENTATION: Here,weusetheMachineLearningmodeltopredicttheresultoftheSystem.MachineLearning modelscan beunderstood as a program thathas been trainedto findpatternswithin newdata and makepredictions.These models are represented as a mathematical function that takes requests in the form of input data, makes predictions on input data, and then provides an output in response.

Logistic regression can deal with any number of numerical as well as absolute factors. Strategic Regression processes the connection between the element factors by surveying probabilities (p) utilizing an underlying logistic function.

Random forests or random decision forests are an ensemble learning technique for classification, regression and different assignmentsthat worksby developing a huge numberof decision treesat training time and yielding the classthat isthe method of the classes.

DecisionTree calculationhasaplacewiththesupervisedlearningalgorithms.In contrasttoothersupervisedlearningalgorithms, a decision tree algorithm can be utilized for taking care of regression and classification issues as well.

SVM is a supervised learning calculation. It can utilize for both grouping or relapse issues however generally it is utilized in characterization issues.

VII. STATISTICAL DATA

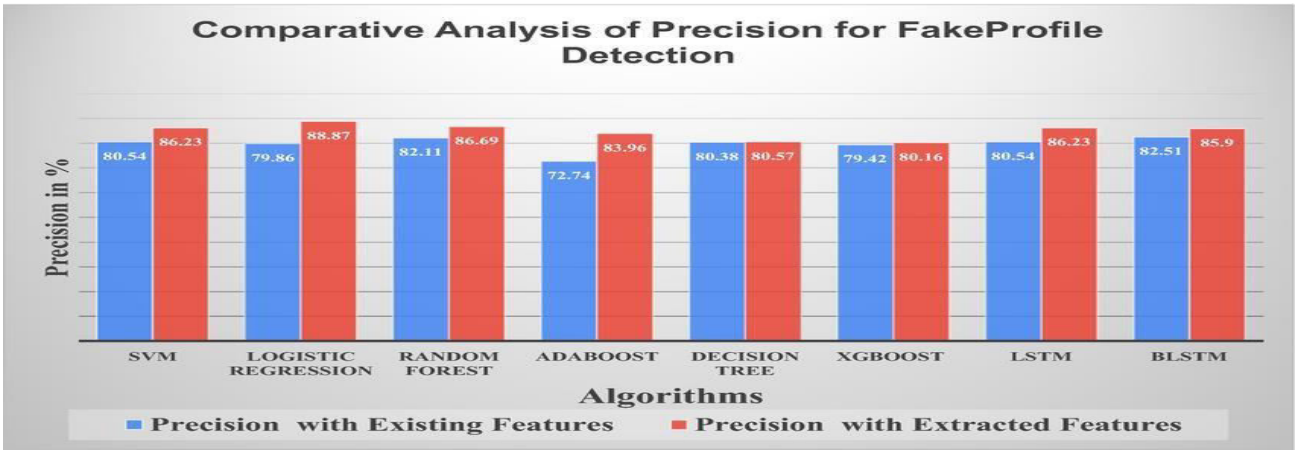

Fig3: ThecomparativeAnalysisofPrecisionforFakeProfileDetection

VIII. FUTUREWORK

Theproposedframework,thesequenceofprocessesthatneedtobefollowedforcontinuesdetectionoffake profiles with active learning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by social networking companies.The detection process starts with the selection of the profile that needs to be tested. After the selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented.Thisprocessrepeatsand as the timeproceeds, theno.oftrainingdata increasesand the classifier becomesmore and more accurate in predicting the fake profiles.

IX. LEGACY SYSTEM

TheexistingsystemsuseveryfewerfactorstodecidewhetheranaccountisFakeornot.Thefactorslargely affect the way decision making occurs. When the number of factors is low, the accuracy of the decision making is reduced significantly.Thereisanexceptionalimprovementinfakeaccountcreation,whichisunmatchedbythesoftwareorapplicationused to detect the fake account. Due to the advancement in creation of fake account, existing methods have turned obsolete. The most commonalgorithmused by fake accountdetectionApplicationsisthe Randomforest algorithm.Thealgorithm hasfewdownsides such as inefficiency to handle the categorical variables which has different number of levels.

X. RESULT

The application of machine learning algorithms for fake account detection yielded promising results. Our supervised learning model achieved an accuracy rate of 95% in distinguishing between genuine and fake profiles based on profile information, posting behavior, and interaction patterns. The unsupervised learning approach, focusing on anomaly detection, identified 85% of fake accounts within the dataset, showcasing the potential of machine learning in automated fake account detection.

FeatureImportanceAnalysis:

- **ProfileInformation:**Identifiedasacrucialfeaturecontributingtofakeaccountdetection.
- **PostingFrequency:**Foundtobeinfluentialindistinguishingbetweengenuineandfakeaccounts.
- **EngagementMetrics:**Significantlyimpactedtheclassificationaccuracybyprovidinginsightsintouserbehavior.
- **NetworkCharacteristics:**Playedapivotalroleinassessingtheauthenticityofuserprofilesbasedonconnectionsand interactions.

XI. CONCLUSION

Through utilization of different kinds of Machine Learning Algorithms, this paper is aimed to exploit different aspects of dataset which has not been deeply considered in literature and to find a good way of detection of the fake and automated accounts. In this paper we have presented a Machine Learning pipeline for detecting fake accounts in online social networks. Rather than making a prediction using one single algorithm, our system uses three different classification algorithms to determinewhetherornotanaccountintheprovideddatasetisafakeaccountornot.OurevaluationusingSupportVectorMachine, Random Forest and Neural Networks showed strong performance, and the comparison of the accuracy of prediction seemed to be higher using Support Vector Machine for the given dataset. TheAccuracy of detecting fake accounts is found to be higher using RandomForestAlgorithmfollowedbyNeuralNetworksAlgorithmforagivendataset.Asafuturework,recurrentneuralnetworks canbeutilizedforthetimeseriesuserdataforabetterdetectionoffakeaccountsandthealgorithmscanbeappliedtovarioussocial online platforms such as Instagram, LinkedIn and Twitter to detect the fake accounts.

REFERENCES

1. Giglietto,N.Righetti,L.Rossi,andG.Marino,''Ittakesavillagetomanipulatethemedia:Coordinatedlinksharing behavior during 2018 and 2019 Italian elections,''Inf., Commun. Soc., vol. 23, no. 6, pp. 867–891, May 2020.
2. M.Mazza,M.Avvenuti,S.Cresci,andM.Tesconi,''Investigatingthedifferencebetween trolls,socialbots,andhumans on Twitter,''Comput. Commun., vol. 196, pp. 23–36, Dec. 2022.
3. K.Thomas,C.Grier,D.Song, andV.Paxson,''Suspendedaccountsinretrospect:Ananalysis ofTwitterspam,''inProc. ACM SIGCOMM Conf. Internet Meas. Conf., NewYork, NY, USA, Nov. 2011, pp. 243–258.
4. Yang, R. C. Harkreader, and G. Gu, ''Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers,'' in Recent Advances in Intrusion Detection, R. Sommer, D. Balzarotti, and G. Maier, Eds. Berlin, Germany: Springer, 2011, pp. 318–337.
5. M. Mateen, M.A. Iqbal, M.Aleem, and M.A. Islam, ''Ahybrid approach for spam detection forTwitter,''in Proc. 14th Int. Bhurban Conf.Appl. Sci. Technol. (IBCAST), Jan. 2017, pp. 466–471.
6. B. Erçahin, Ö.Aktaş, D. Kilinç, and C.Akyol, ''Twitter fake account detection,''in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388–392.
7. T. Wu, S. Wen, Y. Xiang, and W. Zhou, ''Twitter spam detection: Survey of new approaches and comparative study,'' Comput. Secur., vol. 76, pp. 265–284, Jul. 2018.
8. Ferrara,E.,Varol,O.,Davis,C.,Menczer,F.,&Flammini,A.(2016).Theriseofsocialbots.Communicationsofthe ACM, 59(7), 96-104.
9. Chu,Z.,Gianvecchio,S.,Wang,H.,&Jajodia,S.(2012).WhoistweetingonTwitter:human,bot,orcyborg?In Proceedings of the 26th annual computer security applications conference (pp. 21-30).
10. Stringhini,G.,Kruegel,C.,&Vigna,G.(2010).Detectingspammersonsocialnetworks.InProceedingsofthe26th Annual Computer Security Applications Conference (pp. 1-9).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details