Machine Learning Implementation for Identifying Fake Accounts in Social Network

P.Nagaraju[1], J.Akash[2], D.Rakesh[3], D.Rajkumar[4], Ch.Navadeep[5] , J.Chaitanya[1]

[1]Assistant Professor, Department of CSE, Balaji Institute of Technology and Science, Laknepally, Warangal, India

[2,3,4,5]B.Tech Student, Department of CSE, Balaji Institute of Technology and Science, Laknepally, Warangal, India

Abstract: Social Networking is the main era of datatransmissionaswellasdatacreationinalargescaleandthe reason why big data is created is very much known.Social networking is the main platform where tons ofdata is being created and by 2025 even Google datacenters can't handle that kind of huge volume. Increasein the fake accounts are creating exponential growth ofthe volume and in this paper we are proposingarchitecture for identifying the fake accounts in thesocial networking, especially in Facebook. In thisresearch we are using Machine Learning to implementbetter prediction on identifying the fake account basedon their posts and status on their social networkingwalls. We can consider Facebook and Twitter for thisresearchandforthesecuritypurposeandavailabilityofdata, we are considering Twitter for this research.Twitter tweets and tagging, type of posts they arecreating and sometimes some account people createsmess in the society with their posts, identify those andblock the fake and unwanted information circulatingover the network for the peace and security. Twitter isused as main based with ML NLP for the processing ofthe text data and herewe have to use sentiment analysisfor identifying the goals we put on.

***Keywords*:** MachineLearning,SentimentAnalysis,NLP,Twitter, Big Data, Prediction

INTRODUCTION

Text classification in machine learning will teach us the security levels we need to maintain in the social networking and also in our daily basis. In this social networking era we are using tweets to express our feelingsandideasoropinionsintheportalthrough ournetwork andasperanNGOsurvey,thereare more fake accounts being created in the social networking and because of those some of the fake information is being circulating in the portals through

doi: 10.48047/ijiee.2025.15.4.56

un properchannels.In this kindof situationweneed to avoid those un wanted and harmful accounts from the social networking to save space in the data as well and to stop the mess in the society on the social and political issues. Here in this article weare using twitter data collected from public repository as well as our own creation from a survey conducted and every day at least 1000 fake accounts are being created in the social networking and this will create burden on the network and also high volume space is being ruined. To avoid this we need to identify a path for the better implementation of the NLP and the text classification. More than NLP we can use SVM forthiskindoftextclassification asthiscan be considered as the parent algorithm for the text classifications and the data identification in betweenthe texts we wrote on the social networking. Here we implementitwiththeBOW(BagofWords)andit's a common procedure in SVM andCNBclassifiers[19-20]. In CNB classifiers as we use BOW and alsowehavetoimplementthisonasplatformlike WEKA. This tool of machine learning will take thetest data enven though if we are not proving thetraining data it will perform prediction models andgive the accurate results. As per our work we have98% accuracy of SVM to identify the fake accountsand helps to warm the social networking in charges regionally to remove and report the un wantedaccounts and also CNB given accuracy of 97% whichis a little less and the thing here is a criteria thatbothers us is this kind of research is must be implemented in social platforms like Facebook rather than Twitter. Asperasurveythereare500MillionFemale accountsinFacebook,butthepopulationofFemale in world is nearly 300 Million. That means we can assumehowmanyfakeaccountsandunwanteddata is being created. And how we can identify a social account is fake. It's not completely possible on identifying with status, tweets, and posts. We have to go little deeper into theconcept and have toinvestigate into the account. We have some of

doi: 10.48047/ijiee.2025.15.4.56

concepts and architectures explained in this paper which are we very need to follow before creating a social network account and also how to identify the existing accounts trustworthy. [1-22]

In this paper we are trying to explain the existing approachesinthesocialnetworkingonwhichthey are concentrating on identify the better prediction model.Inthenextsectionwewillexplainthe existing scenarios using in the social networking implementation,proposeapproachinthelater section, architecture we would like to follow in thenext one, results and explanation in the later section, finally conclude with conclusion and references.

EXISTINGSYSTEM

In the recent era of technology as the applications and the utilizations increase on our daily life, we continuously posting some unwanted and unawarestuffinthesocialnetworkingandcreatingmessin the social platform. In the issue we can consider fake accounts and the people with fake accounts using this platform for their money and how we can stop in this kind of serious situation. Let's consider few social networking platforms for our research work. First is twitter. As we now that twitter mining is the well known application of research and we can have the public dataset of the twitter mining. In this approachwe need to get the information about the people who are posting some unwanted things and they need be caught and have to remove those before it creates problem. [3-10]

The twitter account will ask some email ID or the phonenumbertocreateanaccountandforthiskind of fake accounts people are creating fake mailaccounts and we don't need to produce any authentication for creating mail Id expect phone number. If you are following any improper things inthe social networking we need to identify that before spreading to others. Some issues like countryproblems. A political drama can be added as a tag inthe twitter with and Hash tags. If the hash tag is not created by the person or account which is not responsible then that will create a social war in the network and they used completely discussing aboutthis with the bad words and the comments. Here wearefocusingonthecommentstooforidentification of the information and the sample hash tagging

scenario will be explained with the image below. Inthe image below that is Figure 1 illustrates that thehash tagging in the twitter will go on continuouslywith unwanted

doi: 10.48047/ijiee.2025.15.4.56

stuff. Once tag is created with the anothertagiscreatedbyanotherpersonandfora limit of tweets or the likes for the concept in the tag twitter will pay some amount for the account holder. Includingmoneyfakeinformationmayspread through it and this causes a big problem.[2-7]

The main problem here is we are not considering the text in with which tag is applied. First we need to identify the whether the tag applied is genuine information of not. If the tag is genuine information then we can make that tag popular. If not we need to spam or report that tag to avoid mess in the social platform. How to identify that a tag is genuine or not. Based on the previous tags and comments of that person who is holding that account. If we track all the tweets and comments of the person who posted that hash tag we can predict that whether that tag can be published or not. For this kind of things we need to discuss the procedure and we will do the same in the proposed approach section which will be explained in the next few lines.[5-13]

Another social networking we consider its Instagram. Instagramisveryfamousforfollowingcelebrities and the fan pages in our own locality or globally. Day bydayfakeaccountsarebeingincreasedin instagram more than facebook. As this was inventedby Facebook, more than facebook Instagram is more popularforcreatingfakenewsandcreating reportable content. If we observer Instagram for a while, we have some many women who are doing unfair things for money through this platform. They used post some unfair words in their instagram story andthatstorywillbeappearfor24hoursfromthe time of publish. The current architecture of Instagramis not bothering about the posts and story of theaccount holders until anyone reports a live video callor a post. We need to identify the words while the account holder posting and we need to identify the sentencemeaning inthatpost.As adignity purpose we are not mentioning those sentences and words inthis article and if they are required further more foranyexplanationandproofpurposeanyonecontact usewareveryhappytoexplainwhichkindof words we need to consider in instagram for

indentifying fake accounts. Figure 2 will explain the architecture of Instagram posting and Figure 3

doi: 10.48047/ijiee.2025.15.4.56

explains the database architecture models for the instagram[10-15].

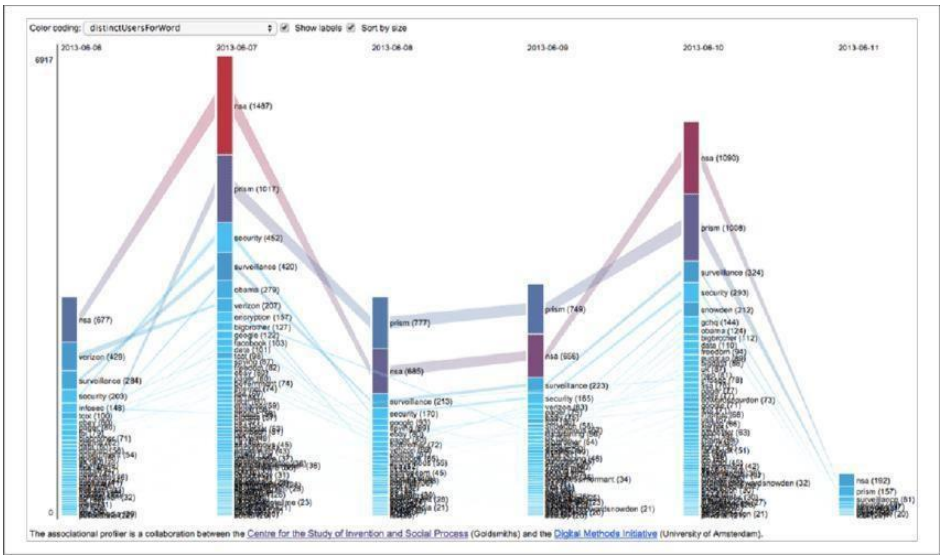


Figure1:TwitterHashTagging Scenario

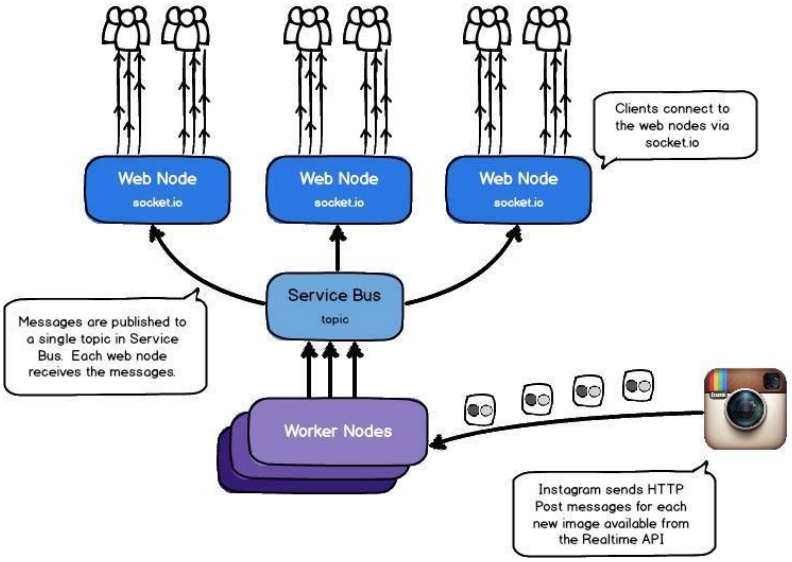
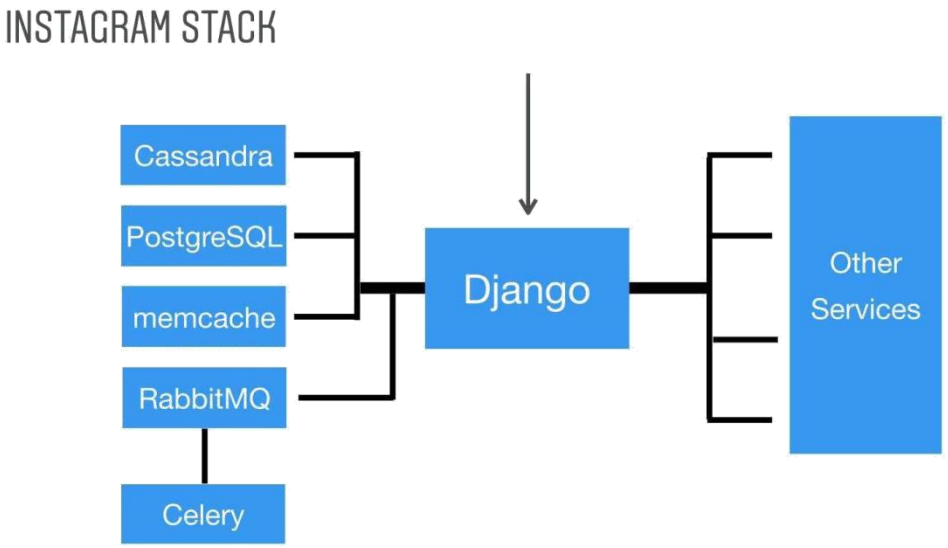


Figure2:ArchitectureofInstagramfollowingforpostingwithnodes

doi: 10.48047/ijiee.2025.15.4.56



In this architecture we need to observe that how data is moving from each edge to other edge. In thisarchitecturewhenthepostissubmittedby the person it will navigate to the worker node in the server. In the real time for each image or the text in the instagram story instagram appwillsend the HTTP request to each image which are available from real time API. These API's are created or when can use existing image handling API's. In this kind of architectures we have multipleworkingnodesavailableandifyou don'thaveanyworkingnodeunavailablethen the posting will be delayed or aborted with time out. The point here is we need to concentrate is whenthedataispostingthroughHTTPrequest to the worker node, we are not validating the content in the post. Whether that post may cause harm to the society, or some nudity is available, somethingrelatedtosocialissueslike prostitution or something related to these. In this case we are failed in development of clientsecured applications though we have high rangeof servers to maintain and manage.[14-18]

The very second example we need to put in frontof the technocrats is unhealthy twitter tags. Improving political and general awareness is a good thing but this kind of unhealthy hash tagswill cause damage to the human behavior this causing some of the quarrels[16] among the communities. Instead of using social network to stop the issue, some fake account holders will create issue with their comments and tags. Our machine learning approaches currently usingfailed to identify those before publishing the post.[18]

Third issue is Fake accounts in Facebook. As I mentionedearlier,therearemorethan200 million Fake Facebook accounts in the name of female. That's a great thing that Facebook is not controlling their accounts and

doi: 10.48047/ijiee.2025.15.4.56

because of these fake accounts money laundering, smuggling and some other anti-social elements are taking place[17].In the next section we will address the proposed architecture for this validations before posting an

status and secondary thing is identifying gender based on the content in the post.

I.PROPOSEDAPPROACH

In this approach we are focusing on an architectural methodology for implementation like below. Which will have few stages in their implementation and the concept here is to predict the Fake accounts in the social networking and also try to avoid the fake status or contents in the social media[18].

a.DataIdentification

Data identification is a great task for social media predictions as this is one of the sensitive areas to discuss. Because of some security issues we are not providing the information abut the public repository where we got the dataset with the relevantinformation. But we are here with the data needed to

identify whether the account is fake or not and the secondary thing is to identify the fake news and block that information to circulate in you locality.

The data we need here is the account holder general information, age given to create account, what is the most used word in their post, are there any contents related to nudity, are there any content of abuse on a community or a gender etc.

Inthispaperweareproposingtwokindsof individualarchitecturesandfinallywewill collaborate two concepts and to make a final product. First one will identify the account details by usingNLPandnetworkidentification.Basedonthe networkonwhichtwoormoreaccountsare accessingthenweneedtoaskthemtoprovide security verifications. That will be explained in this architecture easily.

doi: 10.48047/ijiee.2025.15.4.56

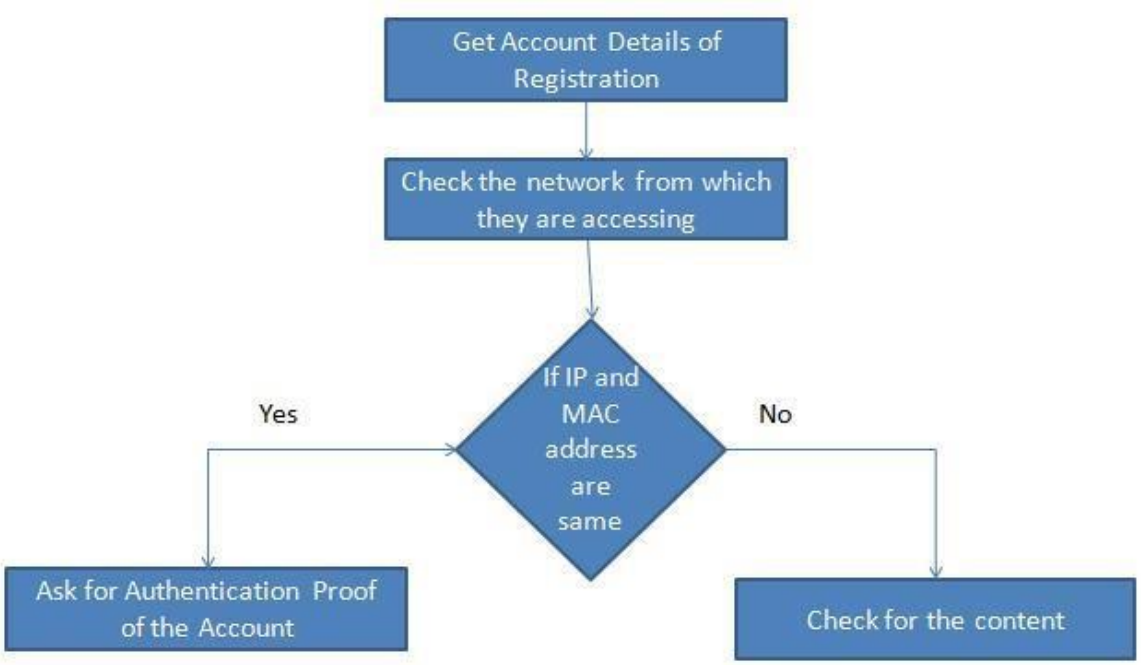


Figure4:Architecture1 foraccount authentication

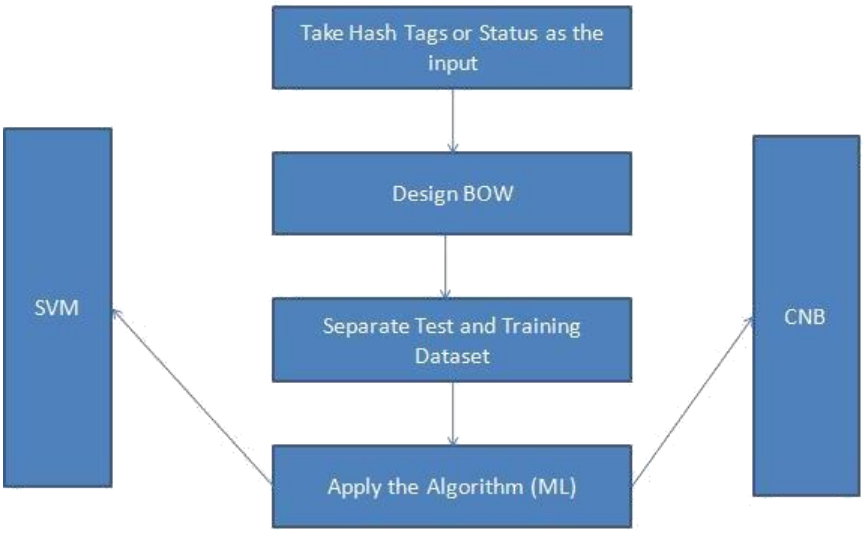


Figure5:Architecture2forAuthentication before usingMLalgorithmsincompleteway

doi: 10.48047/ijiee.2025.15.4.56

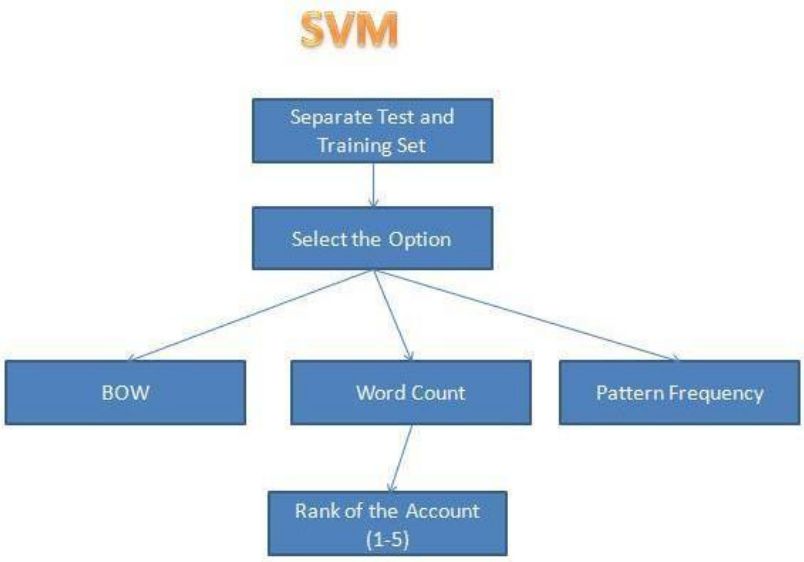


Figure6:SVMclassifierarchitecture1forauthentication

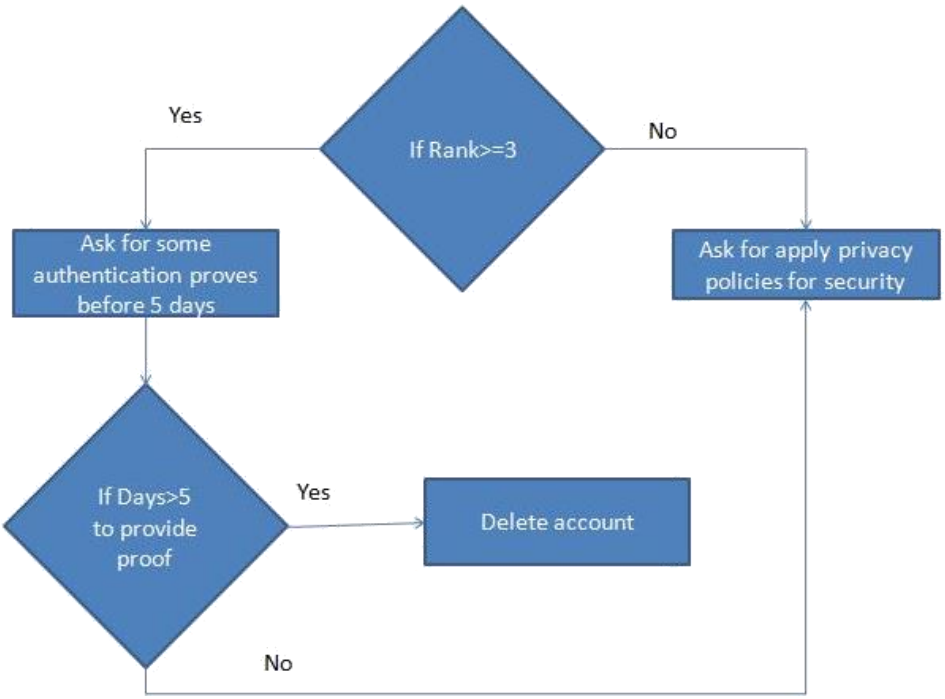


Figure7:SVMarchitecture2forAuthentication

Intheabovescenarioofarchitectureswehave dividedintofourparts,whichistwopartseachin each type. In first architecture part one in figure 4 the client using the account have to face some of the security issues like if two or more accounts are managing from one IP address or MAC

doi: 10.48047/ijiee.2025.15.4.56

address, then our application will ask for authenticate themselves with ID proof. This is because we don't know thesamepersonwithdifferentaccountsismanaging from the same address. If the same is like this " same person is using two or more accounts and if the one is from desktopandothertwoisfrommobiledevice. For these kind of situations based on the common IP address and the name relativity of the account need to authenticate and if there is any security bleach weneed to ask for provide proof for further continuation with the account. If the IP address is different and we can check with MAC address from which the accountis getting access using the server log files and request and response times.

In the second part of the first architecture we are ranking the account with this kind of security bleach and if the rank is 1 or 2 there will be no problem and ask them for apply security privacy settings to protect their account. If the rank is greater than or equal to 3 then we need to ask for the proof.

If the person with multiple accounts failed to provide proofs within 5days then account and the data of that account must be terminated for the security purpose without any intimation. If they provided proofs, then ask them to apply privacy settings after log in into the account.

In the second architecture we are using SVM BOW concept for identification of the number of words are harmful. The harmful words are collected andgathered as the data set or in the text format. We need to divide the test and training dataset and attach the BOW to the prediction model through SVM. It will calculate the number harmful words are there in individual account and this is based on their content

identifying account user and warning him or her to provide the authentication proofs to continue with the account further. In this process we will identify the word count of the single word, number of times a pair of words that are harmful are repeated. So that if the scale is less than 3 then the user is fine, if the scale is

greater than or equal to 3 then the user must provide proofs to continue with the account. This process canbe useful for any social networking account.The below things will explain the data cleaning we need to do before processing any data set .

doi: 10.48047/ijiee.2025.15.4.56

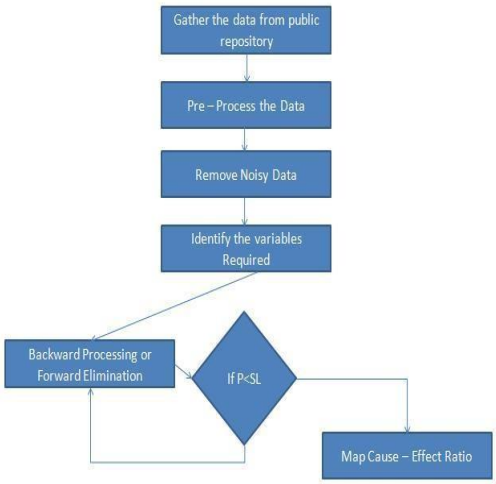


Figure8:Part1oftheProposeArchitecture

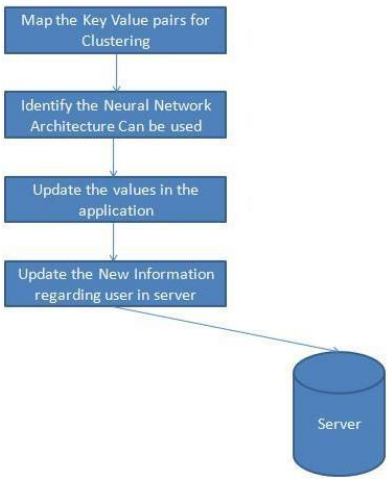


Figure9:Part2of theproposed architecture

doi: 10.48047/ijiee.2025.15.4.56

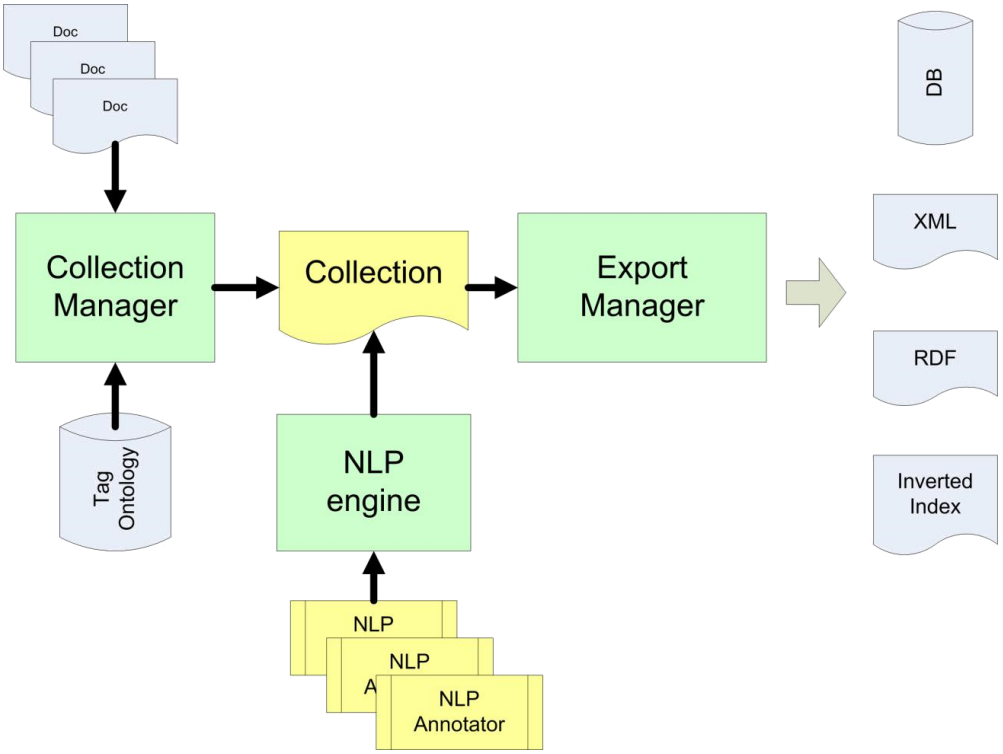


Figure10:NLPArchitecturetouseforconcertingsomeoftheunknown languagetypestounderstandableformat

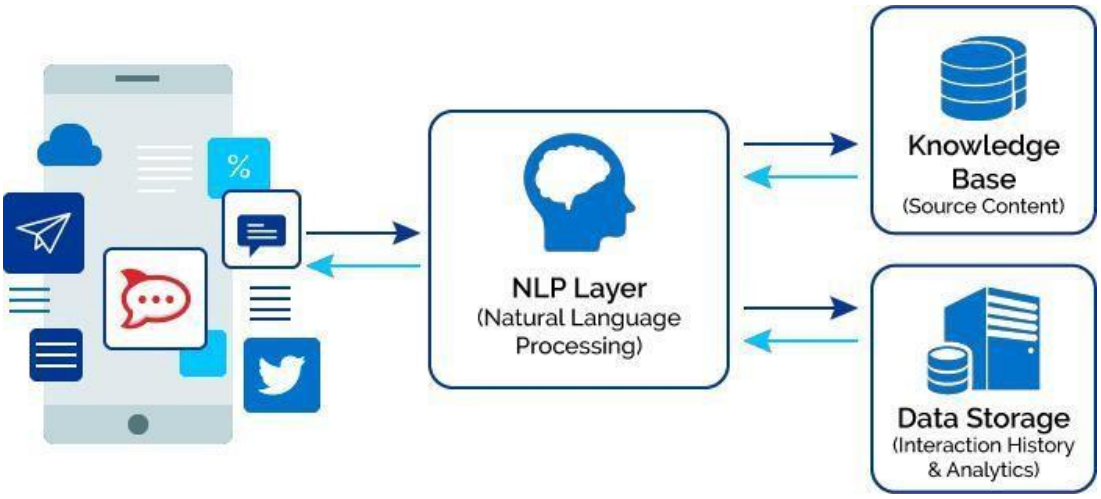


Figure11:NLParchitecturewhichwillmaintainthedatafromapplicationto repository

doi: 10.48047/ijiee.2025.15.4.56

RESULTS

In this section we will discuss about the clusters we formedandinthetablewehavekeyvaluepairs which will have the group of pairs. This will tell the medication limit of the patient based on the age,gender, weight, previous treatments, previous medication, and current scenario. The below is the

table which will give the explanation based in the key value pair. This pair will give the warning to thedoctor if her give the high drug usage.

These are the few clustering results we acquired as mentioned below which will have the values of how many times a pair of key value is being repeated.

doi: 10.48047/ijiee.2025.15.4.56

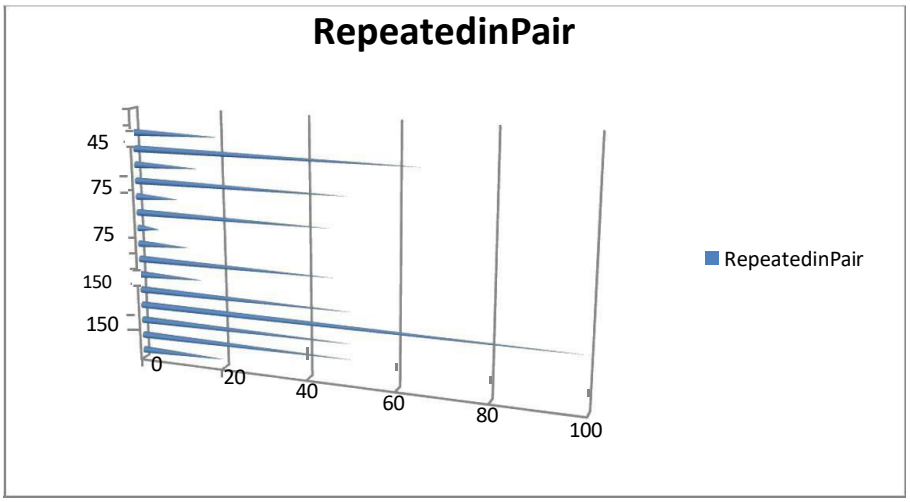


Figure12:KeyValuepairsetsoccurrenceresult

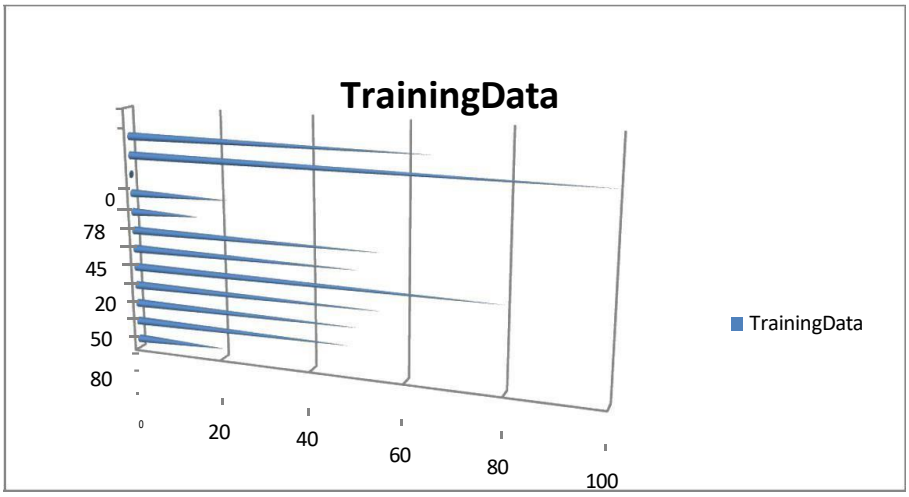


Figure12:Separationoftrainingandtestdatasetavailableaftergettingaccuratekeyvaluepair

The above graphs will explain the cases we are havingbestpairofkeyvaluepairs.Thebelowtable

Table1:Accuracyof SVMandCNBin identifyingFake accounts

will explain the list of variables we will consider for this kind of key value pairs.

Social Networki	SVM Accurac	CNB Accurac	Number of	No.OfValid Accounts	No.OfInvalid accounts	No. Of accounts

doi: 10.48047/ijiee.2025.15.4.56

ng type	y	y	accounts processed			deleted
FB	97	95	15000	12000	3000	1500
Instagram	95	95	15000	12000	3000	1000
Twitter	99	97	15000	12000	3000	1000
YouTube	99	98	15000	12000	3000	500
Whatsapp	89	89	15000	12000	3000	1500

doi: 10.48047/ijiee.2025.15.4.56

CONCLUSION

The main issue with social networking security is not authenticating them properly before publishing thedata.Here we usedsome of the chats, status andallthe account information and proposed an architecture suingwhichweneedtoidentify thegenuinenessof the account so that based on which we can make that account continue with the service or we need to terminate the service. SVM and CNB are used in this process for validating the content based on the text classification and sentiment analysis of the data. Inthis sentiment analysis we need to gather the harmful words count, how many times they are repeating, and what is the harmful pair of words and how many time they are repeating. For Facebook SVM shows 97% accuracy as CNB shows 95% percent accuracy of identifying the fake accounts based on BOW.

REFERENCES

1. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960

2. Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.

3. Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
4. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
5. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
6. Bhukya Madhu, M.Venu Gopala Chari, Ramdas Vankdothu,.Arun Kumar Silivery,Veerender Aerranagula " Intrusion detection models for IOT networks via deep learning approaches " Measurement: Sensors Journal,Volume 25, 2022, 100641
7. Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537
8. S. Rakesh [a], NagaratnaP. Hegde [b], M. VenuGopalachari [c], D. Jayaram [c], Bhukya Mad hu [d], MohdAbdul Hameed [a], Ramdas Vankdothu [e], L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" Measurement: Sensors ,Journal,Volume 30, 2023, 100898

doi: 10.48047/ijiee.2025.15.4.56

9. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.
10. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol. 29, No. 6, (2020), pp. 2875 – 2881
11. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)
12. Ramdas Vankdothu, Dr.Mohd Abdul Hameed "A Security Applicable with Deep Learning Algorithm for Big Data Analysis",Test Engineering & Management Journal,January-February 2020
13. Ramdas Vankdothu, G. Shyama Chandra Prasad " A Study on Privacy Applicable Deep Learning Schemes for Big Data" Complexity International Journal, Volume 23, Issue 2, July-August 2019
14. Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020
15. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)
16. Ramdas Vankdothu, Dr.Mohd Abdul Hameed " Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics", Complexity International Journal , Volume 24, Issue 01, Jan 2020
17. Ramdas Vankdothu, G. Shyama Chandra Prasad" A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools" International Journal For Innovative Engineering and Management Research,Vol 08 Issue08, Aug 2019

doi: 10.48047/ijiee.2025.15.4.56

BIBILOGRAPHY

Iam**J.AKASH.**Iamcurrentlyinmy7thsemesterofComputer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "WEATHER FORECASTING USING MACHINE LEARNING".

I am **D. RAKESH**. I am currently in my 7th semester of Computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "WEATHER FORECASTING USING MACHINE LEARNING".

Iam**D. RAJUKUMAR**.Iamcurrentlyinmy7thsemesterofComputer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "WEATHER FORECASTING USING MACHINE LEARNING".

Iam**CH. NAVADEEP**.Iamcurrentlyinmy7thsemesterofComputer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "WEATHER FORECASTING USING MACHINE LEARNING".

doi: 10.48047/ijiee.2025.15.4.56