Indonesian Journal of Electrical Engineering and Computer Science
Vol. 27, No. 1, July 2022, pp. 563~572
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v27.i1.pp563-572

A semi-automated hybrid approach to identify radicalization on social digital platform

Vandna Batra, Suresh Kumar
Department of Computer Science and Engineering, Faculty of Engineering and Technology,
Manav Rachna International Institute of Research and Studies, Faridabad, India

Article Info

Article history:

Received Dec 27, 2021
Revised May 27, 2022
Accepted Jun 9, 2022

Keywords:

Accuracy
Deep learning
Machine learning
Radical activity
Sentimental analysis

ABSTRACT

The digital social platform is an important medium for sharing or communicating a message from one person to another or one to many. The growth of internet users and social media use has also led to many adverse consequences. Such a platform is also used for radical activity by spreading the radical message in public. The detection of such a message is impossible by human monitoring. Many researchers are continually working on automatic detection of such activity to find a way to stop it. Automatic identification is also not possible due to the massive amount of data present and ambiguity in messages. The proposed work presents a framework for detecting the radical message and taking action by automatically blocking it. A dataset of 33k tweets has been fetched from twitter based on radical words. Two machine learning models, first countervectorizer and Logistic regression-based and second convolutional neural networks (CNN) have been applied yielding 96.97% accuracy. The provision of human intervention is also given in doubt cases which helps further to improve the accuracy of overall model. The framework gives very good results in a simulated environment.

Corresponding Author:

Vandna Batra
Department of Computer Science and Engineering, Faculty of Engineering and Technology,
Manav Rachna International Institute of Research and Studies
Faridabad, Haryana, India
Email: vandna.batra88@gmail.com

1. INTRODUCTION

For the past several decades, digital social media has grown exponentially in tandem with the rise of the digital network. People may express their opinions and ideas on various social media platforms available on the internet. Users on such social media build strong bonds by expressing their views in the form of photographs, comments, text messages, and other mediums. On such social media sites, sharing one's views, ideas, and thoughts is fairly frequent [1].

Twitter is a prominent social media network rapidly developing on the internet. Tweets are brief communications that are generated, updated, and posted on this platform. These tweets can occasionally be used to affect a large number of individuals [2]. Journalists from various media outlets also keep track of noteworthy tweets and retweet them to demonstrate their relevance [3].

The extremists have also used such a platform for spreading radicalization activities to reach out mass public [4], [5]. Sentiment analysis is a scientific method of analyzing these tweets. Sentiment analysis is a method of determining the polarity of language in tweets, which determines whether a tweet is negative or positive [6], [7].

Manual identification is not feasible due to the large volume (Big Data) of unstructured data available on social networking sites. Tweets contain text messages, but it also has some hashtags, which might lead to misinterpretation of data. Fully automatic identification is difficult, being a vast volume of data in an unstructured form. A semi-automated framwork can be used to distinguish radical tweets from normal tweets and human intervention can be taken in case of doubts to further improve the detection accuracy.The suggested research involves employing radical terms to perform emotional analysis on a dataset taken from Twitter. The model is implemented using a variety of machine learning algorithms, each with its own set of benefits and drawbacks. A comparison of all implemented models is conducted, with the most accurate model being chosen.

2. LITERATURE SURVEY

It has recently grown in popularity as a supporter of terrorist organizations such as islamic state of Iraq and Syria (ISIS) [8]. Many scholars have been drawn to social media because of the possibilities of such extreme behavior on an online forum [9]. The main objective is to detect them automatically and take appropriate action. Chatfield *et al,* [10] utilized a machine learning model to scan tweets and find sympathizers of terrorist organizations such as ISIS. The model was created from tweets based on the terms ISIS. All of the tweets that were captured were in English. To develop classes, stylometric characteristics, temporal features, and emotion features were evaluated. Gupta *et al,* [11] presented an automated technique for classifying tweets as radical or non-radical. Machine learning algorithms Support vector machines (SVM), AdaBoost, Random Forest, and Naive Bayes were utilized with various settings. Kalpakis *et al* [12] the features of terrorism-related tweets on Twitter social media for the pre-detection of terrorism activities.

The suspended and non-suspended accounts were both utilized to collect tweet data. Agarwal and Sureka [13] employed a single class SVM and k-nearest neighbors (KNN) algorithm to detect negative emotions in tweet. The KNN classifier has an F-score of 0.6, whereas the SVM classifier has an F-score of 0.83. Rowe and Saif [14] investigates user behavior before, after, and during every ISIS incident. A term-based strategy was utilized to demonstrate radicalization behavior. The suggested method failed to handle lexical ambiguity appropriately. The author has gathered a dataset from social media to demonstrate online radicalization activities in [15]. A psychological and linguistic character is produced by promotion by a certain organization for enlisting individuals in such an action. Using a machine learning method, the author created a model to identify radical behavior [16] dynamically. The tweets dataset is used to train the suggested model. The hashtag 'jihadists' was used to collect the tweets. The fact that features were depending on the dataset was a flaw in their model. The author had set markers for radical behavior in [16]. Tweets based on sham supporters and the status of Iraq were used to create the dataset. They concluded that the model's parameter and the indicators had a substantial link.

There is potential to improve the identification of such behavior in advance by continually monitoring these platforms using powerful machine learning algorithms. Most of the authors have worked on certain popular data gathering phrases. The study of the proposed work was carried out utilizing advanced machine learning methods, which included discovering certain dictionary words that were directly connected to the radicalized words. Different learning algorithms have been used to gain accuracy, and one has been shown to produce the best results.

3. PROPOSED APPROACH

The proposed approach is to detect radical activity on a digital social platform like Twitter. The stated process helps detect a radical activity with the help of the tweets posted on Twitter. The detection of such messages is also performed based on the heuristic approach. In case of doubt in finding negative sentiment for a statement, the decision is taken based on the various parameter of such messages posted earlier. The process helps in discovering the new seed word, which helps find messages corresponding to radicalization. The approach can automatically block tweets when radical activity is confirmed. In case of confusion, an alert is raised for a human intervention to decide based on the heuristic data. The proposed algorithm shows the steps for the detection of radical activity (Algorithm 1). The working of the proposed approach is shown in Figure 1.

3.1. Stages in the proposed approach

The framework for detecting a radical activity as shown in Figure 1 is divided into four significant steps. These steps are data collection and cleaning, training model, testing model, and action performed. The first two steps are to build a model that can efficiently identify the sentiments of the message. These messages mainly have a word that can be used to denote radicalization. Though having such a word is not always the case of radical activity, the model is trained to find its sentiment as positive or negative. The other two steps are to test the real-time tweets and take proper action against them. The move is taken based on the count variable value changed during the testing phase of the approach. The stages of the framework proposed are further discussed in followed sections.

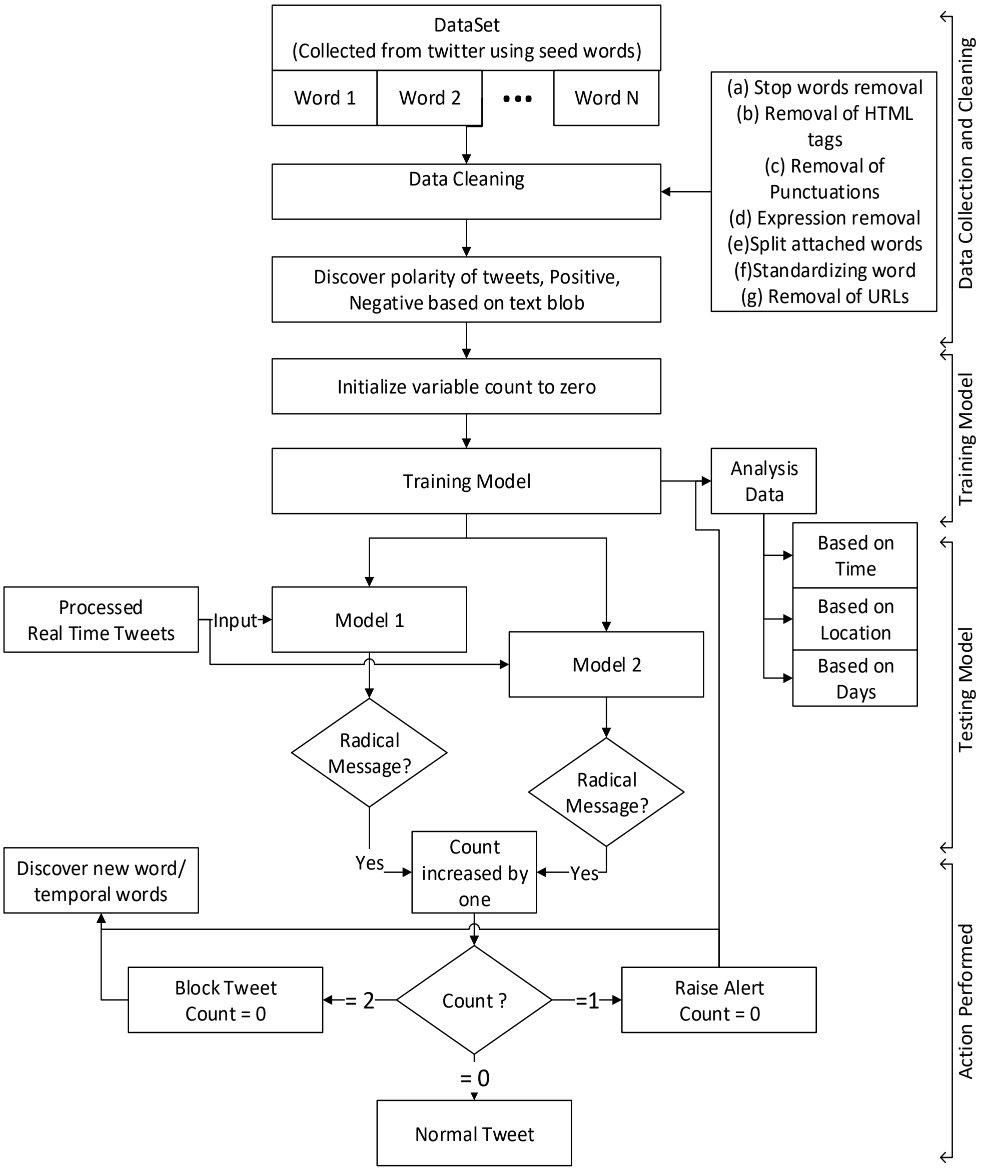
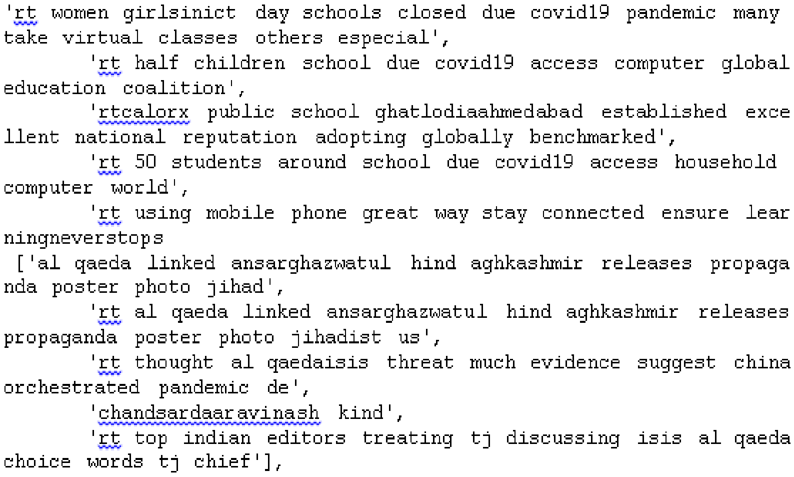


Figure 1. Proposed framework

3.1.1. Data collection and cleaning

The data is collected from one of the largest social, digital platforms, Twitter. The tweets are collected based on the radical activity involving words like jihad, Taliban, etc. The seed words used to collect tweets in the proposed framework are TabligiJamaat, Al Qaeda, and Corona Disease. The three separate datasets are downloaded based on these keywords. The three datasets downloaded have 14071, 3542, and 15825 tweets, respectively. Further, these datasets are combined to make a single dataset and used to train the machine learning model used in the framework. The sample of the collected data is shown in Figure 2.

The data is further processed for cleaning and finding the sentiments or polarity of the tweets [17]. The data cleaning process involves the following steps (i) Stop words removal, (ii) Removal of HTML tags, (iii) Removal of Punctuations, (iv) Expression removal, (v) Split attached words, (vi) Standardizing word and (vii) Removal of URLs.



```
'rt women girlsinict day schools closed due covid19 pandemic many
take virtual classes others especial',
       'rt half children school due covid19 access computer global
education coalition',
       'rtcalorx public school ghatlodiaahmedabad established exce
llent national reputation adopting globally benchmarked',
       'rt 50 students around school due covid19 access household
computer world',
       'rt using mobile phone great way stay connected ensure lear
ningneverstops
 ['al qaeda linked ansarghazwatul hind aghkashmir releases propaga
nda poster photo jihad',
       'rt al qaeda linked ansarghazwatul hind aghkashmir releases
propaganda poster photo jihadist us',
       'rt thought al qaedaisis threat much evidence suggest china
orchestrated pandemic de',
       'chandsardaaravinash kind',
       'rt top indian editors treating tj discussing isis al qaeda
choice words tj chief'],
```

Figure 2. Dataset based on keyword "Tabligi Jamaat", "Al qaeda" and "Corona Disease" (tweets)

Once the data is cleaned, the text blob in python is used to find the polarity of the tweets. The polarity is used to train the model. The negative and positive polarity of datasets is shown in Table 1.

Table 1. Number of positive, negative, and total tweets in the dataset.

Dataset	Positive tweets	Negative tweets	Total tweets
Dataset1	11041	3030	14071
Dataset2	1291	2251	3542
Dataset3	11511	4314	15825
Dataset1 + Dataset2 +Dataset3 (Combined)	23843	9595	33438

3.1.2. Training model

Different combinations of machine learning algorithms have been applied on the three datasets: Countvectorizer & logistic regression, TF-IDF vectorizer & Logistic Regression, and n-gram & Logistic Regression [18]. Since deep learning [19] tries to learn high-level features from data incrementally and can classify text into extremists and non-extremists, deep learning algorithms deep neural network [20], convolutional neural networks (CNN) [21], [22], recurrent neural networks (RNN) [19] have also been applied.

The findings demonstrate that a machine learning system could be useful in detecting radical behavior. The model accuracy of countvectorizer using logistic regression is over 95%. In the case of the deep learning machine model, CNN has the highest accuracy, with a score of more than 93%.

In the proposed approach, the models are trained at two levels. The first model is based on the countvectorizer and logistic regression, showing excellent model accuracy. The countvectorizer and Logistic regression is tested for all the three datasets, and an accuracy of 97% for dataset1, 96% for dataset2, and 97% for the third dataset were observed. Then, the second model in the proposed approach is trained using CNN learning algorithm. CNN model was also tested for all three datasets, and an accuracy of 97% for dataset1, 93% for dataset2, and 93% for dataset3 were observed. Both the models in the proposed approach are finally trained with the combined dataset, i.e., dataset1, dataset2, and dataset3 are combined. It is observed that both models had slight differences in accuracy this difference can be further analyzed to improve the overall accuracy in the proposed approach.

The training phase in the approach also involves the analysis of the dataset based on three parameters, i.e., based on location, based on time, and based on weekdays. This analysis is for the tweets having a negative polarity. The study can help the observer find the time duration, location, and weekdays when most negative polarity tweets are posted.

3.1.3. Testing model

The model is training using the datasets as explained in the above section. The most crucial function in the proposed framework is the testing phase, where the new tweets are tested for their polarity and take the decision based on the results obtained. The automated action taken by the framework is made possible by using a counter; the work of the counter is to count the positive decision taken by both the countvectorizer and logistic regression and CNN model, i.e., the tweets found with negative polarity.

3.1.4. Action performed

The action in the proposed framework is taken based on the value of the count variable used. If both the models find a tweet with a negative polarity, the count value becomes two. It also confirms a tweet related to radicalization; in such cases, the tweet can be automatically blocked. If the value of count is equal to one, then there may be a chance of the tweet related to a radical activity; in such cases, there is a need for human intervention so that it can be further analyzed based on the other parameter of the tweet like location, the time in which tweet is posted, and the day of the week on which it is posted. The Table 2 summarizes the action performed based on the count value.

Table 2. Action based on the count value

Count value	Action performed
2	Autoblock
1	Need a human intervention
0	Normal message

Tweets with count value two will be auto blocked, and new temporal words found can be fetched from such tweets and are added to the dictionary to improvise further analysis. The algorithm proposed for detecting radical activity is presented in Algorithm 1.

Algorithm 1: Proposed algorithm for detecting radical activity

```
Input: Dataset based on seed words SET T= {$t_1$, $t_2$, $t_3$, …., $t_n$}
Output: count value determining radical tweet or not, temporal words
Step 1    for each $t_i$ in SET T
              find polarity based on text blob and store.
Step 2    Set count as 0
Step 3    Train Model 1 and Model 2 using SET T and Analyze tweets based on Time, Location,
          and days.
Step 4    Real time/Test tweets $T_R$ is given as input to Model 1 and Model 2 for testing.
Step 5    while $T_R \neq 0$
              If output of Model1 =radical message
               Count++
              If output of Model2 =radical messag
               Count++
          If count = 2 go to step 7
Step 6    else If count = 1 go to step 8
          else go to step 9
Step 7    Block tweet $T_R$ and assign zero to count. Discover new temporal words
Step 8    Raise Alert for $T_R$. Further investigation required taking help of analysis of data
          in step 3. Assign zero to count. Discover new temporal words.
Step 9    TR Normal tweet no action needed.
```

4. EXPERIMENTAL SETUP

The proposed framework is simulated to test the accuracy of the overall system. The experiments are performed on a laptop with Intel i5 processor 7th generation, 16GB of RAM, and 500 GB SSD hard disk. The python language is used to test and train the models.

5. RESULTS AND DISCUSSION

The dataset of tweets is cleaned, and polarity is assigned. Further, the analysis of negative polarity tweets is done based on location, day of a tweet posted, log of favorites, and time of message post. The analysis is done by visualizing tweets in the form of various bar charts. The chart makes it easy to understand these parameters quickly in the case when the decision is to be made based on human intervention. The sample chart for location-based analysis is shown in Figure 3. Figure 4 visualizes the study based on the day of tweets posted, it can be easily understood from the chart that the frequency of negative polarity tweets is more on Tuesday. Based on the log of favorites the bar chart is shown in Figure 5.

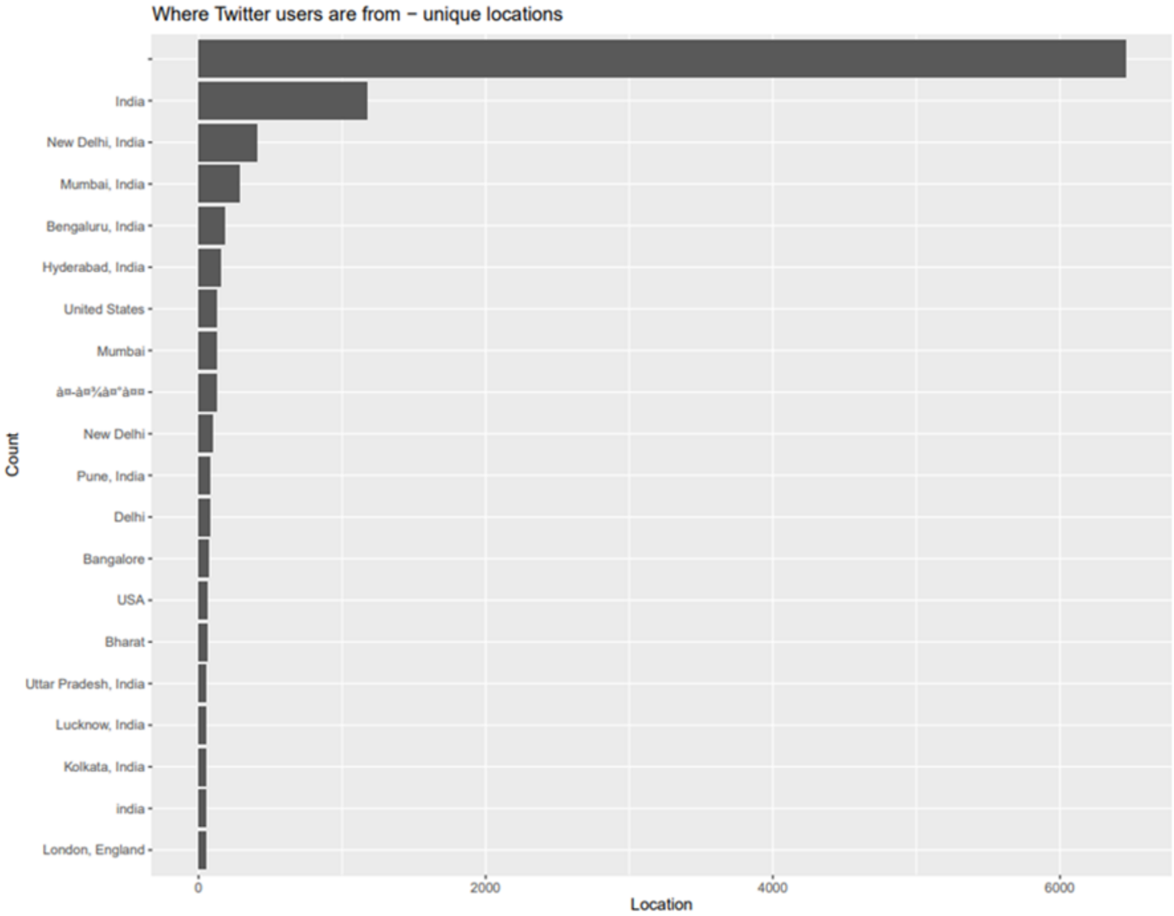
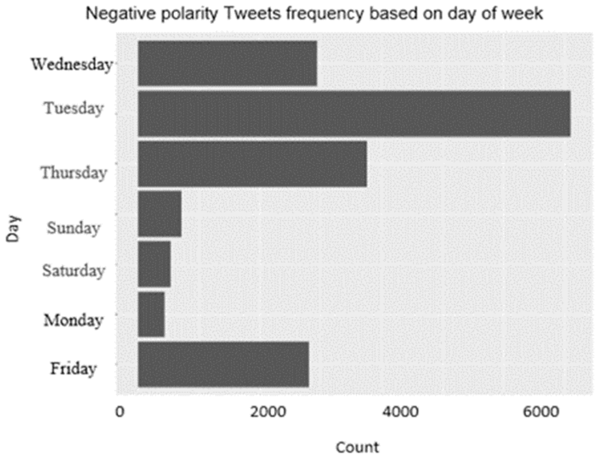


Figure 3. Location based analysis



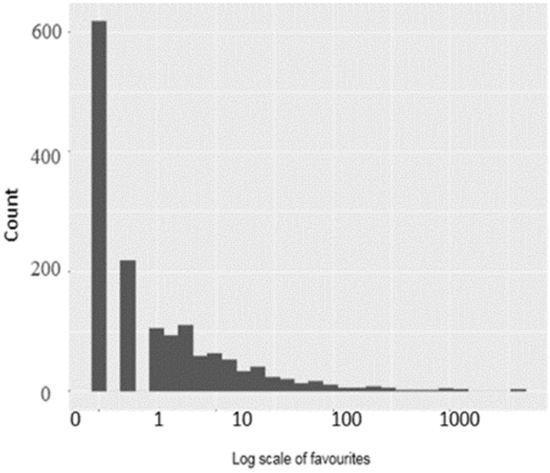


Figure 4. Week day based analysis

Figure 5. Fav based analysis

This analysis is very helpful when human intervention is required to decide to find the polarity of the message. Further, the dataset is used to train two machine learning-based models. One is based on the countvectorizer and logistic regression and the other is CNN based. Both models are tested with a dataset taken as twenty percent from the original dataset. The confusion matrix for the countvectorizer and logistic regression is given in Table 3. The recall, precision, and accuracy for the same are shown in Table 4.

Table 3. Confusion matrix for countervectorizer and logistic regression-based model

	Classification of tweets	
Predicted class	Positive polarity	Negative polarity
Positive polarity	23259	584
Negative polarity	648	8947
Predicted class	Positive polarity	Negative polarity

Table 4. Recall, precision, and accuracy for vountervectorizer and logistic regression-based model

	Positive polarity	Negative polarity
Precision	0.9838946	0.953309
Recall	0.9812607	0.9597104
Accuracy		0.975118129

The confusion matrix of the CNN-based model during the test phase of the framework is given in Table 5. The recall, precision, and accuracy for the same are shown in Table 6. Comparison analysis of both the models based on a confusion matrix is shown in Figure 6. The count value is decided based on the prediction made by the two models. For example, in Table 7, Msg 1 has a prediction of yes by both the models, so the count value is assigned as 2, the Msg 2 has yes prediction by model 1 and no from model 2 so the count value assigned is 1, Msg 3 has No prediction by both the models then count value is assigned as zero and Msg 4 has no prediction from model 1 and yes from model 2 so the count value is assigned as 1. The results obtained by implementing the two model is observed for the count values. The count value for the test case is shown in Table 8.

The Table 7 count value of one is received for 1,291 cases. That means there are 1,291 cases where the prediction made by both the models implemented do not match. In such cases, the concerned tweet needs to be checked by a human to confirm its polarity. On the other hand, there are 8,933 cases where prediction made by both models is matched, and that gives more confirmation about having a message radical. In such a case, the message of the users can be auto blocked by the framework. There are 23,259 cases where both models' prediction messages as normal which needs no action to be performed. The work done by various researchers in this domain is summarized in Table 9. Some of the proposed work has also good accuracy but is such cases the dataset size is too small and may be a condition of overfitting.

Table 5. Confusion matrix for CNN based model

	Classification of tweets	
Predicted class	Positive polarity	Negative polarity
Positive polarity	23,259	584
Negative polarity	648	8,947

Table 6. Recall, precision, and accuracy for CNN based models

	Positive polarity	Negative polarity
Precision	0.9755064	0.9324648
Recall	0.972895	0.9387263
Accuracy	0.963155691	

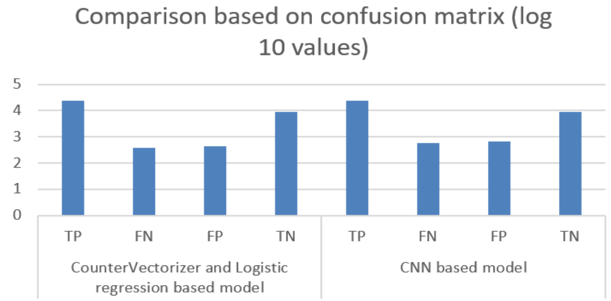


Figure 6. Comparison between two models implemented based on confusion matrix (log 10 values)

The proposed layered approach has outperformed with an accuracy of 96.97% which will be further increased with the help of human intervention. The data size taken is also big compared to many proposed works by various researchers in this domain.

Table 7. Assignment of count value in the framework

Message	Model 1 prediction	Model 2 prediction	Count value
Msg 1	Yes	Yes	2
Msg 2	Yes	No	1
Msg 3	No	No	0
Msg 4	No	Yes	1

Table 8. Count value in proposed framework obtained in the test phase

Count value	Number of tweets
0	23259
1	1291
2	8933

Table 9. A comprative analysis with proposed approach

Refrences	Size of dataset	Techniques	Best accuracy	Verdicts
[23]	346 tweets	Linear SVM, naive bayes, and logistic regression	99.7%	Detected terrorist messages in Arabic, labeling of the dataset into classes was done manually, works on dataset fetched in 2008
[11]	5297 tweets	Naive bayes, random forest, adaboost, SVM	99.02%	Identify radical posts, manual labeling of test data as radical or non-radical was done
[24]	7500 tweets	SVM, naive bayes and adaboost	99.5%	Works with data related to known jihadists
[13]	45.3 million	SVM, KNN	97%	Manual annotation of tweets as positive (promoting hate or radical)
[25]	5000 tweets	Logistic regression, multinomial Naıve Bayesian, support vector machine and decision tree algorithms	98.53%	Labeling of data as propaganda or non-propaganda was done manually by three experts
[15]	Taken three datasets: - 17k tweets related to ISIS from Kaggle. - 8000 random tweets were collected from 10 trendy topics - 1.2k tweets from Kaggle counterpoise to 1st dataset i.e related to ISIS but are non-radical	SVM, KNN, randon forest, NN	80,91 and 100 for different features	Textual, behavioural, and psychological aspects can be used to distinguish radical tweets from normal tweets.
[26]	100 tweets	SVM	83.3%	Detects radical content in tweets in Indonesia language
[27]	25000 tweets	Deep learning (LSTM + CNN)	84%	To categorize tweets as extremist or non-extremist, a tweet classification system is created based on deep learning-based sentiment analysis techniques.
[28]	Taken 5 datasets: 1. 17k tweets pro-ISIS from Kaggle 2. 122k tweets anti-ISIS from Kaggle 3. 2685 tweets ISIS religious texts from Kaggle 4. 9000 tweets new dataset from ISIS related suspended users 5. 7000 random tweets on general topic	Naive bayes, random forest, SVM	87%	The use of religious as well as radical elements is used for detecting radicalization
Proposed Approach	33439 tweets	Countervectorizer and logistic regression-based and CNN	96.91 and more with help of human intervention	Tweets based on radical word as keyword.

6. CONCLUSION

The early detection of radical messages on social platforms can help in preventing any harm in society. There is a need for a robust framework that can help in achieving the said goal. There is also a need for continuous improvement of such a framework as new techniques are always evolving to spread such radical messages. The proposed work is to present a framework to achieve the goal with a better detection rate. The framework has a solution for automaticity detection of such messages by confirming from two machine learning models i.e., countvectorizer & logistic regression and CNN giving better accuracy and provision for autoblocked. It also provides a provision for human intervention for doubt cases and gets better accuracy. The framework is trained and tested with a limited number of samples, in future work the dataset can be increased for further improvement of the accuracy.

REFERENCES

[1] G. B.-Orgaz, J. J. Jung, and D. Camacho, “Social big data: Recent achievements and new challenges,” *Inf. Fusion*, vol. 28, pp. 45–59, 2016, doi: 10.1016/j.inffus.2015.08.005.

[2] R. L.-Cabrera, A. G.-Pardo, and D. Camacho, “Statistical analysis of risk assessment factors and metrics to evaluate radicalisation in Twitter,” *Future Generation Computer Systems*, vol. 93, pp. 971–978, Apr. 2019, doi: 10.1016/j.future.2017.10.046.

[3] S. Valenzuela, S. Puente, and P. M. Flores, “Comparing disaster news on twitter and television: an intermedia agenda setting perspective,” *J. Broadcast. Electron. Media*, vol. 61, no. 4, pp. 615–637, 2017, doi: 10.1080/08838151.2017.1344673.

[4] R. Thompson, “Radicalization and the use of social media,” *J. Strateg. Secur.*, vol. 4, no. 4, pp. 167–190, 2011, doi: 10.5038/1944-0472.4.4.8.

[5] S. Agarwal and A. Sureka, “Applying social media intelligence for predicting and identifying on-line radicalization and civil unrest oriented threats,” pp. 1–18, 2015.

[6] N. N. Alabid and Z. D. Katheeth, “Sentiment analysis of Twitter posts related to the COVID-19 vaccines,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 24, no. 3, p. 1727, Dec. 2021, doi: 10.11591/ijeecs.v24.i3.pp1727-1734.

[7] E. S. Tellez, S. M. Jiménez, M. Graff, D. Moctezuma, O. S. Siordia, and E. A. Villaseñor, “A case study of Spanish text transformations for twitter sentiment analysis,” *Expert System and Application*, vol. 81, pp. 457–471, 2017, doi: 10.1016/j.eswa.2017.03.071.

[8] M. Conway, M. Khawaja, S. Lakhani, J. Reffin, A. Robertson, and D. Weir, “Disrupting daesh: Measuring takedown of online terrorist material and its impacts,” *Stud. Confl. Terror.*, vol. 42, no. 1–2, pp. 141–160, 2019, doi: 10.1080/1057610X.2018.1513984.

[9] P. Wadhwa and M. P. S. Bhatia, “Tracking on-line radicalization using investigative data mining,” 2013. doi: 10.1109/NCC.2013.6488046.

[10] A. T. Chatfield, C. G. Reddick, and U. Brajawidagda, “Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided twitter networks,” *ACM Int. Conf. Proceeding Ser.*, vol. 27-30-May-, pp. 239–249, 2015, doi: 10.1145/2757401.2757408.

[11] P. Gupta, P. Varshney, and M. P. S. Bhatia, “Identifying radical social media posts using machine learning,” 2017.

[12] G. Kalpakis, T. Tsikrika, I. Gialampoukidis, S. Papadopoulos, S. Vrochidis, and I. Kompatsiaris, *Analysis of suspended terrorism-Related content on social media*. 2018. doi: 10.1007/978-3-319-89294-8_11.

[13] S. Agarwal and A. Sureka, *Using KNN and SVM based one-class classifier for detecting online radicalization on twitter*, vol. 8956. 2015. doi: 10.1007/978-3-319-14977-6_47.

[14] M. Rowe and H. Saif, “Mining pro-ISIS radicalisation signals from social media users,” in *Proceedings of the 10th International Conference on Web and Social Media, ICWSM 2016*, 2016, no. Icwsm, pp. 329–338.

[15] M. Nouh, R. C. J. Nurse, and M. Goldsmith, “Understanding the radical mind: Identifying signals to detect extremist content on Twitter,” in *2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019*, 2019, pp. 98–103. doi: 10.1109/ISI.2019.8823548.

[16] R. L.-Cabrera, A. G. Pardo, K. Benouaret, N. Faci, D. Benslimane, and D. Camacho, “Measuring the radicalisation risk in social networks,” *IEEE Access*, vol. 5, no. c, pp. 10892–10900, 2017, doi: 10.1109/ACCESS.2017.2706018.

[17] M. A. Al-Hagery, M. A. Al-assaf, and F. M. Al-kharboush, “Exploration of the best performance method of emotions classification for arabic tweets,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 2, p. 1010, Aug. 2020, doi: 10.11591/ijeecs.v19.i2.pp1010-1020.

[18] S. Sperandei, “Understanding logistic regression analysis,” *Biochem. Medica*, vol. 24, no. 1, pp. 12–18, 2014, doi: 10.11613/BM.2014.003.

[19] N. C. Dang, M. N. M.-García, and F. De la Prieta, “Sentiment analysis based on deep learning: A comparative study,” *Electronics*, vol. 9, no. 3, p. 483, Mar. 2020, doi: 10.3390/electronics9030483.

[20] M. I. Uddin *et al.*, “Prediction of future terrorist activities using deep neural networks,” *Complexity*, vol. 2020, pp. 1–16, Apr. 2020, doi: 10.1155/2020/1373087.

[21] M. Zulqarnain, R. Ghazali, Y. M. M. Hassim, and M. Rehan, “A comparative review on deep learning models for text classification,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 19, no. 1, p. 325, Jul. 2020, doi: 10.11591/ijeecs.v19.i1.pp325-335.

[22] D. A. Jasm, M. M. Hamad, and A. T. H. Alrawi, “Deep image mining for convolution neural network,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 20, no. 1, pp. 347–352, 2020, doi: 10.11591/ijeecs.v20.i1.pp347-352.

[23] N. Al-Harbi and A. Bin Kamsin, “An effective text classifier using machine learning for identifying tweets’ polarity concerning terrorist connotation,” *International Journal of Information Technology and Computer Science,*, vol. 13, no. 5, pp. 19–29, 2021, doi: 10.5815/ijitcs.2021.05.02.

[24] M. Ashcroft, A. Fisher, L. Kaati, E. Omer, and N. Prucha, “Detecting jihadist messages on twitter,” in *Proceedings - 2015 European Intelligence and Security Informatics Conference, EISIC 2015*, 2016, pp. 161–164. doi: 10.1109/EISIC.2015.27.

[25] A. M. U. D. Khanday, Q. R. Khan, and S. T. Rabani, “Identifying propaganda from online social networks during COVID-19 using machine learning techniques,” *International Journal of Information Technology*, vol. 13, no. 1, pp. 115–122, 2021, doi: 10.1007/s41870-020-00550-5.

[26] E. Miranda, M. Aryuni, Y. Fernando, and T. M. Kibtiah, “A study of radicalism contents detection in twitter: Insights from support vector machine technique,” in *Proc. 2020 Int. Conf. Inf. Manag. Technol. ICIMTech 2020*, no. August, pp. 549–554, 2020, doi: 10.1109/ICIMTech50083.2020.9211229.

[27] S. Ahmad, M. Z. Asghar, F. M. Alotaibi, and I. Awan, “Detection and classification of social media-based extremist affiliations using sentiment analysis techniques,” *Human-centric Computing and Information Sciences*, vol. 9, no. 1, 2019, doi: 10.1186/s13673-019-0185-6.

[28] Z. U. Rehman *et al.*, “Understanding the language of ISIS: An empirical approach to detect radical content on twitter using machine learning,” *Computers Materials and. Continua*, vol. 66, no. 2, pp. 1075–1090, 2020, doi: 10.32604/cmc.2020.012770.

BIOGRAPHIES OF AUTHORS

Vandna Batra is a research scholar in Department of Computer Science & Engineering at Manav Rachna International Institute of Research & Studies, Faridabad. She completed her B.Tech degree from UIET MDU, Rohtak in 2009 and M.Tech from Banasthali Vidyapith, Jaipur in 2011. Her background is in the field of computer science with special interests in data mining, machine learning, sentiment analysis and deep learning. She has 10 years of experience in academics. She can be contacted at email: vandna.batra88@gmail.com.

Suresh Kumar is currently working in the Department of Computer Science and Engineering at Manav Rachna International Institute of Research and Studies, Faridabad. He is having more than twenty years of experience. He is a life member of Indian Society of Technical Education (ISTE) and Computer Society India (CSI). He is also a member of IEEE and IACSIT, Singapore. He is working in the area of Artificial Intelligence, Machine Learning, Adhoc Networks. He has published more than seventy research papers in International Journals and Conferences. The HelixSmartLabs a startup incubated at Manav Rachna under his supervision and is registered as a Pvt. Ltd company. He has published two patents and a Technology Transfer in arules package of R Data Analytics Software (included in version 1.5.5 onwards). The package is available at https://cran.r-project.org/package=arules. He can be contacted at email: suresh.fet@mriu.edu.in.