

A Framework for Analyzing Real-Time Tweets to Detect Terrorist Activities

Akshay Karale¹, Pranav Shinde ¹, Pushpak Patil¹, Sanjay Parmar¹, Prof. Niyamat Ujloomwale²

¹Students, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Pune, Maharashtra, India

²Assistant professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Pune, Maharashtra, India

ABSTRACT

Terrorist organizations use different social media as a kind of tool for spreading their views and influence general people to join their terrorist activities. Twitter is one of the the most common and easy way to reach mass people within short time span. We have focused on the development of a system that can automatically detect terrorism-supporting tweets by real-time analyzation. In this system, we have developed a front-end system for real-time viewing of the tweets from twitter that are detected using this system. We also have compared the performance of the two different machine learning classifiers, Support Vector Machine (SVM) and Multinomial Logistic Regression and found that the first one works better than the second one. As our system is highly dependent on the data, for more accuracy we added a re-train module. By using this module wrongly classified tweets can be added to the training dataset and can train the whole system again for better performance. This system will help to ban the terrorist accounts from twitter so that they can't promote terrorism, their views or spread fear among general people in society.

Keywords—Social Media, Twitter, Terrorism, Real- Time Tweets, Machine Learning

Problem Statement: A Framework for Analyzing Real-Time Tweets to Detect Terrorist Activities.

The function of twitter data crawler module is to crawl real-time tweets from Twitter using Twitter Streaming API. The storage module stores the tweets temporarily.

Tweet classification module predicts the category of the tweet. The output module shows the output of the system. The training module builds the classification model which is used to predict the category of each tweet.

I. INTRODUCTION

Internet technology has a lot of benefits. It is also recognized as the fundamental human right. The

Internet has also proven to be highly dynamic means for the communication. One of the biggest technologies of the Internet is our social media technology. Social media comes in many forms

including blogs, photo sharing platforms, forums, business networks, social gaming, chat apps, social networks, etc.

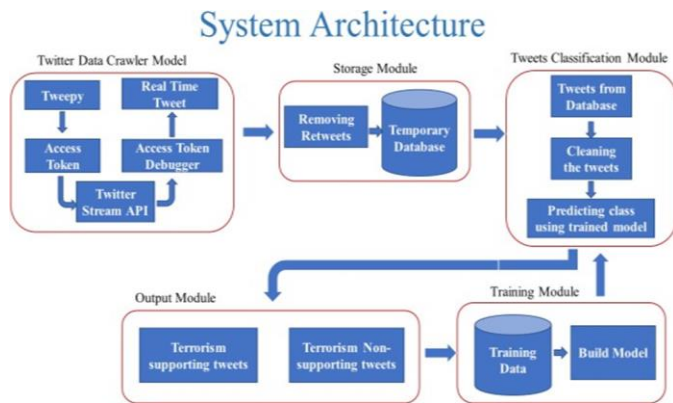


Figure 1: System Architecture

Terrorist organizations which are active on social media to promote their views and spreading propaganda are often leaderless. That makes tackling terrorist propaganda a difficult task. They used social media to recruit new members from all over the world. They also spread fear among the people of different countries by using Twitter and other social media platform. Among all social media platforms, Twitter is more public. When a tweet is posted on Twitter it can reach more people than other social media platforms. So, Twitter is the first choice of terrorist organizations to spread their views and propaganda. In the last two years, Twitter has suspended around million twitter account for spreading terrorism. Their approach of suspending an account is if someone reports any account, then they suspend the account if the account really promotes terrorism. It is a very time-consuming process. The motivation behind this project is to crawl tweets from the twitter in real-time and then analyze the tweets to determine the support of terrorism. This system will significantly improve the time to review the tweets supporting terrorism.

A. The main features:

1. Countering terrorism and protecting human rights as mutually reinforcing goals.
1. Countering violent extremism and radicalization that lead to terrorism.
2. The development of co-operative, community-oriented approaches to counter terrorism.
3. Community policing as part of a comprehensive, human rights-compliant strategy to prevent terrorism.

II. LITERATURE SURVEY

Rupali Patil al. [1] The procedure of sentiment analysis and its visualization is explained in detail concerning the topic Article 370. Sentiment analysis and opinion mining require detailed knowledge of how twitter and its python client Tweepy works to obtain the results. Python libraries like matplotlib and pandas are also used for simpler analysis and visualization of the tweets acquired. As a whole, from this paper it can be concluded that Pakistan is comparatively more concerned about the impact on its trade and has been somewhat more cynical when it comes to the sentiments of its Twitter users whereas India, on the other hand, is more concerned about increase in terrorism with a slightly positive attitude towards the revocation from the country's Twitter users. Therefore, the plots presented here accurately displays users' opinions during such a historical change in a Country's policy.

Babak Yadraniaghdam [2] we have proposed a framework for real-time analysis of Twitter data. This framework is designed to collect, filter, and analyze streams of data and gives us an insight to what is popular during a specific time and condition. The framework consists of three main steps; data ingestion, stream processing, and data visualization. Data ingestion is performed by Kafka, a powerful message brokering system to import tweets, and to distribute it

based on Topics that it defines, and to make it available over consumers' nodes to be processed by analytical tools. Apache Spark is used to access these consumers directly and analyze data by Spark Streaming. This allows not only general processing tasks but more sophisticated and high-level data analytics and machine learning algorithms.

M. Ashcroft et al. [3] made an attempt to detect jihadist messages from Twitter. They used sentiment analysis to detect if a message supports ISIS or not. They used some keyword to extract tweets from the Twitter feed. The advantage of this work is it uses three different features such as Time-based features, Sentiment based features and Stylometric features to detect jihadist text. They got almost 90% accuracy using these features. One of the limitations of this study is they didn't use any real-time validation of their classification algorithm. Also, they didn't build any tools to detect jihadist text automatically.

Priyanka Harjule al. [4] Various techniques for both lexicon-based and machine learning based, have been applied in this project and the results are compared. It has been observed that for a totally new data/text machine learning based models trained over a related data are much more accurate than the classification based on standard dictionaries. This is because of the fact that the text that's being observed i.e the tweets are highly informal and do not use the standard grammar rules or the spelling and thus the data here is highly unstructured. The comparison results can be clearly observed among different machine learning algorithms also. As of now, among the algorithms used, RNN is observed to have the highest accuracy.

Walid M. et al. [5] studied to predict future support or opposition for ISIS from tweets. In this study, the authors used Twitter data to study the ISIS support of users. They used the bag of words model as feature vector which included individual terms, user mentions and hashtags. They used SVM with a linear kernel to train a classifier to predict the support or opposition of ISIS. They obtained about 87% accuracy

using the SVM classifier model. One limitation of their approach is, they didn't consider real-time validation of their method.

S. Azrina et al. [6] studied to detect terrorism from text using sentiment analysis. The advantage of their study is they did a comparative analysis on several techniques to detect terrorism from the text. They did a comparative analysis of Neural Network, Support Vector Machine, Sentiment Analysis with Naive Bayes and Lexicon based approach. Then they finally adopted and improved Naive Bayes method for their research. One of the limitations of this study is it uses user behavioral analysis to improve the accuracy of Naive Bayes algorithm as it shows medium level accuracy compared to other algorithms. But it is not always possible to analyse a user's behavior if he doesn't have that much of tweet history on Terrorism.

Lisa K. [7] studied to classify tweeps and tweets as being multipliers of jihadism. They used Machine Learning to build a classifier that can analyze a tweet to find multipliers of jihadism. They used AdaBoost classifier to train a model. They analyzed both Arabic and English tweets. They obtained about 84% accuracy for Arabic tweets and 98% accuracy for English tweets. They didn't test their model in a real-time environment.

Pooja W. et al. [8] studied to classify radical tweets in the categories such as Media, War terrorism, Extremism, Operations, Jihad, Country and Al-Qaeda. They built a dictionary to classify the tweets into different categories. They built the dictionary by looking at tweets containing hashtags like Al-Qaeda, Jihad, Terrorism, and Extremism and by collecting relevant words for their purpose. They built a process based on the presence of the word in the dictionary. Their process obtained about 90% accuracy. Their study is proof that keywords can be used successfully in classifying tweets.

Lee S. et al. [9] compared four text mining methods: Latent Semantic Analysis (LSA), Probabilistic

Latent Semantic Analysis (PLSA), Latent Dirichlet Allocation (LDA), and Correlated Topic Model (CTM) using topic model and spam filtering. They concluded that PLSA shows the highest performance and next to LDA, CTM, and LSA in order. One of the limitations of this study is they only considered statistical approach and didn't extend their study to syntactical and morphological approach. A work on topic discovery based on text mining techniques was presented by Pons P. et al. [10]. They proposed a hierarchical clustering algorithm that combines partitioned and agglomerative approaches to produce topic hierarchies. They considered document place, time reference, and textual contents. This resulted in less time complexity while detecting a new topic. The accuracy of their proposed method is not satisfactory

III. SYSTEM ARCHITECTURE AND DESIGN

The system architecture of Twitter Terrorism Detection Framework comprises five basic modules:

- 1) Twitter data crawler module
- 2) Storage module,
- 3) tweet classification module
- 4) Output module,
- 5) Training module.

A. Crawling Data from Twitter

We have crawled real-time tweets from the twitter by using twitter streaming API. To do this we have provided four keys that we have collected from the Twitter developer website. The 4 keys are:

1. Access Token
2. Access Secret Key
3. Consumer Token
4. ConsumerSecret Key.

These 4 key are needed to get access to Twitter API. Using these 4 key we can set up a twitter real listener.

This listener will allow us to collect real-time tweets from Twitter. As we have used python to build our framework, we have used a python library that helped us getting access to the Twitter streaming API. We have used a python library 'Tweepy' API. Algorithm 1 illustrates the Twitter. While collecting real-time tweets we have made sure to handle all kinds of error that would break the connection the connection breaks, the crawler module will stop working. That's why we have checked for several exceptions such database exception, limit exceeded exception etc

Algorithm 1: Crawl Real-Time Tweets

Input: Developer Access keys

Require: Real-Time tweets streaming from twitter

1. Begin
2. Call Twitter API
3. Call Twitter Streaming API
4. SetaccessTkn = ""
5. Set accessTknSec = ""
6. SetconsumerKey = ""
7. SetconsumerSec = ""
8. tweets = STREAM-LISTENER(accessKeys)
9. Create a table named all_tweets having the field username, tweet, tweet_id, type
10. if tweets != null then
11. if tweets['retweet'] = False then
12. Insert tweets['text'] , tweets['username'] and tweets['tweet_id'] into the database
13. End

B. Pre-Processing Crawled Data

After data is crawled from the twitter the tweets are in raw form using algorithm 2. We can't use these tweets to classify or train. So, we have cleaned the tweet before using n classification or training. To handle the special component of a tweet, we have done the following pre- processing tasks.

1. URL is removed
2. Any user mention is removed
3. Hash (#) from the hashtag is removed
4. Contracted words are converted to their long form
5. Tokenized the tweet

Algorithm 2: Cleaning raw tweets.

Input: raw tweets

Require: clean the raw tweets

1. Begin
2. remove url from raw tweets
3. remove hash (#) symbol of hashtags from raw tweets
4. remove user mentions form raw tweets
5. remove retweet symbol RT from raw tweets
6. convert the raw tweets into lowercase form
7. search for contracted from in tweets
8. if contracted form found then
9. replace it with long form
10. search for stop words in tweets
11. if stop words found then
12. remove the stop words
13. tokenize the tweets
14. apply stemming on the tweets
15. End

C. Building Model and Generating Output

To predict the class of the tweet we needed a mathematical model which can classify the tweets based on their features. We have used two classification algorithm. These are SVM (Support Vector Machine) and Logistic Regression. Using our training dataset we built a model that can classify the tweets accurately. By using the model that we have built in the previous steps, we can classify a tweet. The classification result is 0 or 1 or 2. According to this result, we can show the type of tweets. Algorithm 3 is used to classify real-time tweets.

Algorithm 3: Classification of real-time tweets

Inputs: model file

Require: Classification of the tweets

1. Begin
2. classifier = load(model)
3. for each tweets in the all_tweets table in the database
 - do
 4. clean the tweets
 5. type = classifier.predict(clean_tweets)
 6. if type = 0 then
 7. result = "Terrorism Supporting"
 8. elseif type = 1 then
 9. result = "Terrorism Non-Supporting"
 10. elseif type = 2 then
 11. result = "Random"
 12. show the result
 13. End

IV. IMPLEMENTATION DETAILS

In this section, we have provided the implementation of our proposed system in details. In order to start crawling from Twitter, we to the twitter developer portal to get access tokens and consumer secrets. An Application Programming Interface (API) is a standardized system of programming instructions that allows web platforms to access and share information from one another. Like many other web tools, almost every social network has released its API for researchers and other web developers to use. We have used Twitter Streaming API to crawl data from Twitter. API (Application Platform Interface) will allow us to authenticate acc by the authority of the social network. If the API keys are valid, the crawler program can access the Twitter API and crawl tweets from the twitter. If the API keys are not valid then the API will send an API access error.

To get the API access keys first we have opened an account on the Twitter developer website. In the website, we have created an app named

"TwitterCrawlerFramework". This provided us with the access tokens.

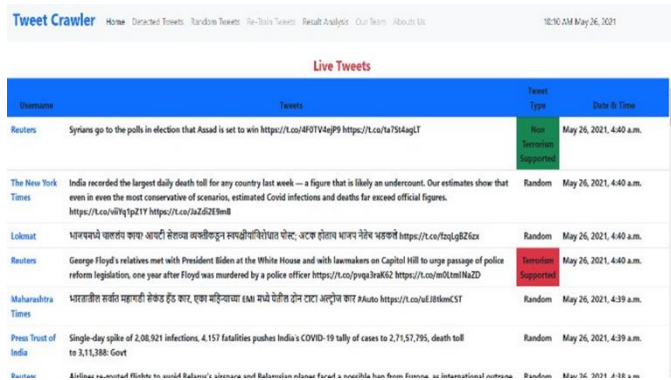


Figure 2: Home.

Fig. 2 shows the screen where live tweets are shown. Each tweet which is random, terrorism supported or terrorism not shown here with respective level. Random tweets are shown as normal box while the terrorism supported are shown using the red color box and non- terrorism supporting tweets are shown using green color box.



Figure 3: Detected Tweets.

Fig. 3 shows the screen of the detected terrorism supported tweets.

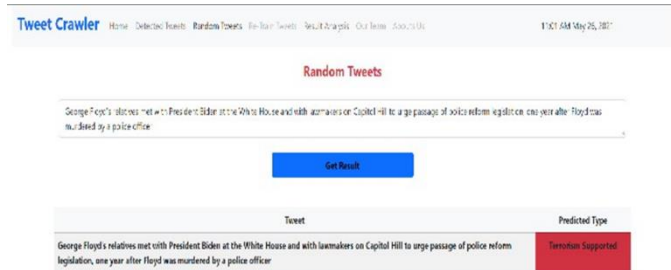


Figure 4: Random Tweets Classification.

Fig. 4 shows the Random Tweets Classification . The Random Tweets tab gives a helping feature to the user

to manual enter any random tweet and check it's nature i.e whether it's terrorism supported tweet, non-terrorism supported tweet or it's just a normal random tweet.

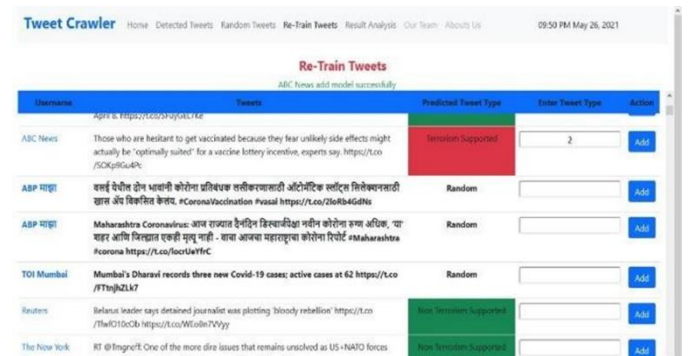


Figure 5: Re-Train Tweet.

Fig. 5 shows the Re-Train Tweets. If model predicts wrong output then we can again re-train tweet model using re-train function.

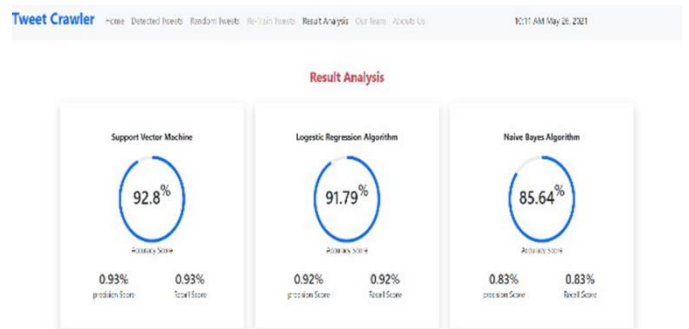


Figure 6: Result Analysis.

Fig. 6 shows the Result Analysis Tab. The Result Analysis tab show the efficiency of the system. It shows the precision of Support Vector Machine (SVM), Logistic Regression Algorithm and the Naïve Bayes Algorithm.

V. IMPLEMENTATION RESULT AND ANALYSIS

A. Experimental setup

The developed Twitter Terrorism Detection System has been implemented on a machine having the windows 10, 3.40 Core i5-8250U processor with 8GB

RAM. The detection system has been developed with Python and the user interface is developed with Bootstrap CSS, HTML, JavaScript, jQuery and AJAX. We have also used postgres database to store our data and used django framework to populate the user interface with data from database. For coding , we have used Virtual Studio Code software for coding .

B. Performance Evaluation

a) Crawling Mechanism of Dataset

We crawled tweets from Twitter to make our dataset. We have collected tweets to make our dataset in three different ways. These are:

1. Collected random real-time tweets.
2. Collected tweets by using some keywords related to Terrorism.
3. Collected tweets from some known terrorist twitter Account.

After collecting all the tweets we manually analyzed the tweets and divided them into three different classes and finally put them in a CSV file. In the CSV file, there are two columns one is tweets and another type. Tweets column contains the tweets and the type column contains the type of that tweet in numeric form. We have used the numeric form to represent the type of tweet because the classifier algorithm needs the type to be in the numeric form so that it can predict the outcome of a tweet.

TABLE 1. Summary of collection method

Collection Type	No. of Tweets
Randomly from Real-Time Tweet Stream	21482
Using Terrorism-Related Hashtags	20557
Crawling Terrorist	18105

Profiles	
Total=	60144

In Table 1, the number of tweets collected using different collection methods are shown. These tweets are further analysed and categorized into different classes to make our dataset.

TABLE 2. Summary of the Training dataset

Types of Tweets	Numerical value in Dataset	No. of Tweets
Terrorism Supporting	0	9397
Terrorism Non-Supporting	1	21650
Random	2	29097
	Total=	60144

In Table 2, a number of tweets of different types in our training dataset are given. Using this dataset we have trained our classifier to build a model

VI. CONCLUSION

In this Paper, We have discussed Twitter Terrorism Detection framework to detect tweets that support terrorism from real-time tweets stream. Our framework collects real time tweets by using twitter streaming API and analyses every tweet. It can categorize the tweet into three different classes and based on the category of the tweet, it is stored and shown in the different screen of our web application. We have also created a re-train module which will be used to retrain our model so that it can perform more accurately. Our framework has a user- friendly interface. The overall accuracy of our proposed system is 92% and 91.7% for SMV and Regression respectively.

VII. FUTURE SCOPE

In our study, the framework is limited to collect and analyze tweets that are written in English. So, further research can be done to extend this study to support other languages. The accuracy of the proposed system can be enhanced by analyzing shared images or videos on Twitter by users. Our framework will falsely detect sarcastic text as a terrorism-supporting tweet. So, further research can include detecting sarcastic tweets which actually doesn't support terrorism. The System should also provide access to the users if the user doesn't have the access to the twitter API.

VIII. REFERENCES

- [1]. Twitter Data Visualization and Sentiment Analysis of Article 370 ,2019.Author: Rupali Patil , Nishant Gada ,Krisha Gala
- [2]. Developing a Real-Time Data Analytics Framework for Twitter Streaming Data,2017.Author: Babak Yadranjiaghdam , Seyedfaraz Yasrobi , Nasseh Tabrizi
- [3]. M. Ashcroft, A. Fisher, L. Kaati, E. Omer, and N. Prucha, "Detecting jihadist messages on twitter," in Intelligence and Security Informatics Conference (EISIC) European, Sept 2015, pp. 161–164.
- [4]. Text Classification on Twitter Data,2020.Author:Priyanka Harjule , Astha Gurjar , Harshita Seth , Priya Thakur
- [5]. M. Walid, D. Kareem and W. Ingmar, “ #FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support,” in Monday, 2015.
- [6]. S. A. Azizan and I.A. Aziz, "Terrorism Detection Based on Sentiment Analysis Using Machine Learning," Engineering and Applied Sciences 2017.
- [7]. K. Lisa, "Detecting multipliers of jihadism on twitter." International Conference on Data Mining Workshop (ICDMW) IEEE, 2015.
- [8]. P.Wadhwaand M. P. S. Bhatia, “ Case study in Computing Achievements and Trends, Radical Messages onTwitter Using Security Associations 273. 2014.
- [9]. P.P. Aurora, R.B. Llavori, and based on text mining techniques." &management, vol-43, no-3, pp.752
- [10].M. Trupthi, S. Pabboju and G. Narasimha, “Sentiment Analysis on Twitter Using Streaming API”, Computing Conference, 2017.
- [11].S. Lee, J. Baker, J. Song and comparison of four text mining methods”. In International Conference on 2010.
- [12]. Tweepy, Streaming With Tweepy [online] Tweepy.readthedocs.io. Available at: http://tweepy.readthedocs.io/en/v3.5.0/streaming_how_to.html 2017