Advances and Applications in Mathematical Sciences
Volume 21, Issue 12, October 2022, Pages 7003-7016

COMMUNALIZATION OF SOCIAL MEDIA: URL DETECTION TECHNIQUE

DIVYANG PANDEY and ANAND PRAKASH SHUKLA

MTech Scholar
KIET Group of Institution
Ghaziabad-Meerut Road NH-58
Ghaziabad, Uttar Pradesh, 201001, India
E-mail: divipol30@gmail.com

Additional HOD and Professor
KIET Group of Institution
Ghaziabad-Meerut Road NH-58
Ghaziabad, Uttar Pradesh, 201001, India
E-mail: ap.shukla@kiet.edu

Abstract

Any pandemic or major events have the capacity to change the world perspective and also can destroy the social fabric by misinformation of hatred spreading. Every major crisis not only brought destruction and public data or opinions about the event but also their thoughts. Most of the thoughts also includes communal attacks on other community or country. In this situation authorities need to identify the perpetrators who generally belongs to big media houses or politically connected. For this we build a classifier which can differentiate between normal and abnormal message and also detects URL for better identification. This classifier can be very helpful in such major events.

1. Introduction

Online social media has become an open place for anyone to make derogatory comments and spreading misinformation. Specially gaining popularity of Twitter, anyone can post their feeling become a place to spread fake messages and target a particular section. Sometimes handling such situations left authorities with no options but to shut down the internet

2020 Mathematics Subject Classification: 68M11.
Keywords: Communal, Post, social media, Data Mining.
Received September 12, 2021; Accepted November 13, 2021

services to stop spreading of misinformation. But with increasing digital world internet shutdown also halt important works. Such examples can be seen recently in Srilanka where government had to shut down internet communication in order to protect communal classes and also in India where recently government had to shut down internet multiple times in order to restrict spreading of misinformation. This paper enables authorities to filter out such posts during any disaster events without going through such hefty process of shutting down the internet. The author further elaborates the existing system by introducing malicious URL detection procedure.

The overview of the paper is organized as follows:

(1) A brief of related works and literature review is done. In next section,

(2) In next section, implementation of the work process is mentioned and data details.

(3) In third section, results are mentioned and explained in detail. In last section the paper is concluded.

2. Literature Review

The overall loss of the energy in the infected populace is one of the catastrophic outcomes. Hatred and disinformation also propagate to the impacted area, which could lead to serious worsening of the law-and-order system, taking advantage of such a vulnerable situation [9]. The general loss of energy among the afflicted populace is one of the troubling tragedies dropping out [10]. Hate and disinformation also circulate in the area affected, which can lead to serious worsening of the environment in law and order, taking advantage of this vulnerable situation [24].

Online social networks (OSM) such as Twitter and Facebook are currently severely infected with derogatory or violent posts, such as spam, cyber bullying, hate speech, and so on. In recent years a lot of research has been done to identify various forms of offensive material automatically [17]. Hate speech can be categorized into several groups in which individuals target different characteristics of the target group, such as faith, age, race, gender, etc. Hatred travels across social media, where Facebook is progressively a powerful tool, is significantly improved. Public tweets directed at certain

religious or racial groups are particularly harmful and potentially dangerous[18]. Microblogging locales like Twitter have become significant wellsprings of ongoing data during fiasco occasions [11]. A lot of important situational data is accessible in these destinations; nonetheless, this data is submerged among a huge number of tweets, generally containing assumptions and assessment of the majority, that are posted during such occasions [2]. In social media stages, abhor discourse can be an explanation of "digital clash" which can influence social life in both of individual-level and nation level [25]. Scornful and adversarial content proliferated by means of social systems can possibly cause mischief and enduring on a person premise and lead to social strain and confusion past the internet [14]. In any case, social systems can't control all the substance that clients post. Therefore, there is an interest for programmed identification of abhor discourse [3].

At the point when a catastrophe happens, all people react to it in their own particular manners [12]. The correspondence needs during the emergency reaction organize are uncommon in both sum and structures. Synchronous correspondence, for example, telephone discussion, is continuously intensely utilized among crisis reaction groups and between individuals in the hazardous situation and those outside the region [5]. In the interim, off beat correspondence by means of the web is similarly significant. For instance, individuals who are in the region of an emergency can give first hand circumstance updates to the general population by means of the web, and individuals who can't arrive at colleagues in the influenced zone can call for help on the web [1]. Social systems administration is as of now a backbone of regular day to day existence, and its utilization and significance inside research and instruction is as of now demonstrated in word related treatment [16]. Twitter and other microblogging administrations have become in superfluous wellsprings of data in the present web [26]. Understanding the primary factors that make certain bits of information spread rapidly in these stages can be definitive for the investigation of assessment development and numerous other conclusion mining errands [19].

Microblogging is one type of social media that is being immediately embraced. It offers approaches to recover, produce and spread data; the nature of that sharing has a lifecycle of data generation and utilization that is quick what's more, tedious [6]. Progressively, microblogging is being

considered as a method for crisis correspondences as a result of its developing universality, interchanges rate, what's more, cross-stage openness. This medium is likewise observed as a spot for "gathering" data during an emergency occasion to figure out what's going on the ground [8].

Social media reach is across the board with the end goal that data ventures exceptionally quick with no topographical fringe or requirements. The period of Internet has changed the way individuals express their perspectives and feelings. It is currently basically done through social media [13]. These days, a great many individuals are utilizing social system locales like Twitter, Facebook, Google Plus, and so on, to express one's feelings, sentiment and offer perspectives about their day by day lives. Be that as it may, they may not know about the issues and conflicts stimulating among various class of individuals in the society [7].

3. Implementation

In this section, the implementation details are mentioned. The software is implemented on java. In the software, the classifier used is support vector machine. In support vector machine, the vectors of each tweet set are obtained and a Euclidean distance is calculated. Then after training, for the test dataset same sequence is obtained. The minimum matching distance is then used for characterizing between communal and non-communal posts. The training data set is taken from the following link: http://www.cnergres.iitkgp.ac.in/blog/2017/11/18/disaster/.

The test example keywords used are - Muslims, Christians, attack, terrorists, and so on as features. The training data set consists of tweets for example- 0, satishgahmari - Earlier today: relief materials and equipment for earthquake assistance being loaded on aircraft bound for... http://t.co/ZvUeRNLcDk. Also, the tests are performed on tweets for example- I hate Muslims.

In the existing communal post detection system, author has given concept to detect normal or communal tweets but not given any concept to detect malicious users and most of the time malicious users are only responsible to spread communal tweets and here new proposed concept is added which is the concept to detect such malicious users. In almost all tweets' users give

URL link to post videos or any other greeting text. URLS will contain a long text but tweeter can accept only 140 characters and to avoid such problem twitter has introduced SHORTEN URL concept where big URL will be map to shorten URL. Shorten URL can give in tweets and when user click on such URL then twitter automatically obtained big URL mapping from Shorten URL.

Example

Stack over flow shorten URL

Short URL = http://s.tk/

When one paste above short URL in browser and then press enter key then automatically that URL changes to big URL as below one

Big URL = https://stackexchange.com/

Malicious users may take advantage of such technique to spread tweets with such Shorten URL which will redirect user to malicious websites upon click by user on such URLS. Malicious Web site then steals information from user system and sent to malicious users.

Always malicious users will have only one or few websites and they create lakhs of shorten URL which map to such few malicious web sites. Upon user click on such URLs users may be redirected to such web sites.

To detect such malicious link twitter is already using black listed URLS but it is not sufficient to detect different shorten URLS. To overcome from this problem, one can analyze all URLS to check whether they are redirecting to same website or not. If multiple Shorten URLS redirecting users to same website, then one can make such URL as malicious and don't require maintaining any black listed URL database. This is proposed concept feature methodology of the system. In figure 1, user case diagram is shown. Figure 2 is flowchart of proposed algorithm.

Below is the code to get expand URL from short URL

public static String expand URL(String shortened URL) throws IOException { URL url = new URL(shortenedUrl); // open connection HttpURLConnection httpURLConnection = (HttpURLConnection)url.openConnection(Proxy.NO_PROXY); // stop following browser redirect

```
httpURLConnection.setInstanceFollowRedirects(false);  // extract location header containing the actual destination URl String expandedURL=httpURLConnection.getHeaderField("Location");

 httpURLConnection.disconnect(); “

   return expandedURL;

}
```

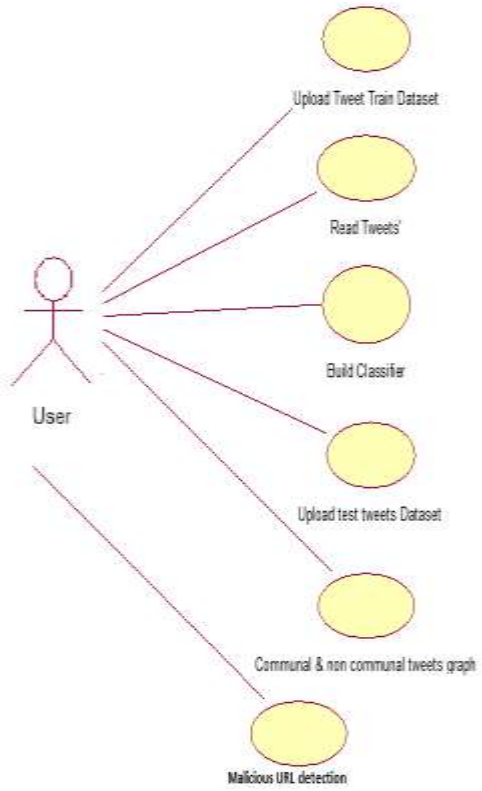

Figure 1. User case Diagram of Proposed System.

In figure 1, it is seen that the user case diagram is mentioned. It consists of the following steps for the processing of the software-upload dataset, read dataset, build the classifier, upload test tweets, communal and non-communal graphs, malicious detection. Out of these all processes can be executed by the user in sequence.

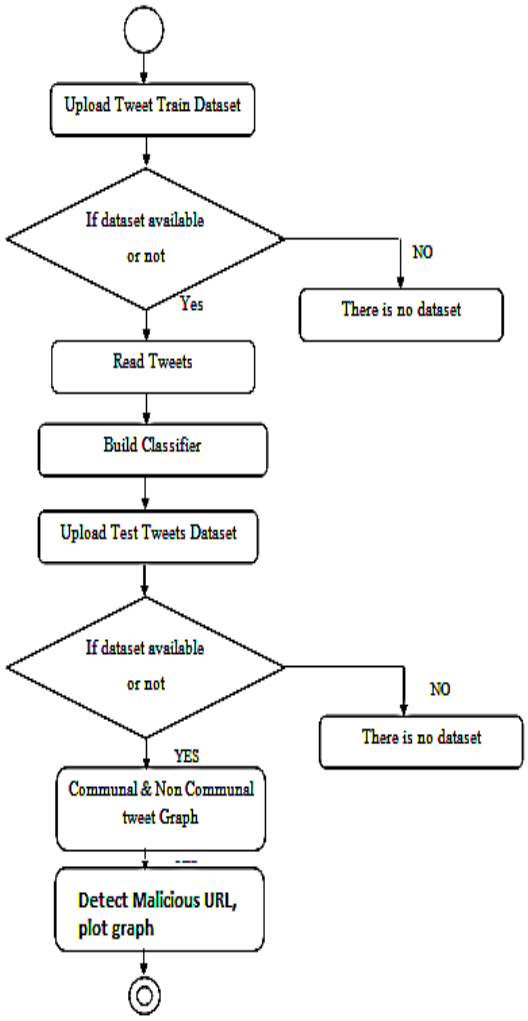

Figure 2. Activity Flowchart of implementation.

In figure 2, the flowchart is mentioned, all the steps are mentioned in the step-by-step guide of the flowchart sequencing as per terms mentioned in the user case diagram for the sequencing of the data. Here, no step can be skipped for proper functioning of the software to obtain correct results and high accuracies.

4. Results

In this section the results are mentioned as obtained from the above

implementation: In table 1, the test results are shown on the basis of communal and non-communal posts.

Table 1. Test Results of Classification.

Tweet Text	Classified Tweet	Classification Result
Muslim terrorist behind all attack	56,gkrajvanshi - Huh, its Muslim behind California attack	Communal
kill all Radical Muslims	39,imJr19 - Radical Muslims want to behead u, moderate Muslims want radical Muslims to behead your n liberals want to save them.	Communal
missionaries who are looting from whatever's left after earthquake	10,arun735 - Fuck these missionaries who are scavenging from whatever's left after the #NepalEarthquake Have some shame and humanity.	Communal
U.S. Sending Disaster Response Team, $1 Million in Aid to Nepal	0,_Sourabh_Singh - RT Times Now “US sending disaster response team and $1	Noncommunal

	million aid to Nepal after earthquake"	
Earlier today: relief materials and equipment for earthquake assistance being loaded on aircraft.	0,satishgahmari - Earlier today: relief materials and equipment for earthquake assistance being loaded on aircraft bound for... http://t.co/ZvUeRNLcDk	Noncommunal
I hate Muslims	39,imJr19 - Radical Muslims want to behead u, moderate Muslims want radical Muslims to behead your n liberals want to save them.	Communal

Table 1 has shown the tweet classification of tweets and it is seen that it is classifying the results correctly, for example, I hate Muslims is correctly classified as a communal post. In figure 3, the chart of communal and non-communal tweets is shown. In this chart it is seen that communal post detected are less than that of non – communal post according to the training dataset.

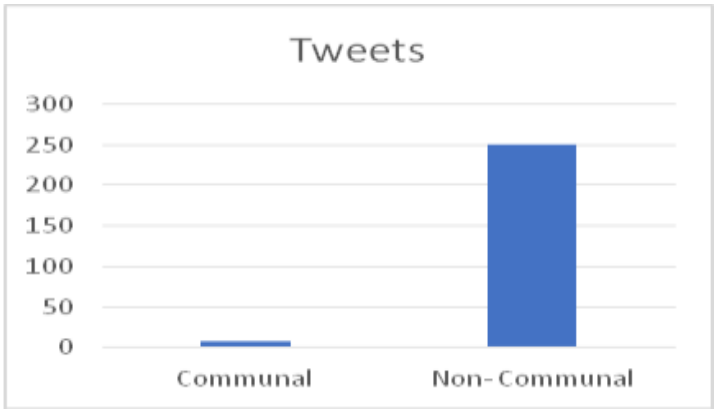

Figure 3. Communal and Non-communal tweets graph.

In table shown below as table 2, the implementation modules are mentioned which can only be performed in sequence starting from the first according to the flow chart definitions. The processes involved are namely- Upload train dataset, in this the train data set is uploaded. Read train dataset is performed to view the trained tweets. Build classifier process involves the execution of the classifier used. The uploading of test dataset is done to obtain the final outputs. Now user can build communal and non-communal charts, and malicious URL is detected next as per implementation and then represented on a chart.

Table 2. Proposed work implementation.

Modules Information
Upload Train Dataset
Read Train Dataset
Build Classifier
Upload Test Dataset
Communal and Non-Communal Tweet Graph
Malicious URL Detection
Malicious URL Chart

Table 2 has shown the malicious URL detection algorithm is also added with chart.

Table 3. Result of Malicious URL detection.

Tweet Text	Short URL	Expand URL	URL Count
1,Prashanth_Cruis - RT @PrashanthCru_PC: Gain followers RT Bisham Bazaar Ambulance service: +977 4244121 http://t.co/vYmnRnSThG	http://t.co/vYmnRnSThG	https://t.co/vYmnRnSThG	7
Patients have been put on parking lot. http://t.co/sR3JuvidaX	http://t.co/sR3JuvidaX	https://t.co/sR3JuvidaX	4
0,EarthquakeLast - ML 2.9 OFFSHORE VALPARAISO, CHILE http://t.co/69xW9srvsm #Earthquake #Quake http://t.co/USGFXXf7GH	http://t.co/69xW9srvsm	https://t.co/69xW9srvsm	6

In table 3, the detection of malicious URL is shown. It shows the tweet, short URL, expanded URL and its counts. In figure 4, chart is represented for malicious URL detection. Its shows that significant number of malicious URL are detected in the training dataset while only a few were detected as communal.

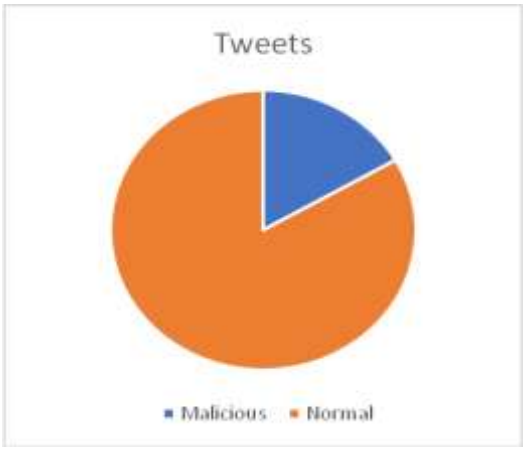

Figure 4. Normal and malicious URL chart.

Conclusion

This paper is the main endeavor toward describing communal tweets posted during the calamity situation and investigating the clients engaged with posting such tweets with malignant URL identification. Here, proposed an occasion autonomous classifier that can be utilized to sift through communal tweets early. Clients associated with starting and advancing communal substance structure a solid social bond among themselves. Furthermore, the vast majority of the clients blow up all of a sudden because of such sort of occasions and express their hates to explicit strict networks engaged with the occasion. see that, during a fiasco, a few clients additionally post against communal substance requesting that individuals quit spreading communal posts, and it is important to counter the potential antagonistic impacts of communal tweets have proposed an occasion autonomous classifier to distinguish such enemy of communal tweets. Be that as it may, have discovered such enemy of communal tweets are retweeted significantly less contrasted with communal tweets and they are likewise not many in number contrasted with communal tweets. At long last, proposed an ongoing framework where tweets are arranged as communal or non-communal and malignant URL are likewise identified for security reason. Furthermore, this classifier can be enhanced with automatic detection of keywords and added to the training data set.

References

[1] Al-Hassan Areej and Hmood Al-Dossari DETECTION of Hate Speech in Social Networks: A Survey On Multilingual Corpus, COSIT, AIAPP, DMA, SEC – (2019), 83-100.

[2] Amr Magdy, Laila Abdelhafeez, Yunfan Kang, Eric Ong and Mohamed F. Mokbel, Microblogs data management: a survey, An Incremental Algorithm for Ranking Twitter Users, In WISE, 201.

[3] N. Antony Sophia, Effective countering of communal hatred during disaster events in social media, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 06(03) (2019).

[4] Bhardwaj Ankur et al., Performance Comparison of De-speckling filters on the Basis of Incremental Iteration in Ultrasound Imaging, 2019 International Conference on Power Electronics, Control and Automation (ICPECA) IEEE, 2019.

[5] Colton David, Hofmann Markus and Ie, Automated Detection of Cyberbullying, 13th International Information Technology and Telecommunication Conference, At Dublin, Ireland, (2014).

[6] Eckberg Deborah, Densley James and Dexter Katrinna, When legend becomes fact, tweet the legend: Information and misinformation in the age of social media 5 (2018), 148-156.

[7] Jenders Maximilian, Kasneci Gjergji and Naumann Felix, Analyzing and predicting viral tweets, WWW Companion - Proceedings of the 22nd International Conference on World Wide Web (2013), 657-664. 10.1145/2487788.2488017

[8] Jin Fang, Wang Wei, Zhao Liang, Dougherty Edward, Cao Yang, Lu Chang-Tien and Ramakrishnan Naren, Misinformation Propagation in the Age of Twitter, Computer, 47 (2014), 90-94. 10.1109/MC.2014.361

[9] Koustav Rudra et al., Characterizing Communal Microblogs during Disaster Events IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016.

[10] Koustav Rudra, Characterizing and Countering Communal Microblogs During Disaster Events, Policy Internet 7(2) (2015), 223-242.

[11] Koustav Rudra, Characterizing and Countering Communal Microblogs During Disaster Events, IEEE Transactions on Computational Social Systems 5(2) (2018).

[12] K. Rudra, S. Ghosh, N. Ganguly, P. Goyal and S. Ghosh, Extracting situational information from microblogs during disaster events: A classification-summarization approach, In Proc. ACM CIKM (2015), 583-592.

[13] Maclean Fiona Jones and Derek Carin-Levy, Gail Hunter, Heather, Understanding Twitter, British Journal of Occupational Therapy 76(6) (2013), 295. 10.4276/030802213X13706169933021.

[14] Paul Avijit, Identifying Relevant Information for Emergency Services from Twitter in Response to Natural Disaster, ISES Solar Energy J., Spec. Proc. 76 (2004), 235-241.

[15] Rastogi Vaishali et al., Deep *Q* learning and its variants: a concise review, Journal of Critical Reviews 7(18) (2020), 1412-1422.

[16] Stowe Kevin, Paul Michael, Palmer Martha, Palen Leysia and Anderson Ken, Identifying and Categorizing Disaster-Related Tweets, Proceedings of The Fourth International Workshop on Natural Language Processing for social media, Austin, TX, c©2016 Association for Computational Linguistics November 1 (2016), 1-6.

[17] S. Vaishnavi, A Survey on Natural Disaster Prediction in Q-Learning, International Journal of Research in Engineering, Science and Management 2(7) (2019).

[18] Sarah Vieweg, Microblogging During Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness, In Proc. Hawaii International Conference on System Sciences 2009.

[19] Sharma Amit and Goyal Aayushi, Tweet, Truth and Fake News: A Study of BJP's Official Tweeter Handle, Journal of Content, Community and Communication 8(4) (2018), 22-28. 10.31620/JCCC.12.18/05

[20] Shukla Anand Prakash and Suneeta Agarwal, An enhanced cellular automaton based scheme for noise filtering, International Journal of Signal Processing Image Processing and Pattern Recognition 7(4) (2014), 231-242.

[21] Shukla Anand Prakash, Training cellular automata for image edge detection, Romanian Journal of Information Science and Technology 19(4) (2016), 338-359.

[22] Shukla Anand Prakash et al., Real time acquisition of vehicle diagnostic data using wireless sensor network, 2009 Fifth International Conference on Wireless Communication and Sensor Networks (WCSN) IEEE, 2009.

[23] Seal Deboshree, A. P. Shukla and Ankur Bhardwaj, Effect of Iterative Variations on Despeckling Filters in Ultrasound Imaging, 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE 1 2019.

[24] Tahora H. Nazer, Intelligent Disaster Response via Social Media Analysis - A Survey, In Proceedings of the 19th ACM international conference on Information and knowledge management, ACM (2010), 759-768.

[25] Wang Tianyi, the power of comments: fostering social interactions in microblog networks, In: Proceedings of the 19th International Conference on World Wide Web, (2010), 591-600.

[26] Wu, Shao-Yu, Wang, Ming-Hung, Chen and Kuan-Ta, Privacy Crisis Due to Crisis Response on the Web, (2011). 10.1109/TrustCom.2011.28