Project Dissertation Report on

Identifying (Mis)Information from Social Media in Operational Crisis Situations: A case of EVM Glitches in India

Submitted By:

Priyanka Kushwaha

2K18/EMBA/531

Under the Guidance of:

Dr. Sonal Thukral

Assistant Professor

DELHI SCHOOL OF MANAGEMENT

Delhi Technological University

Bawana Road Delhi 110042

CERTIFICATE

This is to certify that the Project Report titled **"Identifying (Mis)Information from Social Media in Operational Crisis Situations: A case of EVM Glitches in India",** is a bonafide work carried out by **Priyanka Kushwaha** of EMBA 2018-2020 and submitted to Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42 in partial fulfillment of the requirement for the award of the degree of Executive MBA.

Signature of Guide   Signature of Head

Place :

Date :

DECLARATION

I, Priyanka Kushwaha, student of EMBA 2018-2020 of Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42 declare that Dissertation Report on "**Identifying (Mis)Information from Social Media in Operational Crisis Situations: A case of EVM Glitches in India**" submitted in partial fulfillment of Degree of Executive MBA is the original work conducted by me.

The information and data given in the report is authentic to the best of my knowledge. This Report is not being submitted to any other University for award of any other Degree, Diploma and Fellowship.

Place :   Priyanka Kushwaha

Date :

ACKNOWLEDGEMENT

Accomplishment of a task with desired success calls for dedication towards work and promoting guidance, co-operation and deliberation from seniors.

At the outset, I would like to thank Dr. Sonal Thukral, Assistant Professor, Delhi School of Management for her support and professional approach in guiding me through the careful details of the project.

I would be failing in my duty if I do no express my deep sense of gratitude to Professor, Rajan Yadav, Head of Department and all the faculty members for their valuable advice and guidance in this project.

EXECUTIVE SUMMARY

Twitter is being used as the mass medium by many people to express opinions, post clarifications, share information, advertise, complain, provide feedback, and reporting. Social media have witnessed an explosive growth of malicious and deceptive information. Studies have confirmed that misleading information diffuses significantly farther, faster, deeper, and more broadly than factual information, in all categories of information. Thus, it has become important to detect misinformation at their early stages before it spreads online, thus avoiding risk, damage, errors, hoaxes, and other falsehoods. Twitter can also be used to aid in managing the communication during any operational aspects of large events of national or international importance such as assembly and general elections, Kumbh Mela, Common Wealth Games and epidemic situations like COVID-19. Using the case of malfunctioning of electronic voting machines (EVMs) in the general elections of India 2019, we propose a data science framework that can be used to identify genuine and non-genuine tweet. This study also helps organizations/management to prioritize only genuine tweets during an operational crisis occurring in large events and address the non-genuine tweets to avoid any fake information propagation. To develop this approach, we integrated results and insights from feature engineering, text mining, sentiment analysis, and data mining to detect genuine and non-genuine information using Twitter data.

Using Twitter API and PYTHON, data was collected with '#EVM Malfunction' from twitter feed. This study provides Logistic regression and decision tree models to automate the identification of genuine and non-genuine tweets.

Table of contents

CHAPTER-1

INTRODUCTION

The emergence of social media has drastically altered the way people share content. Social media platforms like Twitter, YouTube, Facebook, Snapchat and Instagram furnish users with the adaptability to impart their insights, pictures, or recordings yet additionally participate in conversations (Tumasjan 2010; LaMarre and Suzuki-Lambrecht 2013). As millions continue to spend time on social networks, more and more user data is being generated every second (Evangelos et al. 2013). As of March 2020, the monthly active Facebook users worldwide are 2.38 billion (Statista, 2020a). In case of Twitter the number of monthly active users for December 2019 stood at 321 million (Statista 2019b). Such a massive repository of personal opinions and beliefs provides an exciting opportunity for researchers and businesses to glean through the sentiments of social media users. For this reason, several researchers from various fields show interest in exploring the opportunities that social media can offer.

In the context of political elections, many candidates resort to social media networks for disseminating information relating to their political campaigns, news articles etc. Twitter seems to be a promising forum for reaching out to their supporter and connecting with them (Stieglitz et al. 2012). It essentially, picked up its notoriety in the political field after Barack Obama's triumph in the U.S. presidential races. A few examinations have ascribed the powerful utilization of online systems and battling as an empowering agent for Obama's triumph (Tumasjan et al. 2010). Earlier writing is devoted to understanding the job of online life in anticipating political decision results. Studies suggest that microblogging sites like Twitter play a pivotal role for “political deliberation” (Tumasjan et al. 2010). Researchers also suggest that candidates have brighter chance at winning the election if they actively engage with voters and/or supporters (LaMarre and Suzuki-Lambrecht 2013). However, posting of opinions, active engagement in discussions can often result in spreading of false information or news. Several authors, therefore, caution against the availability of false content on social media platforms (Castillo et al. 2012; Gupta et al. 2013; Lee et al. 2015; Zeng et al. 2016a; Allcott and Gentzkow 2017). In addition, with the approach of advanced cell phones and diminishing expense of Internet, it has gotten simpler for users to post suppositions and remarks via web-based networking media. However, the conclusions of users on social platform could be emotional and temperamental indicating towards the ‘veracity’ component of big data (Gandomi and Haider 2015). Allcott and Gentzkow (2017) argue that messages can be easily posted on social media platforms without any “third party filtering, fact-checking, or editorial judgement”. Such postings can create confusion and panic during sensitive times as elections as well as alter the public opinion regarding a candidate or a political party. Therefore, identifying false information on social media and restricting its further diffusion has become an urgent need of the hour.

24 suggestions following G20 dissents in April 2009 were made in an ongoing HMIC (Her Majesty's Inspectorate of Constabulary) report, incorporates a proposal that those inside the police accountable for preparing, strategies, and network pressure observing must have the option to identify a circumstance in its early stages and settle on choices on continuous knowledge, with the end goal that they can respond snappier while adjusting to any inescapable change in a possibly socially troublesome circumstance. This includes substantially more master dynamic insight assembling and observing. However, using online data from social media platforms like Twitter to deal with operations aspects of large events is a challenging task. Today, lots of users post their opinions, comments, or information about an event or trend, which can't be filtered or fact-checked easily. Therefore, we need to develop a mechanism using Twitter data to detect real instances of operational crisis as and when it happens. This mechanism can be a great aid in organizing events of national or international importance such as assembly and general elections, Kumbh Mela, and Commonwealth Games. This particular aspect has attracted less attention from the researchers of the Information Systems (IS) area. In this paper, we investigate how live reporting on Twitter can be used to identify genuine information and prioritize genuine issues leading to operational crises occurring in large events and also avoid further diffusion of non-genuine information.

Taking the above view forward, this paper discusses the case of malfunctioning of electronic voting machines (EVMs) in the general elections of India 2019, also known as Lok Sabha elections. EVMs were introduced by the Election Commission of India (ECI) in the 1980s to ensure transparency in the voting process. Preceding the presentation of electronic democratic, India utilized paper polling forms and manual checking. The paper voting forms technique was generally condemned in light of fake democratic, corner catching where party supporters caught stalls and stuffed them with pre-filled phony voting forms. The printed paper polling forms were additionally progressively costly, requiring generous post-casting a ballot asset to check a huge number of individual voting forms. Indian EVMs are independent machines worked with once compose, read-just memory. EVMs or electronic democratic machines furnish the voter with a button for every decision which is associated by a cable to an electronic voting box. An EVM comprises of 2 units - balloting unit and control unit, and these two are associated by a 5-meter cable. At the point when a voter presses a button against the applicant, he/she wishes to decide in favor of, the machine locks itself. This EVM can be opened distinctly with another polling form number. Along these lines, EVMs guarantee that one individual gets the opportunity to cast a ballot just a single time. Implanted EVM highlights, for example, "electronically constraining the pace of throwing votes to five every moment", a security "lock-close" include, an electronic database of "casting a ballot marks and thumb impressions" to affirm the personality of the voter, directing races in stages more than half a month while sending broad security work force at every stall have decreased appointive extortion and misuse, dispense with corner catching and make increasingly serious and more fairer decisions.

However, tweets regarding technical glitches in the functioning of EVMs or malfunctioning of EVMs have been posted on Twitter. These EVM issues result in a delay in the polling process in many polling booths and become serious concerns for the ECI administrators. However, as pointed above several of these tweets could be just a rumor. In order to avoid any uncertain or chaotic situations, it is important to identify whether a tweet is genuine or fake and respond to it accordingly. It becomes imperative for the supervising authority like the Election Commission of India (ECI) to take timely action if any such incident has occurred or clarify the false information. Since, the information obtained through Twitter is massive and real-time in nature, identifying fake messages manually becomes cumbersome. Therefore, we argue that there is a need to address this ‘veracity’ component of big data. Prior literature discusses the development of similar classifiers in the field of crises management (Castillo et al. 2013; Gupta et al. 2013; Liu et al. 2015; Zeng et al. 2016a). These studies have primarily focused on extraction of various types of features and improving the accuracy of their classifiers for fake tweet prediction.

In this study, we plan to develop a framework for data science modeling that can detect genuine tweets about EVM from live Twitter feed and label them. Further, in our modeling effort, we use techniques from feature engineering, text mining, sentiment analysis, and data mining. We believe this study can offer potential insights and help organizations to create mechanism to resolve operational crisis situations using live Twitter feed and will also help government agencies like the ECI of India to manage their election process with higher integrity and to save the cost, time, and effort.

1.1 Objectives of the Study

Primary Objective

- To detect genuine and non-genuine information over social media during situations of operational crisis

Secondary Objective

- To provide potential insights that will help in creating mechanism to address only genuine tweets on Twitter during operational crisis situations using live Twitter feed

LITERATURE REVIEW

The Rising Influence of Social Media

Social media in different forms such as Twitter, WhatsApp and Facebook have become an essential piece of our lives (Steiglitz et al. 2012; Stieglitz and Dang-Xuan 2013; Schoen et al. 2013). It facilitates people to connect with others and participate in discussions on a real time basis (Simon et al. 2015; Zeng et al. 2016b). Smartphones have made it simpler for individuals to associate by means of various online platforms whenever. Twitter permits users to interface with different users of the stage by utilizing their Twitter ID '@username'. Twitter users can thru a discussion towards a specific person by typing their Twitter ID. Also, Twitter users can explore tweets or content on a particular trend or topic or theme of their interest by using another feature of hashtags ('#trendname').

Whether it's a mere sharing of opinion or engaging into discussions or performing daily activities like booking a cab, online shopping etc., every single online transaction is recorded. All this information represents the likes, dislikes, preferences, ideologies, beliefs of users and presents an exciting opportunity for businesses to enhance their promotional campaigns and/or user engagement strategies. Researchers from various fields are finding ways to tap into opinions, thoughts, and reviews of users to understand their general sentiment regarding a product/service (Evangelos et al. 2013; Chae 2015; Chang et al. 2017). Techniques like text mining, opinion mining, sentiment analysis, natural language processing, and visual analytics are being used extensively to glean insights from user-generated content (Chang et al. 2017).

Apart from business entities, government officials also take leverage of social media channels to conduct routine or critical activities (Kavanaugh et al. 2012). While, social forums like Twitter are extensively used for informal communication among users, it is also a powerful medium for discussing about social or current issues (Park 2013). Using social networking services, government officials can identify important events, disseminate important information, identify and classify community issues, respond to crises situations, analyze public sentiments regarding community services or a propaganda etc. (Kavanaugh et al. 2012; Takahashi et al. 2015). Emergency responders have resorted to Twitter to disseminate information to public and coordinate relief efforts during crises like earthquake in Haiti in 2010 and hurricane "Sandy" in 2012 (Simon et al. 2015; Takahashi et al. 2015). On a similar note, Panagiotopoulos et al. (2016) observed that Twitter was utilized by UK local government authorities to spread awareness during heavy snowfall in December 2010 and riots in August 2011. Upon analyzing Twitter feeds, the authors concluded that tweets were predominantly used to inform public about the events, precautions to be taken, progress of managing the situations, appealing for public support etc. In another study, Burnap et al. (2015) utilized conversation analysis, sentiment analysis and ML methods to detect any "spike" in social strain through Twitter feeds.

The Relevance of Social Media in Politics

The relevance of social media can be extended to the context of politics as well. The sudden interest in using social media for electoral campaigning can be attributed to the Barack Obama's triumph during the U.S. presidential appointment of 2008 (Tumasjan et al. 2010). Several politicians since then have resorted to social media to communicate with voters. In their study, LaMarre et al. (2013) identified that approximately 54.4 percent of political leaders using Twitter for their campaigns won the election when compared to only 17.06 percent of non-Twitter users. Researchers recommend that communication with voters and other stakeholders becomes more essential especially during the time of elections (LaMarre et al. 2013; Stieglitz and Dang-Xuan 2013). Due to its characteristics of an "open and broadly-networked forum", Twitter appears to be a popular choice among political institutions to interact with their supporters (Tumasjan et al. 2010; Stieglitz et al. 2012; Park 2013). When compared with Facebook, user accounts on Twitter are easily accessible even by the non-registered users (Stier et al. 2018). Hence, Twitter offers a more flexible platform for candidates to interact with national audience.

However, these interactions are not limited to campaigns and posts shared by political parties. Citizens, journalists, and opinion leaders also participate in the transmission of political news, views, thoughts etc. (Park 2013).

Opinions and thoughts of voters regarding a specific candidate can greatly influence their decisions. Tumasjan et al. (2010) observed that number of tweets shared by a user for a political leader closely follows the number of votes received in the elections. Moreover, examination of tweets can reflect a general sentiment of Twitter users for a political party or a leader (Tumasjan et al. 2010). Therefore, candidates can benefit significantly by observing trends in public sentiments and identifying potential areas for improvement. Several politicians look for suggestions, recommendations, and feedback to improve their current political work (Stieglitz et al. 2012). In this vein, Stieglitz and Dang-Xuan (2013) outlined specific tools for text mining, sentiment analysis, network analysis that could be used by political institutions to scan online data. Interestingly, using text analysis, Stier et al. (2018) discovered that political leaders can tailor the topics of discussions depending on the choice of media (Twitter or Facebook or traditional media). This way, identifying and participating in trending topics of discussion can help political leaders to further improve connections with their supporters (Stieglitz and Dang-Xuan 2013, Stier et al. 2018).

Diffusion of Information (or Misinformation)

Online platforms play a critical role in disseminating information on a real-time basis. Specifically, in the case of Twitter, mechanisms like reposting the content shared by other users or “retweeting” further facilitates information diffusion across larger audiences (Schoen et al. 2013; Zeng et al. 2016b). The phenomenon of information diffusion can be traced back to the time when Rogers (1962) first explained diffusion theory as “the process by which an innovation is communicated through certain channels over time among the members of a social system” (as cited in Lee et al. 2015, p. 998). We believe, a similar process is replicated when users share news, opinions, and reviews with other members in their social network. With the advent of web technologies, computing technologies, and Internet the transmission of information between any two or more users can take place in real-time. Thus, we propose to study the interaction among users across social networking services through the lens of diffusion theory. Several researchers studying the process of information diffusion across social forums have identified features that facilitates this process. For instance, in their study, Lee et al. (2015) identified three variables- reaction time, number of followers, and hashtag usage that hold significant relationship with the degree of message diffusion on Twitter. In a similar vein, Hoang and Mothe (2018) developed a model to predict the retweet of a post based on "user-based, time-based, content-based" features. Further, based on "topological, content-based, and crowdsourced features", Ratkeiwitcz et al. (2011) built a model to detect diffusion of "political misinformation".

However, prior literature also indicates that during emergency or uncertain situations, activities of Twitter users with respect to posting and reposting updates, news, links, photos tend to increase as they try to communicate to as many people as possible (Kavanaugh et al. 2012). This might sometimes result in posting of false information (Kavanaugh et al. 2012; Zeng et al. 2016a). Propagation of false information might result in destructive responses such as defamation, protests etc. (Liu et al. 2015). Therefore, it is extremely important to timely identify the false information and take appropriate actions for its control (Lee et al. 2015). Several studies have attempted at building classifiers to serve this need. Castillo et al. (2013) have identified a detailed list of four characterizing features that might be helpful in predicting information credibility. These features are associated to message-level, user-level, topic- level, and propagation-level. In another study, Liu et al. (2015) recommend the use of 'belief features' (classifying users into who support the event and those who refute the event) along with 'verification features' (source credibility, source identity, source diversity, source location & witness, message belief, event propagation) can help in early prediction of rumors. Taking the case of "Sandy" hurricane, Gupta et al. (2013) developed a decision tree classifier based on user features and content features to identify fake images.

Twitter and EVM operation management

In democratic countries, elections are considered sacrosanct and election periods are extremely sensitive. These periods are characterized by extensive campaigning by politicians of different political parties. ECI focuses on the preparation of the electoral list of voters, the arrangement of polling booths, counting of votes and finally declaration of the result. ECI role in supervising the process of polling and enforcing the norms of conduct for fair elections becomes extremely critical. Voters cast their vote through an electronic voting machine (EVM) in India instead of the old practice of ballot paper. The EVMs, along with Voter-verified paper audit trail (VVPAT) systems that allow voters to verify that the vote was cast to their intended candidate and thus maintain the transparency of the voting system.

Some of the EVM and VVPAT machines being used by ECI on polling days might encounter technical or other functional issues. Whenever such an issue occurs, news agencies publish it, political workers report it on various platforms. Some of these reports are inaccurate and intentionally done to create a situation for their own vested interest. Because of expanded utilization of internet-based platforms, (for example, Twitter) by society at large, many such instances are being tweeted or posted regularly on polling days. It becomes a complex and difficult situation for ECI to address these complaints. Considering the volume and velocity at which the tweets are generated, manually identifying the tweets reporting an actual EVM issue is an arduous activity. Also, the presence of veracity component further adds to this complexity. The proliferation of tweets might not only generate sentiments of agony among the citizens, but it also makes it problematic to identify whether an EVM encountered a technical glitch or not. The social media pressure causes delay for ECI to respond to genuine issues on EVM.

Therefore, it becomes crucial to find an automated solution that can detect whether tweets posted highlight a real issue related to EVM. By identifying which information is genuine promptly, the ECI will be better equipped to prioritize the situations and thus save time and effort.

CHAPTER-3

METHODOLOGY

3.1 Problem Statement

We have observed intense increase in internet penetration and flooding of opinions by internet users on any event. Presently a day's web-based life has become an exceptionally basic piece of everybody's life. Web based life is utilized as a wellspring of news, refreshes, data, imparting one's perspectives and insights, to communicate assent or difference on any choice. Technology has offered users more options to access internet from anywhere and anytime. Both genuine and non-genuine information are tweeted by users intentionally or unintentionally. Many prior researches have also confirmed that fake information propagate more rapidly than factual information. It has also been observed that users with ample of disposable time contribute to the diffusion of fake news and create tension in the environment, which sometimes even causing serious risk and damage in certain situations. Thus, it has become urgent need of the hour to identify which is genuine and which is non-genuine information and prioritize actions to address only genuine tweets during an operational crisis occurring in large events of national or international interest, as well as act to avoid any further propagation of fake information in the public. To address the issue of identification of genuine and non-genuine information, we propose a data science framework to detect genuine or non-genuine tweet.

3.2 Hypothesis

a. Information or misinformation in tweets is classified as inherent features of tweets.

3.3 Research Design

Data fetched from Twitter using Python and Twitter search API, with filter on tweet with "#EVM Malfunction".

We manually performed data cleaning like removing records with blank tweets, contains only URL, image/video and irrelevant or by mistakenly tagged data from the corpus. The corpus was divided into 2 data set – train and test data set.

Training data set holds 2696 records and test data set holds 674 records.

After validating the data from various news resources, each record was manually labeled as genuine - "1" and non-genuine - "0". Other extracted features were converted to binary based on the defined data dictionary for easy computation.

The training informational collection was utilized to prepare the forecast models. Test informational set was utilized to check the precision and accuracy of the model.

This study proposes two models/framework – Logistic Regression and Decision Tree to automatically predict the genuine and non-genuine tweets.

3.4 Sample Design

Data was collected from Twitter with tweets containing "#EVM Malfunction", using Python and Twitter's Search API.

Table.1. Corpus

Pre-Cleaning Corpus	**Post-Cleaning Corpus**
Total number of tweets - 3834	Total number of tweets - 3370
	Training Data set - 2696 and Test Data Set - 674

DATA ANALYSIS

Data Source: Secondary Data

We have sourced this data from Twitter

https://www.twitter.com

4.1 Data Collection, Data Exploration and Data Preparation

Data Collection

Data was collected from Twitter with tweets containing "#EVM Malfunction", using Python and Twitter's Search API.

Total number of tweets - 3370
Training Data set - 2696 and Test Data Set - 674

Data features – The dataset has 3370 rows and 29 attributes. The variable "TV" that is our target variable, indicates whether a tweet is genuine labeled as "1" or non-genuine labeled as "0".

Definition of each variable –

1. TV : Binary, whether an tweet is genuine or non-genuine
2. clean_tweet_text : Tweeted text by the user
3. tweet_created_on_holiday_bool : Binary, indicates if tweet was made on holiday then 1 else 0
4. tweet_created_on_weekend_bool : Binary, indicates if tweet was made on weekend then 1 else 0
5. tweet_created_at_noon_bool : Binary, indicates if tweet was made at noon then 1 else 0
6. tweet_created_at_eve_bool : Binary, indicates if tweet was made at evening then 1 else 0
7. user_screen_name_length : Indicates Twitter user on screen name length
8. user_no_of_tweets : No of tweets per day by a user
9. user_no_of_followers : No of followers

10. user_no_of_followings : No of friends
11. user_account_age : Users account age
12. user_no_of_favourites : Users no of favorites
13. user_average_tweets : Average no of tweets by user till date
14. user_average_favourites : Average no of favorites by user till date
15. tweet_text_length : Length of tweeted text by user
16. tweet_text_optimal_length : Binary, optimal length then 1 else 0
17. tweet_text_no_of_hashtags : No of hash tags used in the tweet text
18. tweet_text_contains_hashtags : Binary, indicates if tweet contains hashtag then 1 else 0
19. tweet_text_contains_url : Binary, indicates if tweet contains any URL then 1 else 0
20. tweet_text_no_of_user_mentions : Indicates no of reference to any user in the tweet text
21. tweet_text_contains_user_mentions: Binary, indicates if tweet contains reference to any user then 1 else 0
22. tweet_text_contains_media : Binary, indicates if tweet contains media then 1 else 0
23. tweet_text_contains_number : Binary, indicates if tweet contains any contact number then 1 else 0
24. tweet_text_contains_upper_words : Binary, indicates if tweet contains text in uppercase emphisizing attension then 1 else 0
25. tweet_text_contains_lower_words : Binary, indicates if tweet contains text in lowercase then 1 else 0
26. tweet_text_contains_excl : Binary, indicates if tweet contains any exclamation marks then 1 else 0
27. tweet_text_contains_retweet_suggestion : Binary, indicates if tweet contains any retweet suggestion then 1 else 0
28. Retweets: No of retweets
29. tweet_polarity : Associates sentiment with the tweet, positive, neutral or negative based on polarity score

Data Exploration

For data exploration Python and MS Excel was used to visualize the dataset.

As a first step, each tweet was manually verified with various news resources to authenticate the event and accordingly data was labeled as genuine (1) and non-genuine (0).

Data Preparation

a. As a first step, the data available was explored for any blank tweets, contains only URL/image/video or wrongly tagged or irrelevant data from the corpus and removed those records from the corpus.
b. Prepared data dictionary to convert data of categorical nature into binary for easy computation.

clean_twe	tweet_cre	tweet_cre	tweet_cre	tweet_cre	user_scre	user_no_c	user_no_c	user_no_c	user_acco	user_no_c	user_aver	user_aver	tweet_tex	tweet_tex	tweet_tex	tweet_tex	tweet_tex	tweet_tex	tweet_tex
this is real	0	0	0	0	11	8853	8857	515	3308	4226	2.67624	1.27751	140	0	0	0	1	0	0
only if it g	0	0	0	0	7	10325	250	309	3066	1427	3.36758	0.46543	86	1	2	1	1	0	0
dragging c	0	0	0	0	15	605	11	163	332	872	1.82229	2.62651	133	0	3	1	1	0	0
dragging c	0	0	0	0	15	605	11	163	332	872	1.82229	2.62651	133	0	3	1	1	0	0
dragging c	0	0	0	0	15	636	12	168	336	940	1.89286	2.79762	133	0	3	1	1	0	0
dragging c	0	0	0	0	15	636	12	168	336	940	1.89286	2.79762	133	0	3	1	1	0	0
for everyc	0	0	0	0	14	647	475	447	2566	169	0.25214	0.06586	140	0	0	0	1	0	0
do know h	0	0	0	0	11	10700	204	573	1942	9038	5.50978	4.65396	140	0	0	0	1	1	1
the electi	0	0	0	0	14	95968	19606	399	3701	148	25.9303	0.03999	140	0	0	0	1	0	0
bjp and m	0	0	0	0	12	553	4	120	430	70	1.28605	0.16279	140	0	4	1	1	0	0
chalo shur	0	0	0	0	11	6557	55	98	1688	6631	3.88448	3.92832	140	0	0	0	1	8	1
oppositior	0	0	0	0	12	72850	1532	286	669	63	108.894	0.09417	131	0	5	1	1	0	0
must thinl	0	0	0	0	11	52077	1643	413	3232	164	16.1129	0.05074	144	0	2	1	1	1	1
must take	0	0	0	0	7	7202	1040	362	1560	7825	4.61667	5.01603	139	0	0	0	1	6	1
it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	1	1
it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	0	0
it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	3	1
it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	1	1
evm fight	0	0	0	0	13	359	145	143	2025	183	0.17728	0.09037	132	0	3	1	1	1	1
who has c	0	0	0	0	6	98529	433	1005	2690	6361	36.6279	2.36468	133	0	2	1	0	2	1
election is	0	0	0	0	11	35006	267	181	3609	2903	9.69964	0.80438	144	0	2	1	1	0	0
do you kn	0	0	0	0	12	113003	2115	0	3214	679	35.1596	0.21126	140	0	0	0	1	0	0
facts avail	0	0	0	0	8	37836	1046	1725	3467	19221	10.9132	5.54399	139	0	0	0	1	0	0
bjp bharti	0	0	0	0	15	2221	43	44	3245	561	0.68444	0.17288	140	0	1	1	1	0	0
kindly mal	0	0	0	0	15	2221	43	44	3245	561	0.68444	0.17288	140	0	0	0	1	2	1
evm malfu	0	0	0	0	10	36565	2145	3693	3601	6712	10.1541	1.86393	130	0	4	1	1	1	1
dear idiot	0	0	0	0	8	37836	1046	1725	3467	19221	10.9132	5.54399	143	0	1	1	1	0	0
love it gra	0	0	0	0	8	1117	149	439	536	1488	2.08396	2.77612	133	0	5	1	1	1	1
guys check	0	0	0	1	11	170	35	153	65	196	2.61538	3.01538	132	0	1	1	1	0	0
the integr	0	0	0	1	12	55435	2122	1132	2856	26688	19.41	9.34454	139	0	2	1	1	1	1
the integr	0	0	0	1	12	55435	2122	1132	2856	26688	19.41	9.34454	139	0	2	1	1	1	1
the integr	0	0	0	1	12	55625	2131	1138	2860	26790	19.4493	9.36713	139	0	2	1	1	1	1
the integr	0	0	0	1	12	55625	2131	1138	2860	26790	19.4493	9.36713	139	0	2	1	1	1	1
evm cann	0	0	0	1	11	30148	130	220	1239	7864	24.3325	6.34705	72	1	2	1	1	0	0
problems	0	0	0	1	14	280	19	291	342	470	0.81871	1.37427	140	0	0	0	1	0	0

Fig.1. Data Collected

Name	TV		Name	tweet_text_contains_hashtags		Name	tweet_text_contains_lower_words	
Actual Defination	Genuine or Non-genuine		Actual Defination	Does the tweet contain hashtags?		Actual Defination	Does the tweet contains text in lower case?	
Flag	1	genuine	Flag	1	Yes	Flag	1	Yes
	0	non-genuine		0	No		0	No
Name	tweet_created_on_holiday_bool		Name	tweet_text_contains_url		Name	tweet_text_contains_excl	
Actual Defination	Was the tweet created on holiday?		Actual Defination	Does the tweet contain URL?		Actual Defination	Does the tweet contains exclamation mark?	
Flag	1	Yes	Flag	1	Yes	Flag	1	Yes
	0	No		0	No		0	No
Name	tweet_created_on_weekend_bool		Name	tweet_text_contains_user_mentions		Name	tweet_text_contains_retweet_suggestion	
Actual Defination	Was the tweet created on weekend?		Actual Defination	Does the tweet contain user?		Actual Defination	Does the tweet contain retweet suggestion?	
Flag	1	Yes	Flag	1	Yes	Flag	1	Yes
	0	No		0	No		0	No
Name	tweet_created_at_noon_bool		Name	tweet_text_contains_media				
Actual Defination	Was the tweet created at noon?		Actual Defination	Does the tweet contain media?				
Flag	1	Yes	Flag	1	Yes			
	0	No		0	No			
Name	tweet_created_at_eve_bool		Name	tweet_text_contains_number				
Actual Defination	Was the tweet created at evening?		Actual Defination	Does the tweet contain contact?				
Flag	1	Yes	Flag	1	Yes			
	0	No		0	No			
Name	tweet_text_optimal_length		Name	tweet_text_contains_upper_words				
Actual Defination	Is the tweet of optimal length?		Actual Defination	Does the tweet contains text in uppercase?				
Flag	1	Yes	Flag	1	Yes			
	0	No		0	No			

Fig.2. Data Dictionary

TV	clean_twe	tweet_cre	tweet_cre	tweet_cre	tweet_cre	user_scre	user_no_c	user_no_c	user_no_c	user_acco	user_no_c	user_aver	user_aver	tweet_tex	tweet_tex	tweet_tex	tweet_tex	tweet_tex	tweet_tex	tweet_tex
1	this is real	0	0	0	0	11	8853	8857	515	3308	4226	2.67624	1.27751	140	0	0	0	1	0	0
1	only if it g	0	0	0	0	7	10325	250	309	3066	1427	3.36758	0.46543	86	1	2	1	1	0	0
1	dragging c	0	0	0	0	15	605	11	163	332	872	1.82229	2.62651	133	0	3	1	1	0	0
1	dragging c	0	0	0	0	15	605	11	163	332	872	1.82229	2.62651	133	0	3	1	1	0	0
1	dragging c	0	0	0	0	15	636	12	168	336	940	1.89286	2.79762	133	0	3	1	1	0	0
1	dragging c	0	0	0	0	15	636	12	168	336	940	1.89286	2.79762	133	0	3	1	1	0	0
1	for everyo	0	0	0	0	14	647	475	447	2566	169	0.25214	0.06586	140	0	0	0	1	0	0
1	do know h	0	0	0	0	11	10700	204	573	1942	9038	5.50978	4.65396	140	0	0	0	1	1	1
1	the electi	0	0	0	0	14	95968	19606	399	3701	148	25.9303	0.03999	140	0	0	0	1	0	0
1	bjp and m	0	0	0	0	12	553	4	120	430	70	1.28605	0.16279	140	0	4	1	1	0	0
1	chalo shur	0	0	0	0	11	6557	55	98	1688	6631	3.88448	3.92832	140	0	0	0	1	8	1
1	oppositior	0	0	0	0	12	72850	1532	286	669	63	108.894	0.09417	131	0	5	1	1	0	0
1	must thinl	0	0	0	0	11	52077	1643	413	3232	164	16.1129	0.05074	144	0	2	1	1	1	1
1	must take	0	0	0	0	7	7202	1040	362	1560	7825	4.61667	5.01603	139	0	0	0	1	6	1
1	it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	1	1
1	it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	0	0
1	it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	3	1
1	it means e	0	0	0	0	15	14076	134	194	291	10916	48.3711	37.512	140	0	0	0	1	1	1
1	evm fight	0	0	0	0	13	359	145	143	2025	183	0.17728	0.09037	132	0	3	1	1	1	1
1	who has c	0	0	0	0	6	98529	433	1005	2690	6361	36.6279	2.36468	133	0	2	1	0	2	1
1	election is	0	0	0	0	11	35006	267	181	3609	2903	9.69964	0.80438	144	0	2	1	1	0	0
1	do you kn	0	0	0	0	12	113003	2115	0	3214	679	35.1596	0.21126	140	0	0	0	1	0	0
1	facts availa	0	0	0	0	8	37836	1046	1725	3467	19221	10.9132	5.54399	139	0	0	0	1	0	0
1	bjp bharti	0	0	0	0	15	2221	43	44	3245	561	0.68444	0.17288	140	0	1	1	1	0	0
1	kindly mal	0	0	0	0	15	2221	43	44	3245	561	0.68444	0.17288	140	0	0	0	1	2	1
1	evm malfu	0	0	0	0	10	36565	2145	3693	3601	6712	10.1541	1.86393	130	0	4	1	1	1	1
1	dear idiots	0	0	0	0	8	37836	1046	1725	3467	19221	10.9132	5.54399	143	0	1	1	1	0	0
1	love it gra	0	0	0	0	8	1117	149	439	536	1488	2.08396	2.77612	133	0	5	1	1	1	1
1	guys check	0	0	0	1	11	170	35	153	65	196	2.61538	3.01538	132	0	1	1	1	0	0
1	the integr	0	0	0	1	12	55435	2122	1132	2856	26688	19.41	9.34454	139	0	2	1	1	1	1
0	the integr	0	0	0	1	12	55435	2122	1132	2856	26688	19.41	9.34454	139	0	2	1	1	1	1
0	the integr	0	0	0	1	12	55625	2131	1138	2860	26790	19.4493	9.36713	139	0	2	1	1	1	1
0	the integr	0	0	0	1	12	55625	2131	1138	2860	26790	19.4493	9.36713	139	0	2	1	1	1	1
0	evm cannc	0	0	0	1	11	30148	130	220	1239	7864	24.3325	6.34705	72	1	2	1	1	0	0

Fig.3. Data Cleaning and Preparation

4.2 Results

In the training dataset there are 1865 Non-Genuine Tweets and 831 Genuine Tweets, adding to 2686 total tweets. In the test dataset there are 466 Non-Genuine Tweets and 208 Genuine Tweets.

Model results on Training Dataset:

Non-Genuine = 1399, Genuine = 623

Logistic Regression		Model	
		Non-Genuine	Genuine
Labelled in Data	Non-Genuine	1360	39
	Genuine	576	47
Accuracy 70%			
	Precision	Recall	F1-Score
Non-Genuine	0.7	0.97	0.82
Genuine	0.55	0.08	0.13

Fig.4. Logistic Regression on training dataset

Decision Tree		Model	
		Non-Genuine	Genuine
Labelled in Data	Non-Genuine	1399	0
	Genuine	4	619
Accuracy 100%			
	Precision	Recall	F1-Score
Non-Genuine	1.00	1.00	1.00
Genuine	1.00	0.99	1.00

Fig.5. Decision Tree on training data set

Model results on an unseen Dataset:

Logistic Regression		Model	
		Non-Genuine	Genuine
Labelled in Data	Non-Genuine	458	8
	Genuine	196	12
Accuracy 70%			
	Precision	Recall	F1-Score
Non-Genuine	0.70	0.98	0.82
Genuine	0.60	0.06	0.11

Fig.6. Logistic Regression on test dataset

Decision Tree		Model	
		Non-Genuine	Genuine
Labelled in Data	Non-Genuine	413	53
	Genuine	96	112
Accuracy 78%			
	Precision	Recall	F1-Score
Non-Genuine	0.81	0.89	0.85
Genuine	0.68	0.54	0.60

Fig.7. Logistic Regression on test dataset

4.3 Statistical Tools

Python programing language has been used to code the retrieval of data from Twitter API and build predictive models.

Python is a deciphered, high-level, broadly useful programming language with accentuation on code lucidness with its outstanding utilization of huge whitespace.

Twitter Search API is a standard hunt API that returns an assortment of applicable Tweets coordinating a predetermined query. Twitter search API is simple to use, fetch meta data, iterable, and friendly to Python

4.3.1 Logistic Regression Test

Logistic regression is utilized to portray information and to clarify the connection between a dependent factor and at least one ostensible, ordinal, interim or proportion level independent factors.

Logistic regression uses algorithm to predict a binary outcome given a set of independent variables.

Y = e^b0+b1x/1+e^b0+b1x

Where, Y = predicted output

Log p(x)/1-p(x)=b0+b1x

4.3.2 Decision Tree Test

Decision tree also known as reduction tree/classification tree is a supervised machine learning technique that does mapping from observations about an item to conclusions about its target variable.

Decision tree internally uses ID3(Iterative Dichotomiser 3) to predict the output.

Y = summation of (p(x)*log2(1/p(x))

4.3.3 Analysis

To predict whether a given tweet is genuine or non-genuine, created below models.

Model	Library:function()
Logistic Regression	glm()
Decision Tree	rpart::rpart()

Code Snippet

```
#Last
consumer_key = 'abrqsNkvMXH54BicIYlkAzuBJ'
consumer_secret = 'tNLyUIelWWIJn0Su2WncYS0BceRpz0LgiGa7yqd7i9mCtPJs1Y'
access_token = '1239448224634531840-y5SPHkhR0EzdbXfmPqo9zBoFToq9pU'
access_token_secret = '99Mgh1RRvk1t8YV9mEtZ9MfNplEBmiNEkIY1IQwbMusMT'

# OAuth process, using the keys and tokens
auth = tweepy.OAuthHandler(consumer_key, consumer_secret)
auth.set_access_token(access_token, access_token_secret)

api = tweepy.API(auth, wait_on_rate_limit=True,
            wait_on_rate_limit_notify=True,
            compression=True)

def clean_tweet(tweet):
   return ' '.join(re.sub("(@[A-Za-z0-9]+)|([^0-9A-Za-z \t])|(\w+:\/\/\S+)", " ", tweet).split())
def contains_numbers(tweet):
    return any(char.isdigit() for char in tweet)
```

4.3.4 Performance measurement

To measure the performance of the machine learning models, confusion matrix is used.

A confusion matrix or error matrix is a table that is frequently used to portray performance of a grouping model (or “classifier”) on a lot of test data for which the true values are known. It permits the visualization of the performance of an algorithm. Confusion matrix is useful in measuring Recall, Precision, Specificity, Accuracy and AUC-ROC curve of a model and gives a way to compare any given models.

Confusion/Error Matrix

	Actually Positive (1)	Actually negative (0)
Predicted Positive (1)	True Positives (TPs)	False Positives (FPs)
Predicted Negative (0)	False Negatives (FNs)	True Negatives (TNs)

Fig.8. Confusion Matrix

Precision

PR = TP / (TP + FP)

Recall

RE = TP / (TP+FN)

Accuracy

CA = (TP + TN) / (TP + TN + FP + FN)

F- measure

F1 = (2 * Recall * Precision) / (Recall + Precision)

Or, F1 = 2TP / (2TP + FP + FN)

FINDINGS

- By labeling and comparing the tweet data, we have found that there is more of non-genuine information on social media platform than factual information.

- By analyzing the features of the tweet, we have found that there are categories of users using the social media platform with different mindset and purpose. Lot of these fake information is propagated by user who have ample of disposable time without sensing the adverse effects or risk it can bring in the society.

- Studying the click graph of user shows that it is an important feature to identify if a information could go viral.

- Taking into account the tons of data that generates everyday as more and more users gets online with ease of availability and technological advancement, it becomes very difficult to manually control or distinguish between what is genuine that needs immediate attention in an operational crisis or other epidemic situations and what is non-genuine information that needs to be stopped from further diffusion into the society.

- Researchers, Marketers, Public, Private organizations, Brands, Politicians use online presence to get information as well as reach their intended target audience/masses in no time in the easiest and the most convenient way

- This data science framework/model based on logistic regression with 70% and Decision tree with 78% of accuracy in automatically identifying genuine and non-genuine information with respect to EVM and thus providing a mechanism to save time, effort, and money that could be of very importance in operational crisis situation management.

CHAPTER-5

RECOMMENDATIONS

- Help agencies like ECM to identify genuine and non-genuine information in real time
- Aids organization and institutes in building a mechanism to deal with urgent operational crisis in large events in effective manner thus saving time and cost
- Officials to stop further diffusion of fake information in public and thus stop any damage or risk condition of potential impact
- Study can be further enhanced to build more advanced data science framework like Random forest with better accuracy
- Study can also be recrafted to address a more generic operational crisis situation

LIMITATION OF STUDY

This study is subject to the following limitations

- Lack of time
- Limited data
- Single channel consideration – Twitter
- Specific issue addressed – EVM
- Geographical constraints
- Basic level models

REFERENCES

INTERNET:

1. Google
2. Twitter

Research papers:

[1.] Allcott, H., and Gentzkow, M. 2017. "Social Media and Fake News in the 2016 Election," Journal of Economic Perspectives (31:2), pp. 211-236.

[2.] Burnap, P., Rana, O. F., Avis, N., Williams, M., Housley, W., Edwards, A., Morgan, J., and Sloan, V. 2015. "Detecting Tension in Online Communities with Computational Twitter Analysis," Technological Forecasting & Social Change (95), pp. 96-108.

[3.] Castillo, C., Mendoza, M., and Poblete, B. 2013. "Predicting Information Credibility in Time-Sensitive Social Media," Internet Research (23:5), pp. 560-588.

[4.] Chae, B. K. 2015. "Insights from Hashtag #Supplychain and Twitter Analytics: Considering Twitter and Twitter Data for Supply Chain Practices and Research," International Journal of Production Research, pp. 257-259.

[5.] Chang, Y.-C., Ku, C.-H. L., and Chen, C.-H. 2017. "Social Media Analytics: Extracting and Visualizing Hilton Hotel Ratings and Reviews from TripAdvisor," International Journal of Information Management, (doi:10.1016/j.ijinfomgt.2017.11.001).

[6.] Election Commission of India. 2019. "General Election 2019 - Election Commission of India," (available at https://eci.gov.in/general-election/general-elections-2019/; retrieved May 1, 2019).

[7.] Evangelos, K., Efthimios, T., and Konstantinos, T.2013. "Understanding the Predictive Power of Social Media," Internet Research (23:5), pp. 544-559.

[8.] Gandomi, A., and Haider, M. 2015. "Beyond the Hype: Big Data Concepts, Methods and Analytics," International Journal of Information Management (35:2), pp. 137-144.

[9.] Gupta, A., Lamba, H., Kumaraguru, P., and Joshi, A. 2013. "Faking Sandy: Characterizing and Identifying Fake Images on Twitter during Hurricane Sandy," in Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, pp. 729-736.

[10.] Hoang, T. B. N., and Mothe, J. 2018. "Predicting Information Diffusion on Twitter – Analysis of Predictive Features," Journal of Computational Science (28), pp. 257-264.

[11.] Kavanaugh, A. L., Fox, E. A., Sheetz, S. D., Yang, S., Li, L. T., Shoemaker, D. J., Natsev, A., and Xie, L. 2012. "Social Media Use by Government: From the Routine to the Critical," Government Information Quarterly (29), pp. 480-491.

[12.] LaMarre, H. L., and Suzuki-Lambrecht, Y. 2013. "Tweeting Democracy? Examining Twitter as an Online Public Relations Strategy for Congressional Campaigns," Public Relations Review (39), pp. 360-368.

[13.] Lee, J., Agrawal, M., and Rao, H. R. 2015. "Message Diffusion through Social Network Service: The Case of Rumor and Non-rumor Related Tweets during Boston Bombing 2013," Information Systems Frontiers (17:5), pp. 997-1005.

[14.] Liu, X., Nourbakhsh, A., Li, Q., Fang, R., and Shah, S. 2015. "Real-time Rumor Debunking on Twitter," in Proceedings of the 24th ACM International Conference on Information and Knowledge Management, Melbourne, Australia, pp. 1867-1870.

[15.] Panagiotopoulos, P., Barnett, J., Bigdeli, A. Z., and Sams, S. 2016. "Social Media in Emergency Management: Twitter as a Tool for Communicating Risks to the Public," Technological Forecasting *& Social Change* (111), pp. 86-96.

[16.] Park, C. S. 2013. "Does Twitter Motivate Involvement in Politics? Tweeting, Opinion Leadership, and Political Engagement," *Computers in Human Behavior* (29), pp. 1641-1648.

[17.] Ratkiewicz, J., Conover, M. D., Meiss, M., Goncalves, B., Flammini, A., and Menczer, F. 2011. "Detecting and Tracking Political Abuse in Social Media," in *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*, Barcelona, Spain, pp. 297-304.

[18.] Schoen, H., Gayo-Avello, D., Metaxas, P. T., Mustafaraj, E., Strohmaier, M., and Gloor, P. 2013. "The Power of Prediction with Social Media," *Internet Research* (23:5), pp. 528-543.

[19.] Simon, T., Goldberg, A., and Adini, B. 2015. "Socializing in Emergencies- A Review of the Use of Social Media in Emergency Situations," *International Journal of Information Management* (35), pp. 609-619.

[20.] Statista. 2019a. "Facebook Users Worldwide 2018," (available at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/; retrieved April 28, 2019).

[21.] Statista. 2019b. “Twitter: Number of Active Users 2010-2018,” (available at https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/; retrieved April 28, 2019).

[22.] Stieglitz, S., Brockmann, T., and Dang-Xuan, L. 2012. “Usage of Social Media for Political Communication,” in *Proceedings of the 16th Pacific Asia Conference on Information Systems*, Ho Chi Minh City, Vietnam.

[23.] Stieglitz, S., and Dang-Xuan, L. 2013. “Social Media and Political Communication: A Social Media Analytics Framework,” *Social Network Analysis and Mining* (3:4), pp. 1277-1291.

[24.] Stier, S., Bleier, A., Lietz, H., and Strohmaier, M. 2018. “Election Campaigning on Social Media: Politicians, Audiences, and the Mediation of Political Communication on Facebook and Twitter,” *Political Communication* (35:1), pp. 50-74.

[25.] Suh, B., Hong, L., Pirolli, P., and Chi, E. H. 2010. “Want to be Retweeted? Large Scale Analytics on Factors Impacting Retweet in Twitter Network,” in *Proceedings of the 2nd International Conference on Social Computing*, Minneapolis, MN, pp. 177-184.

[26.] Takahashi, B., Tandoc Jr., E. C., and Carmichael, C. 2015. “Communicating on Twitter during a Disaster: An Analysis of Tweets during Typhoon Haiyan in the Philippines,” Computers in Human Behavior (50), pp. 392-398.

[27.] Tumasjan, A., Sperenger, T. O., Sandner, P. G., and Welpe, I. M. 2010. “Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment,” in Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media, Washington DC, USA, pp. 178-185.

[28.] Zeng, L., Starbird, K., and Spiro, E. S. 2016a. “#Unconfirmed: Classifying Rumor Stance in Crisis-Related Social Media Messages,” in Proceedings of the Tenth International AAAI Conference on Web and Social Media, Cologne, Germany, pp. 747-750.

[29.] Zeng, L., Starbird, K., and Spiro, E. S. 2016b. “Rumors at the Speed of Light? Modeling the Rate of Rumor Transmission during Crisis,” in Proceedings of the 49th Hawaii International Conference on System Sciences, Washington DC, USA, pp. 1969-1978.