

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Krishna Vaishnav 177364IVCM

HOW INDIAN POLITICAL PARTIES ARE USING FACEBOOK AND TWITTER TO REACH VOTERS' WHATSAPP ACCOUNT

Master's Thesis

Supervisor: **Olaf M. Maennel, Ph.D**

Department of Software Sciences

School of Information Technologies

Tallinn Technical University,
Estonia

Robert Petronic, M Sci.

Professor, Algebra University

Zagreb, Croatia

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Krishna Vaishnav 177364IVCM

ANALÜÜS ENNE ÜLDVALIMISI SAADUD WHATSAPP ANDMETE (LOK SHABHA) 2019 INDIAS

Magistritöö

Juhendaja: **Olaf M. Maennel, Ph.D**

Tarkvara teaduste osakond

Infotehnoloogia kool

Tallinna Tehnikaülikool, Eesti

Robert Petronic, M Sci.

Algebra ülikooli professor

Zagreb, Horvaati

Tallinn 2018

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Krishna Vaishnav

13.05.2019

Abstract

In the recent years, India has embraced new age technology and fast paced internet with open arms. While technology has created new opportunities for millions, it has also brought with it – plethora of new problems, which Indians do not fully grasp and have no resources to fight with. Starting April 2019, India is going to held largest democratic election in the world, with 900 million eligible voters. Small and large political parties are rallying their cause and using every conventional as well as unconventional trick to sway votes in their favors.

Being 2nd most populous country with hundreds of sects, customs and most religions under one roof, India is a perfect breeding ground for identity politics. While in the past, political leaders were limited by the physical reach of the communication methods. Mass adaptation of the social media applications by Indians has made it easy for political leaders to convey their messages in the farthest corners of the country. Seemingly, political parties have adopted use of Facebook and WhatsApp to spread false propaganda to favors their personal agenda.

This being relatively new problem, very few researchers have investigated the use of social media and communication tools like WhatsApp as propaganda machines. This thesis will bridge this gap and examine the specifics of the various method employed by political parties such as generation of malicious content, targeted attacks and exploiting user vulnerabilities to gain votes.

A single WhatsApp group can have a maximum of 256 members. With exponential spread, malicious and fake content can be forwarded to millions with just few clicks. To understand the depth and breadth of this problem we mined data from 54 public WhatsApp groups. We collected messages in the form of Audio, Video, pictures, contact and text. We analyzed more than 19000 messages to present our findings.

Through these finding we want to lay structure around which additional security features can be developed for communication tools such as WhatsApp and Facebook. This thesis also critically examines the systematic exploitation of the democratic system by the

political parties by the use of unexpected tools like WhatsApp. Political parties in India are increasingly relying on WhatsApp for advertisement. There is an urgent need for creating tools for developing user awareness and develop additional security features in applications like WhatsApp to tackle widespread of false news.

This thesis is written in English and is 87 pages long, including 7 chapters, 31 figures and 7 tables.

Annotatsioon

analüüs enne üldvalimisi saadud WhatsApp andmete (Lok Shabha) 2019 Indias

Viimastel aastatel on India omaks võtnud uue ajastu tehnoloogiat ja avatud relvaga kiiret internetiühendust. Kuigi tehnoloogia on miljonite jaoks uusi võimalusi pakkunud, on see toonud kaasa ka mitmeid uusi probleeme, mida indiaanlased ei suuda täielikult mõista ja kellel ei ole ressursse selle vastu võitlemiseks. Alates 2019. aasta aprillist toimub India suurim demokraatlik valimine maailmas, kus on 900 miljonit valijat. Väikesed ja suured erakonnad loovad oma põhjuse ja kasutavad kõiki tavapäraseid ja ebatavalisi trikke häälte austamiseks.

Olles 2. kõige rahvaarvuga riik, kus on sadu sektid, kombed ja enamik religioone ühe katuse all, on India ideaalne identiteedipoliitika alus. Minevikus piirasid poliitilised liidrid kommunikatsioonimeetodite füüsilist ulatust. Sotsiaalse meedia rakenduste massiline kohandamine indiaanlaste poolt on muutnud poliitiliste liidrite jaoks lihtsaks oma sõnumite edastamise riigi kõige kaugematesse nurkadesse. Ilmselt on poliitilised parteid võtnud kasutusele Facebooki ja WhatsAppi vale propaganda levitamiseks, et soosida nende isiklikku päevakorda.

See on suhteliselt uus probleem, väga vähesed teadlased on uurinud sotsiaalmeedia ja kommunikatsioonivahendite, nagu WhatsAppi kasutamist propaganda masinatena. See lõputöö lükkab selle lünga ja uurib erinevate poliitiliste parteide poolt kasutatava meetodi spetsiifikat, nagu pahatahtliku sisu genereerimine, sihitud rünnakud ja kasutaja haavatavuste kasutamine häälte saamiseks.

Ühes WhatsApp grupis võib olla kuni 256 liiget. Eksponentsiaalselt levinud pahatahtliku ja võltsitud sisu saab edastada miljoneid vaid mõne klõpsuga. Selle probleemi sügavuse ja laiuse mõistmiseks lamasime andmeid 54 avalikust WhatsApp grupist. Me kogusime sõnumeid heli, video, piltide, kontaktide ja teksti kujul. Meie tulemuste tutvustamiseks analüüsimisega rohkem kui 19000 sõnumit.

Nende leidude abil tahame luua struktuuri, mille ümber saab luua täiendavaid turvaelemente kommunikatsioonivahendite jaoks, nagu WhatsApp ja Facebook. Samuti uurib see väitekiri kriitiliselt demokraatliku süsteemi süstemaatilist kasutamist poliitiliste parteide poolt, kasutades ootamatuid vahendeid, nagu WhatsApp. India poliitilised parteid toetuvad reklaamiks üha enam WhatsAppile. On hädavajalik luua vahendid kasutajate teadlikkuse arendamiseks ja täiendavate turvaelementide arendamiseks sellistes rakendustes nagu WhatsApp, et võidelda valede uudiste levikuga.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 89 leheküljel, 7 peatükki, 31 joonist, 7 tabelit.

List of abbreviations and terms

| | |
|------|--------------------------|
| T.V. | Television |
| BJP | BHARTIYA JANTA PARTY |
| INC | INDIAN NATIONAL CONGRESS |
| USA | United State of America |

Table of Content

| | |
|--|----|
| 1 Introduction | 16 |
| 2 Research Problem | 18 |
| 3 Literature Review | 21 |
| 3.1 Related Works | 23 |
| 4 Indian Politics | 26 |
| 4.1 Use of Social Media in Previous Indian Elections | 26 |
| 4.2 Propaganda Topics in India | 27 |
| 4.2.1 Hindu-Muslim | 28 |
| 4.2.2 Beef..... | 29 |
| 4.2.3 Rape | 29 |
| 5 WhatsApp Messaging Application..... | 31 |
| 5.1 Features..... | 31 |
| 5.1.1 Messaging – | 31 |
| 5.1.2 Calling – | 31 |
| 5.1.3 Status – | 31 |
| 5.1.4 Contact/ location sharing – | 32 |
| 5.1.5 End to End Encryption – | 32 |

| | |
|---|----|
| 5.2 Popularity..... | 32 |
| 5.3 Use of WhatsApp during Election..... | 33 |
| 5.4 Relation between WhatsApp Users and Voters in India | 34 |
| 5.5 WhatsApp Data Collection by Politician..... | 35 |
| 5.6 WhatsApp Fraud..... | 37 |
| 5.7 Introduction of IT Act in India | 39 |
| 6 Research Methods..... | 41 |
| 6.1 Part – 1 | 42 |
| 6.2 Honeypots | 43 |
| 6.2.1 Set up WhatsApp account..... | 43 |
| 6.2.2 Set up Facebook profiles | 46 |
| 6.2.3 Twitter Profiles | 48 |
| 6.3 Joining the WhatsApp Group | 48 |
| 6.3.1 Honeypot Data..... | 49 |
| 6.3.2 Public Group invitation links..... | 49 |
| 6.3.3 Collecting public group invitation links | 49 |
| 7 Data Collection | 52 |
| 7.1 WhatsApp Message Collection | 52 |
| 7.2 WhatsApp Group Data | 53 |
| 7.2.1 Messages..... | 53 |
| 7.2.2 Types of Messages..... | 53 |

| | |
|--|----|
| 8 Challenges | 55 |
| 8.1 Challenge 1 (Facebook)..... | 55 |
| 8.1.1 Sandeep Jain | 56 |
| 8.1.2 Sikander Khan (Facebook Profile) | 57 |
| 8.2 Challenge 2 (WhatsApp) | 58 |
| 8.2.1 Challenge 3 (Collecting Data) | 58 |
| 8.3 Data Analysis..... | 59 |
| 8.3.1 Step 1 (WhatsApp Group Chat)..... | 59 |
| 8.3.2 Step 2 (Export the group Chat)..... | 60 |
| 8.3.3 Step 3 (Filter the Exported Chat data) | 62 |
| 8.3.4 Step 4 (Processed Data) | 64 |
| 8.3.5 Step 5 (Store the Data)..... | 64 |
| 8.4 WhatsApp Group Data Analysis | 64 |
| 8.4.1 Text Messages Analysis | 65 |
| 8.4.2 Links Analysis | 67 |
| 8.4.3 Media Message analysis | 69 |
| 8.5 Ethical Consideration | 70 |
| 8.5.1 WhatsApp | 70 |
| 8.5.2 Facebook & Twitter | 71 |
| 9 RESULTS..... | 72 |
| 9.1 Part 1..... | 72 |

| | |
|--|-----|
| 9.1.1 Details of the Honeypots | 72 |
| 9.2 Part 2 (Analysis) | 74 |
| 9.2.1 Text Message Analysis | 74 |
| 9.2.2 Links Analysis | 81 |
| 9.3 Media Analysis | 91 |
| 9.3.1 Contacts | 91 |
| 9.3.2 Document File | 93 |
| 9.3.3 Audio Messages..... | 93 |
| 9.3.4 Videos | 94 |
| 9.3.5 Pictures | 95 |
| 10 Future..... | 98 |
| 11 Conclusion..... | 99 |
| 12 References | 99 |
| Appendix 1 – [Heading of Appendix] | 109 |

List of figures

| | |
|---|----|
| Figure 4.1 Fake claim that Congress leader running a prostitution ring from home (Resource: altnews.com) | 30 |
| Figure 6.1 Research methodology structure | 41 |
| Figure 6.2 Phases of Research methodology | 42 |
| Figure 6.3 Methodology for setting up WhatsApp honeypot profile | 44 |
| Figure 6.4 Sandeep Jain WhatsApp profile | 45 |
| Figure 6.5 Methodology for the Facebook account | 46 |
| Figure 6.6 Sikander Khan profile | 47 |
| Figure 6.7 Methodology to collect WhatsApp group invitation links | 50 |
| Figure 7.1 Process to collect the WhatsApp Messages | 52 |
| Figure 7.2 Category of WhatsApp Messages | 54 |
| Figure 8.1 Notification showed on Sandeep Jain’s Facebook account | 56 |
| Figure 8.2 Notification on the Sandeep Jain’s Facebook profile | 56 |
| Figure 8.3 Terms and condition for Facebook user taken from Sandeep Jain Facebook account..... | 57 |
| Figure 8.4 Facebook requesting form to unblock the Facebook profile..... | 57 |
| Figure 8.5 Methodology for WhatsApp message analysis | 59 |
| Figure 8.6 Process of exporting the WhatsApp group data | 60 |
| Figure 8.7 Example of exported .txt WhatsApp group chat for Sandeep Jain WhatsApp profile..... | 61 |
| Figure 8.8 Method to filter the raw WhatsApp exported file | 63 |
| Figure 8.9 Process for text message analysis | 66 |
| Figure 8.10 An Example of the Gmail spam filter | 67 |
| Figure 8.11 Method for the Link Analysis | 68 |
| Figure 8.12 Method for the Media Analysis..... | 69 |
| Figure 9.1 Statistics about domain found in link analysis | 82 |
| Figure 9.2 frequency of spreading malicious links..... | 90 |
| Figure 9.3 Statistics of contacts shared in the groups..... | 92 |
| Figure 9.4 Shared Contact info..... | 93 |

| | |
|---|----|
| Figure 9.5 Tampered picture | 96 |
| Figure 9.6 Image has Misleading Information | 96 |
| Figure 9.7 Screenshot of the Telangana Congress's Manifesto | 97 |
| Figure 9.8 Manipulating Information | 97 |

List of tables

| | |
|--|----|
| Table 1 Political topics related to BJP Parties | 75 |
| Table 2 Political topics related to Congress INC party | 75 |
| Table 3 General topics related to Indian Politics..... | 76 |
| Table 4 Example of the political WhatsApp messages (Collected by honeypot) | 76 |
| Table 5 messages detected by Gmail spam filter | 79 |
| Table 6 Description of Domains found during research..... | 82 |
| Table 7 VirusTotal Results | 84 |

1 Introduction

Nowadays people are more active on social media. Today numbers of social media platforms like Facebook, WhatsApp, Twitter, LinkedIn, Instagram, Snapchat and YouTube, are available to express thoughts, to communicate with different people from different nations and discuss on the different topics. These social media platforms give freedom to share thoughts through videos, audio messages, and text messages with other users. The user-friendliness and convenience are the most important reasons for the espousal of social media. On social media, people are more expressive, more communicative and feel comfortable to palaver freely. The rapid growth of social media made it the best advertising tool for political parties. Now, Political parties apart from the traditional advertisement platforms like – T.V., Radio, Newspaper they are emphasizing on social media platforms [1]. Social Media platforms are a boon for political parties to reach to the voters, to communicate with them, spread the work political party had done for the country, parties' belief and ideology, parties' future agenda for the countries and how they will fight will the existing problems [2]. Social Media seems a good publicity pulpit to lure the voters.

A problem occurs when political parties misuse the social media platform by bombarding the platform with political cyber propaganda attack, Political parties are trying to manipulate the religious minorities, supporter, opponents, and dissenting individuals to elect them by sending fake content, manipulating content and misleading content using social media [3]. It is important to understand how political parties are using social media platforms for election promotions. What content political parties are spreading on the social media platform? And what topics are making social media platform vulnerable? India is the biggest market for Facebook networking website and WhatsApp chat application [4] and that is the reason in our study we are focused on the use of WhatsApp messaging application for the upcoming Indian assembly election from April 2019 to May 2019 by political parties. For the election purpose Indian political parties Bhartiya Janta Party (BJP) and Indian Nation Congress (INC) relatively having approximately 200,000-300,000 and 80,000-100,000 WhatsApp groups to circulate the advertisements in audio, video, text and picture format [5]. We will analysis the advertisements political parties

are circulating on WhatsApp also we will analyze what content political parties are using for the advertising purpose. Is there any offensive, misleading, hoax content or fraud messages or media is circulating with the political advertisement on WhatsApp? This analysis will help to spread awareness among the social media users so they will be able to distinguish between the genuine advertisement and cyber propaganda attacks and the frauds spreading on the WhatsApp.

2 Research Problem

The use of fake news in the 2016 US presidential election of USA shook American democracy to its foundation [22]. While answering a question on the subject "Fake news: A serious threat to democracy" European Parliament answered stated that the use of fake news is an attack on the democracy.; They included the results of the Euro Baromotere survey, where 83% of interviews agreed that "fake news is a threat to democracy". A decision to choose a leader based on false news cannot be an independent and clear decision. Fake news raises the question on the legitimacy of the elections and nobility of democracy.

This study will explore how Indian Political Supporters are using popular WhatsApp messenger and type of content being shared on WhatsApp chat application in the light of the increasing adaptation of Previous use of the social media (Facebook and Twitter) by politicians and now increasing rising popularity of the WhatsApp in India prompt us to conduct the study on how Indian political supporters are using popular WhatsApp chat application. ? And what WhatsApp messages they are posting on WhatsApp messenger? In our study, we are addressing both issues. We will also study the usual tactics employed by the political parties to target unaware voters. By exposing these techniques we want to create awareness among voters and supply them with tools to identify fake news.so voter will be more aware of how he can be targeted by politicians via WhatsApp and what are the probable WhatsApp message could be fake or spams during the election and (s)he can select the right leader without any influence by his own will and choice.

The first issue, how Political parties are employing various methods for reaching to the people's WhatsApp messenger's users' profile and adding them to the political groups.? Indian As we studied the political parties have created thousands of WhatsApp groups, and they hired about .2 millions of IT specialists to write customize messages for WhatsApp messenger to lure the voters [23]. The Research [24] demonstrate three ways an attacker can use to exploit mobile numbers for sending spam on Over the Top application; 1st by exploiting true caller's reverse-lookup contact feature, 2nd by using the public information on social media and 3rd by synchronizing with the address book and

finding out the application mobile users are using. In addition to these tricks, we have also added some of the ways how political parties can get the users' mobile phone numbers to add them to the political WhatsApp groups.

- Mining other social media platforms like – Facebook, Twitter, LinkedIn, Instagram where mobile numbers are public and visible and add them.
- It is also possible for political parties to buy user's data from Carrier Companies.
- Brute force to get the all possible combination of numbers
- Adding known number and asking them to add more known users. Creating a WhatsApp group chain.

In our experiment we are focusing on the social media platforms – Facebook and Twitter to check whether political parties' Information Technology cells are using the data mining techniques on Facebook and Twitter to get the mobile number or not. For this purpose, we created two WhatsApp honeypots for Facebook which are further connected with the two twitter honeypots. These Honeypots are a trap for those social media accounts, political profiles specifically created to scarp the Facebook and Twitter users' data to add them on WhatsApp groups. These Honeypots will target two major parties of Indian politics, named Bhartiya Janata Party (BJP) – The current ruling party and Indian National Congress (INC) – Oldest political party since freedom. The success of this experiment depends on the reachability to the Political Facebook and Twitter profiles which are doing the data mining of Facebook and Twitter users. If the honeypot will able to catch political groups, then this experiment will also explain what type of Facebook or Twitter profiles they are targeting

The second issue is WhatsApp messages (media or text format) and type of content circulating in the political WhatsApp platform as political advertisements. Our study will answer this question by analyzing the content political parties are sharing and rotating on WhatsApp groups. To collect those messages, we will join public political WhatsApp groups in two ways. Firstly, through the honeypot - If political Facebook profile will add our WhatsApp profile in any of the political parties' WhatsApp groups then we will analyze those messages. A second way to get political messages is by joining some WhatsApp groups as a party supporter using the invitation links available publicly on

different websites and also on social media sites like-Facebook. The message analysis will give us some important information like – what messages groups members are spreading? Is the content genuine and not harmful for the other users? Are all messages related to politics? Are there fraud and spam messages also spreading in political groups?

Political cyber propaganda attack on WhatsApp can be controlled or stopped by combining the cyber-security, political science, and psychological sciences. Combination of these three fields highly covers political cyber propaganda. Political science helps to understand how a political campaign works on the ground, how political parties create the headlines for promotions and type of content political parties are using to manipulating the voter. Knowing the message and motivation of political parties helps to understand the topics for manipulating news which are specifically created to polarize the voters for political advantages. Analyzing voter's psychology is important to relate how voter's thought process changes when they read, listen, watch political cyber propaganda, how voters get influenced by the fake news and tactics political parties uses and its psychological effect on voters. Political cyber propaganda could spread using traditional sources like Radio, Television, Newspaper, Hoardings, banners, and also by talking. Significance of political cyber propaganda spreading on social media like WhatsApp is more important because of the increasing popularity of the platform.

This is necessary to know how cyber propaganda is working in upcoming election 2019 as well as in the future elections in the country, voters would be aware and able to fight against the political cyber propaganda attacks through the advertisements. A voter would be more mindful to know about the truth hiding behind the WhatsApp messages they are getting; posts they are receiving from the known users like from family and friends and also from unknown users. Analysis of the cyber propaganda in the Indian election could be helpful for the other countries to know how political parties can abuse social media especially WhatsApp because WhatsApp has their market in 180 countries. Most importantly this study will show the fraud spreading on political WhatsApp groups.

3 Literature Review

India is the 2nd most populated country in the world [8] and home of 1.36 billion people [7], an estimated 17.74 % of the total world population [6]. In 2018 India had about 326.1 million social network users which are estimated to reach to 447.9 million by 2023 [9]. Not surprisingly, India is the largest democracy in the world.

Politicians are increasingly using WhatsApp and social media for manipulating voters. Numbers also support the power of social media Like WhatsApp and Facebook in India. India is the largest market for WhatsApp chat application in the world with more than 200 million users during early 2017, which was expected to grow to 300 million by the beginning of 2018 [10].

According to user-reported WhatsApp statistics, 82% of internet users in India were WhatsApp application users in India [11]. WhatsApp messenger has become the top one mobile application in 2019 in India by overtaking Facebook application and Facebook messenger [11]. It is also relevant to see that India is the second biggest smartphone market in the world after China and India with a 20% yearly growth in the mobile phone market [12]. Based on the Emarketer survey conducted in 2015, it was predicted that by 2019, India would have 800 million mobile phone users [13]. In the same year, 374 million would be smartphone users [14]. The comparison study made by cable.co.uk on data plans shows that India has the cheapest data plan in the world. Availability of cheapest 4G data plans is also a reason why smart social media and smartphone market is growing rapidly in India [15]. With a growing smartphone market, the comparison study made by cable.co.uk on data plans shows India has the cheapest data plan in the world. The cheapest data plans help people to buy a smartphone and use the available application. It is also easy for the population poor population living below the poverty line and people living in the remote locations to buy the cheap smartphone and cheap data plan and use the social media application. The poor migrating population is also increasing using Smartphones to keep in touch with family and friends. Majority of poor people migrate to the other state in India for work. Smartphones and social media platforms help them to be connected with family and friends.

WhatsApp has risen as a potent platform among political parties to communicate with voters Not surprisingly, political parties are already leveraging the relationship between

WhatsApp users and prospective voters to expand their support. It is difficult to quantify the powerful role assigned to Social Media and WhatsApp in upcoming Indian elections. However, it is clear that politicians are increasingly using WhatsApp messenger. Detailed analysis of the political content being circulated on WhatsApp is required to grasp the use of WhatsApp by political parties.

Lack of awareness among the general population is also a reason why politicians are abusing social media is because of the lack of awareness within users for their gain. Mass manipulation techniques are being used worked to influence the election results. Cambridge Analytica case shows the dangers of a social media propaganda attack [16]. If users are being manipulated through what they are reading, listening and watching, how it is affecting their mind? For example, in 2016 USA election was centered around the Facebook, the number one social media site, Facebook is the number one social media platform in India as well as in the world [17]. Few studies also indicate available on how that Cambridge Analytica, a US-based data firm mined Facebook user's' data and sent them personalized political advertisements with misleading and false content to manipulate the voter's minds and shape their opinions. This strategy and laid road work helped the Republican party of the USA and Donald Trump's victory in the 2016 elections [18] [19]. For this manipulation, so Many fake news headlines were in trend against Hillary Clinton as part of the cyber propaganda attack [20]. Some of the most famous headlines in 2016 election were

“WikiLeaks confirms Hillary sold weapons to ISIS... Then Drops another bombshell”

“FBI agent suspected in Hillary email leaks found dead in apartment murder-suicide”

“FBI director received millions from Clinton Foundation, his brother’s law firm does Clinton’s taxes”

“ISIS leader calls for American Muslim voters to support Hillary Clinton”

“Hillary Clinton in 2013: ‘I would like to see people like Donald Trump run for office they’re honest and can’t be bought’”

"Ireland is now officially accepting Trump refugees from America"

“Donald Trump sent his own plane to transport 200 stranded marines”

"Pop Francis shocks the world, endorses Donald Trump for President"

All the headlines were fake, and they were just used to manipulate the reader's thought process and create a different persona of then-candidate Donald Trump by showing a fake good side of Donald Trump. Manipulators invoked fear of Hillary Clinton in voters by associating her with Terrorist Organizations.

whereas how Hillary Clinton is supporting the terrorist organization which created a fake fear in user that Clinton was really supporting the terrorists which could be a big problem if she will win the election. Cases like Cambridge Analytica not only depicts exposes the use of social media in a wrong way by how politicians use the power of social media in a wrong way to win influence the election results which is extremally dangerous for the democracy but are also a statement on the vulnerabilities of the democratic election process.

As per USA today article USA senate report found evidence that the Russian government interfered in the 2016 U.S. election. Russian government created numbers of social media accounts to reach the millions of social media users which were prospective voters in 2016 U.S election [21]. According to the criminal indictments by the special counsel the motives behind the messages circulated by the Russian Government circulated was to "spread distrust towards the candidates and political system in general". Above examples shows how powerfully social media is being used to affect election outcomes by can affect the users' mind by manipulating advertisements. It is also noticeable that if the United States of America, a powerful country nation is not immune to "what could be a successful cyber- political propaganda attack", which influence the election results, then other small countries also have a probability of false election and fake leaders. They have even fewer chances of sustaining a fair democratic process against the new age propaganda machine

3.1 Related Works

A study [62] was conducted by Amila Banerjee and Mehrazun Neesa Haque about the fake news on social media in India. This study focused on the use of social media

including WhatsApp by politicians to spread the fake news. Study says that political parties are spreading a huge amount of money on social media campaigns, easy availability of WhatsApp is putting it top on the list for spreading the misinformation because people rely on the information they are getting on WhatsApp before a proof check. They added that a popular way of spreading misinformation is by creating small and personnel groups and posting the fake content in those groups. Authors concluded that Anti-Religion Messages are often shared on WhatsApp and end-to-end encryption is a stone in tracking down the distribution chain of fake messages.

A research paper [63] explains that WhatsApp features like end-to-end encryption, free usage, support of the multimedia content, ease of use and forming groups for communication and first-time internet users without proper education about the fake news are some factor, contributed to making the WhatsApp a potent propaganda tool in India. This research also states the statement of on the political leader that BJP formed 10,344 WhatsApp group just to coordinate and circulate media among their party worker, the author added the advantages of spreading the fake news through WhatsApp like cost-producing fake news is cheaper than real news, promotion – fake news generator needs no promotion, Anonymity – cannot trace the root of fake news, shelf life – because fake news is based on myths, fear, and hate so it gets the fire rapidly, Impact – fake news twisted according to the user's biases. Overall this research digs the reasons why WhatsApp is vulnerable to the fake news and how politicians are spreading the fake messages in WhatsApp.

Another research [64] done on analysis of the public WhatsApp group data, this study gives an overview about how to use the publicly available WhatsApp group data and how this data can be analyzed for further research. In this research, they collected data from 143 groups, and they found 39% of text their messages have links. Researcher categories the group according to the group topics and they found that 15 groups were political groups, and most were Indian political groups.

During the background studying of Indian politics and use of WhatsApp application in India. We have found evidence that India political parties used WhatsApp application to send personalize or propaganda messages to voters and they are still creating groups for the next 2019 elections. We have also found proper research to support that political parties are spreading the misinformation for political gain, and political parties have

public political WhatsApp groups. But We didn't find research on how political parties are getting inside the voter's WhatsApp account and from where political parties are collecting the mobile number to add the voters on their WhatsApp groups. And, no scientific research is available on whether the political parties are using the other social media platforms for WhatsApp in the 2019 election. Also, no analysis available on what messages are circulating in the political WhatsApp groups. Are the topics and media circulating in the groups are legitimate and safe for other group members?

We will try to answer the missing questions about how political parties are using the other social media platforms for getting voters data for targeting messaging on WhatsApp and what data messages are group members are posting in the public Indian political WhatsApp groups.

4 Indian Politics

U.S.A. president Abraham Lincoln gave a short definition of democracy, "Government of the people, by the people, for the people". On 26 Jan 1950 India became a democratic country. In 2019 India will go for 17th general assemble (Lok Sabha) election. 7 national parties will fight the elections in 2019 [25]. Out of 7, we will focus on only two major National parties of India for further research. First Indian National Congress (INC) – oldest party in India since 1885, so far for 49 years Congress ruled on India [26]. Second Bhartiya Janta Party (BJP) – Founded in 1980, BJP ruled for 9 years and 1.5 months, BJP had massive victory in 2014 and it is the current ruling party in India [27].

In 2019, India will run elections for 2 months from 11 April to 19 May in 7 phases and counting will be on 23 May. This election will be the world's biggest election, almost 900 million Indian citizens are eligible for voting [28]. Indian citizens above 18 years of age are allowed to vote in the election. In the last election, almost 160 million voters were first-time voters and around 23.1 million or 2.7% of the total eligible voters were aged 18-19 years [29].

4.1 Use of Social Media in Previous Indian Elections

2014 assembly elections of India were a #TwitterElection. In 2014 assembly election BJP won the election by 272 seats over 543; that was the biggest victory by any political party in 30 years of history in India. Narendra Modi the leader of BJP was the first person to use the social media for election; BJP launched Facebook page "I support Narendra Modi" and a WhatsApp number to hike the election campaign [30]. Milan Vaishnav¹ said, "What we do know from exit polling data is that if you look at demographic support for the BJP in particular, the BJP dominated the Congress when it came to younger voters" that clarifies that BJP targeted first time voters in 2014. Milan Vaishnav also confessed that Twitter and Facebook helped to break down information barriers between politicians and voters. Another statement by Arvind Gupta² "We saw a trend, we read this trend,

¹ Milan Vaishnav : an associate in the South Asia Program at the Carnegie Endowment for International Peace

²: head of BJP's IT division

where the youth of the country were embracing social media as their first tool when they started using the internet, and we made sure our presence was there" [31]. Arvind Gupta confessed that the social media played the main role in BJP's 2014 success, and they used Standard tool like Facebook, YouTube, Twitter and then lately WhatsApp for the election campaign. Voanews's article claimed that Nilotpal Chakravarti¹ said, "Mr. Modi himself reached out through his Twitter account to the youth of the country, appealing to what the youth are looking for: jobs, security and the use of technology". According to Bharath Gopalswamy² "The type of messaging and the target messaging, and the agenda on which the election was fought, won them the election rather than social media alone", This sentence can be concluded as sole dependence on social media is not enough to win the election, political parties have to actively communicate with the voters by sending them specialized messages. All the information shows how BJP already used the power of social media during the 2014 election to win 16th assembly election and as a result, they won the election with massive votes and in 2014, Facebook and Twitter were important social media platform to spread the political propaganda.

The concern of spreading political propaganda on social media is, if politician will spread misleading content of sensitive topics on social media and if social media gives a fire to the messages then it can cause the riots in the country. Another critical issue is if people will elect the leader based on misleading messages they read or hear on social media then it can affect the democracy of the country.

Research [50] on propaganda explains that propaganda is a dialogue structure used to get the action done by persuading the people; so the goal of the propaganda is to persuade people in action regardless of the facts and true evidence. The propaganda is usually carried out to deceive the large audience and to manipulate them with false information.

4.2 Propaganda Topics in India

Propaganda is not always fraud news but in a political context, propaganda is mostly fake, misleading, hoax or manipulating news. Propaganda could be fake, misleading or

¹ Nilotpal Chakravarti: associate vice president of the Internet and Mobile Association of India (IAMAI)

²Bharath Gopalswamy: Deputy director of the South Asia Center at the Atlantic Council

deceitful information that is specially created to change the reader's mind by showing the wrong information. The idea behind the propaganda is to use strong human emotions (like- fear, happiness, anger, nationalism) to change or influence their decision for a specific purpose. Propaganda plays with human emotions and tries to restrict a person think rationally. In most cases, propaganda news forces human to think by emotion and takes decision when a person is emotionally weak. Propaganda news works when the message is related to an emotionally sensitive topic. In the Indian context, there are many sensitive topics which can be used for propaganda.

4.2.1 Hindu-Muslim

India doesn't have a national religion. According to the constitution, all religions in India have the same rights. R interview bubble says that in country majority population belongs to Hindu religion with 74.33% [51]. In the world, India has the largest numbers of Hindus. Second biggest population is Muslim with 14.02% in the country [51]. India has the world's second highest Muslim population in the country. Hindu-Muslim is always a sensitive topic in India. Both religions have their same rights in the country but because of the long history of the nations after the freedom in 1947, Hindus and Muslims are always in conflict. Hence, Hindu-Muslim became a very sensitive topic in the nation. Politicians are using this sensitive topic as the card of ace to polarize or misleading the audience to get more votes.

Case 1 – In 2013 just before the general election 2014 a Hindu Muslim riot happened in one of Indian town Muzaffarnagar. A report of BBC news [52] the riot started when a Muslim man harassed young Hindu Jat women. After a few days the stalker was killed by victim's two brothers and a few hours later, victim's both brothers were killed too, this is how a riot started between Hindu and Muslim. Riot became worse because of one viral video on WhatsApp showing two boys were slaughtered by a mob. The video was originally recorded in Pakistan a few years ago but, because of lack of awareness about fake news, people believed the video clip. This incident alone lead to 50 death and hundreds of people left their homes because of the violence. Rajeshwar Dutt Tyagi, a senior lawyer in Muzzafnagar told BBC NEWS that "These are politically engineered riots to polarize voters ahead of the next year's general election" [52].

Case 2 – Another news on "Asia & Pacific Edition" about the incident happened in southern state Karnataka where a fake WhatsApp message was spreading on WhatsApp blaming that a Muslim child kidnapper, kidnapping kids by offering chocolates [53]. A 32-year old software engineer Mohammad Azam went for a picnic to Bidar (Karnataka) along with his 4 friends including a Qatari resident Mohammad Salam. A big mob started to beat those 5 friends while they started to share the chocolates among the local kids. In this incident, Mohammad Azam was beaten till death and the other 4 were seriously injured [54]. This type of news show people has insecurities and, it became easy to take advantage of people's insecurities by manipulating or misleading them. Also, these reports show that awareness about the information they are getting on WhatsApp is really important.

4.2.2 Beef

Another sensitive topic in India is beef. The cow is a sacred animal for the Hindus and Hindu is the majority of the country. Hence cow slaughtering, beef selling, and beef eating are banned in most of the Hindu majority states. Fake message on WhatsApp spreading misinformation that Mohammad Akhlaq killed a cow and stored a beef in-house. Instead of complaining to the police, mob went to his village and beat him to death [55].

4.2.3 Rape

A post was shared on the "We Support Narendra Modi" page on Facebook. A post was claiming that Madhya Pradesh's (state of India) Congress leader named Shabana Sara Ali was caught red-handed while running a prostitution ring from home [56]. This post was shared 2600 times on Facebook. During Investigation, Alt news (one of the organizations trying to catch the fake news in India) found that in Madhya Pradesh state there is no Congress leader named Shabana Sara Ali, also the picture used for Shabana Ali was a Congress worker but named Gurpreet Kaur Chadha. The picture used to show the prostitution ring was originally from China [57]. This was a propaganda post, intentionally created by the opposing party to mislead the people by showing the wrong impression of the party. Without proper resource and investigation, people believed in this post and commented on the hatred statement for the party.



HIGHLIGHTS

- Many social media users claim that one Shabana Sara Ali of Congress Party is running a prostitution racket.
- Photo used as that of Shabana Sara Ali, however, is of Mumbai Mahila Congress VP Gurpreet Kaur Chadha.
- Chadha has filed a police complaint against those misusing her photo.

Figure 4.1 Fake claim that Congress leader running a prostitution ring from home (Resource: altnews.com)

There are false messages and modified videos people are sharing, without checking the fact behind the news, without thinking what future consequences may arise by sharing this type of information. Extreme content is not limited to one platform. It starts from one social media platform and shared among all the possible social media platform and lack of awareness spread it further and it causes a big event. Sometimes, instead of stopping fake news, the politician also spread false news within people to polarize people to gets more votes.

5 WhatsApp Messaging Application

WhatsApp is an instant messaging application which works over the internet. WhatsApp is an alternative to the traditional text messaging service; WhatsApp is available in over 180 countries and estimated of 1 billion people are use WhatsApp to share the messages in text, picture, audio, and video, contacts and location [32]. as it uses the internet to send and receive the messages, it is significantly cheaper than texting. The main use of WhatsApp is for calling, WhatsApp has audio and video calling features. WhatsApp can only be authenticated by the active phone number, so each WhatsApp account is connected with the unique mobile number

5.1 Features

5.1.1 Messaging –

WhatsApp is a messaging chat application. WhatsApp messenger is used for sending the text messages, audio messages, pictures, and videos. Received messages can be shared further to 20 chats at the same time. India shares the highest number of messages than any other country.

5.1.2 Calling –

Another functionality that could be the main reason of increasing adaptability of WhatsApp is audio call and video call because of calling feature people are willing to install and use this application, it is affordable to call through WhatsApp without buying separate calling and text messaging plans.

5.1.3 Status –

WhatsApp also has storytelling or status features. The status feature is for broadcasting messaging to all the saved contacts. WhatsApp introduced storytelling feature because users were sending same greeting messages to the number of users at the same time so for user's feasibility storytelling is an option to share messages with the other users this message stay for 24 hours and then it automatically removed from the profile.

5.1.4 Contact/ location sharing –

WhatsApp gives an option to share the saved contact from the personal phone book with the other users. Location sharing is also possible on WhatsApp, a user can share his live location.

5.1.5 End to End Encryption –

WhatsApp implemented end to end security in 2016, which means that media as messages traveling from one recipient to other is encrypted with cryptography lock. The sender encrypts the message with the public key and only the relevant user has the private key to decrypt the message. According to WhatsApp even WhatsApp itself can't decrypt and read the messages and can't listen to the phone calls. The encryption and decryption happen on the sender and receiver's remote devices [33]. This feature is also one of the reasons why politicians are abusing WhatsApp as a propaganda tool. There is no regulation to check who is creating and spreading political cyber propaganda unless the user is inside the network. This feature gives freedom to spread fake, hoax, misleading, fraud or offensive messages. It is also nearly impossible to check externally what content is being shared between the users, and also in the groups.

All these services of WhatsApp made it popular in India. With the increasing number of WhatsApp users use of calling and messaging and sharing media is also increasing.

5.2 Popularity

Statistics and data mentioned in the introduction show that WhatsApp market is increasing rapidly in India. Not only the population living in urban areas, but poor people are also able to buy cheap 4G data plans and cheap smartphones thus people living below the poverty line are also using WhatsApp. People living in remote areas can also access the information by using WhatsApp. Availability of WhatsApp is the reason why WhatsApp became the next targeting platform to spread the propaganda news and fraud messages between the people during the election. Personnel messaging application always an option to talk and discuss the political issues with family and friends whether in private or group chat. People forward the messages.

5.3 Use of WhatsApp during Election

Our research was motivated when some study and news were published on misuse of WhatsApp platform in Brazil election [34] [35] [36]. Last year in 2018 Brazil, Nigeria, Mexico had elections. Numbers of reports, news articles published on how Brazilian political party abused WhatsApp during the Brazil election to manipulate the voters [34] [36] [35]. As research in Portuguese [37] revealed how misinformation spreads, They collected more than 100,000 political images from 347 groups, they selected 50 most popular images and in a review they found 56% of those 50 images had misleading content. Only 8% of 50 images were genuine and true. To understand how manipulating and misleading images were used 'The New York times' gave an example of WhatsApp message – message displayed the name of a presidential candidate, Luiz Inácio Lula da Silva, next to the number 17; When Brazilians vote, they punch in a number for a candidate or party in an electronic voting machine but the information in the photo was wrong; The number 17 was for Mr. Bolsonaro's party. Mr. da Silva was no longer even in the race' His running mate, Fernando Haddad, had taken his place. Brazil's top electoral court ruled on Aug 31 that Mr. da Silva, who is serving a 12-year sentence for corruption, cannot run for a third term [38].

Another news article published by BBC news on Brazil election was "how political campaign in Brazil have used software that scrapes Facebook for citizens' phone numbers, and then automatically sends them WhatsApp messages and add them to WhatsApp groups" [35], this BBC News article explained that how political parties mine the Facebook users' personal information and used that information specifically phone number, by using software these people were added to the political WhatsApp groups without their consent. BBC interviewed many people involved in a political campaign, they revealed the use of scraping and bulk-messaging tools to send the political advertisement. To add the people in WhatsApp group without their consent is against the WhatsApp rules. It can be counted as an electoral crime. Though Facebook blocked thousands of suspicious WhatsApp accounts and also closed hundreds of Facebook pages and accounts linked with political advertisements.

A similar report on misuse of WhatsApp noticed during the Columbia and Nigeria election, 87.3% of the Columbia population are active WhatsApp users [39] [40]. That dominate market was used during the election to spread the fake news about the

presidential candidates and their political motive over WhatsApp. That political cyber propaganda created distrust and insecurity in voters about the presidential candidate. In Nigeria a fake news trend over WhatsApp during the election about the death of the president. The news was so strong that president himself denied the news. The trend of using WhatsApp as a political propaganda tool is also increasing in Indian elections.

5.4 Relation between WhatsApp Users and Voters in India

A survey done on the usage of WhatsApp in India by LiveMint shows that within a year WhatsApp usage is doubled in rural India [41], most probably because WhatsApp supports 10 Indian languages [42]. Where in urban India it increases from 22% to 38% [41]. The most amazing result of that report is that 49% of WhatsApp users belong to the 18-25 years age bracket, they are almost half of all WhatsApp users [41]. This age group was the target of politicians in the 16th assembly election in 2014. First-time voters are the easy target of the politician because for the first vote they start to think about the politics and nation and they evaluate the ideology of the party, impression of the party and work done by the leaders for the nation. They are more active on social media and share the messages which relate to them. At this stage influence them and misguide them is really easy, WhatsApp is really useful when it used to reach out to the youth of the country for sending the propaganda advertisements and misguiding information about the opponent. Hence it leads to the election manipulation. 35% of WhatsApp users belongs to the 26-35 age [41]. Those are probably the 3rd, 4th-time adult voters. These voters are working people, and these are the target of the opponent parties by propaganda news, creating a false environment of insecurity, issues related to jobs and development of the country are topics used to polarize these voters and influence the election results. As an article on Indian election in 2014 explained one of the reasons Bhartiya Janta Party gain the massive victory was because of targeting the 18-23 age group Facebook users.

A report during the Karnataka state election [43] says that politicians are using the WhatsApp and spreading news about how Hindus are in danger, critiques about current state government and jokes on Congress party's Leader (Rahul Gandhi); during

Karnataka state election B.J.P and Congress parties set up at least 50,000¹ WhatsApp group between them to communicate within the party as well other people [43]. Further "daily hunt" a news source verified that to reach out to the people on social media BJP's Delhi unit has formed 1,800 WhatsApp group also party national president Amit Shah is a member of all WhatsApp groups [44].

Fake posts are created by all the parties to mislead the people and spoil the image or opponent party members also they are spreading bragging message about their party.

As we can see why WhatsApp become an easy target and what could be the consequences of spreading false news on WhatsApp. That's why it is also important to figure out how to educate the people to use the WhatsApp, so they can avoid the false news. Because India is WhatsApp's largest market so WhatsApp itself is trying to aware people about fake news [45].

5.5 WhatsApp Data Collection by Politician

Tradition Indian political parties were mainly depended on the polling booth data to change voter's preferences, reward and punish them whom they voted in the previous election; but now they are moving to the quick and efficient social media platforms [1]. For politicians, WhatsApp is an easy and cheap tool to reach out to the voters. Because of cheap data plan and cheap smart mobile phone availability in the market, people are using the WhatsApp but without having the proper knowledge and the education about the information(messages) they are getting on WhatsApp. Without knowing the negative and positive effect of WhatsApp people are using it. All these reasons are making people an easy target of political propoganda, misleading campaign, fraud, and spams. Also, WhatsApp supports 10 Indian languages that another factor of the increasing use of WhatsApp in India. WhatsApp limited the number of times a message can forward further at the same time to 5 in India but still a single group can have the 256 members so if 5 groups have 256 members than with one click a message could be forwarded to at most 1280 people. Amit Sinha the owner of fact check website(www.altnews.com) said "The

¹ The number of WhatsApp groups created can vary according to the date news published and it can vary according to state to state

velocity that misinformation gets once something is out there and it is something which captures people's imagination, then it is shared like crazy, and it's that velocity that one needs to arrest, so that the least amount of people is affected." This statement explains how difficult it is to track and stop the rumours on the WhatsApp platform once they shared or goes viral.

In India rumours spreading on WhatsApp already had devastating results, according to news report [46] till July 2018, 8 people had been killed because of the rumours spreading on WhatsApp; Overall including past year (2017-2018), 30 incidents of murder by mob were recorded in the whole country, the reason being fake rumour of child abduction on WhatsApp. These incidents show the trust people had on the messages they received on WhatsApp inbox in India. Now WhatsApp is taken to another level by politicians to spread political cyber propaganda advertisements and fraud. Some news reports [47] [48], reports on how Indian politicians are preparing to fight the 2019 election through WhatsApp. One of main lead data analyst of Bhartiya Janta Party, Shivam Sankar Singh¹ said 2019 Indian election is WhatsApp election. He explained how BJP and Congress are not only buying phone numbers and voters' data illegally, but they are also using the publicly available data to analyse voter and then targeting them on WhatsApp. He mentioned some tricks political parties are using to gather the publicly available data as following [49].

- After every election, the Indian Election Commission publishes a report with the all details about election. The report includes a number of votes per assembly, number of votes each candidate got in the election.
- Another platform to get the publicly available data is from Chief Electoral Officer website, each state of India has CEO website, each website has electoral roll, an electoral roll has details about each voter in that assemble, voters' full name, full name of husband/ father, House Number, Age, Gender, Personnel Voter ID Number and serial number of voters. All this information used to separate the voter in different clusters according to caste and religion that can be determined

¹: author of a book "*How to win Indian election*", Former lead data analyst of Bhartiya Janta Party

by the last name, Age is another important factor which can be used to cluster voters according to age and add them in specific WhatsApp groups.

- Politicians are also buying voters electronic bills to determine voters' financial states and send them personalized WhatsApp messages.
- Political parties' private mobile applications, web sites are other options to collect the data. User register with the personal details like phone number, email, in some cases they also give their personal id number (Aadhar number, voter id number, PAN number).

The study [25] discussed the use of personal data in elections how political parties are using social media to collect the voters' data, Unlike in 2014 where political parties spread general messages to all the voters but now in 2019, the motive of political parties is to connect the voter to their issues and motivation. For this purpose, politicians are clustering Indian voter according to the caste, religion, age, gender also financial status and then adding them into different WhatsApp groups. These WhatsApp groups are created for specific reasons they only send advertisement which is relevant to voters. For the example – Hindu Brahmins will be added to the groups where all the messages will be concerned about Hindutva and messages will point how Muslims are a danger for the Hindutva or issues about Lord Ram's Temple. For female voters' advertisements about women safety, for Muslim female voters – advertisements related to 'teen talak'. Though Indian politician always denied buying the data illegally from the dark market, and telecom companies but they accepted that they use the user's data like phone numbers if the owner willingly give them.

5.6 WhatsApp Fraud

Social media not only targeted by the political parties to reach to the voters but study [58] found that fraudsters are also spreading the phishing messages using the social media platforms. A study [58] also confirms that most of the phishing referrals are coming from popular social media platforms like YouTube, Facebook, m.facebook.com, Twitter, LinkedIn. Which means Now Fraudsters are not only using the tradition way to send the phishing content via email, but they are moving to the social media networks probably the reason is quick reachability to the wide network of the people. Another article [59]

claims that scams are not only on popular social media platforms but they are also using the WhatsApp messaging application, according to this article the scammer tries to scam people by tricking them that they are going to win a gift or a deal, and for that they need to click on the given link which further redirects the user towards some form or on malicious webpages which steal their data or force people to download and install some malicious applications.

News [60] showed that by Jun 2018 Indian police collected 1,122 complaints related to credit/debit card fraud, 181 complaints of Facebook cheating fraud, 183 internet fraud and then they have also got 70 complaints of WhatsApp fraud. This data clarifies that Indian WhatsApp users are victims of WhatsApp fraud and scams are rampant on the WhatsApp. As our study is focused on the use of WhatsApp application during the election and the content is being shared in the political WhatsApp group so we are also considering whether the scam and phishing messages are spreading in the political WhatsApp groups or not. The study [61] lists the 19 social media threats for privacy and information security, we have chosen some of the threats as defined in below section

Spam - Spamming is sending unwanted and irrelevant messages over the Internet to many users mostly spamming used to send the malware, phishing, and advertisements.

Phishing – study quoted the cisco.com “Phishing is the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine.”. Phishing can be different type like spear phishing, mishing, whishing and whaling.

Online Predators – These people use social media to target the children of all ages for sexual or other abusive purposes.

Internet scams and frauds – These are the fraudulent activities on social media to take advantage of the gullible user by tricking them and get the money or useful data like – lottery scams, Nigerian scam, Phishing scams

Social bots - Social bots are specific programs created to mimic like a human on social media, the purpose of these programs is to write messages, support campaign, follow users to collect personal data and connect with the other social media users.

Inference Attacks – These attacks generated to scrap the user’s publicly available data using data mining techniques. These attacks carry out to collect the data like user’s choices in order to know about users

5.7 Introduction of IT Act in India

In background study we briefly mentioned the loopholes in IT acts to understand Why political parties are freely using the voters' data for political advertisement, adding them into random WhatsApp groups, sending them political messages. Because weak IT Act laws for social media misuse gives an option to politicians to escape the IT Act law and continue their practices.

P0o9-1x8"Section 66A publishing offensive, false or threatening information – Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine."

Section 66E Publishing private images of others – If a person captures, transmits or publishes images of a person’s private parts without his/her consent or knowledge.

Section 43A compensation for failure to protect data – Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

IT act 66A only apply if the spreader is knowing that the content is false, and he has some motive to spread false information. WhatsApp messages have encryption so first, it is difficult to reach the spreader than spreader can't be guilty if he/she is not aware that information is false. Section 66E applies to the private parts of the body, politicians use the picture of the opponent party (face) with misleading content. 43A is strong law but it says only if a fraudster uses the information for wrongful loss or wrongful gain towards

any person, it is not explained the use of data for the political campaign is a wrongful gain or not.

6 Research Methods

Based on the research question we have divided the research methodology into two parts and conclude both parts for the final results.

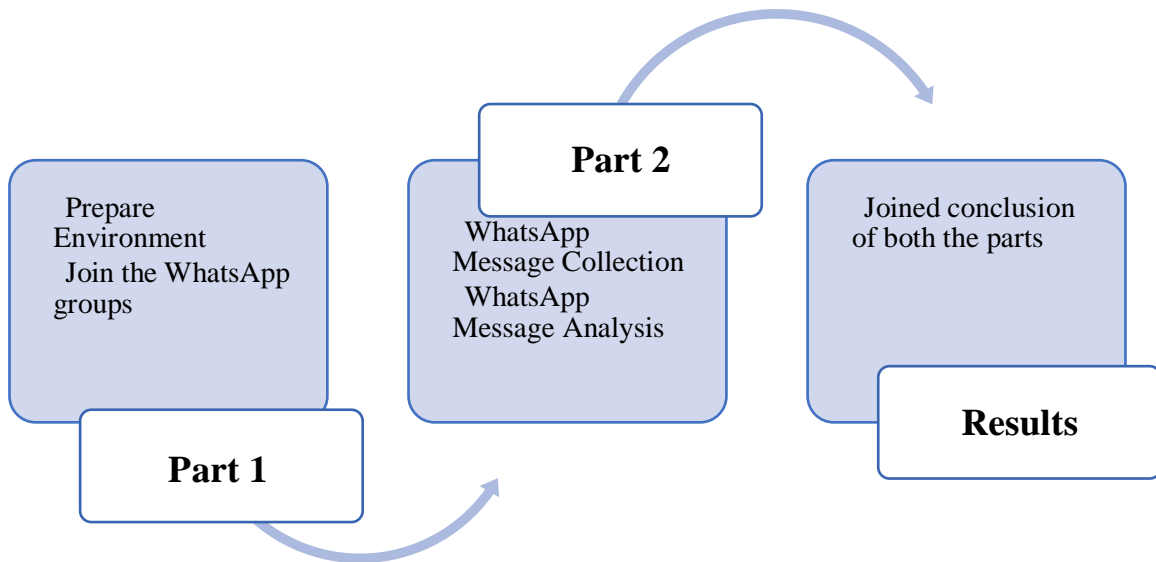


Figure 6.1 Research methodology structure

In the First part, we will set up the legitimate environment to lure the political parties to add our honeypots into the political groups to prove a political connection between other social media and WhatsApp. Then in the second part, we will collect the messages circulating in the public WhatsApp groups and analysis these messages based on different parameter.

Each phase of the research methodology is based on the results of the previous step so the synchronization between the phases is important and the result of the previous step should be correct, so next step will not produce a wrong result. The brief summary of all the step is given below.

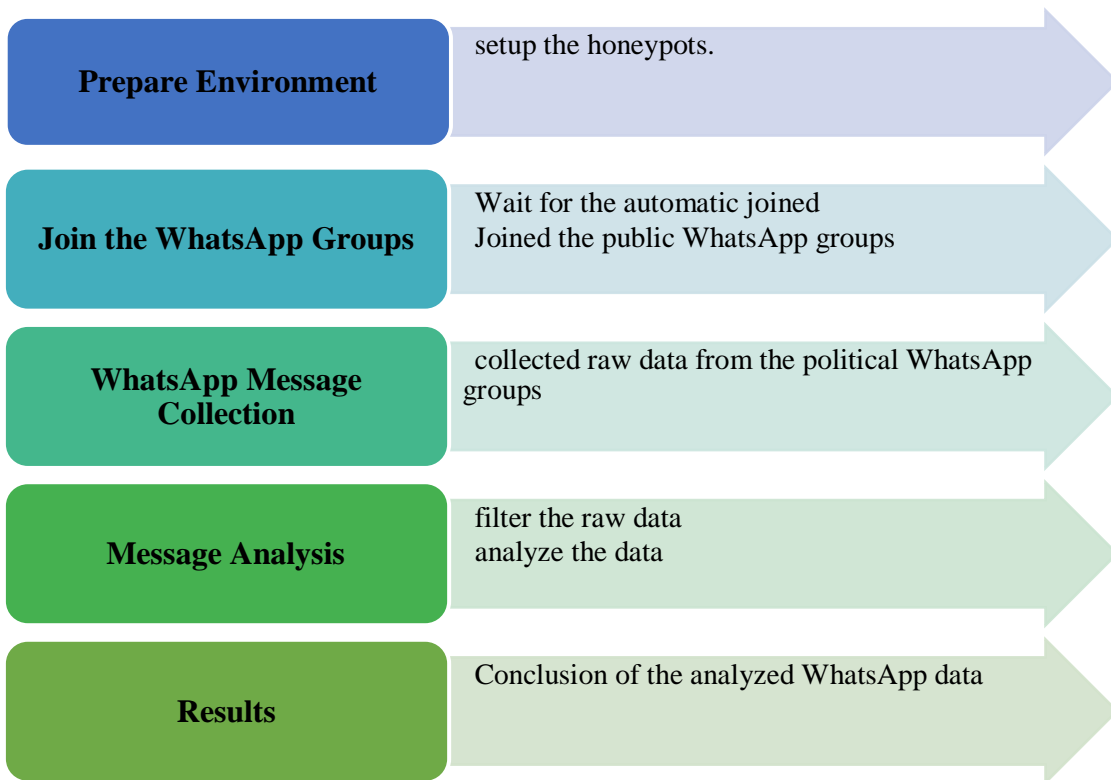


Figure 6.2 Phases of Research methodology

6.1 Part – 1

Part-1 is further divided into two sub-parts to prepare the environment so we can reach to the political parties and they will add our WhatsApp account into the political groups and then gathered the data for WhatsApp message analysis.

In this section, we will set up the honeypots so political parties can add our honeypot profiles into their political WhatsApp accounts. The idea behind this approach is that if political parties will add our profiles into their political WhatsApp groups or if our accounts will be added automatically to the political WhatsApp groups then we will conclude that political parties are adding voters to political groups without their concern. As we know WhatsApp account need authentication with the phone number so if our honeypots are added into some political group(s) then that depicts that political parties are getting the voters mobile number. WhatsApp groups. A question arises from where they are getting the voters' mobile number to add them to the WhatsApp groups. We have already mentioned the possible answers to this question in the introduction. Out of all the possible platforms, for our study, we are researching on the popular social media platforms to see how they are interconnected and linked together in the context of

politics? How political parties are using the complex network of the social media platforms to connect with the voters on WhatsApp. To get the political messages we will use the two most popular social media sites in India, which helped the BJP in 2014 to win the election as mention in chapter 2. One is Facebook, a networking social media site, and another is Twitter, a microblogging social media platform.

As mention above we are considering only two main national political parties, Congress (INC) and BJP. Thus, we have set up two independent environments for both the parties so we can get the proper independent data from both parties.

6.2 Honeypots

According to the Technopedia, “honeypot is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the internet.”¹

In our term honeypots would be those social media accounts, purposely created to trap those social media users, who are spreading the cyber propaganda, spam messages, suspicious links on WhatsApp messenger and also those political supporters who are purposely sending bulky, suspicious messages to other users. We have created the two WhatsApp honeypots to attract those political WhatsApp users who are targeting the voters on the WhatsApp messaging platform.

6.2.1 Set up WhatsApp account

we will create the two different WhatsApp accounts which are our honeypots, one for each political party. Both the WhatsApp accounts are independent and have no contact or common ground of connection. The process of how we set up our both honeypots is shown below.

¹ <https://www.techopedia.com/definition/10278/honeypot>

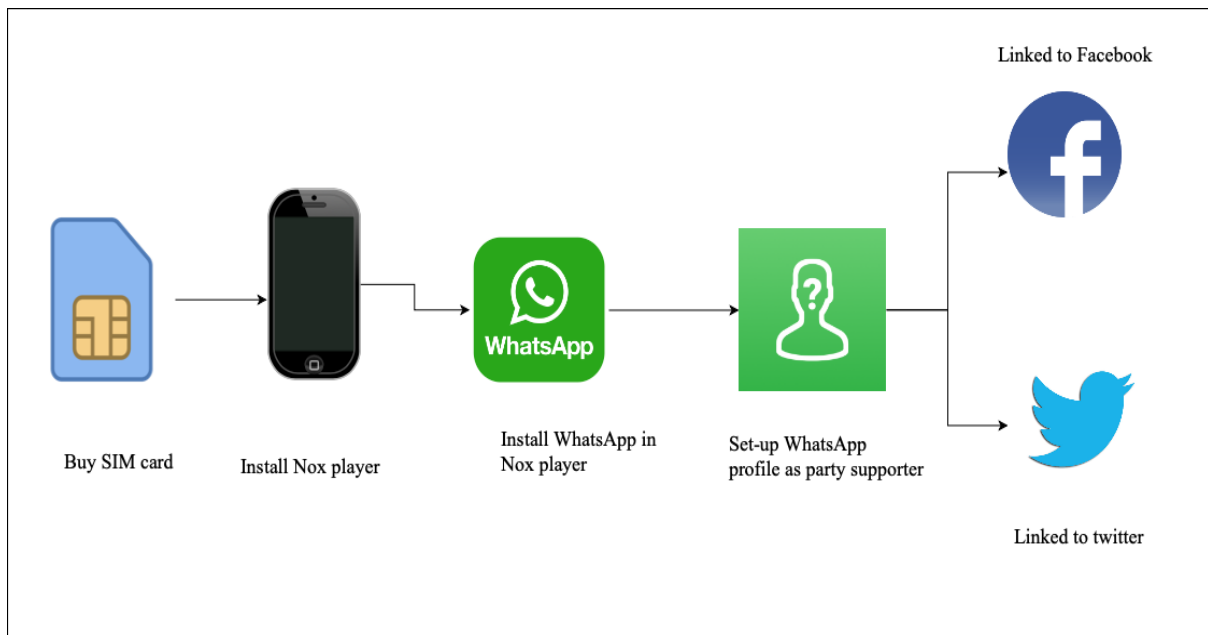


Figure 6.3 Methodology for setting up WhatsApp honeypot profile

Step 1 - An active mobile number is required to create the WhatsApp account. Hence, we bought two new mobile numbers from two different telecom providers. One Mobile number is bought from Airtel mobile provider and another is from Jio (reliance telecom). The purpose of buying a mobile number from two different telecom provider is to avoid any common connection between both honeypots.

Step 2 - WhatsApp application needs a suitable Operating System to run the application. Android running OS 4.0.3+, iPhone running iOS 8+, Windows Phone 8.1+, a phone running kaiOS 2.5.1+, including Jio Phone and Jio Phone 2, all these devices are supported by the WhatsApp¹. To run the WhatsApp application, we have selected the Nox App Player virtual Android environment. Nox App Player is a free Android Operating System emulator application, it supports the Google application from google play store and games. We run "Nox App Player" on top of macOS for both the honeypots

Step 3 - We will install WhatsApp messenger Application on Nox Player from google play store.

¹ <https://faq.whatsapp.com/en/android/26000006/>

Step 4 - After installing the proper WhatsApp application in Nox player we use the mobile number we bought from Indian telecom operators to set up the WhatsApp honeypots' profiles. We set up different WhatsApp profile for both the WhatsApp honeypots.

6.2.1.1 Honeypot 1 (Sandeep Jain)

1st WhatsApp honeypot is in support of the BJP governments. The profile name is Sandeep Jain, we used Airtel Mobile number for this profile and uploaded the picture of the current PM as a profile picture.

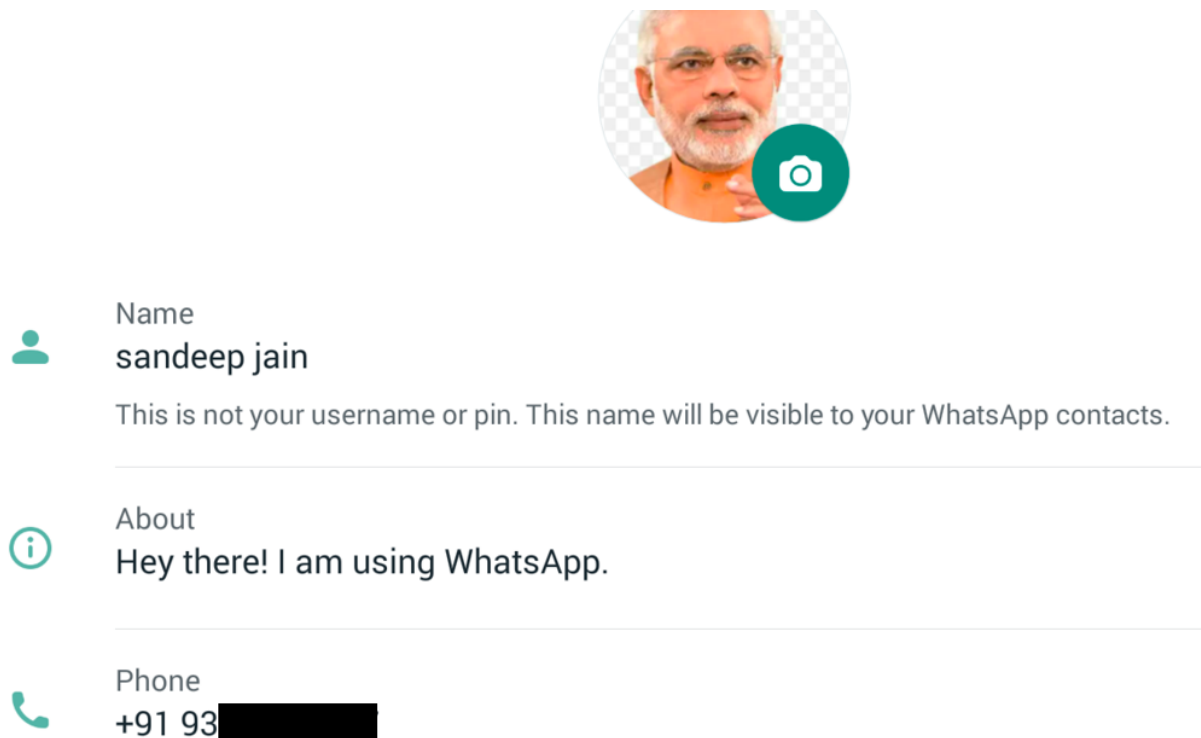


Figure 6.4 Sandeep Jain WhatsApp profile

6.2.1.2 Honeypot 2 (Sikander Khan)

Our 2nd WhatsApp profile is as congress supporter. Name of the profile is Sikander Khan and we did not add any profile picture to this honeypot. We used Jio telecom for this account.

Further we will use these WhatsApp profiles (honeypots) to setup and interlinked with Facebook and twitter accounts.

6.2.2 Set up Facebook profiles

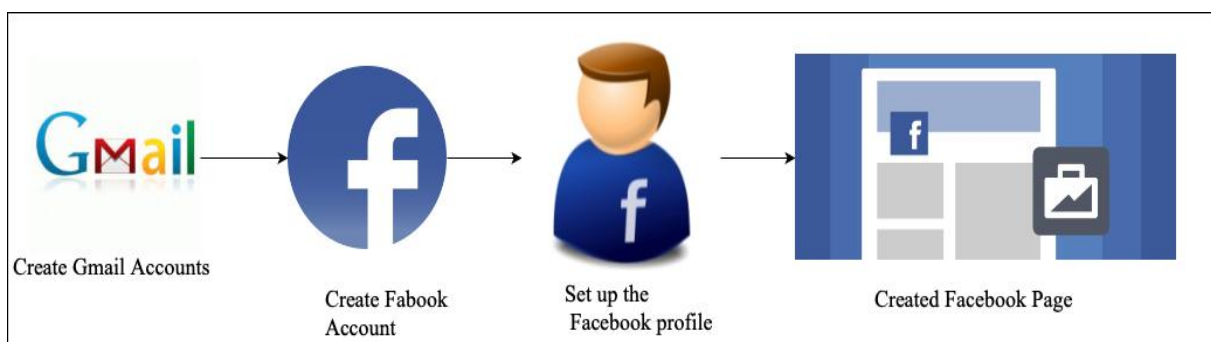


Figure 6.5 Methodology for the Facebook account

Step 1 - We created two Gmail accounts and used these Gmail accounts to create the interlinked Facebook profiles. The reason we used Gmail is, both mobile numbers are from Indian telecoms. It seemed good reason to use the Email over phone number so if future complication arises to mobile number then it won't affect the Facebook profiles and our research.

Step 2 - We used the Gmail accounts to create the Facebook account. For both the honeypots we used the separate Gmail accounts.

Step 3 - We Set-up the Facebook profile same as the WhatsApp profile.

6.2.2.1 Sandeep Jain

This profile is in the support of the BJP, so we set-up same account name as WhatsApp account (Sandeep Jain). We have also uploaded same BJP leader's picture as WhatsApp profile picture. Linked Sandeep Jain Honeypot mobile number to the profile and also Linked the Twitter profiles

Activities – We send Facebook friend request to BJP politicians, party members and workers like – Narendra Modi, Amit shah and their public friends. We will also like Facebook pages like – “I support Narendra Modi”, “BJP India”, “Bjp Itcell Ratlam”, “BJP Rajasthan”, “Bhartiya Janta Party” and so on.

6.2.2.2 Sikander Khan

We used the information from Sikander khan WhatsApp honeypot to set-up linked Facebook profile, named Sikander Khan. We added the mobile number we used for

Sikander Khan's WhatsApp account also we uploaded the Congress president Rahul Gandhi's profile picture to the Facebook profile. We have also added the related twitter profile's link (we will create next) to this account.

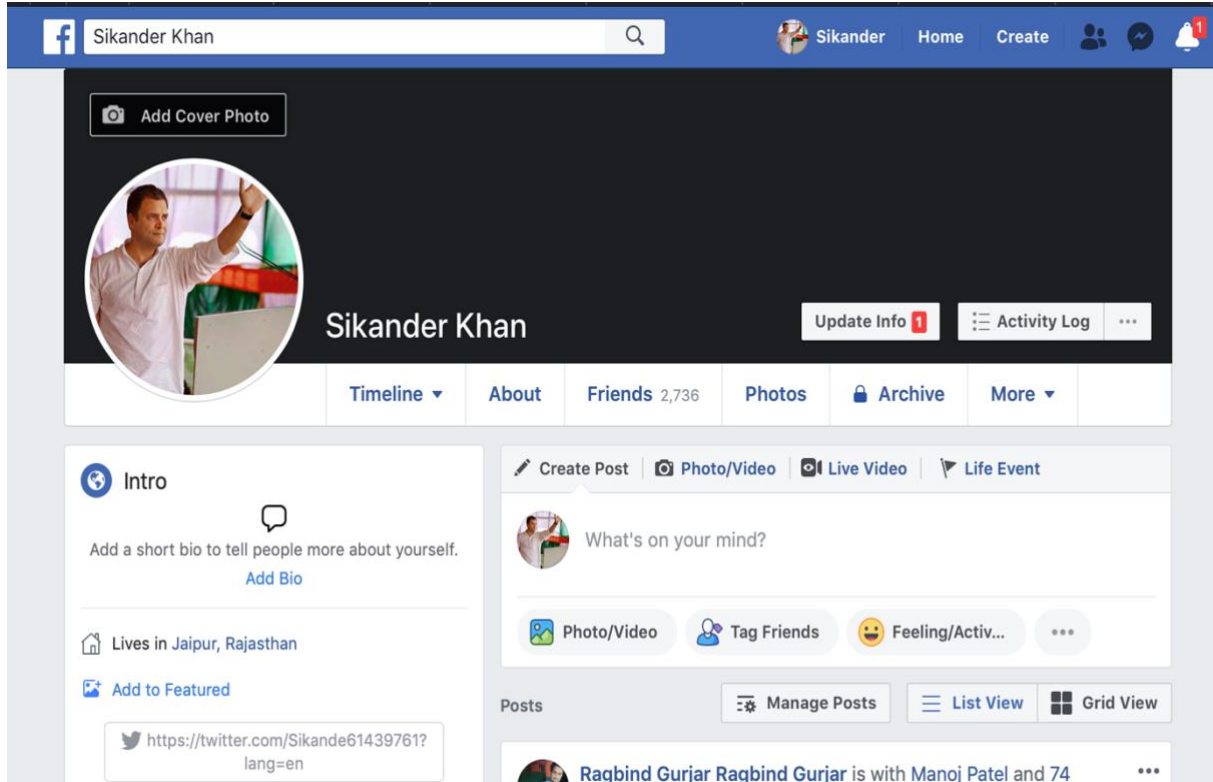


Figure 6.6 Sikander Khan profile

Activity – we have connected with 2,736 Facebook friends, by sending and accepting the Facebook friend requests. We followed 109 Facebook profiles which support the congress. We also joined 18 groups and we liked 82 public Facebook from this profile. like – “I support Rahul Gandhi”, “Indian National congress”, “Priyanka Gandhi”, “Congress It Cell kota Dehat”, “It Cell INC Bharatpur Rajasthan”.

Step 4. After setting up profiles as BJP and congress supporter on Facebook account we also created a Facebook page from both the accounts as a party supporter. From Sandeep Jain we added a “Narendra Modi 2019” page. And from Sikander Khan account we created “Rahul Gandhi 2019”. On both the account we have added the connected mobile numbers and made them public.

6.2.3 Twitter Profiles

Another important social media platform. Twitter known as microblogging social media account. In India twitter is popular among politicians. All the higher political leaders have teams to who handles their social media accounts but some of the politicians handles twitter by themselves which shows the importance of the twitter platform in India. A continuation of Tweet and Retweet make this platform famous, and also a trend of #tag is become popular from twitter platform. We have created two twitter accounts connected with each WhatsApp honeypots.

6.2.3.1 Sandeep Jain

We have created the twitter accounts for honeypot 1(Sandeep Jain) which has the same name, mobile number as the WhatsApp honeypot. This profile is linked with facebook profile as well.

6.2.3.2 Sikander Khan

This twitter account was same as the Sikander khan WhatsApp and Facebook profile. We used same information we used to create the Facebook account and linked with the Sikander khan Facebook profile and WhatsApp honeypot.

In overall to reach to the research question we created 2 different profiles to target to two different political parties we used 4 different social accounts (Gmail, WhatsApp, Facebook, twitter). And the we connected all the social media profile using the phone number so honeypot can trap the political parties' WhatsApp groups and it can gather the sufficient information from the users.

6.3 Joining the WhatsApp Group

After setting up our all the social media connection and profiles, the next challenge is to get inside the political WhatsApp accounts. WhatsApp has end-to-end encryption policy so only sender and receiver can decrypt the conversation. A third-parties including WhatsApp are not able to read or decrypt the messages without being a part of the groups. Hence it was needed to be the part of the political WhatsApp groups to read and gathered the messages for analyzing purpose.

To join the political WhatsApp groups, we worked on two options. First to use already settled honeypot and another way to use the WhatsApp group invitation links.

6.3.1 Honeypot Data

In previous sections, we linked WhatsApp profile with Facebook and twitter profiles to see whether political parties are using other social media platforms to send the targeted message on WhatsApp or not. According to assumption if our honeypot will expose enough and it will reach to those political Facebook profiles which are scrapping the Facebook user's data and adding their WhatsApp number to the political WhatsApp groups, if everything will go in right direction then our honeypot will be automatically added into the political WhatsApp groups. use the messages posting in these political groups. The problem encountered when we have to wait until any political parties will notice the honeypot and add it into groups. And another problem was with confirmation because it could be only possible if political parties will are doing this and using Facebook to add voters into the political groups.

6.3.2 Public Group invitation links

To answer the question related to the use of honeypot for joining the WhatsApp groups we have used the other methods. Waiting problem could be solved by using the group invitation links to join the WhatsApp groups. WhatsApp Groups invitation links are the direct public links which are mostly used to invite the other users to join a certain group. These links are the open links so other user can use the groups without any permission. Also, WhatsApp group invitation links is shared among the user so by using that links and accepting the term and condition a user can be a member of the group and he/she can receive the groups messages. This method also has a problem to get the groups invitation links.

6.3.3 Collecting public group invitation links

The issue with group invitation link was to get these links.

6.3.3.1 Facebook Search Engine –

To get the publicly available political WhatsApp group links we have used Facebook search engine. We have noticed that both the parties have Facebook profiles to motivate

users to join the party's WhatsApp groups. On congress we have found Facebook profile "WhatsApp Congress" whereas BJP also has a Facebook page for WhatsApp users, named "BJP WhatsApp Group" and "WhatsApp channel of BJP MP". Have joined one of the congress group "lol" using the link available on the Facebook page.



A background picture of Facebook page Taken from "WhatsApp congress" Facebook page

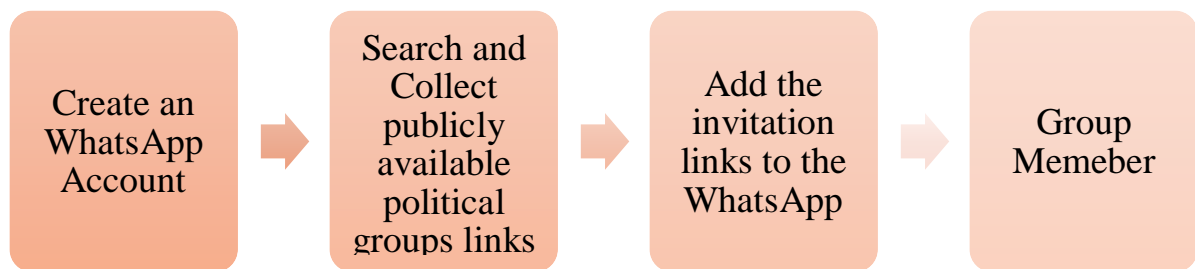


Figure 6.7 Methodology to collect WhatsApp group invitation links

6.3.3.2 Google Search Engine

We used the google search engine to search for the political WhatsApp group links. We found webpages with the links of political WhatsApp groups. We have found almost 100+ WhatsApp invitation links of BJP groups and 65 invitation links of the congress supporter groups. All the links were given on webpages were not correct or active but most of links were real political group's links.

We used Facebook and google search engines to search for the political WhatsApp group links. We made the list of the publicly available WhatsApp groups of both the political

parties. We joined the WhatsApp groups using invitation links from Sandeep Jain's (honeypot 1) WhatsApp account and we waited for the honeypot's automatic response on Sikander khan (honeypot 2) WhatsApp account.

7 Data Collection

Second part of methodology is based on the approach we are using to collect and analysis of the message content spreading on the political WhatsApp groups.

7.1 WhatsApp Message Collection

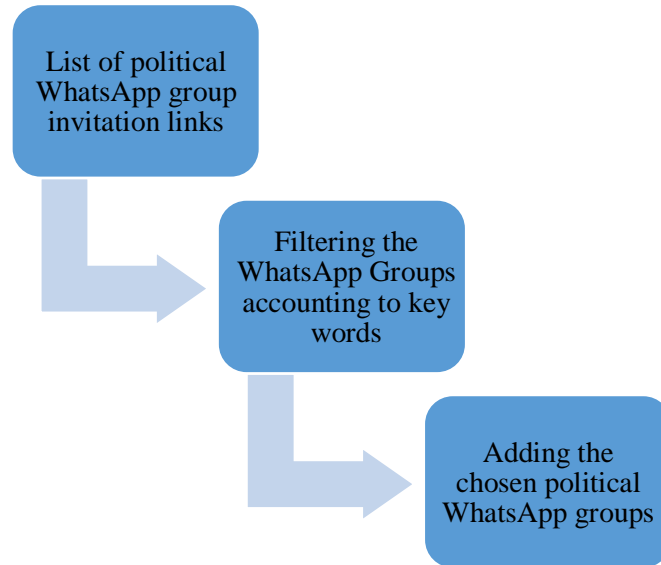


Figure 7.1 Process to collect the WhatsApp Messages

Step 1 – To join the political WhatsApp groups we used list of WhatsApp invitation links that we collected from different platforms to join the political WhatsApp groups. We added Sandeep Jain WhatsApp profile to these political WhatsApp groups.

Ste 2 – Filtering the WhatsApp groups from 100+ BJP and 70+ congress WhatsApp invitation links we have joined 63 groups. We chose the groups based on their name. If the name of the group has keywords like - ‘BJP’, ‘Bhartiya Janta Party’, ‘Narendra modi’, ‘Namo’, ‘Congress’, ‘Rahul gandhi’, ‘Priyanka gandhi’, ‘Chowkidar’, ‘Pappu’, ‘Feku’ which are related to politics than we joined the group. If the group names are not related to political parties or based on other topics like – “जन जीव कल्याण सेवा जोधपुर”, “हिंदू युवा शक्ति (चौक)”, “हम पंछी उन्मुक्त गगन के”, ”जय हो राजद”, ”खबरे ही खबरे” then we didn’t join these groups. Though just to see what WhatsApp messages they are spreading we joined the “online best income”, ” वन्दे मातरम🇮🇳🇮🇳🇮🇳🇮🇳”, “Pawjel”, ”Digital Indian 🇮🇳🇮🇳”, “ Govt jobs guru(32)”, “Indian army Fan” WhatsApp groups.

7.2 WhatsApp Group Data

After filtering we have decided to go with 63 WhatsApp groups. Out of 63,17 WhatsApp group's names were not directly related political parties but the posts they shared were political posts and messages. 3 WhatsApp groups were direct congress groups and 43 groups were in direct support of the BJP.

We Started to join the groups from 23, February 2019 and started to collect the posts and messages from political WhatsApp groups.

7.2.1 Messages

Message is the last part of the row and it could be a single line or numbers of lines. Message started after the : symbol till the end of the message.

7.2.2 Types of Messages

A message can be a text message, or it can be a media message. short text message, long text message, text message with the links and only links considered as the text messages while pictures, videos, audios, documents considered as the media messages.

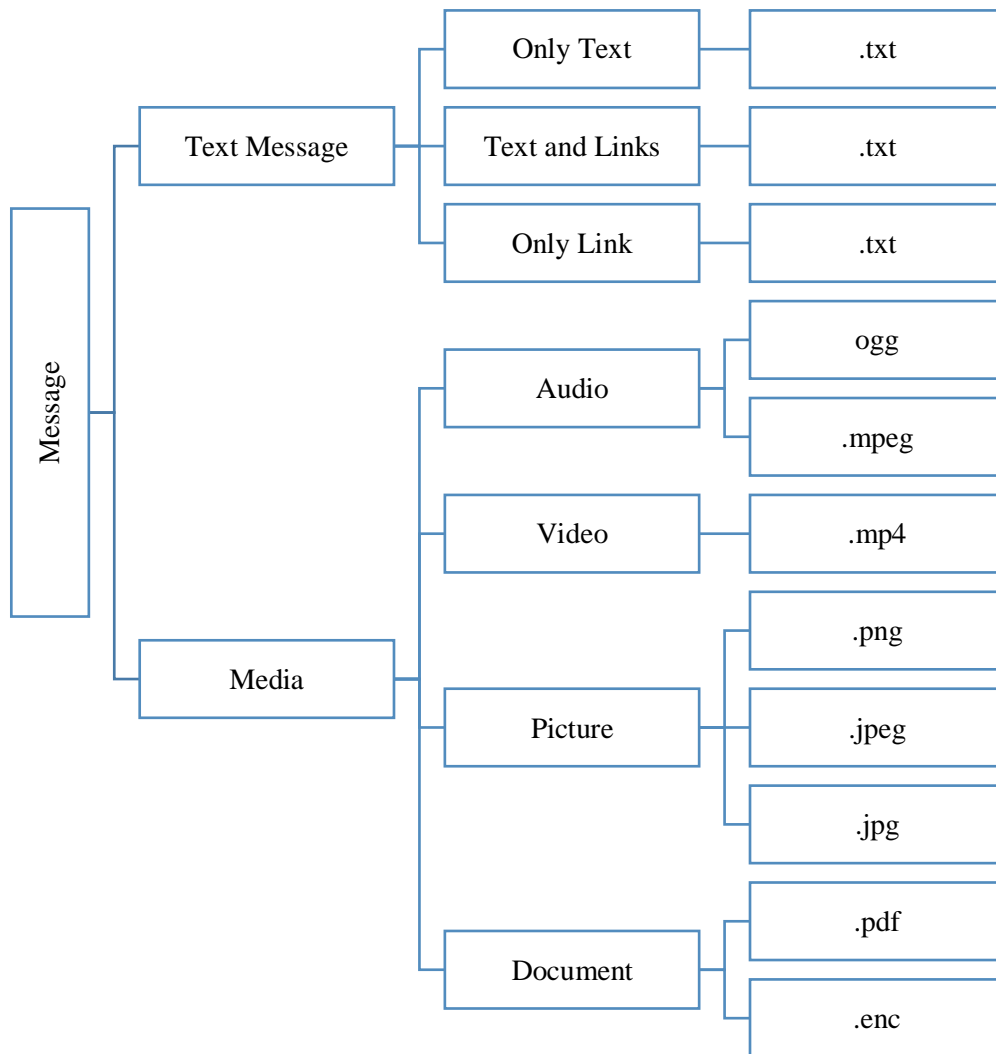


Figure 7.2 Category of WhatsApp Messages

In exported .txt file the text messages and links are within the files. But the media messages are included explicitly and in .txt file a sentence is written on the place of media. ‘.txt’ file has two sentences for the media message. One sentence for the picture messages and other messages is for the Audio/Video/Documents messages.

Picture - <Media Omitted>

Videos/ Audios/ Documents – file name (file attached)

8 Challenges

After setting up the experiment, we have faced a few challenges from Facebook and WhatsApp to proceed further for the results and analysis. Facebook, WhatsApp, and Twitter actively working on stopping the fake accounts in India, especially during the elections. To make the platform safe they are blocking accounts which are suspicious and violating the terms and conditions

8.1 Challenge 1 (Facebook)

We have created the Sandeep Jain, Sikander Khan Facebook profile on Dec 7, 2018, and uses the profile as an active user. We actively used these accounts for connecting to the other political Facebook members. After more than 30 days, we speed up the activity by adding the political page to both accounts also we increased the number to join the political groups and so forth, in a day we started to get 200+ friend requests from political party supporters like voters and workers as well as non-political profiles. We accepted only those profiles which were posting political content also the profile which shows the users belief or connection with the politics.

After a few days later being overly active on Facebook from both the Facebook profile, we have got an error message while we tried to log in to Sandeep Jain Facebook account saying that Please **“upload a photo of yourself which clearly shows your face”**. After a few days later of being locked out from Sandeep Jain's profile, we also locked out from Sikander Khan Facebook profile. Both the accounts were showing the same error message. We have used the same method to unblock the account for both profiles (picture is taken from Sandeep Jain's Facebook account)

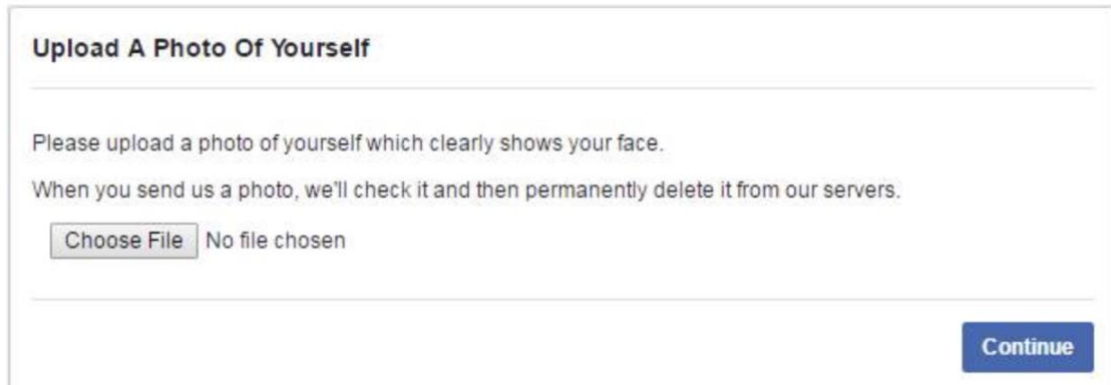


Figure 8.1 Notification showed on Sandeep Jain's Facebook account

8.1.1 Sandeep Jain

For Sandeep Jain, we have used the Google search engine to search for the Prime Minister Narendra Modi' picture. And as mentioned in the messages we chose one picture from search engine and uploaded that picture for the Facebook review.

Facebook Review – After a few days when we logged in again to check the status of the Sandeep Jain profile we have got another message displaying on the profile. Your Account Has Been Disabled. (picture from Sandeep Jain's account)

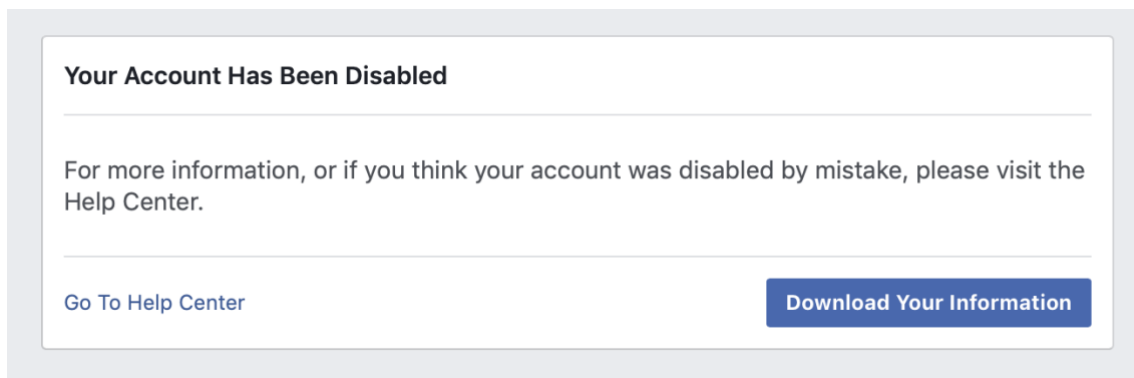


Figure 8.2 Notification on the Sandeep Jain's Facebook profile

We have investigated further, and we found the reasons why Facebook blocked the account. Reasons are written in the picture below. (picture from Sandeep Jain's account)

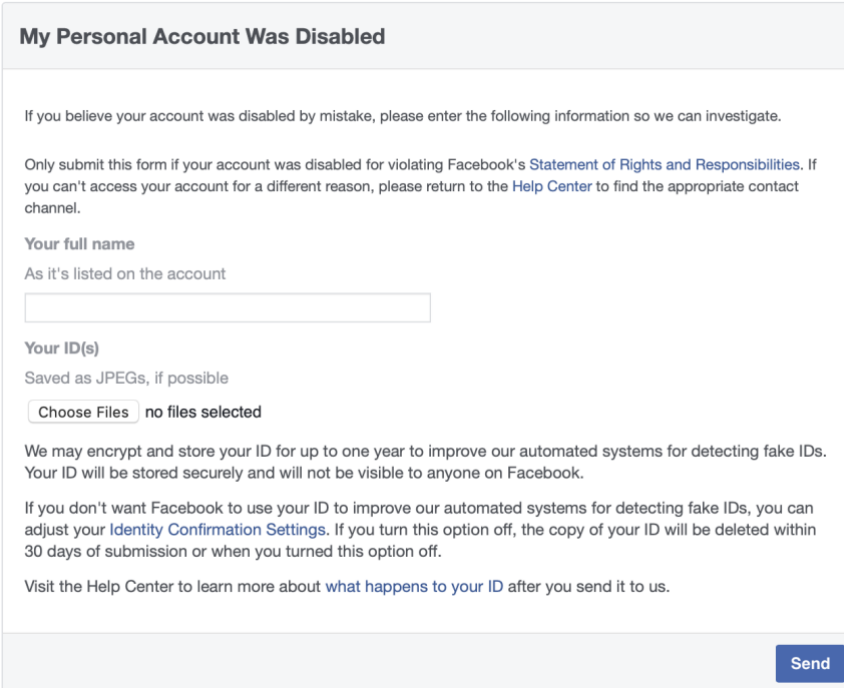
Why is my account disabled?

We disable Facebook accounts that don't follow the [Facebook Terms](#). Some examples include:

- Posting content that doesn't follow the Facebook Terms.
- Using a fake name.
- Impersonating someone.
- Continuing behavior that's not allowed on Facebook by violating our Community Standards.
- Contacting other people for the purpose of harassment, advertising, promoting, or other conduct that's not allowed.

Figure 8.3 Terms and condition for Facebook user taken from Sandeep Jain Facebook account

We have concluded that it is possible that Facebook has marked our profile under "**using a fake name**" or "**maybe impersonating someone**". We proceeded for a request form to unblock the accounts. In the form, Facebook asked for the personnel id and full name and then we stopped the unblocking process at this step. (picture is taken from Sandeep Jain's Facebook account)



My Personal Account Was Disabled

If you believe your account was disabled by mistake, please enter the following information so we can investigate.

Only submit this form if your account was disabled for violating Facebook's [Statement of Rights and Responsibilities](#). If you can't access your account for a different reason, please return to the [Help Center](#) to find the appropriate contact channel.

Your full name
As it's listed on the account

Your ID(s)
Saved as JPEGs, if possible

no files selected

We may encrypt and store your ID for up to one year to improve our automated systems for detecting fake IDs. Your ID will be stored securely and will not be visible to anyone on Facebook.

If you don't want Facebook to use your ID to improve our automated systems for detecting fake IDs, you can adjust your [Identity Confirmation Settings](#). If you turn this option off, the copy of your ID will be deleted within 30 days of submission or when you turned this option off.

Visit the [Help Center](#) to learn more about [what happens to your ID](#) after you send it to us.

Figure 8.4 Facebook requesting form to unblock the Facebook profile

8.1.2 Sikander Khan (Facebook Profile)

To unblock the Sikander Khan Facebook profile we uploaded the Congress president Rahul Gandhi's picture which we found from the Google search engine.

Facebook Review – after reviewing the picture and account, Facebook unblocked the Sikander Khan Facebook profile in a week and we were able to login into the account and we continue to be active with the Sikander Khan profile.

8.2 Challenge 2 (WhatsApp)

WhatsApp also working on disabling the fake accounts. It is blocking the accounts which were not using the official WhatsApp's application to using the WhatsApp services and the account which are violating the WhatsApp term and conditions. We created the Sandeep Jain WhatsApp account by installing the WhatsApp application from the Google Play Store in the Nox App Player. For Sikander Khan WhatsApp account we have installed the dual app player and we copied the WhatsApp account in the dual app player and created the Sikander Khan profile. After approx 15 days of creating the account, we have locked out of the account and got an error message "**Your Phone Number +91 6375 XXX XXX is banned from using WhatsApp. Contact Support for Help.**"

Solution – We have sent a descriptive email to support@support.whatsapp.com and requested to re-enable the WhatsApp account. A few days later they replied with the possible reasons why WhatsApp disabled the account and WhatsApp again activated the account. Though after the account was active again it has a problem with logging in. Request for further issues is still in the queue on support@support.whatsapp.com.

8.2.1 Challenge 3 (Collecting Data)

After Sandeep Jain Facebook account was permanently blocked it was hard to reach to the BJP political Facebook pages and publish the phone number attached with the Sandeep Jain honeypot. The mobile number linked to Sandeep Jain was also blocked by Facebook so we were not able to create another Facebook profile with the Sandeep Jain WhatsApp number and hence it became hazardous to collect the data from BJP Facebook page.

Solution – To set up the new honeypot was not feasible because of the lack of the time and to collect the proper data from the different political groups was a big challenge hence we have joined the publicly available WhatsApp groups for analysis purposes. we have

used the public search engine as mentioned in the Methodology, part-2 for invitation links to join the public political WhatsApp groups.

8.3 Data Analysis

We have observed the 63 WhatsApp Groups from 23, February 2019 to 7, April 2019 for almost 43 days we collected the medias and messages circulating in all the groups. To analyze what type of messages and content group members are posting in the political WhatsApp groups it is important to have the WhatsApp groups chat and proper data scrapper from that chat and hence we have followed the following process cycle for analyzing the message data.

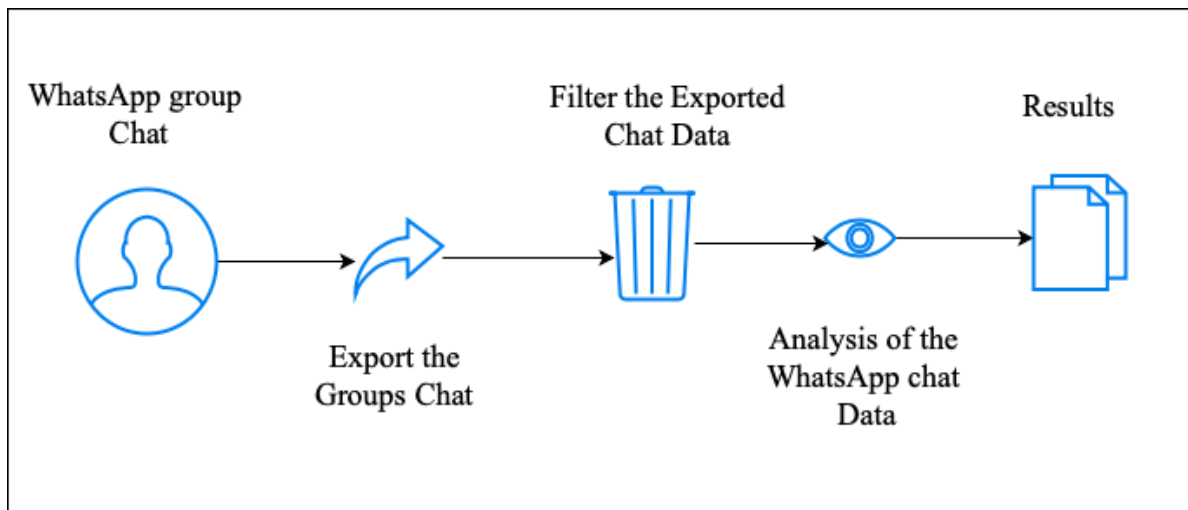


Figure 8.5 Methodology for WhatsApp message analysis

8.3.1 Step 1 (WhatsApp Group Chat)

We had 63 WhatsApp groups but for proper analyses we have chosen only those accounts which were active. We have found that some of groups didn't have any message, and some have only few messages. We have considered only those groups as active who have at least 20 messages for 43 days. We have also not considered those groups which are posting the non-political messages but the groups which have minimum 10 political messages for 43 days we considered those groups as political groups and included the all messages into messages analysis.

8.3.2 Step 2 (Export the group Chat)

After applying filter on 63 groups we have filtered 32 WhatsApp groups chat which were active groups and circulating political messages.



Figure 8.6 Process of exporting the WhatsApp group data

For exporting the 32 chats we used the WhatsApp's export chat options. We run WhatsApp messenger in Nox App Player so forth we only an option to export the chat in .txt format. We chose to export the group chat with the media this option used export the media as audio, pictures, videos, attached file posted in the group. We sent exported .txt group chat files with media to another independent personnel WhatsApp account.

We downloaded all the 32 WhatsApp .txt files and the attached media from the personnel WhatsApp account and saved them for the future analysis. The exported .txt chat file has a structured data with the information about each message posted in the group. This .txt file includes the information's like – date and time when message was sent, phone number of the sender and the message sent by the user.

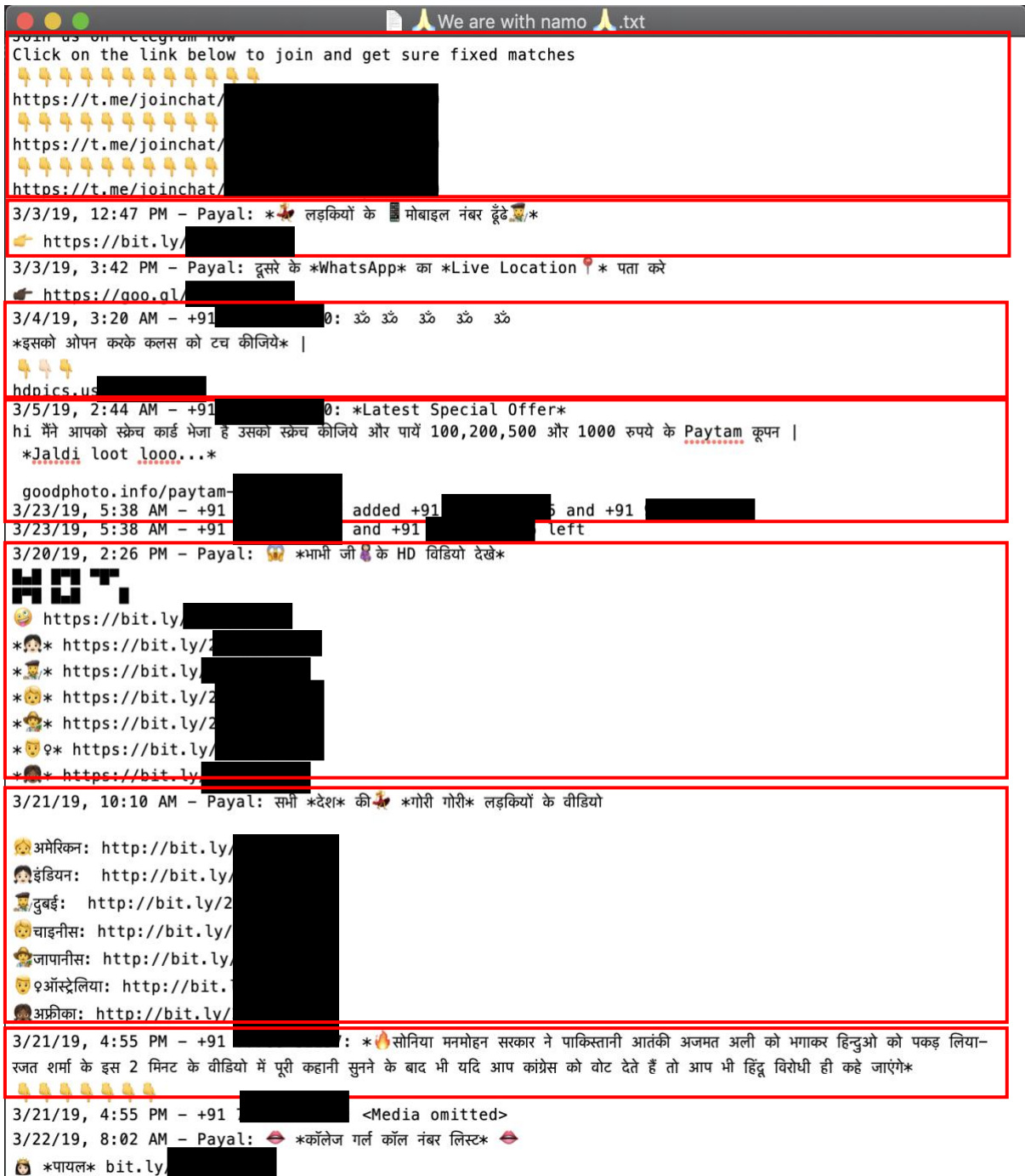


Figure 8.7 Example of exported .txt WhatsApp group chat for Sandeep Jain WhatsApp profile

Date – each new message start with the date in dd/mm/yy format and at the end it has ‘,’ delimiter.

Time – Time is separate by the , and - delimiter. Time is in the HH:MM and 12 hours clock format. The time is followed with AM/PM.

Phone Number – After time phone numbers is in between + and :. Mobile number has three parts. 1st part of mobile number is country code which is followed by +sign, Second part is the National destination code (NDC) and last part is a subscriber number (SN)¹.

8.3.3 Step 3 (Filter the Exported Chat data)

Data filtration is a process where important and useful data is filtered from the raw data. Data filtration gives the proper data without outlier. Data filtration can be done by removing the unnecessary data which can further cause the wrong analysis or by taking out the important data from the raw data. It is good practice to filter the data as required from the raw data, so system will not use the resource and time for the unnecessary data. For analysis filter data gives more accurate results than the raw data and it take less time to analyse the data.

For this research, it is required to process and filter the exported .txt file and only work with the important and necessary data. A general approach used for data filtration process for this research is shown in figure below.

¹ <https://www.cm.com/blog/how-to-format-international-telephone-numbers/>

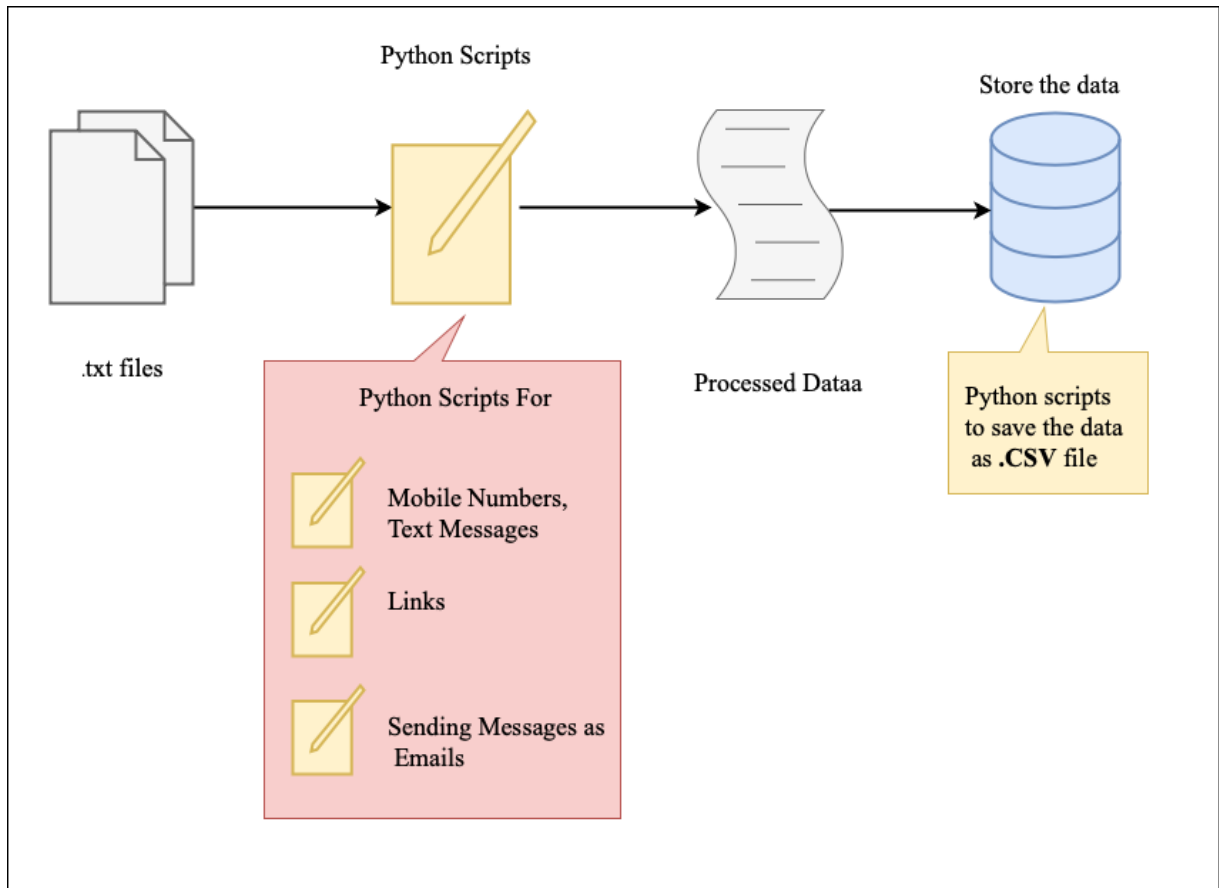


Figure 8.8 Method to filter the raw WhatsApp exported file

Step 1 (.txt files)

The raw .txt file a WhatsApp group chat file needed filtration so processed data can be used for the further analysis. As explained in step 2 exported .txt group chat file has date, time, phone numbers and messages. For further analysis we needed the following data.

Mobile Numbers - Mobile number to see how many common people are in the 57 groups? and what they are spreading in the groups? It also gave a number how many users are political or social advertisements bots and only sending the Political or advertisements in the groups.

Text messages – Text message which is the main part of this study we needed to collect the all text messages and analysis them whether they are spam message or not, the messages are fake or not and how does they effect the other members.

Links – Most of the text messages has links. Some active groups have over 100+ links. Text message with links says, “click on the link”. For the further analysis of the links

whether they are legitimate and directing to the said address or they are suspicious, link filtering is also required.

Step 2 (Python Scripts)

Python is object-oriented, high-level programming language use for the Application Development as well as for the scripting. We have used Jupiter notebook to write the python scripts for extracting the data from the .txt files. We wrote three different scripts and then combine them together.

Script 1 – 1st python script we wrote to extract the mobile phone numbers and text messages from the .txt file. As input, we gave the extract text .txt file from WhatsApp groups. In results we got two a list with two columns. First columns were to save the phone number and second column to save the text messages sent by the same phone numbers.

Script 2 - 2nd script we wrote to extract the links included in the text messages. To extract the links, we gave 2nd column of the list we got from script 1 as a input and in result it extracted all the links which were included with the messages.

Script 3 – This script we used to send each text message we extracted using the script 1 as a email to the sj7469620@gmail.com and to the cristinarimi1234@gmail.com. As a sender we used three different email address, because Gmail allows only 550 Email/day.

8.3.4 Step 4 (Processed Data)

After running the first two scripts we got the phone numbers, text messages and links which used as processed and filtered data.

8.3.5 Step 5 (Store the Data)

We used another python script, script 4 to save the processed data list created by script 1 in .CSV format in the device.

8.4 WhatsApp Group Data Analysis

The final and most important part of this research is political group chat analysis. We have gathered the WhatsApp group messages for 43 days. We filter the raw data and used

processed data for analyses. From .txt file we have filter the gathered two types of data, messages sent by the group members and links included in the groups. Apart from the .txt file we also exported the media included in the group chat. As we have three different types of data hence, we have used three different approaches for each data type to analyze the data.

8.4.1 Text Messages Analysis

The purpose of the Political groups is to connect the voters and publishes the political advertisements in the groups also to talk and discuss on the political issues so in political groups numbers of political messages being posted by the group members. To analyses what exactly the group members are posting in the political groups. Are they only posting the political messages? or group members are using the political WhatsApp groups to spread the spams and virus.

To categories the messages into spam or genuine we have used the Gmail Spam filter. Gmail spam filter is used to detect the spam Emails. It can detect the suspicious and spam Emails. Gmail spam filter uses the blacklist to check whether Email has any blocked or reported IP addresses or linked, if it finds any blacklist address it marked the email as the spam and show a spam warning to the users or else it will place the Email into the inbox.

We have used the Sandeep Jain's (Honeypot 1) Gmail address as a main recipient address and also Cristina Rimi's address as a secondary Email address. As a sender we have used the 3 different account because of exceeding daily quota. We have used the sikanderkhan, cristinarimi1234 and alpeshearora's Gmail accounts to send the messages.

To send the political messages as Email we wrote the python scripts which take the list of messages as input and then take every message and add that message to the smtp message body and added subject as group name + id numbers so it would be easy to check how many messages were sent by the script and how many reached to the recipient.

The details methodology to scrutinizing the WhatsApp messages are explained below:

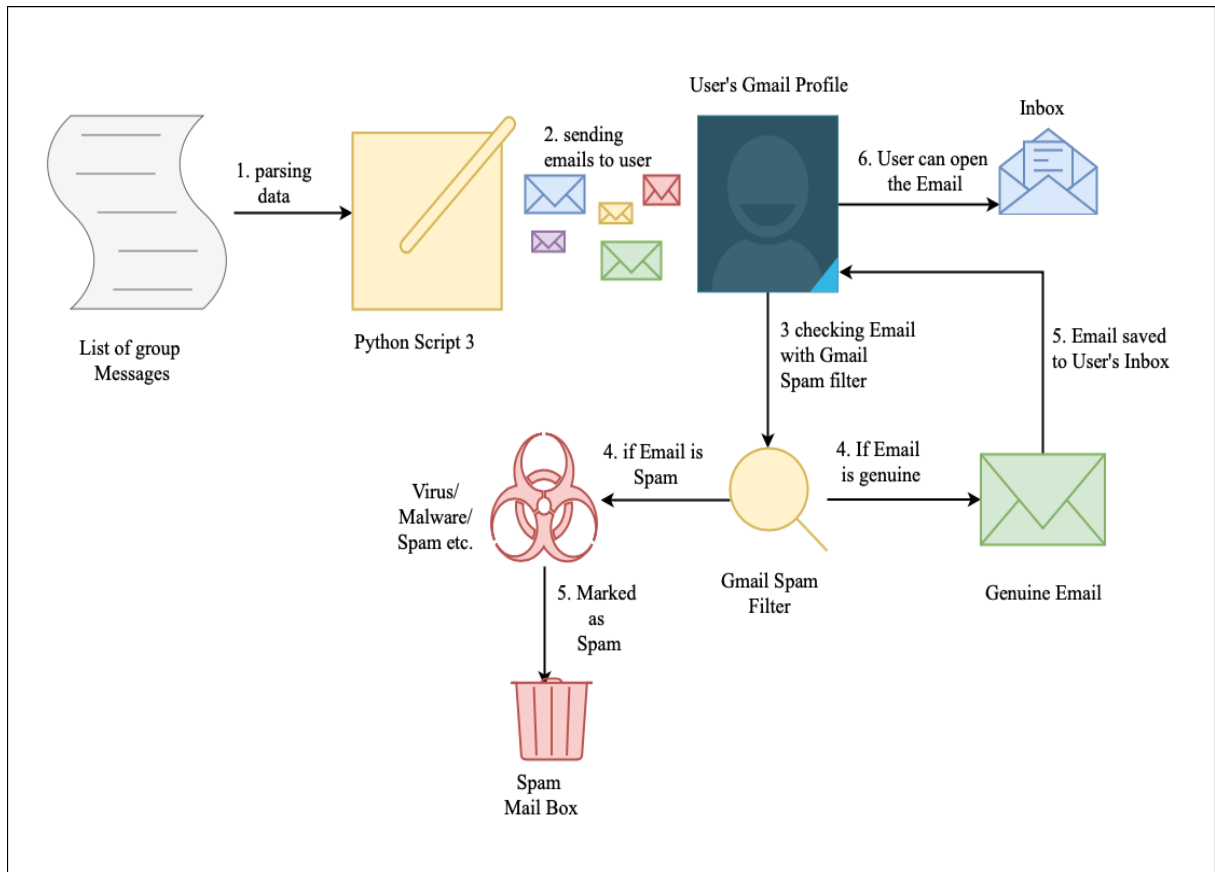


Figure 8.9 Process for text message analysis

Step 1 – We have used the list of group messages generated by the script 1 during the filtering process

Step 2 – Then we used the python script 3 to send each message from message list to the Users Gmail Profile.

Step 3 – Send Gmail has inbuild spam filter which can categories the Email as spam or not spam. If Email has malicious content, then Gmail marked the Email as the Spam messages and if the Email seems legitimate than Gmail marked as safe and put in the Inbox.

Step 4 – Categories the Email as marked email as the spam or not spam. (picture is taken from the Sandeep Jain Gmail's account)

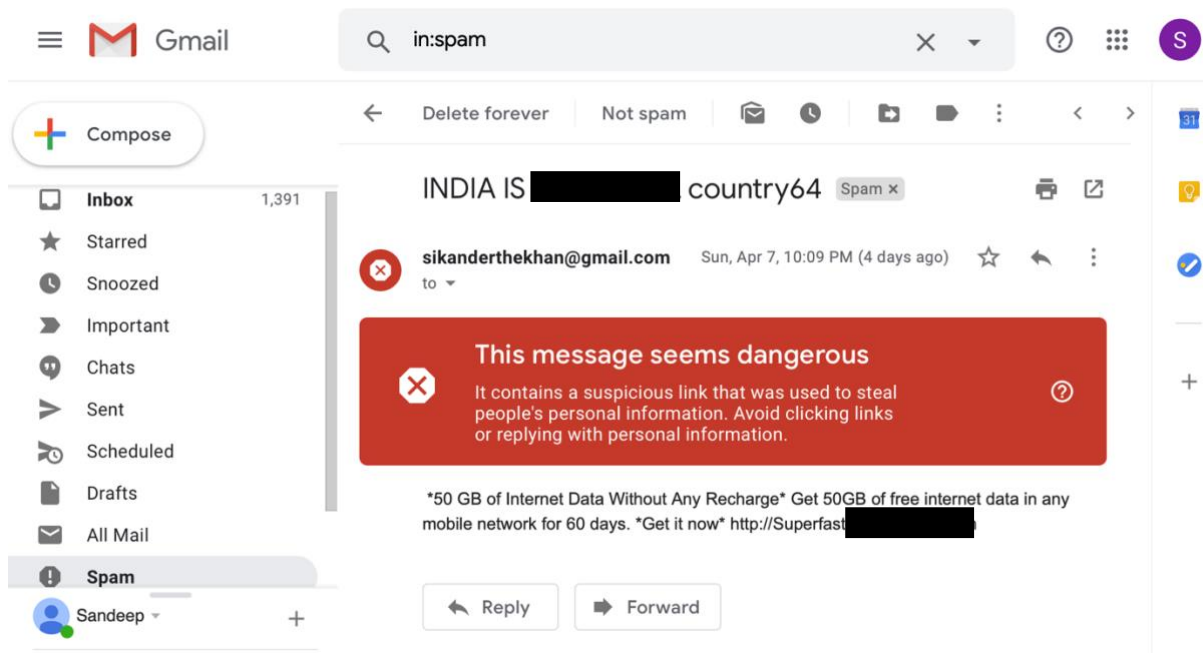


Figure 8.10 An Example of the Gmail spam filter

At the end in Sandeep Jain's and Cristian Rimi's Gmail accounts we would have the normal and safe messages in the Inbox folder or malicious in the spam folder as shown in above picture. There are some exceptions in the spam filtering. If users will customize the spam filter according to the user wants to filter, then spam filter can work differently.

8.4.2 Links Analysis

To analyze the links posted and included with the text message we have collected all the links using python script 2. In most cases the text included with the links asks users to **touch the link below** or **touch the icon below**. We have collected all the extract link in an excel from all the groups. To check whether the links are legitimate or not, whether it redirects to any malicious webpages or website, whether it is malware or not we have needed a good URL scanner. A URL scanner used to scan the url to check whether the url is redirecting to the safe webpage or to the malicious or dangerous web page.

To scan the links, collected from the political WhatsApp groups we used VirusTotal. VirusTotal is a free online File and URL scanner and it also has search engine to scan the URL, IP, Domain and file hash. VirusTotal is a strong tool to scan the malicious files because it scans the files on 63 different antivirus and shows the results.

Our approach to scan the links is shown in the below process diagram.

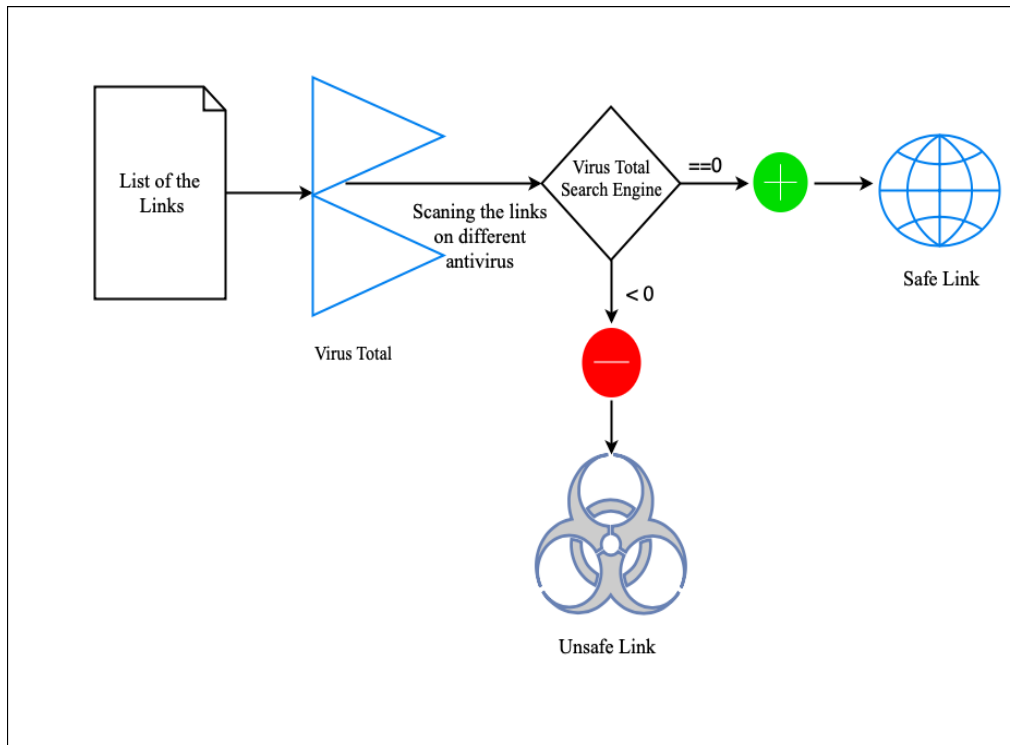


Figure 8.11 Method for the Link Analysis

Step 1 – We gathered all the links circulated in the all the WhatsApp groups and then created a main list of all the links. We have separated the links according to their main domain. Most of the links were from <https://bit.ly/>, <https://goo.gl/>, <https://youtu.be/>, <https://facebook.com/>, <https://twitter.com/>, <https://chat.wahtsapp.com/>, <https://t.me/joinchat/> domain. We haven't the links which were from any of the before mentioned domain.

Step 2 – We have divided the links in the common and unique category. In common category we have put all the link from <https://bit.ly/>, <https://goo.gl/>, <https://youtu.be/>, <https://facebook.com/>, <https://twitter.com/>, <https://chat.wahtsapp.com/>, <https://t.me/joinchat/> domain and where in unique category we have those links which were totally different than these common category links.

Unique links - We have considered only unique category links for virus total Scanning. After the distribution of links, we have scanned the unique category links on VirusTotal URL scan. After scanning each link, we have stored the results given by the VirusTotal.

Common links – from the common link list we have scanned the https://bit.ly domain using the virus total API. We Have used the python script 5 to scan the all the bit.ly links on VirusTotal. If the score is greater than 0 than script record the link in file.

Step 3 – For each scan VirusTotal gives the score. The score is equivalent to the positively detection by the antivirus so if no antivirus will detect the link as malicious then score will be more than 1 So if the Score is zero then VirusTotal status is positive and link is safe but if the score is higher than 0 that means at least one antivirus had detect something negative in the link. Positive link is concluded as safe link where malicious links are with negative response.

8.4.3 Media Message analysis

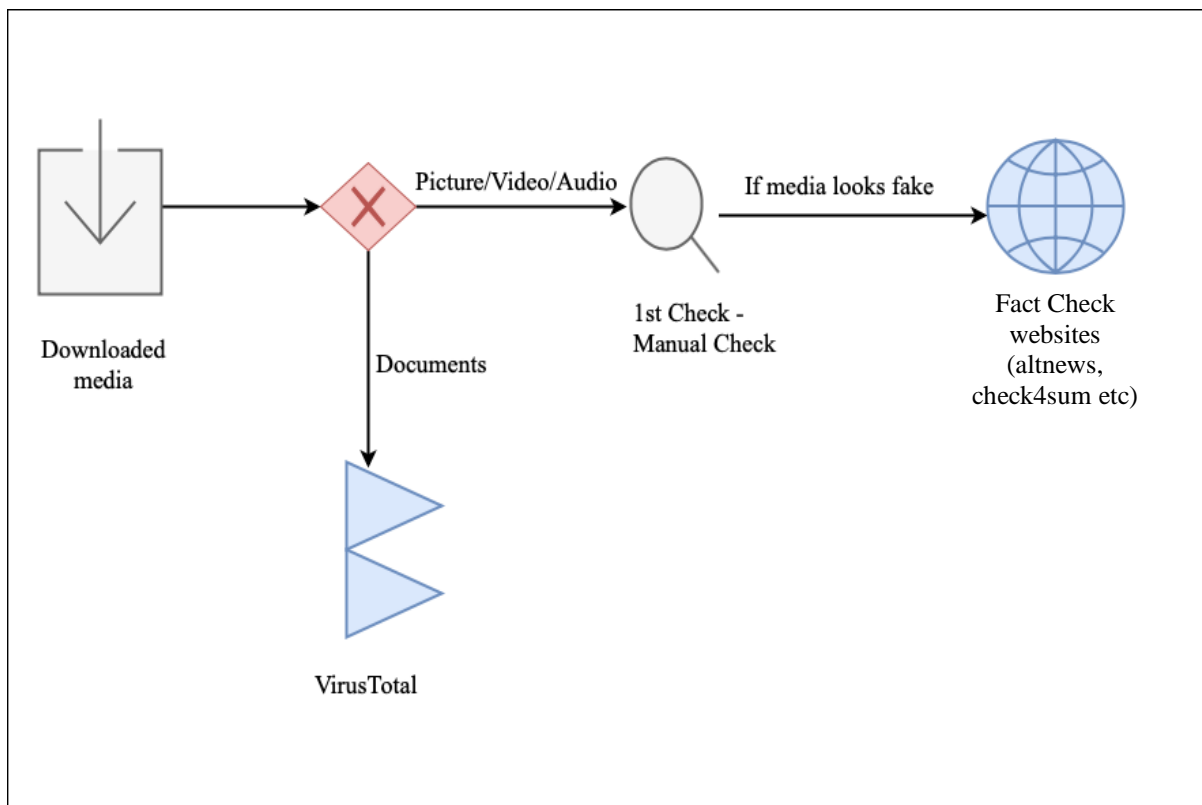


Figure 8.12 Method for the Media Analysis

Step 1 - We have downloaded media attached with the exported group chat and saved them according to the media type.

Step 2 – For the further analysis we have separated the media into two groups. In Group-1 we have put audio, video and pictures together and document in Group-2.

Step 3 – in this step we have checked the Group-1’s media messages manually. The manual check-up is to pick only those media messages which are looks fake news for the further analysis. The manual check is based on the few points. If after reading media messages if individual feels the change in the thinking, if message points political issues, or if message is based on the past facts than we have considered these messages as the red flag messages. Or other messages as the green flag messages.

For the media in Group-2 we have checked the document files on virus total to check whether the file is safe or unsafe.

Step 4 – We have used the red flag messages and analysis them on the www.altnews.com and we checked on the google search engine if the media is tampered or not.

8.5 Ethical Consideration

8.5.1 WhatsApp

Since we are working with the sensitive data from public political WhatsApp groups, we would collect phone numbers and messages which would be posted by group members. To maintain the privacy and anonymity of the group members, we only retrieve the country code from the publicly available phone numbers for this study. The phone numbers and any related collected data are not disclosed beyond this research study. After analysis, relevant information is deleted from our database and from repositories in which we had stored the WhatsApp group data. Subsequently, all WhatsApp honeypots and Nox app players including log files and backups used on the duration of this research are destroyed

During data gathering, the automatic download feature for our WhatsApp honeypot was turned off to ensure research-related messages (and even unsavoury and unwanted messages) are not stored on any of our devices. This maintains the isolation of our research environment.

In accepting WhatsApp’s Terms and Conditions, users consent to share their profile and last seen information, and even phone numbers with other WhatsApp users. Any WhatsApp user can collect, use, share messages and call the group members without needing additional consent from the users.

8.5.2 Facebook & Twitter

As part of the study, initiating and accepting friend requests from both Facebook and Twitter are necessary, and since this is part of the whole concept of social media, there is no ethical concerns here.

Creating a fake profile in Facebook and Twitter opens ethical questions. The following measures are done to simulate a profile with an active political affiliation:

- We did not use any copyright pictures as profile pictures
- all the profiles were not impersonating any real profile or persons,

During the study, no personal information from accepted friends and groups are disclosed. Only information relevant to the study will be processed, this exclude personal messages and public posts. Unless there is sufficient grounds to investigate the association between WhatsApp's groups and Facebook and Twitter, then the suspected political connection is scrutinized.

9 RESULTS

To get a better understanding of the results we have also separated the results in two parts, according to the research question as we did for the methodology. The first part of the results is acknowledging the first question "how political parties are reaching to the voter's WhatsApp chat application" according to the environment set up in methodology part -1. Where the second part of the results is the analysis of the political WhatsApp messages we have collected on the honeypots.

9.1 Part 1

As in methodology part one, we have interlinked the both WhatsApp honeypot accounts with their respective Facebook profile, Facebook page, and Twitter accounts. We used these Facebook profile, Facebook page, and Twitter to publish it's respective honeypot's number and connect with the political parties. Our results for both the honeypots are different according to the challenges we have faced during the research. First, we will discuss the details description of the honeypots we have set up and the results at the end.

9.1.1 Details of the Honeypots

9.1.1.1 Sandeep Jain

This honeypot is a WhatsApp Profile named Sandeep Jain, created as a BJP supporter. This WhatsApp profile was created with the Indian Mobile number (+91 9358375XXX). This account was not used before for any type of WhatsApp communication and never exposed to the political platforms. As mentioned in the methodology we have connected this Sandeep Jain Honeypot profile with a Facebook Profile, a Facebook Page, and a Twitter profile. All the profile except a Facebook Page are named Sandeep Jain and has current Indian Prime Minister Narendra Modi's Picture as a profile picture.

Social media Connection - A Facebook profile created on 07-12-2018. It had 2000+ connections and a connect Facebook page named Narendra Modi - 2019. This Facebook profile is further connected with the Sandeep Jain WhatsApp honeypot (+91 9358375XXX) and also with Twitter account @sandeep05575580. Twitter account @sandeep5575580 was created on the 15-02-2019 and this account follows the BJP leaders.

Results – As mentioned in the Challenges, the Facebook profile connected with Sandeep Jain's honeypot blocked by Facebook after a few days of active use. We were not able to continue our study with this account. Though we got a private message on Sandeep Jain honeypot from +919897095XXX before Facebook blocked the Sandeep Jain Facebook profile.

In the private message the Facebook user said that he took the mobile number from Facebook profile and he also made a phone call on the mobile number published on the Sandeep Jain Facebook profile, but he couldn't reach out. For a few days, the user also shared religious pictures as greeting with the honeypot.

After Facebook blocked Sandeep Jain Facebook profile, we have joined the 73 public WhatsApp groups from Sandeep Jain account as describe in the methodology and save the messages we received in those group for further message analysis for part-2.

9.1.1.2 **Sikander Khan**

Another WhatsApp account, a honeypot we created as an imposter of a congress supporter named Sikander Khan and it was created with the Indian phone numbers (+91 6375 424 XXX). This account also has a Facebook profile, a Facebook page, a twitter handle platform. Facebook profile and twitter handle have the same name Sikander Khan, but the Facebook page has Rahul Gandhi 2019 and has Congress (INC) chief leader Rahul Gandhi's picture as the profile picture. All the account registered with same mobile number (+91 6375 424 XXX).

Details of Social Media – the Facebook account was created on 07 December 2018. After a Facebook profile settled up we have created a Facebook page linked with Sikander Khan Facebook page named Rahul Gandhi 2019 and this page is Politician page and this is also linked with the (+91 6375 424 XXX) phone number. We have shared few political pictures on this page and also send invitations to like this page. None of the posts shared on this Facebook page was fake or manipulative. Then we have created a Twitter account on February 02, 2019. Twitter handle ID for this account is @Sikande61439761. This twitter handle was also registered with the (+91 6375 424 XXX) mobile number. And we have added this twitter handle link (<https://twitter.com/Sikande61439761?lang=en>) to the Sikander Khan Facebook profile.

Results – After setting up Facebook and Twitter profiles we have used the dual app player software to run the WhatsApp and as mentioned in the challenge at challenge 2, that we have locked out from the account and still the WhatsApp account is not active again. Hence, we are not able to go inside the Sikander Khan HoneyPot. Without opening the account, we are not able to write the results whether our honeyPot got success to catch the political groups or not. Though the Facebook profile, Facebook page, and Twitter handle is still running, and we are contacting the WhatsApp to unblock the account.

9.2 Part 2 (Analysis)

Part 2 of the result is targeting the second part of the research question "What content political parties are spreading in the political WhatsApp groups". To understand and analyse what political parties and group members are posting and circulating by the WhatsApp messaging application, we have made the process flow in different parts according to the type of messages as it is explained in methodology part 2. As in Methodology, we have mentioned two main approaches to analysis the text messages and media messages, analysis results are also in the two parts. In the first part, we will analyze the text message with the Gmail spam filter and VirusTotal. Where in the second part we will analyze the media circulated in the WhatsApp groups. We have collected 19075 messages from the 54 groups.

9.2.1 Text Message Analysis

Text Message Analysis is done with the help of python scripts, VirusTotal URL scan, Gmail spam filter. We analysed the text messages; we have collected from the political WhatsApp groups on the Sandeep Jain honeyPot. We will analysis the Text messages in the first section than we dive into the links we found on the text messages to analysis whether group members are using the political groups for political discussion and political news or they are also spreading the spam and virus.

We have collected the 19075 overall messages. Out of 19075, we have got 12000+ text messages which we consider further for the analysis. As for the analysis we have selected 54 groups which were more into the politics and political news. Though we have also added 5 groups which were non-political groups because the non-political messages were the same in non-political and political both types of the groups were sharing the same

non-political messages from same WhatsApp account. Some WhatsApp account were into more than 1 political groups we were following, and they were sharing the same content in all groups they were members of.

We have used the following keywords to check whether the groups are a political group or non-political group. As Hindi is an official language of India and more messages are in Hindi than English, so we used Hindi and English both the keywords from both the party to check whether the group is political or non-political.

Bhartiya Janta Party (BJP)

Table 1 Political topics related to BJP Parties

| BJP | Narendra modi, | Modi Government | Modi | Namo | Chowkidar | Ram Mandir | Prime Minister | Bhajpa | Achhe Din |
|--------|----------------|-----------------|--------------|------|-----------|------------|----------------|--------|-----------|
| बीजेपी | नरेंद्र मोदी | मोदी सरकार | मोदी, मोदीजी | नमो | चौकीदार | राम मंदिर | प्रधानमंत्री | भाजपा | अच्छे दिन |

These keywords are related to the BJP government like the name of the main leader, his old name, the current #Chowkidar trend started by the Narendra Modi, Party name and slogans

Congress (INC)

Table 2 Political topics related to Congress INC party

| Congress | Rahul Gandhi | Pappu | Sonia Gandhi | Manmohan Sarkar | Pradhan Sevek | Indira Gandhi | Jawahar Lal Nehru | Feku |
|----------|--------------|-------|--------------|-----------------|---------------|---------------|-------------------|------|
| कांग्रेस | राहुल गांधी | पप्पू | सोनिया गांधी | मनमोहन सरकार | प्रधानसेवक | इंदिरा गांधी | जवाहर लाल नेहरू | फेकू |

All the above mention keywords are related to the Congress president name, all the previous leader's name, we also added the other names used for the party president.

General Key Words

Table 3 General topics related to Indian Politics

| Pakistan | Notebandi | Ram Mandir | Hindu | Muslim | Remove poverty slogan | poverty | alliance | political | kashmir | Surgical Strike |
|-----------|-----------|------------|-------|---------|-----------------------|---------|----------|-----------|---------|------------------|
| पाकिस्तान | नोटबन्दी | राम मंदिर | हिंदू | मुसलमान | गरीबी हटाओ का जो नारा | गरीबों | गठबंधन | राजनैतिक | कश्मीर | सर्जिकल स्ट्राइक |

We have added all the other words which are general for both the parties and massively used in India to address the political topics. These words are used by the voters and political party supporters in everyday life.

We have chosen groups, which has these keywords in the exported .txt file for the analysis but as mentioned earlier, we have also chosen 5 groups which used to spread same messages as the political categories' groups. As we have analysed 12000+ text messages to see what group members are spreading in the political groups.


The table below shows the types of messages circulating in the public political WhatsApp groups.

Table 4 Example of the political WhatsApp messages (Collected by honeypot)

| Original Messages | English Translation |
|--|--|
| India Against Dalal media | |
| मेने तो कभी ऐसा प्रधानमंत्री नहीं देखा और नहीं देखना चाहूंगा जो अपने प्रचार के लिए जनता के रुपये खर्च करेजो सरकारी संस्थाओं का समर्थन की बजाए निजी कंपनियों का प्रचार करजो HAL को छोड़ कर अम्बानी को राफेल का ठेका देदेजो उसकी रैली के लिए किसानों की फसल बर्बाद करवा देजो किसानों को दिल्ली बुलवाकर लाठीचार्ज करवाए | I have never seen such a Prime Minister and I would not like to see people who spend public money for their publicity, instead of supporting government institutions, instead of supporting private companies, leaving HAL and giving Amban to Rafel, waste farmers' crops for its rally. Callao Deo farmers call Delhi for lathi charge |
| #पुलवामा मे शहीद 44 जवानो की राख अभी ठण्डी भी नहीं हुई ओर फेकू ने पाकिस्तान को बधाई दे डाली.. 🇵🇰 नीच | The ashes of Shaheed 44 soldiers in #Pulwama have not been cold yet and feku congratulated Pakistan. |

| | |
|---|---|
| <p>*कल हरियाणा का वीडियो आया, आज उत्तर प्रदेश के फर्रुखाबाद का जहाँ खुलेआम 'हर हर मोदी' के नारे लगाते और दलित समुदाय के लोगों को मारते भाजपा समर्थक देख लीजिए New India and shining का ट्रैलर है ये*</p> | <p>* Yesterday came the video of Haryana, today from Farrukhabad, Uttar Pradesh, where BJP supporters openly slogan 'Har Har Modi' and kill the Dalit community. This is a trailer of New India and shining.</p> |
| <p>Spin The Lucky Wheel! - AR – xxxu.xxvxn.com https://buc.kim/d/3p7QWUNY8fte?pub=link</p> | <p>-</p> |
| <p>https://chat.whatsapp.com/FWDXnGCa3qQ756EAENKucz Only congressitNJoin this group Farzi deshbhakt ...aur uske Bhakt are not Allowed... Will be kicked out immediately.</p> | <p>-</p> |
| <p>Only BJP News</p> | |
| <p>*Latest Special Offer* hi मैंने आपको स्केच कार्ड भेजा है उसको स्केच कीजिये और पायें 100,200,500 और 1000 रुपये के Paytam कूपन *Jaldi loot looo...* goodphoto.info/paytam-scrach</p> | <p>* Latest Special Offer * hi I sent you the scratch card, scratch it and get 100,200,500 and paytam coupon of 1000 rupees. * Jaldi loot looo ... * goodphoto.info/paytam-scrach</p> |
| <p>भाजपा समर्थक कहते हैं कि उम्मीदवार को मत देखो मोदी को देखो, वहीं कांग्रेसी कहते हैं कि उम्मीदवार को देखो राहुल को नहीं ...</p> | <p>The BJP supporter says that don't look at the candidate look at Modi, Where as Congressmen say that the look at candidate not at Rahul ...</p> |
| <p>वाराणसी में प्रियंका वाड़ा का भयानक रोड शो, इससे ज्यादा लोग तो JCB से खुदाई चल रही हो वहां आ जाते हैं।</p> | <p>Priyanka Vadra's awesome road show in Varanasi, more people then this are coming at excavating from JCB.</p> |
| <p>MODI NAMO INDIA</p> | |
| <p>*डाउनलोड करे ये ऐप* और आपके मोबाइल में हो जायेंगे *दो केमेरे* http://bit.ly/2G1eOfY</p> | <p>* Download this app * and your mobile will have * two cameras * http://bit.ly/2G1eOfY</p> |

| | |
|--|---|
| <p>₹ *गोरी गोरी* लड़कियों के वीडियो *डाउनलोड* https://goo.gl/HHUsWu</p> | <p>₹ * Blonde Girl * Girls Video * Downloads * https://goo.gl/HHUsWu</p> |
| <p>पीएम मोदी ने कहा कि हमारे लिए भी कर्जमाफी का वादा करना आसान था, हम भी रेवड़ी बांट सकते थे पर मोदी ऐसा नहीं सोचता है और ऐसा पाप नहीं कर सकता है। आज हम इतनी बड़ी राशी इस योजनाओं में लगा रहे हैं ताकि जो सालों से लटकी हुई सिंचाई परियोजनाएं हैं वो पूरी हो सकें। हमने ऐसी 90 परियोजनाओं को चुना और आज उनमें से 70 अब पूरी होने वाली हैं। हम ऐसा इसलिए कर रहे हैं ताकि हमारी योजनाओं से देश का किसान लाभान्वित हो सके।</p> | <p>PM Modi said that it was easy for us to promise debt forgiveness too, we could also share Rewadi, but Modi does not think so and cannot do such a sin. Today, we are putting such a big amount in these schemes so that the irrigation projects which have been suspended for years can be fulfilled. We have selected 90 such projects and 70 of them are going to be completed today. We are doing this so that the farmers of the country can benefit from our plans.</p> |
| <p>प्रधानमंत्री नरेंद्र मोदी ने पवित्र संगम में डुबकी लगाई और अब पूजा अर्चना कर रहे हैं।</p> | <p>Prime Minister Narendra Modi immersed himself in the holy rivers and now worshipping.</p> |
| <p>*फोन* कॉल में *लड़की* की *आवाज* में बातें करें *डाउनलोड ऐप* https://bit.ly/2JJWUfs</p> | <p>Talk in girl voice on phone calls *Download App :* https://bit.ly/2JJWUfs</p> |
| <p>Bjp Social Media Team</p> | |
| <p>अच्छा हुआ जो यह वीडियो मिल गया। वायरल करने में सहयोग कीजिए। 🙏</p> | <p>Good that got this video Support to viral this.</p> |
| <p>आजीवन राहुल गांधी को वोट दूंगा अगर वह वायनाड में जनों तिलक धोती रुद्राक्ष पहन कर दिखा दे बोल जनेऊ धारी है क्या दम ?नौटंकी साला🤔🤔</p> | <p>I will vote for Rahul Gandhi if he wear Tilak dhoti Rudraksh in Wayanad and. Overacting</p> |
| <p>Congress Warriors</p> | |
| <p>https://www.facebook.com/848798528638160/posts/1031294540388557/ सभी मित्र इस वीडियो पोस्ट को केवल 21 टाइम (Facebook Group's/ Facebook Friends Timeline) शेअर जरूर कीजिए।आपके अमूल्य सहयोग से आजादी की ये दूसरी लड़ाई में मदद मिलेगी।</p> | <p>https://www.facebook.com/848798528638160/posts/1031294540388557/ All friends share this video post only 21 times (Facebook Group's / Facebook Friends Timeline). Your priceless collaboration will help in this second fight of independence.</p> |
| <p>"BJP " ने एक काम बढ़िया किया है #गौमांस निर्यात में देश को No.-one बनाया.#मोदीजी इस काम पर वोट क्यों नहीं माँगते 🤔</p> | <p>"BJP" has done a good job # Made the country No.-one in #Beef exports. # Why doesn't Modi seek vote for this work?</p> |

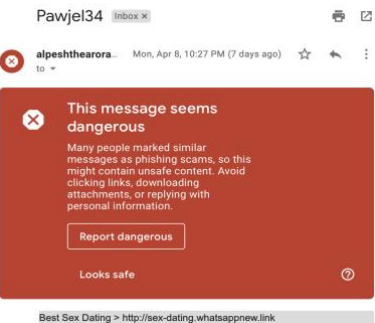
| | |
|--|--|
|  | |
| <p>Hey,I am using Futuresow for earn money.Futuresow is best app and website for earn money.Use my referral code : PrfuqY http://futuresow.com/admin/register?id=PrfuqY</p> | |
| <p>*राशिफल 27 फरवरी 2019: आज धन लाभ के बन रहे प्रबल योग, परिवार के साथ बिताए वक्त:* http://chhattisgarhtoday.co.in/?p=246</p> | <p>* Horoscope 27th February 2019: Today is great day of earning money, spend time with the family: * http://chhattisgarhtoday.co.in/?p=246</p> |

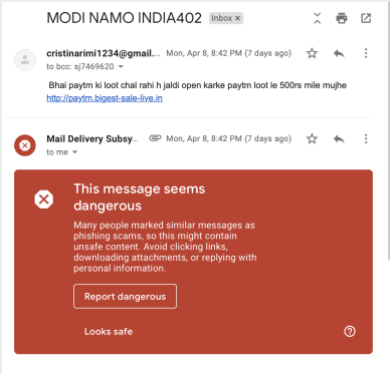
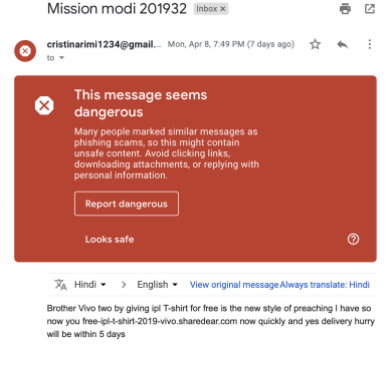
We found political 49 groups have political messages, but they also have unimportant and unnecessary spam messages. After taking out the picture, file attached message thread we had 12000+ text messages.

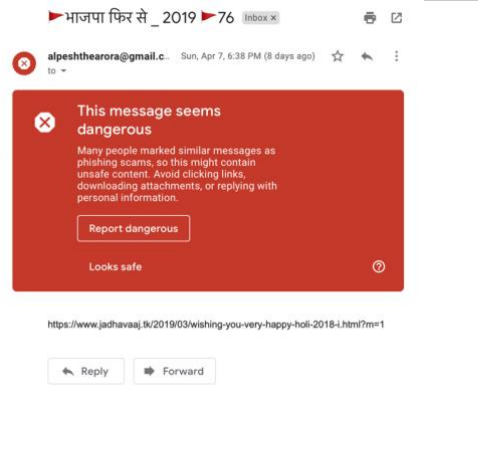
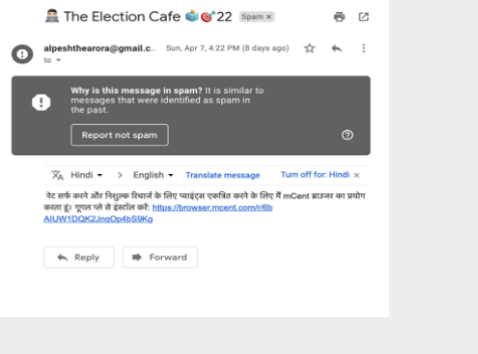
To check whether the text messages are spam messages or not we have used the google spam filter. We have sent chose 3957 text messages from 26 different political groups to the Gmail account, the purpose of the Gmail spam filter was to see whether google can detect the spam messages by its self or not.

Gmail has detected 18 messages as spam messages

Table 5 messages detected by Gmail spam filter

| Group Name | Messages detected as Spam | Note |
|-------------------------|---|---|
| We support narendr modi | Free Sex Dating > http://sex-dating.whatsappnew.link | This Message seems dangerous |
| Pawjel34 | Best Sex Dating > http://sex-dating.whatsappnew.link |  |

| | | |
|----------------------------------|---|---|
| <p>MODI NAMO INDIA</p> | <p>Bhai paytm ki loot chal rahi h jaldi open karke paytm loot le 500rs mile mujhe http://paytm.biggest-sale-live.in</p> <p>Bhai maine tujhe ek App ka link bheja hai maine isse 1800 Rs Paytm Cash Jeeta Muje to mil gaye tum bhi try kar lo. *Limited Time Offer Hai* Lekin Bdia Hai Bhai, Meri Maan toh Ek Bar Try le *Jaldi loot looo...* http://bitly.com/2F5zLTw</p> | <p>This Message seems dangerous</p>  |
| <p>Mission modi 2019</p> | <p>* Prime unemployment allowance scheme in 2019 * As part of the plan is to get every unemployed * Rs 3,500 * The Czech monthly The scheme fill the final date is March 31, * Registration FREE filled my form here * Http://indiagovtkclub/unemployment-allowance-registration/ * request: * 👤 please message to Share your friends, relatives and all groups in order to benefit from the scheme to all unemployed.</p> | <p>This Message seems dangerous</p>  |
| <p>INDIA IS POWERFUL country</p> | <p>https://www.onlyadult.tk/2019/03/18-shay-evans-brazzers-video-2019-hdrip.html</p> <p>*50 GB of Internet Data Without Any Recharge* Get 50GB of free internet data in any mobile network for 60 days. *Get it now* http://Superfast-4G-Offer.com/en2/27/19, 12:41 PM –</p> | <p>This Message seems dangerous</p> |
| <p>INI love IndiaIN</p> | <p>भाई Vivo ने प्रचार का नया तरीका निकाला है free में ipl T-shirt दे रहा है मैंने तो बुक कर दी है तुम भी यहाँ से free-ipl-t-shirt-2019-vivo.sharedear.com जल्दी बुक कर दो और हाँ delivery 5 दिनों के अंदर हो जायेगी जल्दी करो</p> | <p>This Message seems dangerous</p> |
| <p>INभाजपा कार्यकर्ताIN</p> | <p>do you know? Jio has Krdi start "Jio Dish TV" pre booking. They're giving 5 million customers a free subscription of 1 year Hankni Free, also set JIO DTH Setup box Click here to Jaagakapana connection now. http://bit.do/jio-dth 👤 Please note: 👤 Spread this message to his family, relatives, friends and WhatsApp groups. So, other people can also benefit. http://helplineoffer.com/jiodth/</p> | <p>This Message seems dangerous</p> |

| | | |
|------------------------------|--|--|
| <p>▶ भाजपा फिर से_2019 ▶</p> | <p>www.jadhavaaj.tk</p> |  |
| <p>The Election Cafe</p> | <p>Surf the net and free to collect points to recharge I use mCent browser. Install the Google Play: https://browser.mcent.com/r/6bAIUW1DQK2JnqOp4bS9Kg</p> |  |

We have collected the messages which seems to be suspicious or spam emails but google spam filter didn't mark as the spam emails. WhatsApp group members are not only spreading the malicious or spam message but they also sharing contact numbers and extreme content in the groups. The text messages are used to write the blogs over 5 pages to support the party. In these WhatsApp groups we, have collected spam texts messages, with extreme content, political messages and small chat messages.

9.2.2 Links Analysis

After collecting all the messages, we have also collected 4620 URLs included in the text messages. To check whether the URL attached with the text messages are legitimate or not, whether it is redirecting to the safe page or not, we have used the VirusTotal as mentioned in the methodology part 2.

Below graph shows the most common domain address shared in the WhatsApp groups.

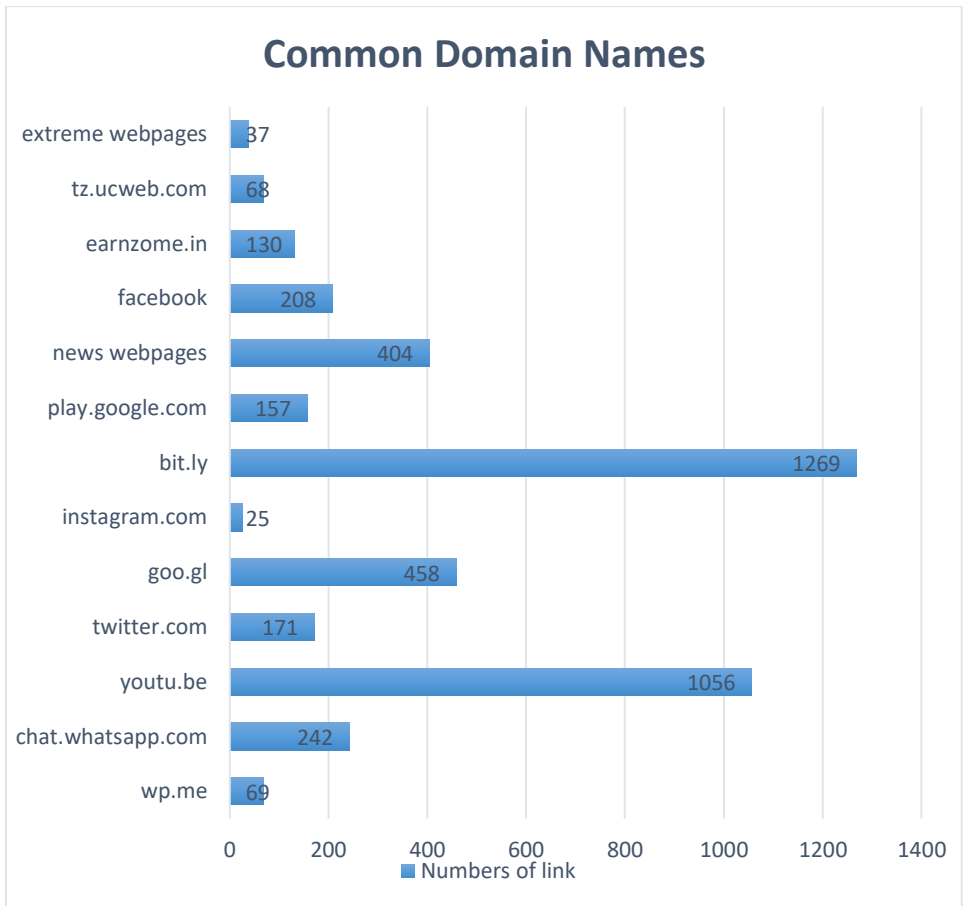


Figure 9.1 Statistics about domain found in link analysis

Description of the Domain Names

Table 6 Description of Domains found during research

whatsappnew.link We have combined the links which were related to the extreme content, these links were just shared in the groups without much text to tempted user to click on the link.

<http://www.sex.telegram.com>

<http://sexuality.whatsappnew.link>

<http://sex-dating.whatsappnew.link>

| | |
|--------------|--|
| tz.ucweb.com | url is - http://tz.ucweb.com/ |
|--------------|--|

| | |
|----------------|---|
| | This link redirects UC browser. 58 links are shared to install the applications. |
| earnzone.in | Host – www.earnzone.in earnzone is online income site. 130 links are redirecting to this web page. |
| facebook.com | 208 links were of Facebook, these links redirecting to the Facebook users' post. |
| New Webpages | We have added 22 different official news agency's domains to show group members are also sharing the news links. Using the news webpages groups members are sharing the articles, news published by the Indian news agencies. We have combined the dailyhunt, aajtak, livemint, hindustantimes, altnews, indiatoday, bbc.in, Bhaskar, boltahindustan, abplivenews india express, chattisgarh today, bbc.co.uk, times of India, hindi graph, Hindustan bbc, business insider, janman india, economic times, amarujala, ndtc, business-standards. |
| play.goole.com | These links were used to redirect the members to google play store to install the applications and games. |
| bit.ly | bit.ly has 826 http links and 443 https links. Bitly is famous URL shortner service use to shorten the long URL for the convince. These URL can be genuine or could be a spam or phishing web sites. 1042 links were shortened by the bitly service. |
| instagram.com | Instagram is another social media platform to post the picture and post. 25 links were redirecting to the Instagram users' posts. |

goo.gl goo.gl domain is also a URL shortener service by google. Google user can short the URL by using the goo.gl. 458 links were shortened by the goo.gl.

| | |
|-------------------|--|
| twitter.com | Twitter is microblogging social media service. Twitter is famous among political leaders. |
| youtu.be | YouTube is collection of videos. A YouTube user can post a video on YouTube so users other can watch that video. Where youtu.be is a short URL of YouTube. |
| chat.waatsapp.com | These are the invitation links to join the other WhatsApp groups. 242 WhatsApp joining links were shared during analysis. |
| wp.me | These are also WhatsApp links. This are direct messaging link. By accessing this link, a user can direct messages to the users. |

We have collected 210 different domain address from the 54 WhatsApp groups. Apart from all the popular domains we have also found some suspicious URLs. We scanned the unknown URLs with VirusTotal and we got the following results.

Table 7 VirusTotal Results

| S. | Links | Virus Total Results |
|----|---|---|
| No | | |
| 1 | https://t.co/ | Result – 0/66 Community score - -65 VT Community – Probably scam site |
| 2 | https://lh3.googleusercontent.com | Result – 0/69 |

Community score - -30

| | | |
|---|---|--|
| 3 | http://juarinly.xyz/ | Result – 0/69 Forcepoint threatSeeker - Suspicious |
| 4 | https://buc.kim/d/0MGJaVvtIi4B?pub=link | Result – 0/69 Forcepoint threatSeeker - Suspicious |
| 5 | https://za.gl/ | Result – 2/69 Ariva - Malware AdminusLabs - Phishing |
| 6 | https://ylink.cc/ | Result -1/69 Forcepoint ThreatSEeker - Malicious |
| 7 | https://ethclick.me/ | Result - 6/69 CRDF – Malicious Dr.Web – Malicious Fortinet – Malware G-Data – Malware Malwarebytes hpHosts – Malware Sophos AV – Malicious |
| 8 | https://www.jadhavaaj.tk/ | Result – 0/69 |

forcepoint threatSeeker –
Suspicious

| | | |
|---|---|---|
| 9 | http://Superfast-4G-Offer.com/ | Results – 3/69 BitDefender – Phishing Fortinet – PhiPhishing phos AV -Malicious CLEAN MX – Suspicious ESET – Suspicious Community score - -11 |
|---|---|---|

10 <https://etrustbux.com>

Result -0/69

Spamhaus – Spam

11 <http://zo.ee/>

Result - 0/69

Quttera – Suspicious

12 <http://birdslife.xyz>

Result - 0/69

Forcepoint ThreatSeeker –
Suspicious

13 <https://awsmining.com>

Result - 2/69

CLEAN MX – Malicious

DNS 8 – Malicious

14 <https://get.cryptobrowser.site>

Result - 0/6

Forcepoint ThreatSeeker –
Suspicious

SpamHaus – Spam

| | | |
|----|--------------------------|---|
| 15 | https://www.onlyadult.tk | <p>Result - 0/69</p> <p>Foecepoint threatSeeker – Suspicious</p> |
| 16 | http://dingtone.me | <p>Result - 0/69</p> <p>Foecepoint threatSeeker – Suspicious</p> |
| 17 | https://rebrand.ly | <p>Result - 1/69</p> <p>Dr.Web - Malicious</p> <p>Quttera - Suspicious</p> <p>Community Score - -66</p> <p>Community – Phishing site from junk email</p> |
| 18 | http://tiny.cc | <p>Result - 1/69</p> <p>DNS8 – Malicious</p> <p>Community score - -117</p> <p>Community -</p> <p>EmilianoJJ - #malware</p> <p>Deleted_user -This site is a link shoshortenerich is used aloa lotth viruses like malware</p> |
| 19 | http://paise-kamao.tk | <p>Result - 0/69</p> |

| | | |
|----|---|--|
| | | Forcepoint ThreatSeeker – Suspicious |
| 20 | https://fainbory.com/ | Result - 0/69 Spamhaus – Spam |
| 21 | https://www.mahitikhajana.xyz | Result - 0/69 Forcepoint threatSeeker – Suspicious |
| 22 | https://www.wishesmyfamily.tk | Result - 0/69 Forcepoint ThreatSeeker – Suspicious |
| 23 | http://bit.do/jio-dth | Result - 1/69 AutoShum – Malicious |
| 24 | https://ref-workzone.com/?mref=bhartendraClick | Result - 0/69 Fortinet – Spam Spamhaus -Spam |
| 25 | http://xxxu.xxvxn.com/ | Result - 2/69 Fortinet – Phishing SCUMWARE.org – Malware |

Above links were detected as either malware, phishing, malicious or spam, suspicious by VirusTotal URL scanner. VirusTotal scan link upto 69 antivirus engines. Result shows which engine marked the link as unsafe with probable reason. The frequency of sharing these links were noticeable and can be used to understand that the spammers are really using the WhatsApp groups to spread the malicious links and spams. These links were

shared in more than 1 political WhatsApp group. The graph below shows numbers of times each link was shared among all 54 groups during the observation. It is clearly understandable from the below graph that high-risks (red) were shared more frequently than the low risk (yellow) and clean links (green). We have also noticed that same links were shared by different people not only in different group but same party supporter but also in the different party support groups. Like - <http://bit.do> link was shared between 27 different groups by different WhatsApp accounts, this link was shared among BJP supporter groups as well as in the Congress (INC) supporting groups. Not only this links but rebrand.ly, ylink.cc, za.gl links were also shared among the different support groups.

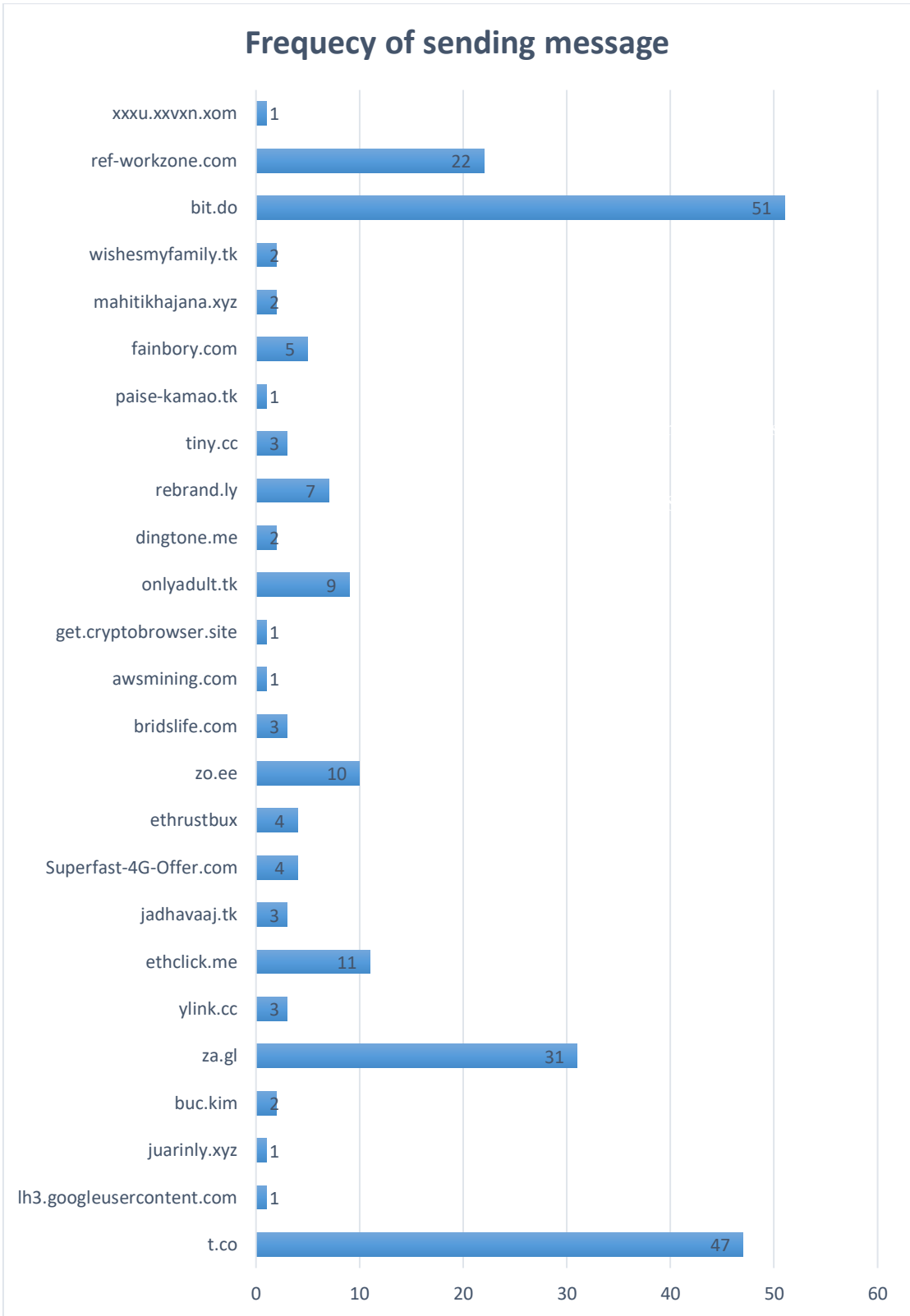


Figure 9.2 frequency of spreading malicious links

In above graph the clean links (green) were not detected unsafe by any search engines but they have negative community score which means there are high chances that these links

could be spams or malicious. We have also found 85 links which has sex' word. These links were redirecting to the extreme content webpage, www.injoy.fun, whatsappnew.link, sex.telegram.dating, bit.ly, www.the-hindi.in, these were the domain spreading these links. Some of the bit.ly links were also redirecting to the extreme content webpages.

9.3 Media Analysis

We have collected big amount of media messages from the 54 WhatsApp groups. These media messages have pictures, videos, audios, pdf file and contact number as well. We chose most active WhatsApp groups from both political parties to analyses the media content shared in these groups, whether the media content is genuine or not. We have exported the media messages from Sandeep Jain WhatsApp honeypot and separated the media according to the format. From WhatsApp groups we collected .jpeg, .mp4, .pdf, .enc, .ogg, .mpeg. we have analysis .jpeg in picture analysis, .mp4 video analysis, .pdf and .enc both are document file analysis, and .mpeg and .ogg are audio file analysis. We also received shared contact numbers of unknown people on Sandeep Jain honeypot. In this part of the analysis we, will analyses each media format separately than at the end we will mix the results to conclude the results.

9.3.1 Contacts

During the analysis, some group members used to share the mobile numbers mostly during the night. Mostly the text message attached with the contact number used to claim this are call girls' number. Our honeypot collected 46 contact number from different country from all over the world.

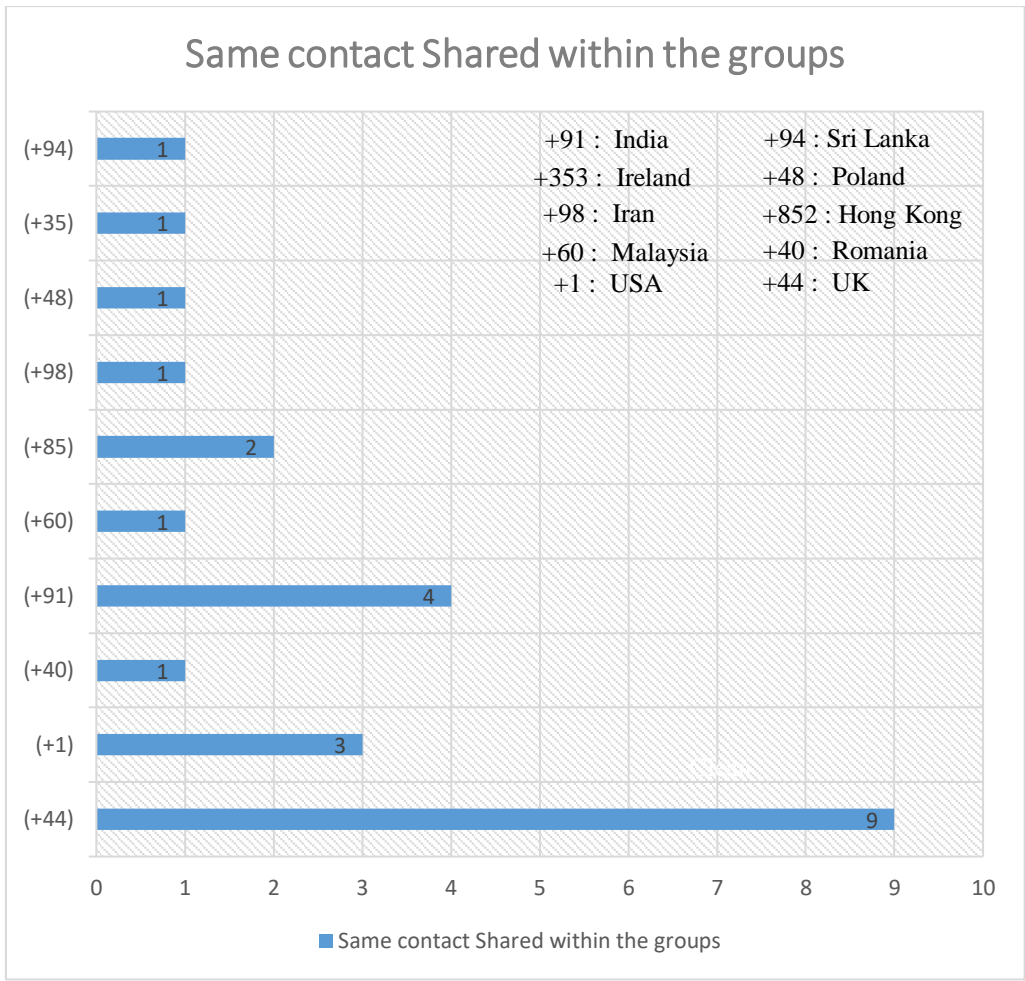


Figure 9.3 Statistics of contacts shared in the groups

Some contact also has Gmail address attached with the contact info. Contacts from Ireland, Sri Lanka and UK has same pattern of the Gmail address. Contacts from all these countries also has same message attached, like USA, Malaysia, UK, Hong Kong, Poland has **“I want Funny good Friendship”** the spelling mistake (Friendship) is same in all countries contact number with the same profile picture. Other status **“I need boys Good Friend”** and **“I want honest boy friend”** are also same in different countries contacts info.

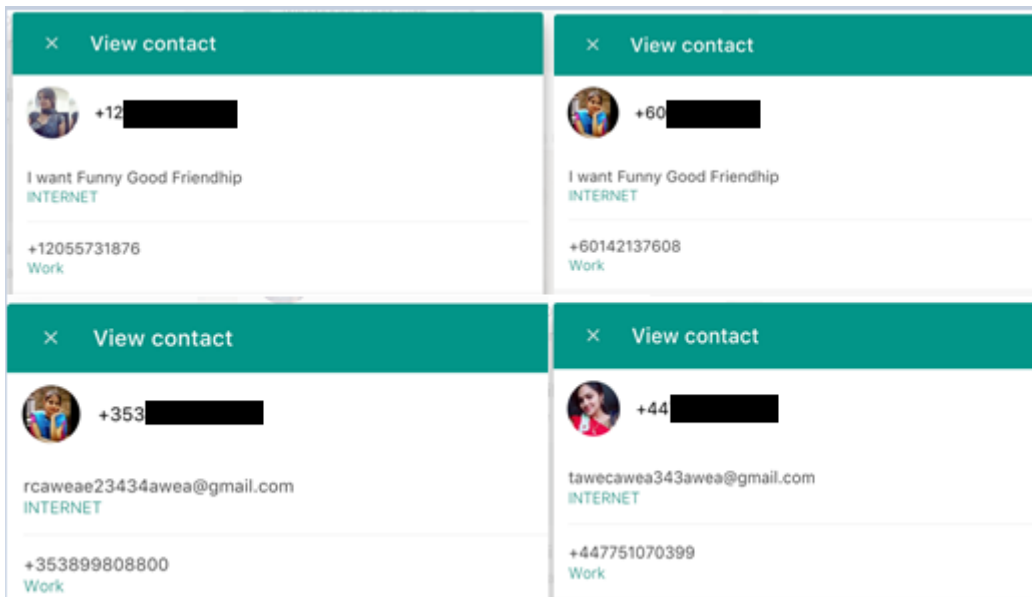


Figure 9.4 Shared Contact info

These 4 contacts are from 4 different countries USA, UK, Malaysia, Ireland but the profile set up are same. In first two contacts the info is same where in last two the email formatting is same. Apart from this, contact 2 and 4 has the same profile picture. Which could be concluded that the contacts shared in the political WhatsApp groups were same and internally connected

9.3.2 Document File

We have chosen 8 documents for our analysis. We notice different group members circulated same document files in different groups. This shows the message circulating speed of the WhatsApp application. We have collected chose two .enc file and 6 .pdf file. We have scanned all these files with VirusTotal scanner and according to VirusTotal all files were clean and safe.

9.3.3 Audio Messages

We received more than 10 audio files from all the groups. And like document and contact we found the same audio were also circulated in the different WhatsApp groups. For analysis we have filtered those audios, which were used for chatting. After filtering we chose 5 audio files for manual testing. These Audio files has two different formats (.ogg and .mpeg). After listening to all the 5 audios we have caught two suspicious files.

Audio 1 – “Please! Forward to all friend This is an urgent notice from the Indian Hyderabad police to all over the India: please for upcoming few days do not drink any soft drinks like maza, fanta, coca-cola, 7-up, mountain dew, pepsi etc” because one of the workers from one company has mixed Ebola virus infected blood into these drinks. Yesterday, this news was also shown on NDTV (one of India popular new channel). Please help to forward this message as soon as possible to your friends and family.

Audio 2 – “Hello friend! This girl has meet with accident and for operation she needs 10 lakh rupese. Please! share this picture, for 1 share she will get 5 rupees so number of times you will share you will help her. Please don’t take this message as a joke, It is too dangerous. Our one share will help this girl please.”

We have used google search engine to get the details about the claims has been made in the audio 1 about Ebola virus. We found three independent viral new verification webpages 1) Hoax-slayer.net, 2)hoaxorfact.com, 3)check4spam.com verifying that this message was a hoax message, and no such incident reported by Hyderabad police neither Hyderabad police published any such notice, nor NDTV shown any report similar to this message on Ebola virus in soft drink. We also checked Hyderabad police website to check whether they published any notice in past related to Ebola and same we also checked NDTV website, but we could not find any evidence which supports the claim made in the audio 1. All information we found clearly says this audio message was a hoax message.

Where in audio 2 two a woman was asking to share the picture to as many people as possible to help a accident victim. This was a clear hoax because Facebook and WhatsApp never pay for such a message spreading chain.

These both audios were hoax audios, hoax messages are not a virus which can cause harm to computers or mobile devices or hoax are not used to steal the information, but this type of hoax message can be used for denial of service attack and to harm the reputation of the organization or even person. Audio 1 was reputation harm where audio 2 can cause a flooding of unwanted messages.

9.3.4 Videos

Form 54 WhatsApp groups we have saved 50+ videos. We did the manual analysis of the videos to gather the information about the videos being shared in the groups. We

analyzed what type of videos are circulating in WhatsApp groups. For this we have collected 18 videos from two most active groups from both the party supporter. We have categorized the videos in political, satire, non-political. After the general classification we also checked whether video is genuine or tampered.

We have found that 14 videos were political videos, 1 video was clipped of Pakistan news channel's report, another video was sarcasm videos on Indian PM Narendra Modi, 1 was on religion and patriotism, where one video is completely non-political video.

14 videos were related to Indian politics. 1 political video was claiming that BJP is bribing the voters, this video was a mix of few small videos, videos shoot on different places were joined in this video. This video was also posted on the YouTube. 2 videos were from the tik-toc application used to create and edit the video as needed, 1 of the tik-toc videos showed that a fighter jet suddenly started to fly which could be possible so that video was false. One video was for entertainment purpose where small video clips were joined together, video was on PM Modi. The other political videos were pointing the issues arising during the election. Most of political videos were addressing the problem but most of the videos were ducted videos as they were series of the small videos.

9.3.5 Pictures

We received more than 100 pictures from all the political WhatsApp groups. For the analysis we have considered the images from two political active groups. Image analysis will give information about the images shared in the WhatsApp groups are those pictures are legitimate and used for the good purpose. We have already mentioned in 2016 USA election how picture tampering used to change the election results; hence it is important to analyze the picture. We have manually analyzed 57 WhatsApp images taken from the Sandeep Jain honeypot.

Image analysis is to check whether the image is fake, edited or original. We manually checked the pictures by using the google search engine. 54 images were related to politics means this picture has political content.

9.3.5.1 Tampered picture -



Figure 9.5 Tampered picture

Picture like shown above are tampered pictures, in their picture these faces have been edited with Indian political leader's face. These pictures were circulated in most active WhatsApp groups. In our research we found the first picture 28 (left) is originally from Virat Kohli and Anushka Sharma's (Indian Celebrity's) wedding. Picture 28(right) we found on the Political meme webpages.

9.3.5.2 Misleading Images



Figure 9.6 Image has Misleading Information

The above picture is fake news it says in Telangana (State in India) congress wrote in manifesto that they will give free electricity to mosque, 2 million help for Muslim

youngster, IT corridor for Muslims, loan on 4% rate for Muslims and in insideock box it saysayster all this would you still think conCongress seca ular party.

We have checked the congress's Telangana manifesto 2019 available on (<https://drive.google.com/file/d/1LRDYMcy3I3wY5zwRbSTcuXEcOX8utMIY/view>).

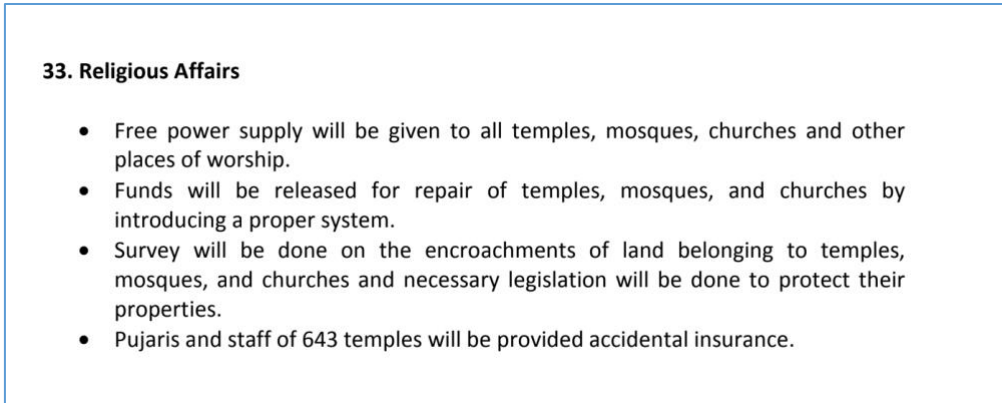


Figure 9.7 Screenshot of the Telangana Congress's Manifesto

We have found that on point 33 they have mentioned about the temple and churches also along with mosques. This purpose of this image was the mislead the reader by hiding and twisting the information.

9.3.5.3 Manipulating News



Figure 9.8 Manipulating Information

Above pictures are genuine but the comments written on the picture are false. In picture 1 comment show that popular wing commander Abhinandan Sharma is saying that "In past also army was powerful, but government was not powerful". This comment was

never made by the Abhinandan Sharma. Where another picture shows that Indian PM Modi and BJP leader Amit Shah are talking, and Modi is saying "see! Congress manifesto is full of lies" and Amit Shah replies that "see carefully! This is our manifesto of 2014". This picture is edited, and comments are written in a way reader can think may Abhinandan Sharma made this comment and also to show that BJP's 2014 manifesto was full of lies and PM and party leaders admitted that this is manipulative content used to manipulate the voters.

From 57 images, almost 50 images were either, hoax, fake, misleading or they were manipulative. This manual image analysis shows that groups members as a political party supporter are spreading the news using the pictures.

10 Future

This research also has future scope to expand the study further in important areas. Some of the areas are:

- The research could be further expanded to create tools to recognize the offensive, fake, hoax and misleading advertisements during the election by using the machine learning or text analysis techniques.
- It could be taken to the next level to study all the possible tricks politicians are using to abuse social media platforms. This study will give a clear view of how political parties are abusing the platforms.
- The importance of the study on WhatsApp chat application will also help to analysis the political cyber propaganda attacks on the similar messaging application to WhatsApp like -Telegram, Instagram.
- It can be taken as a reference to study the political cyber propaganda in other countries before the election.
- An awareness campaign can be run based on the results of the message analysis.

11 Conclusion

WhatsApp is a good social media application to contact the people in cheap and fast way. WhatsApp group is a feature of WhatsApp application where more than two people can talk in same inbox. In WhatsApp group one member of the groups can broadcast the messages to all the group members. Political supporters are creating hundreds of the WhatsApp groups to connect with the voters. Political leaders are also using WhatsApp to communicate internally with party worker and sharing the political messages.

It is a common practice on WhatsApp to share the message which is forwarded by the other people. In India WhatsApp is a popular messaging app, Indian WhatsApp users use WhatsApp for everyday communication. IT is common practice in India to share the WhatsApp messages and forward them further to their friends and family and it became a long chain of forwarding a message and that is how the WhatsApp messages goes viral in India. Indian WhatsApp users also share the political messages not only WhatsApp message but also messages from Facebook, Twitter, Instagram and other sources.

Political party supporters have created public WhatsApp groups to share the political information, they are sharing these group invitation links in other WhatsApp groups, other social media platforms and also has some private webpages which shares these group invitation links further. Groups members of these groups are posting the political messages. They are posting messages in text, video, pictures and audio format along with messages they are also posting links contacts numbers. During the research we found the messages, which were not related to election in India or politics.

The messages forwarded by the group members includes extreme content, they shared messages with suspicious links these links redirect to virus, malware, spam or phishing webpages. According to the messages they have shared the contact number of call girls of different countries. Group members are also spreading the hoax audio messages, fake, misleading and manipulating text messages. The spreading of harmful content in political WhatsApp group could be dangerous. These messages also urge people to forward the messages further to the family and friends. These messages are so powerful that during over analysis we have found different group members from different WhatsApp group have shared the same messages.

WhatsApp is a strong platform to share the message and news, but the fraud is spreading via WhatsApp. Political WhatsApp group admin should be responsible for all the fraud links and messages, fake images, manipulating and misleading content, tampered videos

and hoax audios spreading in the political WhatsApp groups. Lack of the security and easy availability is making the WhatsApp messaging application vulnerable for the abuse. In the election people are more curious to read, watch and listen to the political news and for that, they join the political WhatsApp groups and from these group they get all this false news and malicious links.

As we can understand that people are not using the WhatsApp only for the spreading the propaganda but in India WhatsApp is being used for the good work as well. Like - Delhi government shared a WhatsApp number for the women safety purpose. So, when women is travelling she can post the taxi number and driver name in the group and Delhi police will follow the taxi route is it dropping the girl at right place. Some of the state government also published the WhatsApp number to complain about the traffic or complain about the corruption they faced. So, WhatsApp is a two-side sword with positive and negative effect on the society. we can't eliminate the application because of the false it has because we also had the positive effect of WhatsApp in the society.

WhatsApp should improve functionality to eliminate the fraud and propaganda from its platform specially during the election season. A spam filter needed to filter the good messages from the spam messages. During election it should work more actively to eliminate the false news from the platforms and stop the spreading propaganda via WhatsApp. WhatsApp could be a good political news platform if all the news are general or it has a feature to check the legitimacy of political news. WhatsApp can help for the uninflected election in India by eliminating the fake news and making the platform more secure, by creating another option where WhatsApp can post famous fake news messages it has detected on the platform. Instead of helping in spreading the fake political propaganda

12 Bibliography

- [1] G. V. a. S. Hangal, "India's political parties have mined voter's psychographic data for years," Quartz India, 2018.
- [2] K. P. G. M. Meti V, "Social Media for Political Mobilization in India: A study," *J Mass Communicat Journalism*, 2015.
- [3] S. B. Snigdha Poonam, "The Atlantic," 1 April 2019. [Online]. Available: <https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/>.
- [5] "WhatsApp," [Online]. Available: <https://www.whatsapp.com/about/>.
- [6] Statista, "Statista, [Number of social network users in India from 2015 to 2022 (in millions)]," [Online]. Available: <https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/>.
- [7] wikipedia, "2014 Indian general election".
- [8] WhatsApp, "Faq, [Security and Privacy]," [Online]. Available: <https://faq.whatsapp.com/en/android/28030015/>.
- [9] "The Washington Post," 2018. [Online]. Available: https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads/?noredirect=on&utm_term=.84fa66452756.
- [10] Which?, "How to stop social media scams".
- [11] BBC, 18 Feb 2019. [Online]. Available: <https://www.bbc.com/news/world-south-asia-12557384>.

- [12] worldometer, “Worldometers,” march 2019. [Online]. Available: <https://www.worldometers.info/world-population/india-population/>.
- [13] statista, “The Statistics Portal,” Aug 2019. [Online]. Available: <https://www.statista.com/statistics/274658/forecast-of-mobile-phone-users-in-india/>.
- [14] I. Times, 15 Jan 2019. [Online]. Available: https://www.indiatimes.com/technology/news/smartphone-users-in-india-smartphone-penetration-is-set-to-reach-373-million-users-in-2019_-360475.html.
- [15] Statista, “The statistics portal,” Jan 2019. [Online]. Available: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.
- [16] ETCIO, “ETCIO.com,” 13 June 2018. [Online]. Available: <https://cio.economicstimes.indiatimes.com/news/social-media/up-bjp-to-prepare-cyber-sena-of-2-lakh-social-media-experts-for-2019-polls/64569317>.
- [17] S. Sahu, “Indian National Congress,” International Encyclopedia of the Social Science.
- [18] TimesofIndia, “From 1980 to 2018, this is how the BJP has risen,” timesofindia.com, New Delhi, 2018.
- [19] NDTV, “Election Results 2014: 5 Factors that helped BJP and Narendra Modi win the election,” 16 May 2014. [Online]. Available: <https://www.ndtv.com/cheat-sheet/election-results-2014-5-factors-that-helped-bjp-and-narendra-modi-win-the-election-562309>.
- [20] C. B. C. T. N. P. O. F. B. Chico Marés, “Fake news is poisoning Brazilian Politics. Whatsapp can stop it”.
- [21] News18.com, “dailyhunt, [Here's the inside story on why the BJP President Amit Shah joined 1,800 WhatsApp Groups],” 23 Jul 2018. [Online]. Available: <https://m.dailyhunt.in/news/india/english/news+gram+24-epaper->

newsgram/here+s+the+inside+story+on+why+the+bjp+president+amit+shah+joi
ned+1+800+whatsapp+groups-newsid-92927738.

- [22] PTI, "Business Today," 18 Dec 2018. [Online]. Available:
<https://www.businesstoday.in/technology/news/whatsapp-launches-tv-campaigns-to-fight-fake-news-in-india/story/296805.html>.
- [23] R interview Bubble, "Indian population religion wise 2018 Religious Population in India," 9 Jul 2018. [Online]. Available: <https://interviewbubble.com/indian-population-religion-wise-2018-religious-population-in-india/>.
- [24] R. Iyengar, "In India's last election, social media was used as a tool, This time it could become a weapon," CNN Business, New Delhi, 2019.
- [25] M. Krishnan, "India fight fake news on social media ahead of election," Deutsche Welle (www.dw.com), New Delhi, 2019.
- [26] I. W. Stats, "Internet World Stats," 20 Mar 2019. [Online]. Available:
<https://www.internetworldstats.com/stats8.htm>.
- [27] S. Dogra, "News18," 25 Feb 2017. [Online]. Available:
<https://www.news18.com/news/tech/whatsapp-reaches-200-million-monthly-active-users-in-india-1353068.html>.
- [28] M. Iqbal, "Business of Apps," 2019 Feb 19. [Online]. Available:
<http://www.businessofapps.com/data/whatsapp-statistics/>.
- [29] S. Kedem, "Verdict," 16 Apr 2018. [Online]. Available:
<https://www.verdict.co.uk/indias-smart-phone-users/>.
- [30] T. E. Times, "The Economic Times," 06 Mar 2019. [Online]. Available:
<https://economictimes.indiatimes.com/tech/internet/india-has-the-cheapest-mobile-data-in-world-study/articleshow/68285820.cms>.

- [31] F. House, "Freedom House," 14 Nov 2017. [Online]. Available: <https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy>.
- [32] A. Chang, "Vox," 2 May 2018. [Online]. Available: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>.
- [33] S. B. Psaila, "Digital Watch," 24 Apr 2018. [Online]. Available: <https://dig.watch/trends/cambridge-analytica>.
- [34] H. Ritchie, "CNBC," 30 Dec 2016. [Online]. Available: <https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html>.
- [35] W. Cumming, "USA Today," 18 Dec 2018. [Online]. Available: <https://eu.usatoday.com/story/news/politics/2018/12/17/russia-social-media-senate-report/2334382002/>.
- [36] A. J. Gaughan, "Illiberal Democracy: The Toxic mix of fake news, hyperpolarization, and partisan election administration," *Duke Journal of Constitutional Law & Public Policy*, 2017.
- [37] P. G. M. A. P. K. Srithi Gupta, "Exploiting Phone Numbers and Cross-Application Features in Targeted Mobile Attacks," *ACM*, 2016.
- [38] E. Hickok, "The Influence Industry Digital Platforms, Technologies and Data in the General Elections in India," 2018.
- [39] B. News, "India election 2019: voting kicks off in world's largest election," 11 Apr 2019. [Online]. Available: <https://www.bbc.com/news/world-asia-india-47878085>.

- [40] I. Ali, "Voanews," 06 Jun 214. [Online]. Available:
<https://www.voanews.com/a/social-media-emerges-as-a-key-tool-in-indias-election/1931238.html>.
- [41] D. Arnado, "Computational Propaganda in Brazil: Social Bots during Elections," *Univeristy if Oxford*, 2017.
- [42] A. Boadle, "Reuters," 20 Oct 2018. [Online]. Available:
<https://www.reuters.com/article/us-brazil-election-whatsapp-explainer/facebooks-whatsapp-flooded-with-fake-news-in-brazil-election-idUSKCN1MU0UP>.
- [43] J. G. F. S. Matheus Magenta, "How WhatsApp is being abused in Brazil's election," 24 Oct 2018. [Online]. Available:
<https://www.bbc.com/news/technology-45956557>.
- [44] F. B. P. O. By Cristina Tardáguila, "The New York Times," 17 Oct 2018. [Online]. Available: <https://www.nytimes.com/2018/10/17/opinion/brazil-election-fake-news-whatsapp.html>.
- [45] B. bucher, "Columbian Election 2018," 9 Apr 2019. [Online]. Available:
<https://www.messengerpeople.com/election-campaigns-via-whatsapp/#Columbia>.
- [46] P. k. Sanjay Kumar, "livemint, [How widespread is WhatsApp's usage in India?]," 18 Jul 2018. [Online]. Available:
<https://www.livemint.com/Technology/O6DLmIibCCV5luEG9XuJWL/How-widespread-is-WhatsApps-usage-in-India.html>.
- [47] C. smith, "DMR Business statistics | Fun gadgets, [65 Amazing WhatsApp Statistics and Facts (August 2018)]," 10 Nov 2018. [Online]. Available:
<https://expandedramblings.com/index.php/whatsapp-statistics/4/>.
- [48] V. Goel, "The New York Times, [In India, Facebook's WhatsApp Plays Central Role in Elections]," 14 May 2018. [Online]. Available:
<https://www.nytimes.com/2018/05/14/technology/whatsapp-india-elections.html>.

- [49] m. safi, "The Guardian," 3 Jul 2018. [Online]. Available: <https://www.theguardian.com/world/2018/jul/03/whatsapp-murders-india-struggles-to-combat-crimes-linked-to-messaging-service>.
- [50] B. Perrigo, "TIME," 25 Jan 2019. [Online]. Available: <http://time.com/5512032/whatsapp-india-election-2019/>.
- [51] A. K. Sankalp Phartiya, "Reuters," 6 Feb 2019. [Online]. Available: <https://www.reuters.com/article/us-india-whatsapp/indian-political-parties-abuse-whatsapp-service-ahead-of-election-executive-idUSKCN1PV1E3>.
- [52] S. S. Singh, "Weaponizing Data for Politics," in *HasGreek TV*, 2018.
- [53] D. Walton, "What is propaganda , and what exactly is wrong with it," *Public Affairs Quarterly*, vol. 11, 1997.
- [54] B. News, "[Muzaffarnagar: Tales of death and despair in India's riot-hit town]," 25 Sep 2013. [Online]. Available: <https://www.bbc.com/news/world-asia-india-24172537>.
- [55] X. Peerzada Arshad Hamid, "Asia & pacific Edition, [1 killed, 4 injured by mobs in India on rumors of child kidnapping]," 15 Jul 2018. [Online]. Available: http://www.xinhuanet.com/english/2018-07/15/c_137325867.htm.
- [56] K. Iwanek, "The Diplomat, [WhatsApp, Fake News? The Internet and Risks of Misinformation in India]," 30 Jul 2018. [Online]. Available: <https://thediplomat.com/2018/07/whatsapp-fake-news-the-internet-and-risks-of-misinformation-in-india/>.
- [57] A. Jazeera, "[Deadly rumours: India's WhatsApp dilemma]," 16 Dec 2017. [Online]. Available: <https://www.aljazeera.com/programmes/listeningpost/2017/12/deadly-rumours-india-whatsapp-dilemma-171216091928319.html>.

- [58] R. Pathania, "Facebook, [मध्यप्रदेश कांग्रेस नेता शबाना सारा अली अपने घर में चलाती थी बैश्यावरती का धंधा। पुलिस की रेड में पकड़ी गई खुद भी और अन्य।]," 14 Nov 2018. [Online]. Available: <https://www.facebook.com/groups/NARENDRAMODI31/permalink/3207144945975782/>.
- [59] P. Chaudhuri, "ALT news, [Photo of Congress leader misused and linked to prostitution racket]," 15 Nov 2018. [Online]. Available: <https://www.altnews.in/photo-of-congress-leader-misused-and-linked-to-prostitution-racket/>.
- [60] P. K. Srishti Gupta, "Emerging Phishing Trends and Effectiveness of Anti-Phishing Landing Page," *Cybersecurity Education and Research Center (CERC)*, 2014.
- [61] P. S. Chadha, "Honey traps or online scams, fraudsters use social media as their new hunting ground," *Hindustan Times*, Gurugram, 2018.
- [62] A. M. Amishi Arora, "Threats to Security and privacy of Information due to growing use of social media in India," *Asian Journal of Managerial Science*, vol. 6, 2017.
- [63] M. M. H. Amila Banerjee, "Is Fake News Real in India," in *Research Gate*, 2018.
- [64] G. Farooq, "Politics of Fake News: How Whatsapp Became a potent propaganda tool in India," 2018.
- [65] G. T. Kiran Garimella, "WhatsApp, Doc? A first look at WhatsApp public group data," in *International AAAI Conference on Web and Social Media (ICWSM 2018)*, 2018.
- [66] L. S. Sterling, *The Art of Agent-Oriented Modeling*, London: The MIT Press, 2009.

Appendix 1 – [Heading of Appendix]