IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

Perception-Based Geographical Analysis of Cybercrime: Assessing Vulnerability of Women, Child and Senior Citizens in Palam Colony, NCT Delhi

Heena Kumar[1]. Garima Chauhan[1] and Dr. Shweta Rani[2]

B.A. Programme, Dyal Singh College, University of Delhi, Lodhi Road, New Delhi, India[1]

Assistant Professor, Department of Geography, Dyal Singh College, University of Delhi, Lodhi Road, New Delhi, India[2]

Corresponding Author's Email: shwetarani@dsc.du.ac.in

Abstract: The Internet has become a necessity in today's world. It is one of the most useful and harmful things depending upon its usage. In the world of crimes also internet plays a significant role in helping black hat hackers in committing cyber-crimes and steal personal information. Electronic devices and the internet are used in these types of crimes like cyber pornography, email booming, exposure to harmful content, grooming, harassment, sexual abuse, cyber-stalking, virus attacks etc. Educated as well as uneducated, both are the victims, and the most vulnerable part of society is children, women, and senior citizens. Children are among the newest victims of cyber-crime. Our study area is the cyber city Delhi, which is secondarily survey including a case study of Palam district. The present study is concerned with finding and examining the problems and impact of cyber-crime on children, women, and senior citizens by suggesting some mitigation measures to boost cyber security. Questionnaires are discussed and results show how much people are aware of cyber-crimes, the connection between cyber-crimes and children, women & senior citizens, and what kind of problems they face in dealing with such kinds of crimes. The findings suggest that people do know about this current problem, but more awareness is needed from a small level like school discussions should have this kind of topics, elderly people don't use social sites much but receive fake calls from banks and companies which try to manipulate them. To reduce the level of cyber-crime, some suggestions and solutions are discussed at the end.

Keywords: Cybercrime, Internet, Child, Women, Senior Citizens, Delhi, Palam

1. INTRODUCTION

India is the land of diversity giving shelter to majority of world's population. Due to vast geographical expends from latitudes 8°4′N and 37°6′N and longitudes 68°7′E and 97°6′E, with varied topographical features from Himalayas and Great Indo-Gangetic Plains in the North to Indian Ocean in the South and conducive monsoonal climate, this nation is one of the most favorable destinations for human habitation. With the attainment of independence India saw a momentous growth in its population reaching to an all-time high figure of 1.21 billion in 2011 and 1.40 billion in 2021*. While on one hand, increasing population adds to the man-power and human resource development of the nation, the continuous and rapid growth in population without being productively utilized, on the other, also results in a growth of a number of negative impacts of the society. Criminal activities are one of such ill effects of perpetuating population who are not adequately recognized in the society and a devoid of any means to sustain their life.

In India, criminal activities have been carried out by various means during1990s. For example, people do crimes related to chain snatching and thieving. But with the passage of time and strict laws and action there has been declined in both the cases registered and reported. Amidst such scenario and with the development of Research and technology, people find newer ways to commit crimes in a digital way with the aid of computers smartphones and other electronic gadgets in a fast and smarter way. While on one hand technology helps and makes our lifestyle easy; it also renders our lifestyle more challenging on the other. The crimes and frauds committed via digital gadgets and online mediums are termed as cybercrimes. Cybercrime refers to crimes which took place with the help of the internet and electronic devices (phones, laptops etc.) and mostly attacks on the vulnerable side of society including children, women, and senior citizens. We must all accept that internet has given rise to new opportunities in the fields of education, business, entertainment and acts as a source of livelihood for many. With the emergence and spread of Covid-19, the entire world came to a standstill with a nation-wide lockdown imposed. The geographical diffusion and contagious nature of this pandemic was such that people became prisoners in their own home and many lost their jobs and other related source of

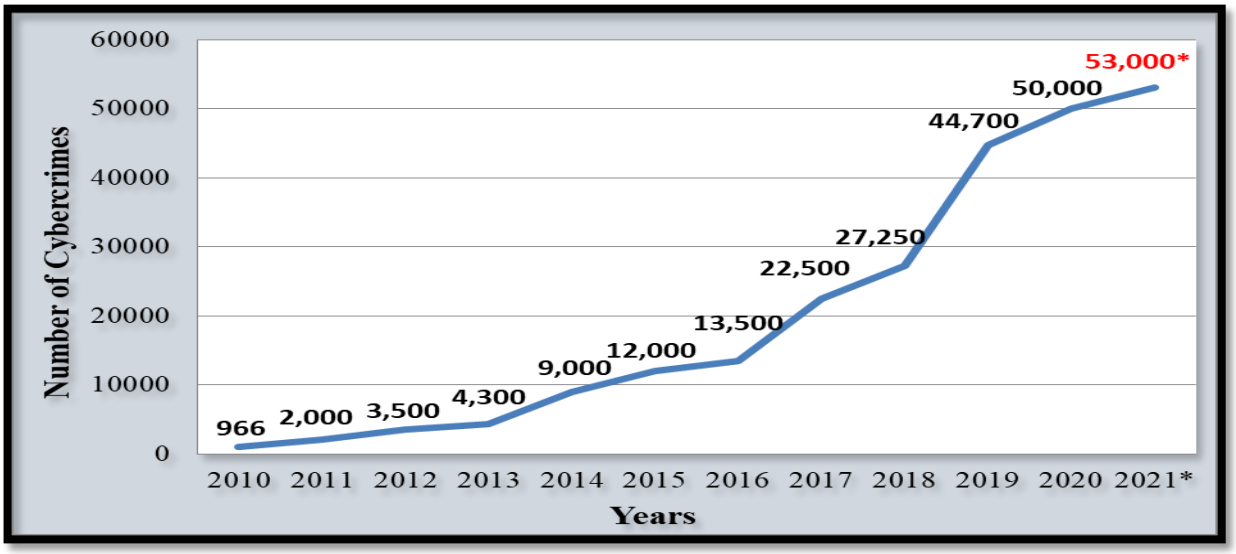
DOI: 10.17148/IJARCCE.2023.12502

livelihood. Resorting to digital and online mediums for various daily activities was the only option available to them to sustain their life. In fact, due to lockdown reasons, people were not able to move outside and the usage of electronic devices and the internet increased, which helped criminals to perform such crimes. The increase in online users especially during the pandemic provided a breeding ground and the right platform for the sudden surge in the digital criminal activities and growth in cybercrimes is no exception to this. Crimes such as harassment via e-mail, cyber-stalking, cyber defamation, morphing, hacking, cyber pornography, cyber flirting, bullying, threats, posting and publishing of obscene sexual content and the establishment of fake profiles etc. are the classic examples and related forms of cybercrimes.

1.1 Cybercrimes: An Indian Perspective

Cybercrimeis considered as one of the leading human-made disasters in the present times. The first case of cybercrime in India was reported in 1999 and it was a case of using an unauthorized trademark or domain name 'yahooindia.com'. After this, the number of related crimes increases day by day.

Figure 1: The Trending Pattern of Cyber Crimes in India (2010-2021)



Source: National Crime Records Bureau of India (2023)

***Provisional Data of 2021**

Figure 1 shows the increasing trend of cybercrimes in India from 2010 to 2021. There were 966 cases of cybercrimes reported in India in 2010 which doubled to 2000 cases in next one year in 2011. Since then, the trend witnessed a momentous growth in the number of cases and reached to 13,500in next 5 years i.e. in 2016. Due to rapid advancement in science and technology, the number of cybercrime rates also increased and rose to a record level of 53,000 registering a growth rate of almost 400% in 2021. At disaggregate level of temporal scale, there was a 6% increase in the rates of cyber rime in 2021 from the previous year. Today India ranks 3rd among the nations facing cyber threats in the world.

One of the major reasons attributable for such markedly increase in its rate is the low difference in literacy levels between men and women and non-fulfilment of basic human needs. India's literacy rate was 74.04% in 2011 with female literacy at 65.46% and male literacy at 82.14%. The gender gap in literacy level was almost 17%. Women's literacy plays a vital role in every aspect and social factors should improve with time. With the passage of time, the female literacy improved and reduced the existing gaps. Amidst, increasing population pressure and lack of alternative sources of living, people chose the wrong paths and made cybercrime a means of life for earning money or taking revenge. Based on preceding discussion, an attempt has been made to represent the highlight the top 5 motives for committing cybercrimes in India in 2021.

Figure 2 portrays the most important causes for committing cybercrime. People who indulge themselves in activities related to cybercrimes mostly do so to commit fraud, sexual harassment, extortion, reputational damage, personal revenge etc. Involvement in cybercrime is considered to be one of the best ways to get more money in lesser time. Out of the above cited motives for cybercrime, almost 30,142 cases have been registered involving Fraud. Sexual

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

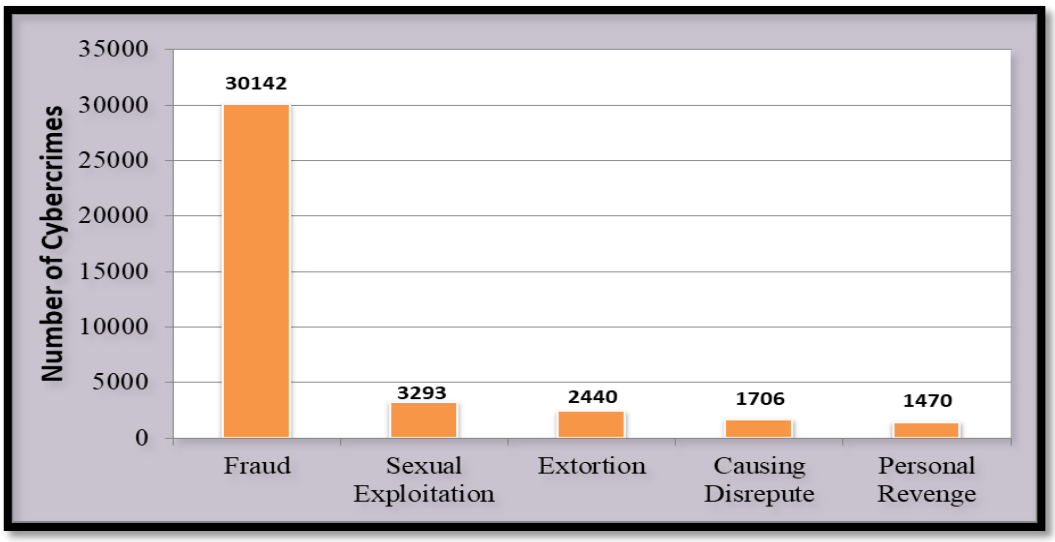
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

exploitation with 3293 cases takes the second instance followed by extortion (2440), reputational damage (1706 and personal revenge with 1470 cases registered in 2021.

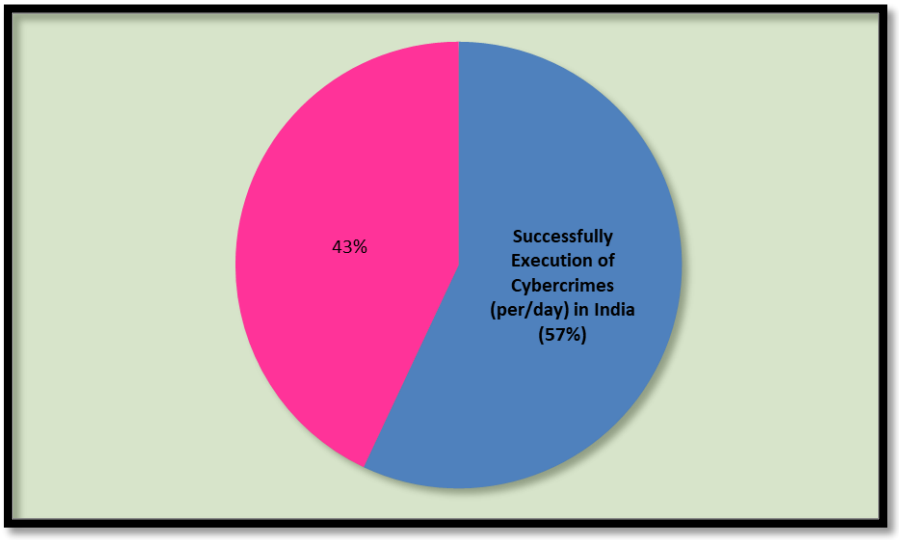
Figure 2: Top 5 Motives for Committing Cybercrimes in India (2021)



Source: National Crime Records Bureau of India (2021)

It is a general perception that less educated people who are unaware of such kinds of human-induced disasters can be more easily fooled and bluffed and they are the immediate victims of such cyber frauds. Indians are recognized as one of the hardest working species in the world. In fact, people earn money and more importantly reputation and self-respect by working their whole life and by the single click of cyber fraud, they are on the verge of losing everything. It earns a social disrespect and monetary loss to them. We must understand that being tech savvy is good to accept but more digitization leads to more devastation and penetration to our privacy. It is seen that after Covid 19 attack and with subsequent lockdowns, people were not able to move out and relied heavily on digital medium for their day-to-day activities. In fact, the usage of internets and digital gadgets increased tremendously and conspicuously. Rampant and frequent usage of such electronic devices and the internet provided the breeding grounds for the crimes related to digital mediums i.e., cybercrimes. Since, this phenomenon was on a rising trend and technological advancements lured them to perform such crimes more easily and proficiently. Following this trend, figure 3 shows that the causes of cyber-crimes got extenuated and the per day successful ratio increased to more than 50% in India in 2023.

Figure 3: Successfully Execution of Cybercrimes (per/day) in India (2023)



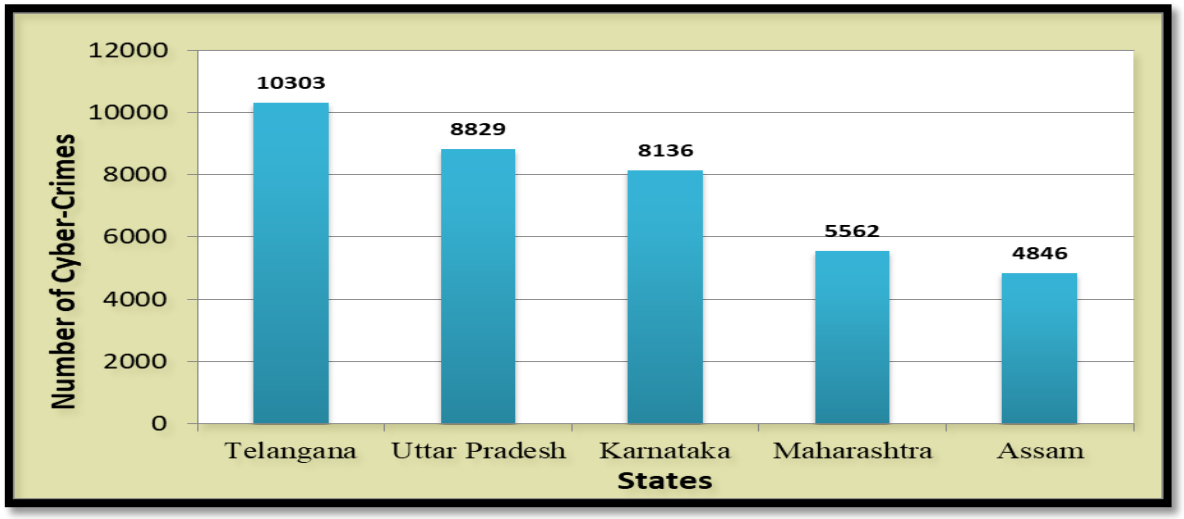
Source: Statista (2023)

DOI: 10.17148/IJARCCE.2023.12502

In relation to the growth of cybercrimes and rural urban divide in India and, it has been observed that such kind of crimes are more geographically suited with increasing cases reported especially in the urban areas. Urban dwellers and people living in cosmopolitan society have a busy lifestyle with no time to regularly check and suspect the fake calls and messages received. Hence, they easily get trapped into such crimes in no time.

A state level analysis of occurrences of cybercrimes in India reveals there existing state wise variations. The state of Telangana topped the list among all the states in India. The national capital of Delhi, however occupied 19th position among the States and Union Territories (UTs) in India. At disaggregate level, among the important Indian cities largely hit by cybercrimes, the city of Bengaluru tops the list among the other cities followed by Hyderabad and Mumbai.

Figure 4: States-wise Number of Cybercrimes in India (2021)



Source: National Crime Records Bureau of India (2021)

Figure 4 shows the top 5 states in India where both the rates and trends in cybercrimes in perpetuating day by day. The southern state of Telangana lies at the top of the list with one of the highest cybercrime cases i.e., 10,303 reported in India in 2021. Uttar Pradesh is at the second position with a total reported case being 8,829. The state of Karnataka lies at the third spot with a total case of 8,136. It is followed by the next Southern state of Maharashtra with a reported case of 5,536. The state of Assam which belongs to the seven sister states of North-East India, occupies the fifth position which a total registered case of cybercrimes being 4,846. This explains the geographic discrete nature of origin, distribution and penetration of cybercrimes in India. Cybercrime is increasing exponentially day by day. The main reasons attributable for such a high trend in cybercrimes are better technological advancements with a low level of knowledge to use and operate such technology, lack of effective implementation of government plans and policies with a view to provide a better living condition. The National Capital of Delhi is no exception to this witnessing a propulsive increase in the rates of cybercrimes. The population of Delhi is increasing by leaps and bounds since independence with its diverse nature. At the same time, the limited geographical area puts a pressure on the existing land resource and limited urban facilities and job opportunities to the fresh new migrants added every year. As a result of this, people belonging to diverse backgrounds are found indulged in easy and unethical means of living like crimes, robbery, theft etc. Cybercrime is one such unethical means of urban living.

1.2 Growth of Cybercrime in Delhi NCT

Delhi is the national capital of India, the centre of Indian politics, a metropolitan city with smart CCTV surveillance, and as the hub of educational institutions have cosmopolitan culture, better health facilities, free travel in DTC buses for women, high job opportunities etc. Owing to such facilities, this city acts as the suction point attracting the pool of migrants from neighbouring states of Uttar Pradesh, Haryana, Rajasthan and even labour work force from states like Odisha and Bihar. Due to non-availability of proper job opportunities, deep rooted poverty, low level of income and education and stiff competition are some of the luring factors that compel the migrants and the residents of Delhi to do malpractices and use inappropriate ways to fill their family's empty stomach. Delhi is one of the fastest growing city in the world and as per World Urbanization Prospects, the city of Delhi ranks second in the world next only to Tokyo in terms of population growth.

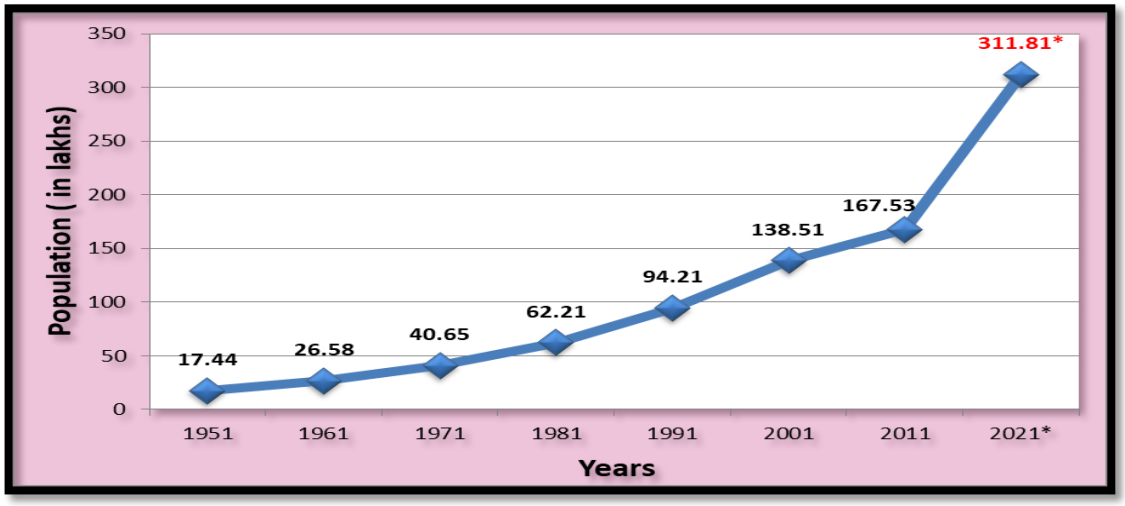
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

Figure 5: Growth of population in Delhi from 1951-2021



Source: Census of India (2011)

***Provisional Data of 2021**

Figure 5 explains the rising trends of population growth of Delhi NCT from 1951 to 2021 *. In 1951 the total population of Delhi was 17.44 Lakhs which increases to 94.21 Lakh in 1991 and to a high of 167.53 Lakh in 2011 (PCA, 2021). According to the provisional data of 2021*, the population of Delhi rose to all time high figure of 311.81 Lakhs. The increasing trend in urbanisation and fresh migration waves from different parts of India is further adding to this growing scenario of population and putting a pressure on the carrying of the National Capital.

The National Capital Delhi is divided into 9 districts: Central Delhi, East Delhi, New Delhi, North Delhi, North East Delhi, North West Delhi, South Delhi, South West Delhi, West Delhi. The study area Palam colony is situated in South Delhi which is one of the highly developed areas of Delhi. People living in this area are professionals in their fields and most of them have a good educational background. No one has ever researched this area but it is suitable to study the treading crimes like cybercrimes in these types of areas. The scientific world is full of technologies but doing things wrong doesn't makes things and situations right. Hackers use non-registered identities and contact with other gang members and some chosen people with a lot of valuables. Now, the Aadhar card is necessary to link with a bank account, pan card, voter Id card etc., and it dissolute our privacy. They are very intelligent and smart in manipulation with their sweet voices. They identify victims 'weaknesses and use them against them. They attract children through games and bribe them to get money through false links, women and senior citizens through fake lottery winning calls, bank card renewal calls, fake relatives to transfer money etc. They use copies of trusted websites and fool individuals through their pirated links. Here comes the role of education and awareness, those who have knowledge of such kinds of incidents can ride off it but those who are illiterate and unaware of cyber-crimes get caught and bear great losses. It's the duty of the government or state to provide primary education and cybercrime topics should be included in the syllabus. Initiatives should be taken and hard rules are needed to threaten the wrong and protect the right. There are no such hard and fast rules for cyber security in India but we're growing rapidly in the surfing world of the internet so seeing the increasing rate of cybercrime, the need becomes stronger than before.

2. CONCEPTUAL FRAMEWORK

An attempt has been made by the researcher to explain the difficult terminologies for cybercrime. A conceptual framework includes one or more formal theories (in part or whole as well as other concepts and empirical findings from the literature. It is used to show relationships among these ideas and how they relate to the research study.

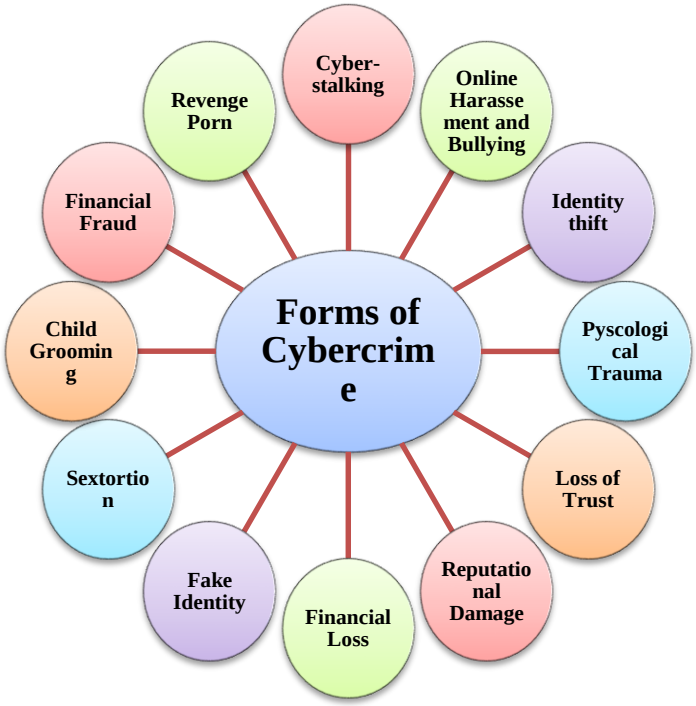
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

Figure 6: Cybercrimes and its Arena of Influence



Source: Self Prepared by Author (2023) based on Concepts derived

- **Cyber-Stalking**: This is the act of using the internet or other electronic communication to harass or intimidate someone. Cyber stalking can involve sending threatening messages or making unwanted advances, among other things.
- **Online Harassment and Bullying**: This includes the use of the internet or social media to humiliate or intimidate someone, often using derogatory comments or threats.
- **Revenge Porn**: This involves the distribution of sexually explicit images or videos without the consent of the person depicted, often as a form of revenge or harassment.
- **Financial Fraud**: This includes scams and other forms of fraud that target seniors or other vulnerable populations, often involving requests for money or personal information.
- **Child Grooming**: This involves an adult building an online relationship with a child with the intention of engaging in sexual activity.
- **Sextortion**: This is when someone threatens to release sexually explicit images or videos unless the victim agrees to certain demands, such as sending more explicit content or paying money.
- **Faking Identity:** This is when someone fakes social media account of some known women and share videos, images or content to harass her.
- **Financial Loss**: Cyber-crime can result in significant financial losses for victims, particularly if their bank accounts or credit card details are stolen. This can affect their credit score and make it difficult for them to secure loans in the future.
- **Identity Theft**: Cybercriminals may use stolen personal information to commit identity theft, which can cause long-term damage to a victim's credit history and financial well-being. It can take months or even years to clear up the damage done by identity theft.
- **Psychological Trauma**: Victims of Cyber-crime may experience psychological trauma, such as anxiety, depression, and post-traumatic stress disorder. This can affect their quality of life, relationships, and work performance.
- **Loss of Trust**: Victims of Cyber-crime may lose trust in online platforms and may become less likely to engage in online activities or make purchases online. This can have a significant impact on their daily lives, particularly if they rely on online services for work or personal reasons.
- **Reputational Damage**: Cyber-crime can cause reputational damage, particularly if personal or embarrassing information is stolen and shared online. This can have long-term consequences for a victim's personal and professional life.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

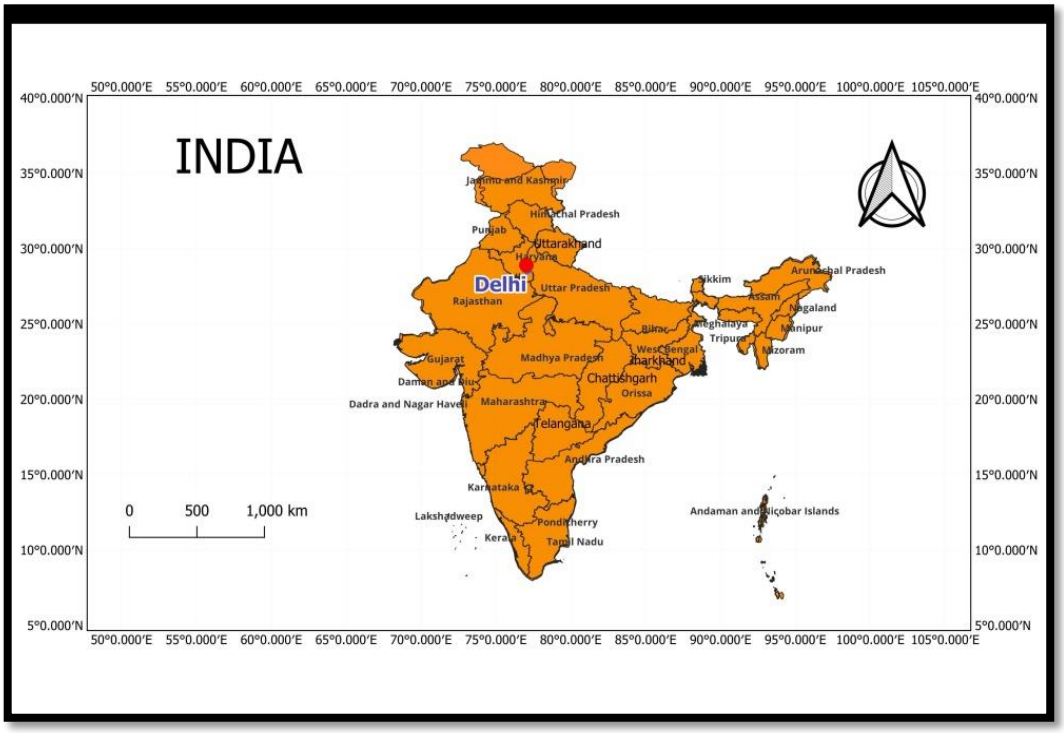
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

3. THE STUDY AREA: DELHI (PALAM COLONY)

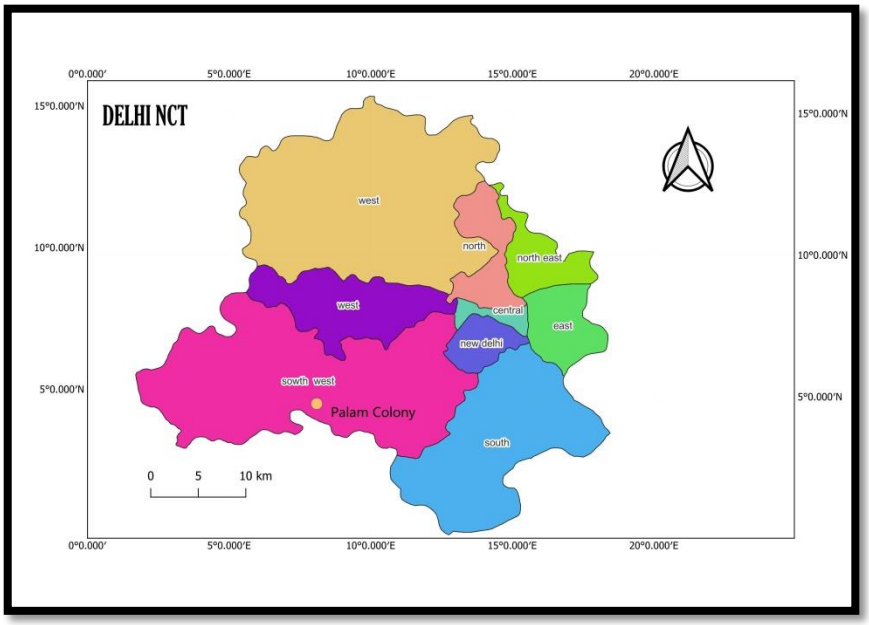
Delhi is the Capital of India; it is an administrative centre of the country. Geographically speaking, Delhi NCT extends from 28°36′36′′N, 77°13′48′′E and covers a total geographical space of 1,484 square kilometres (see figure 7a). The study area extents from 28°35’21” N latitudes and 77°5’9” E longitudes covering a total geographical space of 510.61 Square kilometres (see figure 7b).

Figure 7a: Geographically Setting of Delhi NCT in India



Source: Prepared using QGIS (2023)

Figure 7b: Location of Palam in Delhi NCT



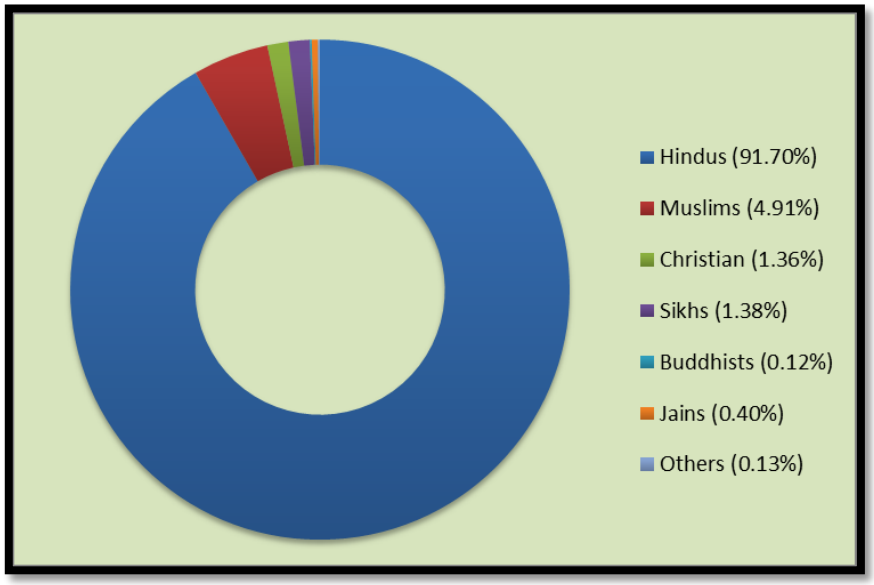
Source: Prepared by author using QGIS (2023)

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12502

The study area Palam is a major residential area located in Southern part of national capital, Delhi within the South West district. It is one of the 70 Vidhan Sabha constituencies located in Delhi National Capital Territory. According to Census of India, 2011, the total population of study area was 2,00,000+.

Palam is situated 20 km South West of the hub of New Delhi City Centre. Palam is divided into 2 sub-divisions, Raj Nagar and Sadh Nagar. Raj Nagar is divided into 2 parts: Raj Nagar Part 1 and Raj Nagar Part 2. Similarly, Sadh Nagar is divided into Sadh Nagar Part 1 and Sadh Nagar Part 2. The Palam is famous for Khap Panchayat. There are 9 districts in Delhi and Palam comes under Southwest Delhi. Palam is a populated area as many people migrate in this area to find job opportunities, education, hospital facilities. Figure 7 depicts the demographic composition of South-West Delhi is 91.70% are Hindus, 4.91% Muslims, 1.36% Christian 1.38% Sikhs, 0.12% Buddhists, 0.40% Jains, 0.13% Others. It comprises a large population which brings many problems such as frequent power cuts, narrow roads that create hassle in the commuting, water logging etc.

Figure 8: Demographic profile of South-West Delhi



Source: Census of India (2011)

4. LITERATURE REVIEW

Hati (2016)opined that cybercrime is one of the major disadvantages of the internet which is used for crimes like cyber stalking, child pornography, copyright infringement etc. He further stated that at the global level, both the government and non-state actors are engaged in fighting cybercrime. Malicious use of information technology was difficult to be tracked back to its origin. There is a severe lack of information security awareness among technology users. He raised his concern and suggested that though Indian laws are well-defined and capable of handling such crimes, yet, law enforcement agencies need to be well-versed with the technology and keep themselves abreast of continuous changes and new avenues of cyber-crimes emerging on a regular basis.

Muthulakshmi (2017) viewed that Cybercrimes are those criminal activities where a computer or network acts as the source, tool, and it targets poor place of crime. During a survey on B.Ed. students, he found that males are more aware of these types of typical crimes than women.

Jazeel (2018) observed that number of Cybercrimes is increasing day by day all over the world. Jazeel further opines that people are less aware of Cybercrimes. Even educated teacher trainees are less aware of such type of crimes and only a few of them have a high level of awareness. On grounds of gender, males are more educated than females and on grounds of locality; urban dwellers are more aware than their rural counterparts. But the irony is that, be it rural or urban, educated or less educated, majority of the people lack sound knowledge of computers and that also only a few of them own their own computers. They do have appropriate knowledge of their subjects but not everyone is fully aware of perpetuating trends in Cybercrimes.

Khan (2023) discussed the concept of cybercrime and defined the rate at which cybercrime is increasing nowadays. He also suggested some preventive measures in his paper. He stated that internet and electronic gadgets harm our privacy. He further suggested that there should be laws about 'confidential personal data', which guarantee data protection and privacy of people.

DOI: 10.17148/IJARCCE.2023.12502

Aliperti (2021) posit that the majorly affected group is senior citizens as they are the most trustworthy than youngsters and have a lot more wealth. It's easy to make them fool and most of the time they feel ashamed to tell others about their loss and prefer to remain quiet so that they don't lose their family's trust. He also discussed the major type of cybercrimes and preventive measures.

Mishra (2018) put forward the definition of cybercrime, and then discussed about cybercrime against women, computer viruses, cyber-terrorism, and phishing scams. Cybercrime includes cyber-stalking, harassment via e-mails, cyber-bullying, morphing, email spoofing, cyber-defamation, trolling and gender bullying. Article 19of the Constitution provides the Fundamental Right to Speech and Expression. The Information Act 2000 has provided reasonable restrictions against cybercrimes. The act does not provide any remedy to control cyber tolling and gender bullying which is one of the lacking point of this act. He also talked about the offensive speech against women and a case study was also given in this paper. The Indian Penal Code provides knowledge about various offences against women. There is a need to create separate cells for the investigation. The country's judicial system should try to tackle the problem of cybercrimes against women effectively.

Sarmah.et.al (2017) threw some light on the history and evolution of cybercrime which depicts the type of cyber-attacks from 1997 to the present time, and then the author defines the classification of Cybercrime which is broadly classified into the following types: Cybercrime against an individual, Cybercrime against property, Cybercrime against an organization, Cybercrime against society. He pointed out a few safety measures, for example, the use of two-step verification, the guidelines for a strong password, protecting personal information etc. Some cases are also given in this paper. He talked about the important cyber laws, awareness, a few important acts etc.

Joshi and Kandpal (2020) talked about cybercrime awareness among adolescents. The author defines the awareness level of Cybercrime among boys and girls, he also depicts the awareness level of Cybercrime with the help of a bar diagram, and he shows the percentage of awareness in the rural and urban areas.

Parikh and Patel (2017) talked about the attack, threats, and vulnerability of cyber security. Cyber security threat is a wide range of potentially illegal activities on the internet. Cyber threat results from the exploitation of cyber system vulnerability by users with unauthorized access. Cyber thieves use tactics like plagiarism, hacking, piracy, espionage; DNS cache poisoning and identity theft. He said about web jacking, stealing card information, cyber terrorism, cyber terrorism, child pornography, spam, cyber trespass, logic bombs, drive-by downloads, cyber assault by threat, script kiddies, attacks, and untargeted attacks. He concludes that while technology has a behavior, human impulses and psychological predispositions can be influenced through education.

Das and Nayak (2013) discussed the issues and challenges of Cybercrime. The author also categorized Cybercrime like data, network, access, etc. He defines the type of Cybercrimes. He expressed that misuse of internet is the root cause of increasing rate of cybercrime. To eradicate its misuse awareness level should be raised.

The literature gap we can find in this literature is that they don't identify the geographical space, and we can't find the study related to the Palam colony. The literature gap in this literature is also that we don't find any solution related to if the data is misused with the help of the VPN (Virtual Private Network).

5. AIMS AND OBJECTIVES

a) To find out the causes of Cybercrime against women, children, and senior citizens.
b) To examine the impact of Cybercrime on the mental health of children.
c) To analyse the existing problems and suggest mitigation measures for controlling Cybercrime among social groups.
d) To evaluate the current government initiatives regarding Cybercrime.

6. MATERIALS AND METHOD

6.1 Sources of Data Collection

Source of data collection is used to collect the different types of data from the study area.

The below flow chart shows the types of data collection used with its sub-divisions: -

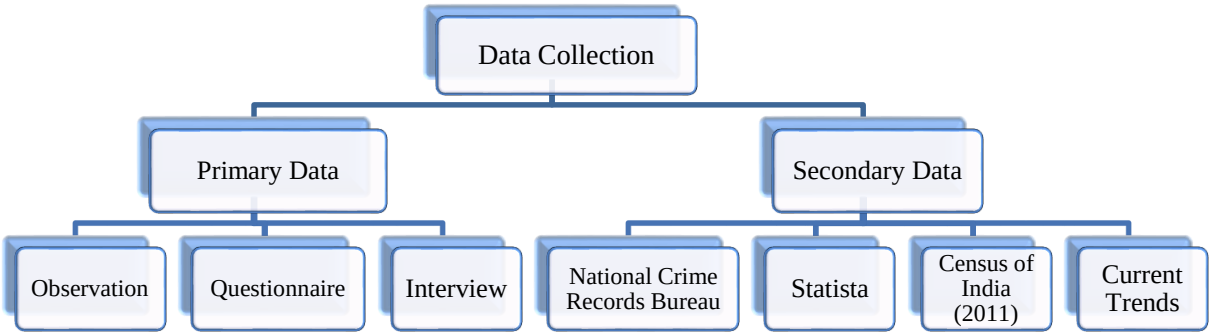
The **Primary Data** is collected through the survey which is used to gather information related to the awareness level, knowledge about cybercrime and suggestions of respondents. We take interviews with different types of people and different age groups; everyone has a different educational status, different environment and different answers. We observe the people's behaviour during the field survey and everyone responded differently, some people are very cooperative and some do not want to cooperate with us.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502



6.1.1 Observation: In observation, the data is collected by observing the field survey. We observe the behaviour of the respondent and then we collect the information. When we are doing the observation technique we see what people tell about us when we go to collect the data, is they understand what we are doing and why we are doing it, are they ready to give the answers to our questions, how they react while asking the questions, are they are comfortable while sharing their personal information, they trust on us or not.

6.1.2 Interviews: while taking interviews with the respondents we asked the personal details like gender, age, educational, educational qualifications, is they are working class, and in which sector they are working, then we asked a few questions related to cybercrime, do you know about the cyber-crime, how much you are aware of this, how much you have the knowledge, how to deal this if this happens one of your family members, what are the suggestions you give the protect ourselves from this type of crime.

6.1.3 Structured Questionnaire

The structured Questionnaire Method is a method for research and was constituted by Emile Durkheim. This is often done by market research firms or marketing departments of companies but is not usually regarded as satisfactory by sociologists. We make a questionnaire which is divided into four parts We divide our questionnaire into four part in the first part we ask the personal details related to their age, gender, and educational qualification, in part second we asked about the knowledge related to this disaster commonly people don't know about this disaster, then we asked about the few questions related the awareness level of the people, then in the last we asked the suggestion with the people in which we asked their opinion as a preventive measure to how to protect ourselves from this type of disaster, then the set of 20 questions related about awareness of the people, which crime is most common in the study area, how much people know about cybercrime. We collect 50 responses from the study area and everyone has their own opinion regarding cybercrime.

The **Secondary Data** has been used to make the literature reviews, we take 10 different works of literature to study and find some gaps in these works of literature and we also use the data to make the bar, line graphs and pie charts to show the different types of information.
Sources like National Crime Records Bureau (NCRB), Statista, and Census of India is used in this paper.

6.1.4 Current trends: We use some data to make the line graph to show the current trend of Cybercrime from 2010 to 2021 and growth of population in Delhi from 1951-2021.

6.2 Methodology

Two methodological approaches were employed for the present research work i.e., Sampling method and Statistical techniques.

6.2.1 Sampling

The present sampling is done using simple random sampling method as we have chosen women and man both to answer the questionnaires randomly from three age groups: children (1-15), working class (15-60), senior citizens (60 and above). Each one of them gets an equal chance to give their opinions and interviews with each and every person has been taken.

6.2.2 Statistical Techniques

The data collected from the different sources has been classified and arranged in tables according to the requirements of analysis. For the analysis of results, the following statistical techniques have been applied. Different charts and graphs are used for data analysis such as line graphs showing the increasing trend of cybercrime from 2010-2021 and growth

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

of population in Delhi from 1951-2021,pie charts showing the successfully executed Cybercrimes per day in India in 2023, demographic profile of Palam Colony, gender ratio, most vulnerable among women, children and Senior citizens, bar graphs showing top 5 motives of committing cybercrimes in India, state-wise number of cybercrimes in India, cybercrimes witnessed by common people.

QGIS 3.30.1 Software has been applied for making the maps for study area i.e., maps of India and Delhi NCT showing our study area- Palam Colony.

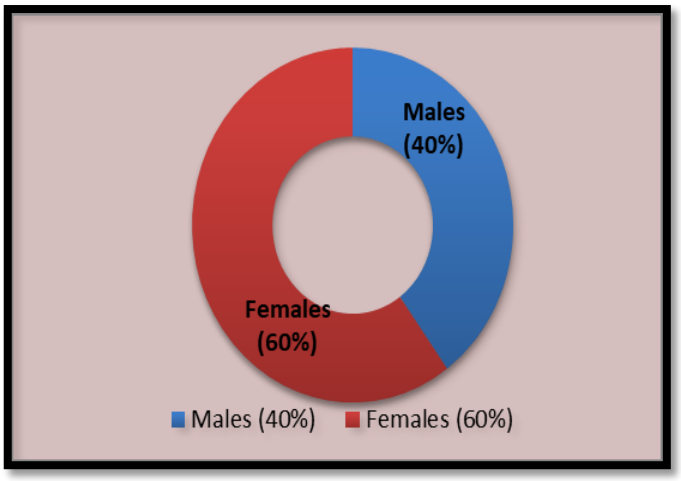
7. RESULTS AND DISCUSSION

The results of the study are discussed into 3 parts. In the first part, we discussed about the personal details including age, gender, education etc. In second part we discussed the knowledge about cybercrime. In the third part we discussed about the awareness level among the people. In the fourth part we have given some preventive measures to reduce the increasing rate of cybercrime in India.

7.1 Personal Details

Palam is a well-settled colony in which people of different age groups, occupational lines, castes, colours and creeds live with their families and some live alone on a rental basis also. A total of 50 respondents are taken in this project report. People of different age groups participated, a major portion is covered by the working class (about 60%) and the rest is covered by children and elderly people. They belong from different educational backgrounds and work in different fields of interest. Their education qualification differs from an 8th-classstudentup to the Ph.D. level. About 40% of males and 60% of females are included in this survey. One of the main reasons to choose more females as our respondents is to check their literacy and awareness level of them as compared to males about cybercrime and its mitigations.

Figure 9: Gender Ratio



Source: Primary Survey (2023)

Figure 9 shows the gender ratio i.e., 60% females and 40% males from the 50 respondents has participated in our field survey.

7.2 Knowledge about the Disaster: Cybercrime and its Occurrence

Use of internet is very common and related crimes are also becoming a major threat for common people. A criminal activity that harms cyber security is known as cybercrime, which is well-known among the major group of society. They do know about cybercrime in brief but the risk and possibility to become a disaster are still unknown to them. The use of electronic items becomes a part and parcel of life but how much it can harm our social and private life is beyond someone's expectations. Educated as well as uneducated both are vulnerable to cybercrimes but being an uneducated person increases the risk of being trapped in it.

7.3 Awareness Level

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

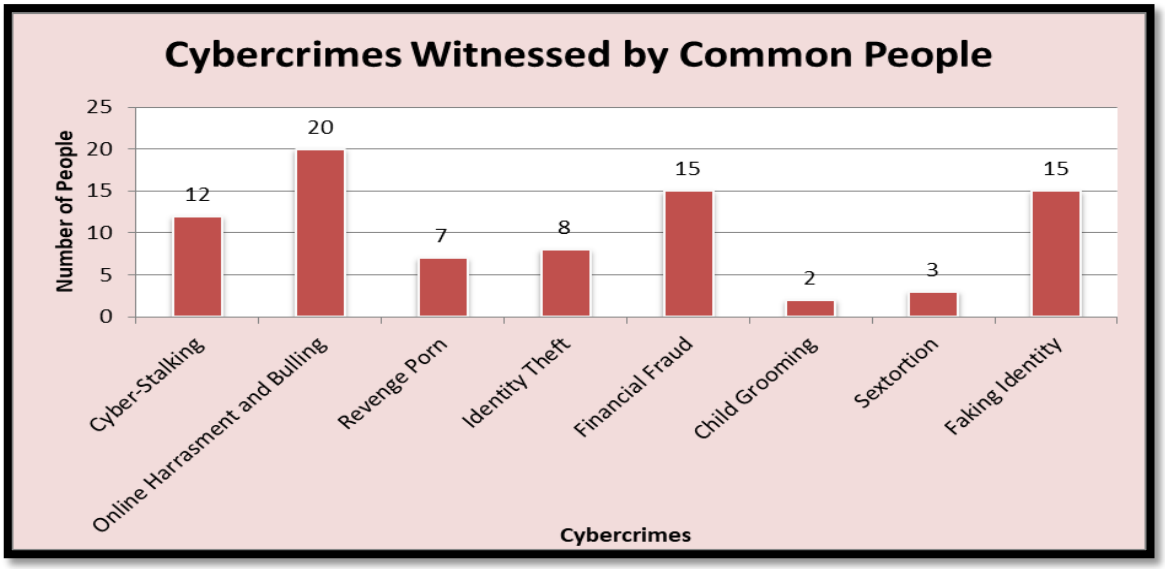
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

Majority of the people (about 92%) are aware of cybercrimes against women, children, and senior citizens. They have faced many types of cybercrimes in real life situation such as cyber-stalking, child grooming, online harassment and bullying etc.

Figure 10: Number of Cybercrimes Experienced by Common People in Palam Colony



Source: Primary Survey (2023)

Figure 10 depicts the most common types of cybercrimes witnessed by common people in their day-to-day life. These basically includes; online harassment and bullying at the top chosen by most of the respondents and child grooming and sextortion is not that much prevalent in that area.

They have experienced cybercrime through different aspects and methods, majorly like deliberately spreading fraudulent reverse mortgage and loan offers, pressuring the elderly to pay in whole or in part upfront for services rendered by unregistered contractors, pretending that family members creating credit cards in the victims' names or stealing money from their accounts, charging fraudulent or unnecessary services using elderly victims' Medicaid or Medicare information, targeting seniors with get-rich-quick pyramid schemes, or telling victims they've won a contest or the lottery, etc. Most of people don't share their OTP and unknown links and messages with other people. They receive international calls from different phone numbers. About 60% of respondents have child security and anti-virus software installed on their electronic devices. People are aware of the cybercrime helpline number (i.e., 1930) and women's helpline number (i.e., 181). People will help the victims of cybercrime according to their knowledge level. They spread this knowledge with their family members and friends.

7.4 Preventive Measures

Cybercrime is a leading disaster and it's important to analyse its impacts and try to minimise them. According to the survey report, women are the most vulnerable group to cybercrime as their literacy is much less than that of males and they are mostly engaged in their household work and with their families. In some urban areas, working women are there, who have knowledge about these types of crimes but a major portion of the women population is not that educated and aware.

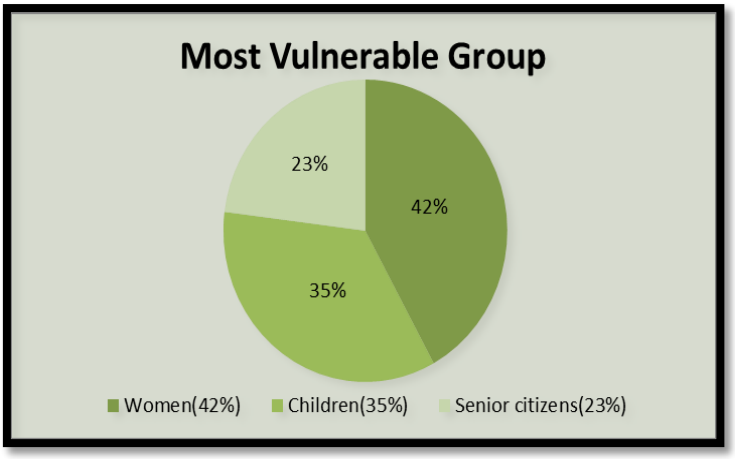
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12502

Figure 11: The Most Vulnerable Group among Women, Children and Senior Citizens



Source: Primary Survey (2023)

Figure 11 shows the comparison between 3 groups of people including women, children and senior citizens. Most of the respondents vote for the maximum chances of cybercrimes among women and they could be the most vulnerable part of society in this context.

People have witnessed fake money-making apps, some suspicious fraud links of lottery, etc. but most of them avoid these kinds of scams. Still, there are some common mistakes that people do that make them vulnerable to cybercrime like using weak passwords, connecting public WIFI for free internet, ignoring software updates, etc. Social profile is not that secure as most of them are not end-to-end encrypted and fear of data leakage and hacking of account is always there. So we should try to use authentic sites and apps for work to maintain our privacy.

There are some long-term effects of cybercrime as financial loss, identity thief, psychological trauma, loss of trust, reputational damage, etc. faced by the victims. Sometimes they recover with time and sometimes they need medical attention to be cured. There are some laws related to cybercrimes in India and crimes against women, children and senior citizens to decrease the rate of crime but their implementation is not that effective on the ground level.

8. MAJOR FINDINGS FROM THE STUDY AREA

a. Cyber-crime is leading to becoming a big human-made disaster.
b. People are aware of this threat but don't know how to tackle it safely.
c. There is a lack of awareness about the types and technological approaches among vulnerable groups.
d. Importance of role of female literacy and child safety programs.

9. SUGGESTIONS

The literacy level of people in India is about 86.21% (estimated 2023) but their knowledge is not much about the practical world and technical crimes. About 70% of respondents believe that female illiteracy and social factors play an important role in dealing with cybercrime. Educational programs related to cybercrime, online harassment and child mental health development should be held at the school level. By organising campaigns and awareness programs we can try to reduce the rate of cybercrime in India. Articles containing information about this topic can be published both online and offline, some basics of the internet overall should be taught to elderly people, including the basic unwritten rules like not sharing a password, PIN or OTP with anyone, not clicking on random links without knowing the sender or the link's address and meaning. The younger generation should discuss these kinds of problems with their elders and make them aware of the threats of cybercrime. Provide basic cyber security training, encourage open communication, monitor internet usage, emphasize the importance of privacy, encourage two-factor authentications, and stay up-to-date with cyber threats. If we get in a troublesome condition then we should contact our parents and elderly first and then report it to the police. The best practices to secure VPN services are to enforce strong authentication methods, re-evaluate all points of entry, and secure remote wireless networks. In addition to VPNs, all points of entry should be evaluated by the organisations into their network, like from web applications to e-mail to cloud, identification of any vector which can adversely gain access to their environment with a compromised username and password.

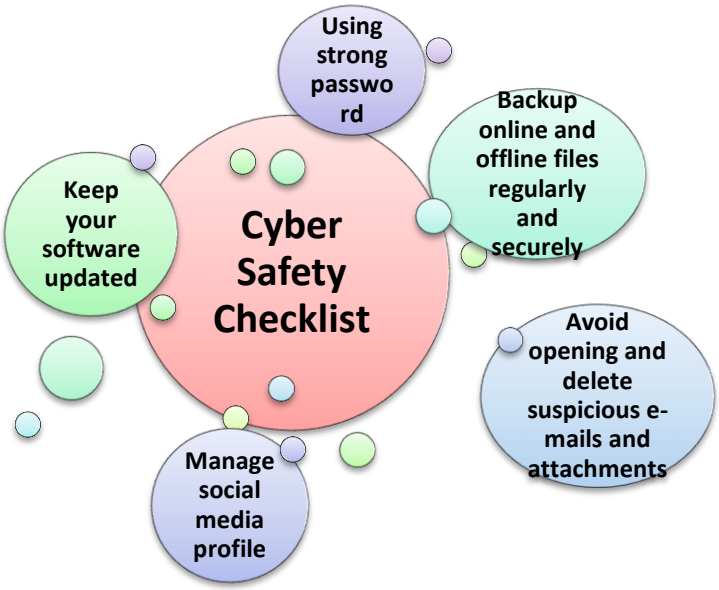
DOI: 10.17148/IJARCCE.2023.12502

Government should run cybercrime awareness programs at institutional levels and provide more job opportunities which will decrease the rate of unemployment. Employed person has money to fulfil their basic needs and education is the key to think practically about the right and wrong.

Figure 12: Cyber Safety Checklist

Figure 12 shows some of the checklist measures for cybercrime safety in context of India as well as the whole world. These are-

- Keep your software updated
- Backup online and offline files regularly and securely
- Avoid opening and delete suspicious e-mails and attachments
- Manage social media profile
- Using strong password



Source: Self Prepared by Author (2023) based on Concepts Derived

10. SUMMARY AND CONCLUSIONS

Lack of education is the root cause of most of the present times problems. People do know how to read and write but their mental and social development is still below the mark. Women are somehow educated but don't have a proper right to speech. They are bound to follow the roles set by their families and society. Their level of education is not much higher even in a developed area like Palam colony. Most of them are unemployed also. Children don't pay much attention towards the advice of their parents; they are highly influenced by social media and the internet. They use it as a medium of fun but its harmful outcomes are beyond their mental level. They become addicted to some dangerous games and it will affect their mental and physical health. Senior citizens don't have proper access to high-level internet apps but they are easy to fool and highly targeted by criminals as they have money and they are not highly aware of such kinds of upcoming crimes through technological advancements like cybercrimes. Some of the major cybercrimes are discussed and increasing education and awareness level is one of the impactful mitigation measures to fight against cybercrime. The government has started some programs and enforced some laws like the Information technology act (IT Act), 2000, especially to regulate e-commerce. IPC sections are there to protect us from such crimes. Implementation of these laws is also very important and the need of the hour. Rather than only on papers it should be implemented in real life scenario in local grounds either it's male or female, rural or urban, educated or uneducated or belonging to any age group be it women, children or senior citizens all should be treated equal before such laws. If this is achieved, we will live a hassle free and digitally sustainable life.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12502

REFERENCES

[1]. Aliperti M. (2021). How to Protect Seniors against Cyber-crime and Scams? *Multistate Information Sharing and Analyse Center*, Vol. 16.
[2]. Primary Census Abstract, Delhi (2011), Census of India, 2011, Office of the Registrar General and Census commissioner, India.
[3]. Provisional Population Totals, Census of India, 2021.
[4]. Das, S. &Nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges, *International of Research in Modern Engineering and Emerging Technology*, Vol. 6.
[5]. Hati, M. (2016) Cyber Crime: A threat to the nation and its Awareness, Jamshedpur, Jharkhand(India).*International Journal of Advance Research in Computer and Communication Engineering*, Vol.5.
[6]. Jazeel A. (2018) A Study on Awareness of Cybercrime among Teacher Trainees in Addalaichenai Government Teachers' Collage, *Journal of social welfare and Management*, Vol. 10
[7]. Joshi. A., Kandpal S. (2020) Cyber Crime Awareness among Adolescents, *Internal Journal of Creative Research Thoughts*, Vol.8.
[8]. Khan S. (2023) Cyber-crime in India: An Empirical Study, *International Journal and Engineering Research*, Vol. 11.
[9]. Mishra S. (2018) Dimensions of Cyber-crime against Women in India- An Overview, *International Journal of Research and Analytical Reviews*, Vol. 5.
[10]. Muthulakshmi R. and Kumar T, (2017) Awareness of Cybercrime among B.Ed. students-A Gender wise Analysis, *Indian Journal of Applied science*, Vol.7.
[11]. National Crime Records Bureau
[12]. Parikh T., Patel A. (2017) Cyber Security: Study on Attack, Threat, Vulnerability, *International of Research in Modern Engineering and Emerging Technology*, Vol. 5.
[13]. Sarmah A., Sarmah R., Baruah A., A brief study on Cyber Crime and Cyber Law's of India, *International Research Journal of Engineering and Technology*, Vol. 4.
[14]. Statista (2023)

Web links

[1]. https://cybercrime.gov.in/ (Accessed on 02 February 2023)
[2]. https://en.m.wikipedia.org/wiki/cybercrime (Accessed on 15 February 2023)
[3]. https://cybervolunteer.mha.gov.in/webform/Volunteer_AuthoLogin.aspx(Accessed on 03 March 2023)
[4]. https://www.google.com/amp/s/www.cnbctv18.com/india/mumbai-cyber-crime-cases-rise-by-more-than-63-pc-in-2022-compared-to-2021-report-15710371.htm/amp (Accessed on 9 March 2023)
[5]. https://www.indiatoday.in/technology/features/story/cyber-fraud-incidents-rising-in-india-how-to-file-a-complaint-online-on-cyber-crime-portal-2335149-2023-02-15 (Accessed on 16 March 2023)
[6]. https://gujaratCyber-crime.org/eng/ (Accessed on 01 April 2023)
[7]. https://infosecawareness.in/cyber-laws-of-india (Accessed on 07 March 2023)
[8]. https://www.kaspersky.co.in/resource-center/definitions/how-does-vpn-keep-me-safe-online(Accessed on 20 April 2023)

