IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Cyber Pandemic: Roots and Solution

Saleha Ubaidullah[1] and Sudeshna Roy[2]
Student, Master in Computer Application[1]
Professor, Master in Computer Application[2]
Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, India

Abstract: *Since the pandemic started and a lockdown was announced , we witnessed the unlocking of different solutions switching towards digitization. With an increase in digital devices, internet usage and a decline in the economy globally due to Covid 19, there is a rise in cybercrimes. With technology and online systems in demand, almost the majority of people own at least one of these devices, which include smartphones, personal computers, laptops, tablets etc. People were leaning towards online classes, work, shopping, and had access to the internet for more hours as compared to previous usage records. During this period people were unaware of the possible cyber fraud activities that may harm them, as cybercrime is harder to detect and even more difficult to solve. This paper focuses on finding the most prevalent type of cybercrime, the category of people targeted for cyber fraud, and providing a model of solution for the prevention of the same using computer vision as a core technology for secure access to digital devices and the internet.*

Keywords: Cybercrime, cyber fraud, digital, computer vision, phishing, cyber-attacks, online classes, cyber law, IT act 2000, secure web surfing, pandemic, Covid-19.

I. INTRODUCTION

Cybercrime is a term that has evolved and adapted to different definitions as the internet makes progress in the digital era. It can be defined as "cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud; trafficking in child pornography and intellectual property; stealing identities, or violating privacy." [1]. To prevent such crimes, we need to understand what these crimes are and how these crimes work against us in the current times. The internet can be the perfect weapon to destroy the property of an individual or an organization with the help of techniques that include hacking, spoofing, sniffing, denial of service etc. While the world was locked due to pandemic restrictions, cybercriminals were not deterred. The rise in these types of crime in the past two years is about 81% since the global pandemic [2]. According to a report in The Hindu, the inclination towards cybercrimes during the pandemic in India was 500% [3] and crime against children rose to 400% according to NCRB data [4]. Hackers and attackers are really smart and use the latest technology to trap people. To have better recognition, the common category of cybercrimes and their types are listed below [5]

Cybercrime against an Individual

This includes the action or crime done against an individual to harm or threaten them illegally to gain money or assets or to satisfy a personal grudge against someone. List of crimes against an individual via the Internet -

1. Cyber Stalking
2. Defamation
3. Hacking
4. Identity Theft
5. Online Harassment
6. Cyber Bullying
7. Cyber Fraud
8. Spoofing
9. Phishing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Cybercrime against an Individual or an Organization's Property

The crimes related to Intellectual Property Rights and harm to the property of an individual with the help of electronic media are considered Cybercrime against Property. The following are included in this type of Cybercrime -

1. IPR crimes
2. Spying and Virus transmitting software
3. Online Thefts
4. Trespassing security online
5. Accessing Unauthorized Information
6. Hacking Server
7. Vandalism via Internet
8. Denial of Service
9. Salami attacks
10. Social Engineering

Cybercrime against the Government of a Country

When a group of hackers or an individual tries to threaten or harm the international government using the internet is a crime against the government and it includes -

1. Cyber Terrorism
2. Cyberwarfare

Cybercrimes committed don't usually need the person to be in cyberspace over the internet, the crime can be committed without being online on the internet, for example, Software Piracy.

To protect ourselves and others from any probable online crime we need to understand people's behavior towards digital devices and their perception of cybercrime. We need to analyze different domains to understand the pattern of attacks and constructive defending and prevention systems to avoid casualties in future.

II. CYBERCRIME EVOLUTION IN INDIA

India is one of the largest populated countries in the world with 1.3 billion people residing in it and has access to the internet. As time passes people are more into digital services because of their cost-effectiveness and time-saving features. Pandemics too, facilitated the encouragement of the use of the internet. The internet in India was introduced in 1995 by Videsh Sanchar Nigam Limited (VSNL) and in 1999 India's earliest cybercrime was reported. Since then, the attackers have searched for new ways and technologies to complete their actions without leaving a trace. The NCRB data shows the surge in cybercrime in the past few years, where crime against women and children grew exponentially. The rate of increase in these crimes was more than 70 per cent yearly [6].

The top most prevalent cybercrimes highlighted by NCRB are:

1. **Phishing:** Phishing involves the activity of sending fraudulent messages or emails to an individual with the motive of collecting sensitive information such as credit card details, passwords etc. [7].
2. **Identity Theft:** Stealing someone's identity and pretending to be another person is known as identity fraud. Impersonating another person to gain access to money or assets that belong to the real identity without their knowledge is an illegal act included under identity theft [7].
3. **Denial of Service:** The attacker sends multiple fake requests which are beyond the capacity of the server to handle it, and it stops or crashes is known as a denial of service [7].
4. Online Harassment and Bullying: The indecent, iterative harassing behavior with the intention to threaten, blackmail or bully someone online is known as Online Harassment and Bullying [8].
5. **Spyware and Ransomware:** Spywares are malware that is programed to get into a computer system to spy and collect the details of users, which may include vulnerable information. Ransomware is malware that encrypts the device and asks for Ransome to be paid in order to get the device unlocked [7].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

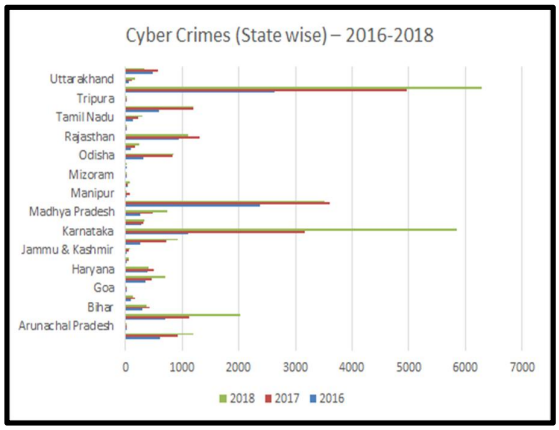

Fig 1: NCRB data of Cyber Crime 2016-18

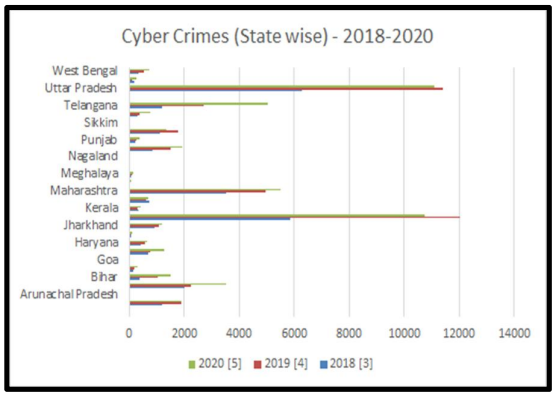

Fig 2: NCRB data of Cyber Crime 2018-20

III. OBJECTIVES

The prime objective of the paper is to analyze the most common type of cybercrime, its source, and a model that can cater as a solution to prevent the attacks of hackers via the internet. To attain the main objective, sub-objectives are needed to be fulfilled.

Since phishing, spoofing, worms and viruses are enhanced to attack the systems, the objective can be further segregated into finding the deportment of people towards digital devices and the consumption of the internet by an individual daily. Once we have the data, we can further compute it to comprehend when a person is highly vulnerable while using the internet and its impact. It is also important to study the relationship between the apparent source of crimes and other factors facilitating them. When clarity is observed a proper model is designed for the prevention of prevalent cybercrimes.

IV. METHODOLOGY AND DATA COLLECTION

This paper is based on a qualitative and descriptive approach. The focus is mainly on identifying the factors involved in the increase in cybercrimes and construct a possible solution from the data collected.

The collection of data is done with the help of primary and secondary sources. The primary source is the survey form that helped in collecting the data from different individuals and studied for analysis. The secondary source is the documents and records that are made available by the government to its citizen to work with, analyze and conclude. Both of these sources will be made to contribute to the study and ease the formulation of the solution.

V. DATA ANALYSIS AND RESULTS

5.1 Understanding the Fata

The data collected from the primary source, i.e. Google forms includes 63 people from different backgrounds and different experiences while using the internet. Since the main motive is to identify the most vulnerable state of people

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

while using digital devices and the most prevalent cybercrime that can harm them during that period of vulnerability. The data collected from NCRB's records will be used for a more accurate analysis and understanding of the common type of cybercrime in India and which set of people were victims. It has a record of past complaints regarding the crimes via the internet and also the crime against children and women for the same.

5.2 Selecting Relevant Data and its Interpretation

Google Forms

In the collected data, the audience was divided into age groups where 68% of the responses were from people who belonged to the age group of 18-25 yrs. The rest was divided into 14-18 yrs, 25-40 yrs, and 40-60 yrs age groups with 6.3%, 17.5%, and 7.9% of the population, respectively.

The general analytics and data interpretation shows:

- More than 50 per cent of people have 5 or more devices at home and 31% of people spend 5hrs or more on the internet and social media whereas 60% accept that they do share sensitive information such as location, pictures etc. over social media.
- More than 90 per cent of people switched to online learning methods, and 79.4 per cent were involved in online shopping and banking methods where almost 40 per cent of them experienced online fraud.
- Almost half of the population experienced fraudulent spam calls, messages and emails that lead to phishing and online scams.
- During online classes, 30% of them witnessed people gaining unauthorized access to the classroom meet and while making transactions the bank servers turned down.
- Online hate and bullying was witnessed by 40% of the population and 60 per cent were familiar with the IT act 2000.
- Many of them agree that they download movies from third party websites like torrent, and more than half of them don't have antivirus installed on their system.
- Moreover, a quarter of the population doesn't use licensed software.
- The above points enlighten the fact that people are victims yet are careless towards the safe use of the digital medium and the internet. Many of them are aware of cyber frauds and different cybercrimes, but they do not take preventive measures to be protected on the internet.

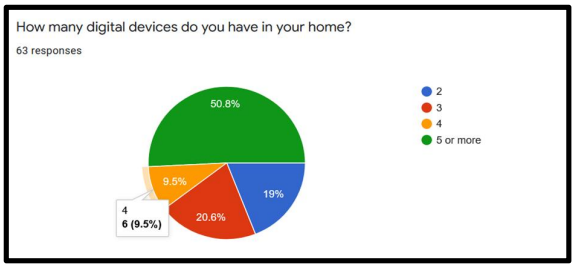

Fig 3: Google Forms Data 1

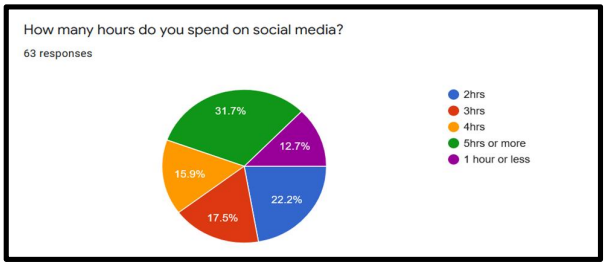

Fig 4: Google Forms Data 2

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

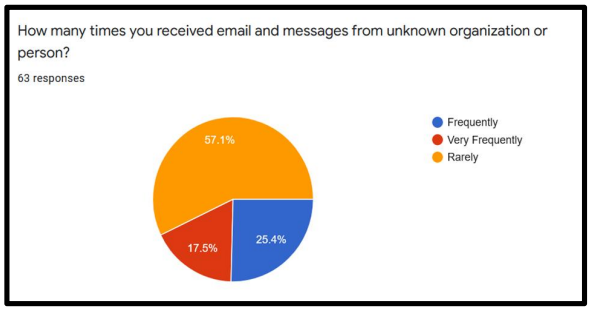

Fig 5: Google Forms Data 3

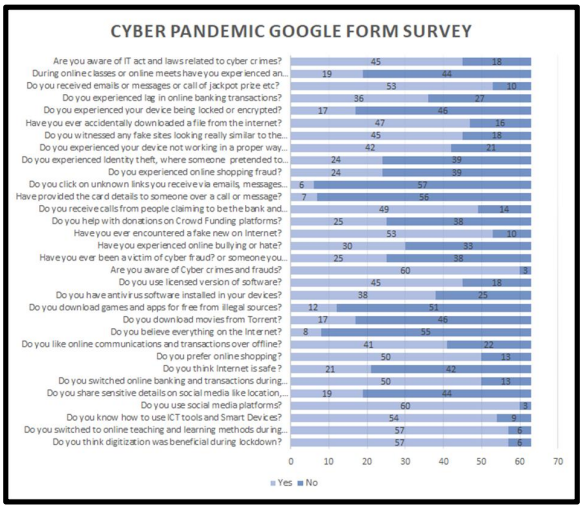

Fig 6: Google Forms Data 4

5.3 NCRB Data

The documented data from NCRB shows the details of the cybercrime in India in the past few years and the following point can be listed as the findings from the data [6] –

- The crimes kept on increasing yearly.
- Crime against children is at its peak including crimes such as online bullying, harassment, pornography etc.
- Crime against women increased with more cases of identity theft, defamation, sexual exploitation, cyberstalking etc.
- Online fraud to gain access to banking details, fake lotteries, and internet scams lead to a hike in phishing attacks.
- Fake news, Piracy and invasion of Privacy were the other most prevalent crimes in the internet world.

5.4 Results

Interpreting the data, it is evident that people are engrossed in technology and dependent on it. While using the internet, they knowingly or unknowingly give the chance to the attacker to fulfill his motive. The behavioral study suggests that people are less aware and less cautious about using digital media and the internet effectively. The lack of knowledge and careless behavior while accessing the electronic and smart devices led to cybercrimes like phishing, fraud, spyware, viruses, and crimes against children and women that are easy to execute when an individual's existence on the internet is vulnerable.

VI. SOLUTION

After looking at the analysis, we can say that phishing, worms, viruses, spyware and potential ransomware attacks can lead to attacks on an individual. To tackle this, we need a solution that monitors a person's activity on the internet in real-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

time and keeps track of the user's web surfing history and generates reports and prevents them from entering into an illegal realm of the internet, maintaining the user's safety.

6.1 Safe Web Surfing System Model

Safe Web Surfing System improves the protection of an individual from the cyber-attacks that are caused by the lack of precautious Ness of an individual while surfing the web and accessing the internet and making way for viruses and trojans to enter the system to corrupt it or to make the victim lose his money or greater harm.

This system constitutes of different modules working together to assure the maximum safety of the individual, be it a child or an adult, with the help of Computer Vision as its core.

The system allows the user to log in to activate it.

- If the user is a child then the credentials of the child will be accessible by the parents and after entering it the child mode will start automatically.
- If the user is an adult, he/she has to enter his/her credentials and the system will start working.

Once the system is activated, the computer vision is activated which takes care of what a user sees on the screen. The computer vision program will be trained with the help of relevant datasets in a way that it can visualize the user's screen, web browser and apps connected to the internet that allows the Safe Web Surfing to connect and work. Every obscene and explicit content such as indecent images, child abuse and dark sites are instantly blocked once recognized and only sophisticated content is visible to the user. The modules of the system

- **Safe Ad Blocker:** It blocks the ads that are from unauthorized websites and doesn't display any advertisement that has any connection with the fraudulent websites.
- **Safe Download Manager:** It will allow the download of files from genuine websites and won't allow any potentially harmful files like spyware, or worms to be downloaded into the system.
- Timer: It monitors the screen timer of the user and will freeze the system if the time exceeds the time limit set in the system.
- **Tracker and Logger**: It keeps track of the online activity of the user by collecting information such as search history, website visits, daily screen time, download records etc. and saves it in the local database of the user.
- **Behavioral Analysis:** This module will be programmed to analyze the behavior of the user activity with the help of tracking records entered in the database. This will help the parent to keep a check on their child's activity as well as can help an individual to introspect his/her behavior on the internet.
- **Report:** After the collection of data that includes logs of activity performed over the internet by the user, reports will be generated for better precautions and will provide suggestions to be safer from attacks.

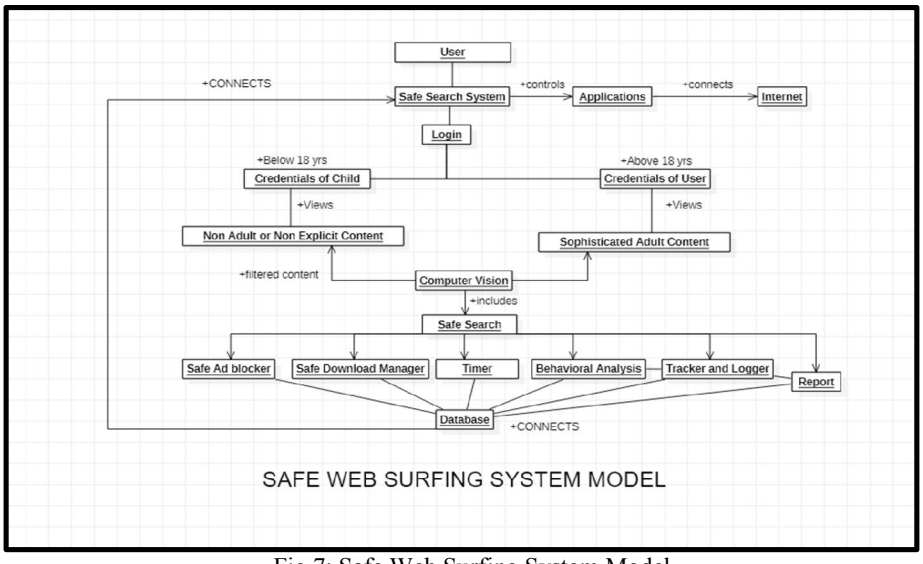

Fig 7: Safe Web Surfing System Model

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Cybercrime against children increased during the pandemic as the use of smart devices and the internet were directly proportional to cybercrimes. This system is designed to keep a child and an adult safe from common attacks that occur due to common mistakes made during the usage of digital devices and the internet.

VII. LIMITATIONS AND SCOPE

The model is effective only if the implementation and the use of the model are in a precise way. Identifying the best suitable technology for the model is really important as it requires computer vision. It will go through several changes during the development phase so it's hard to decide the exact architecture of the system. Safe Web Surfing System works on the device when it is turned on and the credentials are accurate. It can protect an individual to an extent where he is safe from the dark web of the internet only if the user isn't willing to protect himself and keeps the system turned off then it's completely useless. The system will need frequent updates as the technology keeps on upgrading and the ways of attacks by the attacker get enhanced. Maintaining the performance of the system and the security of the system is a challenge. Regression Testing and beta-testing are a must to fill the loopholes in the system which may allow the attacker to trespass the security. In future, this system can be integrated into various other applications for better protection with the help of Artificial Intelligence and Machine learning algorithms that understand human behavior with the respective system and provide the best protection possible.

VIII. CONCLUSION

The study accentuates key points that describe the unending and propagating nature of cybercrime, as these crimes are hiking every year with a double progress rate as humans keep on upgrading technologies and become more dependent on computers for every kind of chore. In order to overcome the problem of being the target of an attacker via computer, before having a huge change, small scale awareness and precautionary steps are essential. Hence, the model Safe Web Surfing System is designed to be implemented so that even if humans fail to take the precaution, the system will. It can be concluded that in the era of a technology-driven world, it's almost impossible to completely stop the cybercrimes but with the help of cautiousness and precautionary measures that the Safe Surfing Web System can take after development and deployment, an individual can protect himself from potential digital harm

REFERENCES

[1]. Britannica, “”Cyber Crime and its definition” https://www.britannica.com/topic/cybercrime
[2]. Businesswire, “Cyber Threats have increased by 81 per cent since Global Pandemic” https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic
[3]. The Hindu, “Cyber Crime went up by 500 per cent during pandemic” https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece
[4]. Economic Times, “Over 400 per cent rise in cybercrime cases committed against children in 2020 : NCRB data” https://economictimes.indiatimes.com/news/india/over-400-rise-in-cyber-crime-cases-committed-against-children-in-2020-ncrb-data/articleshow/87696995.cms?from=mdr
[5]. Legal Service India, “Cyber Crime in India: An Overview” https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
[6]. National Crime Record Bureau, Crime in India Table Contents https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?page=27
[7]. Mimecast, “Types of Cybercrime and its protection” https://www.mimecast.com/blog/types-of-cybercrime/
[8]. The Dark Side, Michael Cross- Social Media Security, 2014