# NEED OF TECHNOSCIENCE AND DIGITAL FORENSIC IN EMERGING CRIME: A STUDY ON CYBERCRIME

**Arpita Singh[1], S. K. Singh[2], Nilu Singh[3] and Sandeep K. Nayak[4]**

[1] Research Scholar, Amity Institute of Information Technology, Amity University, Lucknow, India

[2] Professor, Amity Institute of Information Technology, Amity University, Lucknow, India

[3] Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation

[4] Associate Professor, Department of Computer Science & Application, Integral University, Lucknow, India

[*]Corresponding author: singharpita999@gmail.com

## *Abstract:*

*With the number of crimes on the rise around the world, digital forensic investigators are turning to technology as a tool to combat crime and apprehend criminals. Technology makes life easier, which is a positive element of technology. People are completing transactions without traveling to the bank and standing in a big line, people doing internet shopping from home, and so on. We unwittingly rely on the internet and digital devices from the moment we open our eyes in the morning until we retire for the night. We frequently utilize digital gadgets for a variety of purposes, including office activities, e-shopping, e-banking, business transactions, recharging mobile phones, TV, fitness tips and tricks, stock market, gossiping, emotional support, and so on. As a result of this reliance, understanding how to use the internet and digital gadgets are becoming increasingly important. Lack of security information may lead to E-fraud, cybercrime, and other forms of fraud. The authors have given a study on how cybercrime occurs and how to defend ourselves from it in this research paper. Furthermore, the writers attempt to investigate different threats of cyber security, security flaws, and real-world challenges that internet users face as a result of the internet.*

***Keywords****: Digital Forensics, Digital Forensic Investigation, Cybercrime, Electronic Frauds, Technoscience.*

# I. INTRODUCTION

Nowadays, technology is present everywhere, and no one is immune to its effects. In addition, there is still ongoing progress in all areas of its use. Every element of life has been influenced by technology. If we go back one or two decades, money was such an important and private element of our lives that everyone kept it hidden and secret from others or from themselves while making any kind of purchase or transaction. While technological advancements have changed many aspects of human life, internet transactions and purchases have been the most affected. Anyone can conduct online transactions with third-party gateways using the various application and the internet. These transactions are not safe somehow. This allows for a new type of thief known as cybercriminals, as well as a new type of theft known as cybercrime [1-3]. Simple crime is transformed into cybercrime through the use of electronic devices such as laptops, computers, smartphones, and other similar devices.

A new section of forensic science called Digital Forensic Science (DFS) has emerged to identify these types of crimes and to eradicate cybercrime. This includes the investigation, the tracking of evidence using electronic media, and the retrieval of data from digital devices. Although forensic science, medicine, law, and psychology are all involved in the investigation, the biological aspects are the focus of forensic science. When forensic science and computer science are combined to aid in the investigation and the discovery of electronic evidence, the result is known as digital forensic science. [2].

In a workshop, Ajit Doval, National Security Adviser (NSA) of India, said that citizens must be careful while they are using online banking, shopping, or any kind of transaction. Caution is required more because due to the Corona pandemic, digital payment platform dependency has been exponentially increasing. Mr. Doval also said that cybercrimes increase by 500 % because of less cyber hygiene and limited awareness of internet users [1].

This study focuses on new forms of cybercrime and how they affect ordinary people. The general public uses the internet for day-to-day transactions, shopping, and other critical tasks. The following are the research's main contributions:

- It presents a discussion of the financial frauds faced by the general public while online transactions.
- It presents and discusses the cyber laws of India.
- It also presents a discussion of data theft, with auto intelligence of digital devices.
- It discusses the further effect of the internet on our daily schedule.

In this study paper, we look at digital forensics and the need for it in the present crime epidemic. Then we talk about the role of digital forensics in crime prevention in society. In this study piece, we also covered cybercrime, and the necessity for digital forensic investigation in developing crime is a result of that discussion. This study also includes some recommendations for coping with cybercrime.

### *SIGNIFICANCE OF THE STUDY*

The study's findings may offer regular people some protection against cybercrime. This study offers suggestions for overcoming the obstacles to increasing and strengthening cybercrime awareness. May provide useful information to the general public on how to protect themselves from cybercrime. It may aid stakeholders and digital forensic investigators by

allowing them to comprehend the difficulties that ordinary people confront when submitting complaints against cyber offenders and generating a sense of shared vision and belonging. It may also benefit researchers by providing extra information to existing findings that may be used as a reference for future research.

***OBJECTIVE OF THE STUDY***

As computer users increase exponentially from the last two decades so it also affects internet users and a hike in the use of the internet is also noticed [14]. Therefore, lots of new challenges are coming in this field. In this study, the author is trying to figure out some challenges in the daily life of a common user of the internet (These findings concluded by an online questionnaire, which is communicated by the author to different ages and occupations people). Some are listed below-

- To know the perception of common people for online banking and online shopping, in the era of the Internet.
- To analyze the fact of personal information of people is sound and safe, after using artificial intelligence and autosave feature of the internet.
- To know awareness of common people regarding digital forensic, cybercrime, and cyber laws.
- To evaluate a different kind of risk and loss due to computer and cyber frauds.
- To analyze by what ratio common people prefer traditional market and traditional banking over the online market and online banking.

The above is the objective of the study for research. While keeping these objectives author designed a questionnaire from which these objectives can be fulfilled.

## II. Literature Survey

Evidence and reports demonstrate that illegal actions on internet platforms are on the rise. Crimes are no longer being committed in a simple manner; they are now being committed with the aid of computers, laptops, and other multimedia or electronic devices. These crimes fall within the heading of digital forensics, a new term for crimes involving digital technology. "Digital forensics is a modern science that involves DNA testing, fingerprinting, and data collection from digital devices, among other things." Intelligence agents and police officers are now tracking evidence and conducting examinations with the assistance of forensic experts and cutting-edge investigation procedures. Digital forensic assistance finds many difficulties from multiple perspectives and across various areas. It has been discovered by researching several types of cybercrime, it is observed that newly emerged crimes are having different patterns and styles. These types of crimes can be tackled by digital forensics. [3, 4].

People used to rely on paper documents for their trustworthiness and authenticity, but times have changed, and digital documents are now equally acknowledged by all organizations. Digital documents have recently taken the role of printed ones. Almost every piece of information on any firm, institution, organization, or individual, whether private or public, can be found on the internet [4]. Data theft, often known as data leaks, is a new type of crime that has emerged as a result of the digitization of records [3-5]. Digital forensics helps to combat this form of growing crime caused by data theft.

Cybercrime is on the rise all around the world, and digital forensic investigators are utilizing technology as a weapon to combat it and arrest criminals. Technoscience is aiding research and development in the security sector, as well as other sectors, to increase safety and security in the context of cybercrime [17]. As sophisticated technology becomes more widely used, issues in the fields of crime detection, prevention, and control are rapidly increasing.

By inventing various strategies and tools for crime detection, prevention, and control, technoscience provides a solution to this key problem (the rapid increase in crime rates). The major objective of technoscience in digital forensics is to track using basic forensic science applications, techniques, and procedures combined with the latest technology and instruments. Technoscience assists digital forensic investigators in investigating items or data discovered in digital devices, and it may also assist in data recovery from digital devices. The data devices that have been extracted are then used as evidence in a court of law. Internal corporate investigations and computer hacking investigations are two examples of how technoscience and digital forensics are applied in the corporate world. Many firms want to exchange data across networks, and technoscience can help with cyber security, which protects data from cybercriminals. [6].

**Need of digital forensics-**

Digital gadgets such as cellular phones, laptops, desktop computers, CCTV cameras, and other digital devices are now used by criminals to steal information [6]. Digital Forensics Investigators (DFI) officers/teams and other connected authorities use information acquired from these devices as evidence to apprehend suspects involved in a certain crime. Financial institutions, multinational corporations, law enforcement agencies, policymakers, academics, the government, and investment firms are all incorporating digital forensics as a legal corporation into their architecture [7, 8].

**Impact of digital forensic in Crime Control-**

Digital devices must be inspected in digital forensics cases in order to retrieve data and gather information. Digital forensics is the name given to this discipline of forensic science. Digital forensics was first referred to as computer forensics [8]. After that, computer forensics became a subset of digital forensics, which broadened its scope to include investigations involving any device or internet area capable of storing binary data. Identifying digital devices that can be used as evidence, gathering all of those devices, preserving, analyzing the devices and their data, maintaining documentation that can be utilized in a court of law, and reporting are all part of the digital forensics process. These procedures are carried out by digital forensics investigators [11, 12]. The evidence is followed by a digital forensic investigator who attempts to solve the case online. As a result, a digital forensic is really helpful to recover documents, e-mails, images, and other transient data from damaged or altered data on computer/laptop hard drives and electronic data storage devices such pen drives, external hard drives, zip, and flash drives [9, 10].

***Digital forensics components-***

Digital forensics is dependent on digital evidence, which exists in computers, communication network systems, and embedded systems. Digital pieces of evidence are very rigorous to

destroy and can be patterned exactly. Digital data can be found very easily from GPS, routers, phones, and computer storage devices like hard drives, flash drives, tablets, and multimedia devices. The court of law needs only reliable and relevant evidence [13, 7]. In recent many tools & techniques available for help in forensic investigations. The digital forensics investigation process can be divided into broadly three stages-

1.Collection
2.Examination and analysis
3.Reporting

- **Collection –** This stage of digital forensics investigation is the initial state of investigation which mainly focused on the collection of data from all authentic available resources and collection of all media devices which can help further in the investigation. This is a crucial stage of the investigation, if one fails to collect evidence properly or disable to maintain the integrity of found data then the question can be raised on authentication of evidence [3, 7-8].
- **Examination and analysis-** After the first stage of digital forensic investigation second stage examination and analysis of collected data comes in sequence. This stage is largely attentive to examine collected data whether in crime scenes or the lab. Examiner sometimes creates a hypothesis based on collected data and scenarios. After setting a hypothesis, he/she observe information from collected data to prove his/her hypothesis or to contradict the hypothesis [3, 7-8].
- **Reporting-** The last stage of digital forensic investigation is to report analyzed data in the court of law as evidence. This stage involves some legal aspects as well to present that information as evidence in court [3, 7-8].

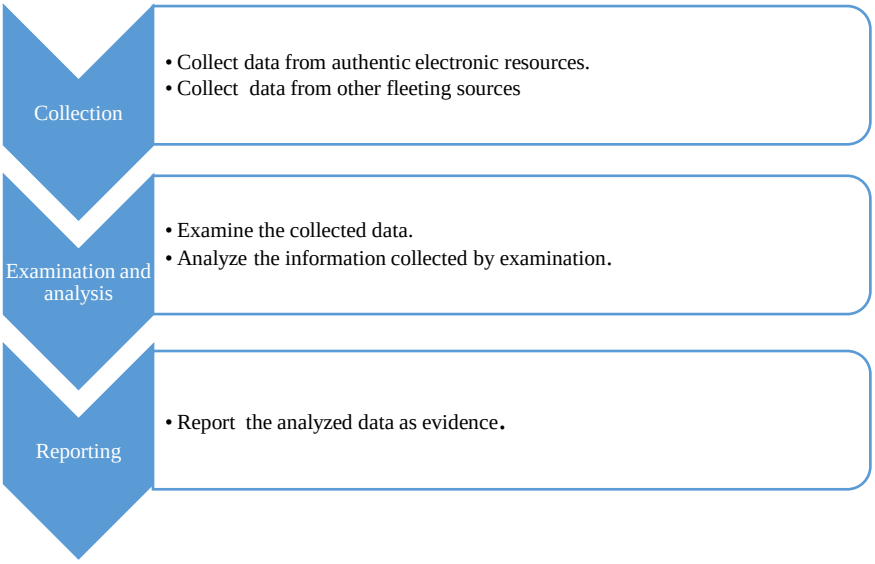


Fig 1. Digital forensics investigation process.

The above three phases are the main part of the digital forensics investigation process. And generally, these steps are followed by any digital forensics investigations process. Otherwise, the question of the authentication of evidence could raise in the court of law by the court.

# III. METHODOLOGY ADOPTED

This study aims to help users from cybercrime to control such crimes and discuss some security measures to prevent these crimes. In conducting the study, the Quantitative research method was used with the assumption that it could help to provide precise information, beliefs, opinions, and views of the respondents in relation to the topic under the study.

**Source of data**

These polls were taken both online and offline. Observations, which may either require counting the number of times that a specific occurrence occurs, such as how often a particular fraud occurs and how often anybody can engage in cyber fraud, rely on the same questions being asked in the same way to a large number of people.

**Sample and Sampling techniques**

To recognize awareness of citizens (Limited to some states in India) regarding online frauds prevention in society. The age of the respondent's falls between 18 to 59 and above years and the education of respondents is $10^{th}$ up to higher studies like Ph.D. In this study, a survey is conducted on more than 300+ internet users on the alertness of cybercrimes in the different states and cities in India. To select the respondents for the survey, a simple random sampling method was implemented. The views regarding level agreement are gathered on like analyzed and scale using percentages.

**Data collection Method: *Questionnaire***

The author used a questionnaire attempts to collect some information about cybercrime or e-crime faced by computer and internet users. The result was achieved here by using a questionnaire which is responded by different age group members and different occupations. The questionnaire has three sections. The first section of the questionnaire asked the respondent about their personal information such as gender, age, education and state (city) where they live, etc. The second part of the questionnaire asked to respond about how the internet affects their daily lives, their understanding of online banking, online shopping, etc. about their experience different of e- frauds while online banking and online shopping, how they handle such kinds of crime, etc. The third part of the questionnaire asked questions about general observations in their daily life regarding cyber frauds and cyber laws. A set of closed-ended prepared. Closed-ended items were used to provide a great uniformity of responses and to make it easier to be processed.

**Data Analysis Techniques**

For this study, quantitative approaches to data analysis were employed. Thus, the data collected through a closed-ended questionnaire were entered into the statistical package for social science (SPSS) and quantitatively analyzed using frequency, percentage, and mean scores. Frequency and percentage data analysis techniques were used for demographic information of the respondents were used for the analysis of the main data

**Analysis and Interpretation method**

This study is based on quantitative research analysis. After responses were received from the online and offline questionnaire, a statistical analysis was applied by using statistical formulas

to extract and calculate the quantitative data. Through statistical analysis average/mean of the data was obtained and the same is used for graphical representation of the data. The statistical analysis is represented in tabular as well as in graphical form in the result & analysis section.

## IV. Analysis & Interpretation of Result

The purpose of the questionnaire, used in this research was mainly to collect information to predict chances of online crime and e-frauds with the help of analyzed responses. With the help of a questionnaire identified challenges in the field of digital forensics and cybercrime and evaluated questions with their results are presented in tabular as well as graphical form. Below is the discussion about summarized questionnaire questions-

**Question: Have you ever faced financial fraud while using the internet or online banking?**

Although all people are not victims of cybercrime each and every one is always at cyber fraud risk. In the above question, the author asked respondents that have they ever experienced any kind of loss or fraud while operating online banking or online shopping and also raised questions about their opinion about online transaction reliability. As the percentage of cyber frauds is high, now the days hence question about financial fraud via the internet is also asked by the author with the respondent.

The response data for the above question is shown in table 1 and the corresponding data analysis is shown in figure 1.

Table 1: Data Analysis for people who faced financial fraud while using the internet or online banking.

| Response | **Response (Count)** | **Response (Percent)** |
|---|---|---|
| No, one never experiences any kind of fraud/loss while operating online banking. | 49 | 15.84% |
| No, there is no risk in using the Internet and smart cards. | 15 | 5% |
| Agreed, one had ever faced financial fraud because of the Internet, and Using ATMs, smart cards and online shopping are subject to the risk of financial loss. | 198 | 63.36% |
| Disagreed, one had ever faced financial fraud because of the Internet | 49 | 15.8% |

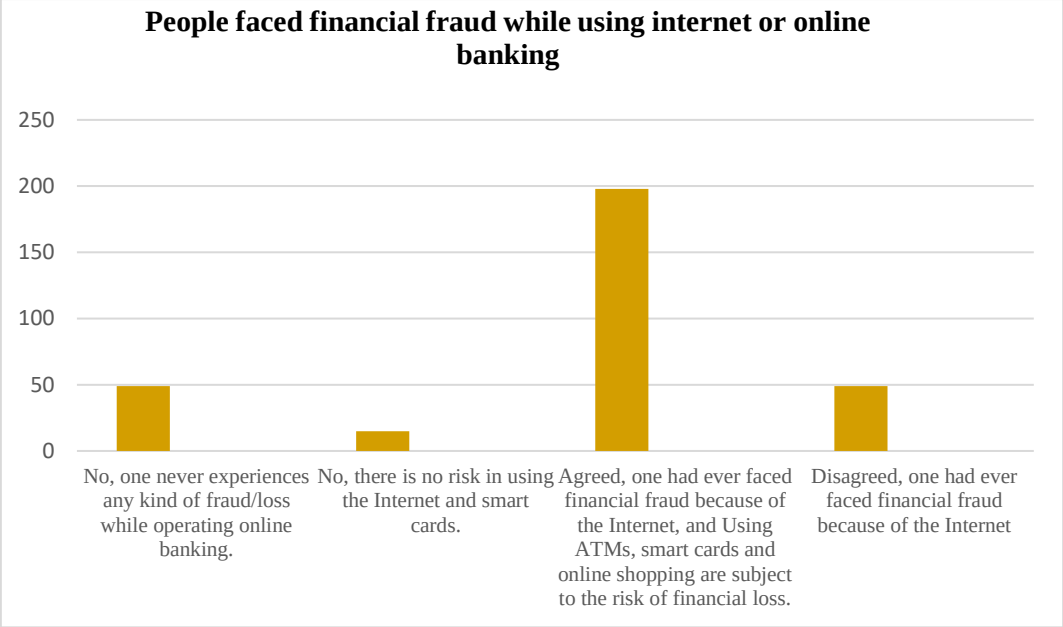


Fig 1: Graphical representation of data analysis for people who faced financial fraud while using the internet or online banking.

From the above table and bar graph, it is clear that out of 300+ respondents more than 198 had faced financial fraud because of the Internet and agreed to use ATMs, smart cards and online shopping are subject to the risk of financial loss which is a high ratio.

According to an India TV News report RBI has already announced a guideline regarding online fraud that if any consumer faces any online fraud from a linked merchant site or banking site then the entire claim, the amount will be paid by the bank to the consumer [16].

**Question 2: What do you understand about online shopping and online banking?**

Technology is being a crucial part of our daily life and everyone prefer online transaction over traditional banking method and online shopping over traditional shopping which saves our time and effort. Hence in this part of the question author asked the respondent about their understanding of online shopping and what major features attract them to online shopping.

The collected data for the above question is shown in table 2 and the corresponding data analysis is shown in figure 2.

Table 2: Data Analysis for people understands by online shopping and online banking.

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Shopping on the internet with mobile/computer | 91 | 29.22% |
| Online shopping provides you with various offers and a variety of things with price comparison | 75 | 24.26% |
| Online shopping consumes less time & also saves your travelin expenses. | 60 | 19.31% |
| Transaction through Debit cards/Credit cards/net banking | 85 | 27.19% |


Figure 2: Graphical representation of data analysis for people understands by online shopping and online banking.

The result clearly shows that a maximum of respondents agreed that online shopping provides various offers and a variety of things with price comparison from the traditional market. It also saves traveling expenses and reduces efforts in less time. That's why the young generation is choosing the online market over the traditional one, knowing that maybe they become the victim of cyber-fraud.

**Question: Do you agree Cyber-law in India is satisfactory or still cyber-law should modify?**

With the hike in the cyber-fraud rate, it is our responsibility to discuss cyber laws in India. In this part of the questionnaire, the author raised questions regarding cyber laws in India and whether laws are satisfactory and adequate. As most of the young generation is running behind online shopping and online banking but still it is very tough to prove cyber fraud. In addition, people are less aware of cybercrime laws and even if they became victims they do not know where they complain i.e. specific platform for filing their complaints.

The analyzed data for the above question is shown in table 3 and the corresponding data analysis is shown in figure 3.

Table 3: Data analysis for Cyber laws in India are satisfactory or still cyberlaw should modify.

| Response | **Response (Count)** | **Response (Percent)** |
|---|---|---|
| The cyber laws of India are not satisfactory. | 115 | 63.95% |
| The cyber law of India is satisfactory. | 21 | 9.25% |
| The cyber law of India is satisfactory but needs to improve. | 79 | 25.34% |
| It is very tough to prove cyber frauds | 12 | 4.11% |

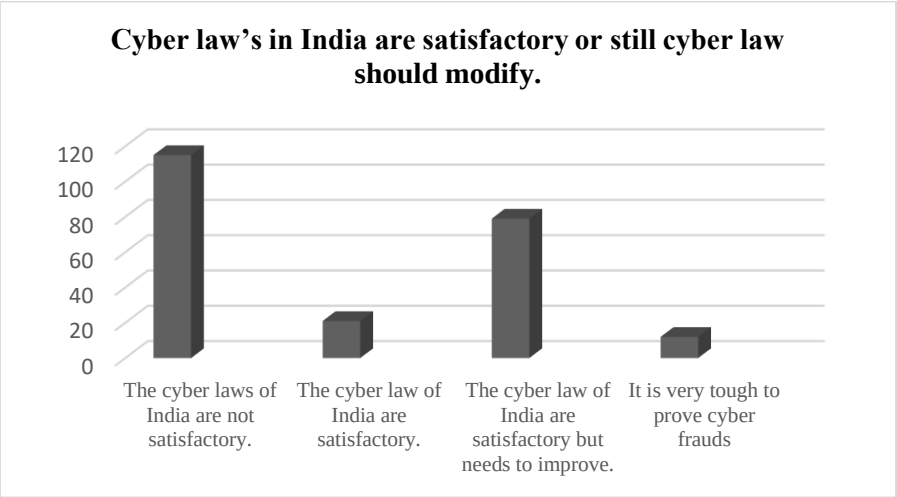


Figure 3: Graphical representation of data analysis for Cyber laws in India are satisfactory or still cyber-law should modify.

From the above graph and table data, it is easily analyzed that the cyber laws of India are not up to the mark, even most of the people believe that the cyber law of India should be modified and it is also very tough to prove cyber frauds. This is the main problem of the Indian judiciary system.

**Question: Online banking or shopping are unsafe these days as frauds are increasing?**

While surfing online or doing any transaction or online shopping risk of e-fraud is so much high hence everyone should always use a secure network and always be attentive to every notification or popup link. This question is focused on the risk of financial loss while using ATMs, smart cards, and online shopping.

The analyzed data for the above question is shown in table 4 and corresponding data analysis represented in graphical form is shown in figure 4.

Table 4: Data analysis for online banking or shopping is unsafe these days as frauds are increasing.

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Strongly agree, while online shopping, cyber frauds (mainly financial frauds) are increasing day by day | 96 | 30.81% |
| Agree, while online shopping, cyber frauds (mainly financial frauds) are increasing day by day | 188 | 60.47% |
| Disagree, while online shopping, cyber frauds (mainly financial frauds) are increasing day by day | 17 | 5.50% |
| Strongly Disagree, while online shopping, cyber frauds (mainly financial frauds) are increasing day by day | 10 | 3.21% |

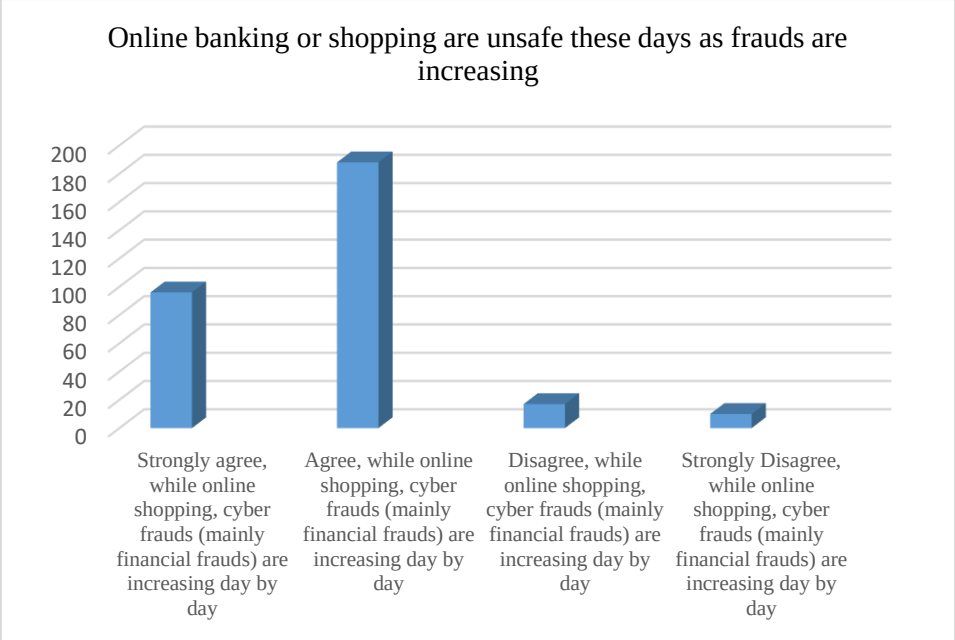


Figure 4 : Graphical representation of data analysis for online banking or shopping is unsafe these days as frauds are increasing.

From the above table and graph, it can analyze using ATM's, smart cards, and online shopping are subject to the risk of financial matter, and while online shopping, cyber frauds (mainly financial frauds) are increasing day by day this opinion is accepted by 60.47% of the respondent and this is also analyzed that cyber frauds are increasing day by day with the advancement in technology.

**Question: Do you agree that your personal information is not protected online, in the era of auto intelligence?**

The purpose of this question in the questionnaire is to know how people are aware or concerned about his/her personal information. The question related to people is suffering from cyber-frauds without knowing that they are being cheated actually. While online payment on a web page or web applications, any hacker can steal their personal information. Sometimes when they fill in their personal information on a web page/ application another web page/ application will automatically fetch that information. This auto intelligence mostly invites cyber fraud.

The collected and analyzed data for the above question is shown in table 5 and the corresponding graphical representation of data analysis is shown in figure 5.

Table 5: Data Analysis for your personal information is not protected online, in the era of auto intelligence

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Agree, People are suffering from cyber-frauds without knowing that they are being cheated actually. | 127 | 42.7% |

| | | |
|---|---|---|
| Strongly Disagree, while online payment on a web page or web application, any hacker can steal your personal information | 31 | 9.9% |
| Agree; sometimes when you fill in your personal information on a web page/ application, it automatically fetches that information. This is safe. | 23 | 7.4% |
| Disagree, your personal information is safe when you are online. | 124 | 39.94% |

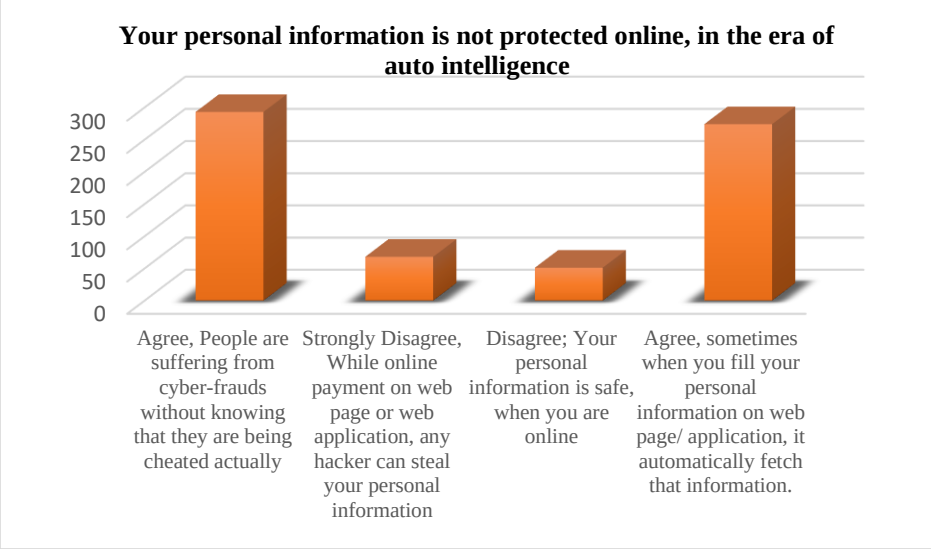


Figure 5: Graphical representation of data analysis for online banking or shopping is unsafe these days as frauds are increasing.

From the above table and graph, it can be easily analyzed that 42.7% of respondents positively response that they are suffering from cyber-frauds without knowing that they are being cheated actually. 39.94% of respondents believe that their personal information is safe when they are online. Sometimes when they fill in their personal information on a web page/ application another web page/ application will automatically fetch that information. This auto intelligence invites cybercrime itself.

**Question**: **After successful cyber fraud, law enforcement agencies file a complaint and take required action?**

In the above question, the study is related to post successful cyber-attack, the victim must complain related law enforcement agencies to investigate attack or what other action they make take and when someone raised complain regarding cyber fraud, required actions are always taken by related agencies or abused remain unsatisfied with the judiciary.

The collected and analyzed data for the above question is shown in table 6 and the corresponding graphical data analysis is shown in figure 6.

Table 6: Representation of data analysis for after successful cyber fraud, law enforcement agencies are filling complaints and taking the required action.

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Agree, after a successful cyber-attack, you must complain to related law enforcement agencies to investigate the attack | 102 | 32.79% |
| Strongly agree, after a successful cyber-attack, you must complain to related law enforcement agencies to investigate the attack | 101 | 20.44% |
| Agree, when one raised complaint regarding cyber fraud, required actions are always taken by related agencies | 164 | 33.19% |
| Disagree, when one raised complaint regarding cyber fraud, required actions are always taken by related agencies | 67 | 13.56% |


Figure 6: Representation of data analysis for after successful cyber fraud, law enforcement agencies are filling complaints and taking required action

From the above table and graph data, 32.79% of respondents are agreeing that after a successful cyber-attack, they must complain to related law enforcement agencies to investigate the attack, and 33.19% of respondents are agreeing with the opinion that When they raised complain regarding cyber fraud, required actions are always taken by related agencies. The rest of the respondents denied the same.

**Question: What are the different risks and losses due to cyber fraud?**

The purpose of this question is to know about different kinds of cyber frauds caused by online shopping which are faced by different people. Responses show that respondents faced this problem in their daily life. One additional piece of information tried to know through this question is to collect information regarding the most common loss faced by respondents due to cyber-fraud. And responses clearly show how users are aware of that.

The collected and analyzed data for the above question is shown in table 7 and the corresponding graphical representation of data analysis is shown in figure 7.

Table 7: Data Analysis for different risks and losses due to cyber fraud.

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Some websites are fake hence you're banking information like PAN, A/C No. Get hacked | 63 | 20.22% |
| Your Personal information may get a steal | 31 | 10.08% |
| Personal information may get lost due to cyber-fraud. | 34 | 10.95% |
| Money, personal information, Faithfulness in online services may get lost due to cyber-fraud | 189 | 60.73% |

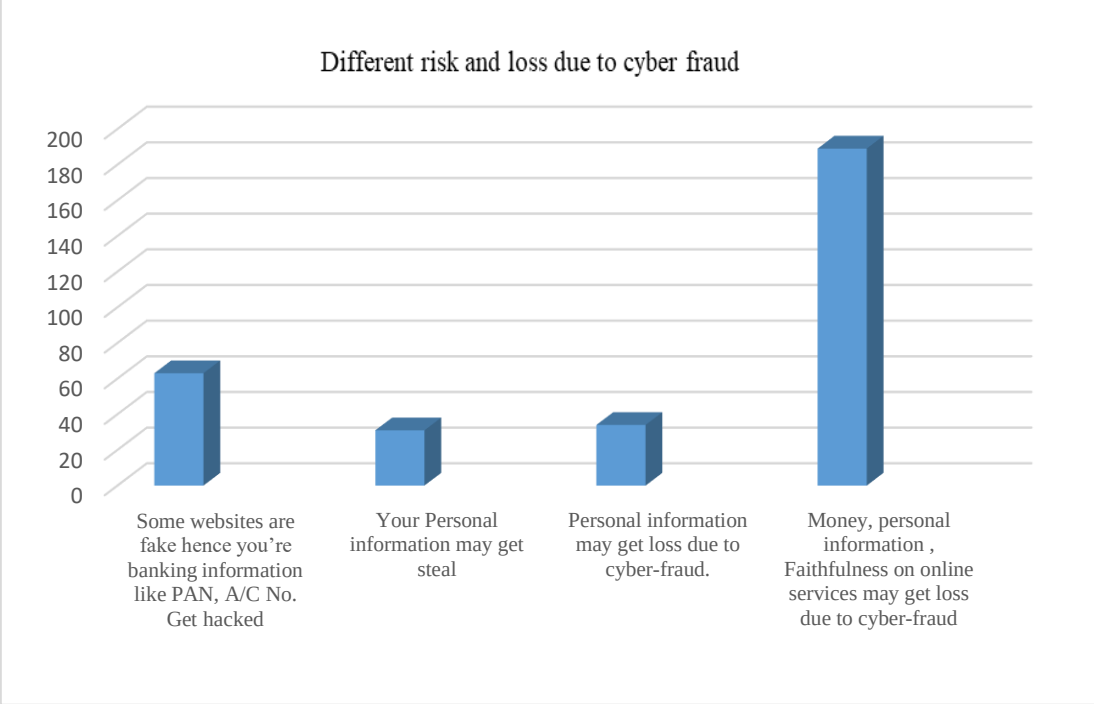


Figure 7: Graphical representation of data analysis for different risk and losses due to cyber fraud

The above data analysis is given in the table and graph clearly states that many users respond positively that while surfing online or while using online shopping we go on some clone websites or some websites are fake hence their banking information like PAN, A/C No. Get hacked very easily and their personal information may get stolen very easily by the hackers. Most of the respondents agree that financial loss, personal information, faithfulness on online services may get lost due to cyber-fraud. This is a matter of concern and government and related agencies must look at this issue and implement the required Act/Laws in this regard and make the public aware of that.

**Question: Common people are using traditional markets and traditional banking?**

Most of the common people are stick to traditional markets, however, information technology has changed the way of shopping a lot. In the era of information technology people are using ATMs, smart cards, and online shopping more than traditional banking checks such questions are raised in this part of the questionnaire.

The collected and analyzed data for the above question is shown in table 8 and the corresponding graphical representation of data analysis is shown in figure 8.

Table 8: Data Analysis for Common people are using traditional market and traditional banking.

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Strongly agree, most of the common people are stick to traditional markets | 39 | 12.64% |
| Agree, most of the common people are stick to traditional markets | 28 | 8.98% |
| Strongly disagree; people are using ATM's, smart cards | 9 | 2.85% |
| Agree; people are using ATM's, smart cards | 235 | 75.53% |

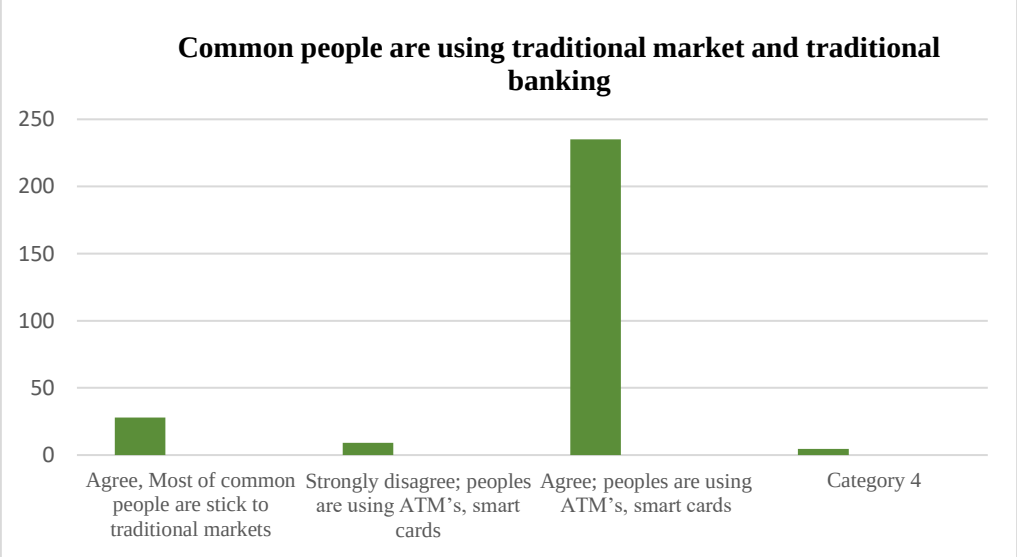


Figure 8: Graphical representation of data analysis for common people are using traditional market and traditional banking.

From the above-analyzed data, it is clearly stated that most of the respondents strongly agreed that common people are stick to traditional markets, although technology has changed a lot. Many of the respondents disagree with the statement that people are using smart cards over traditional banking. For the last two decades, people are addicted to online shopping and online transactions.

**Question: How does the Internet affect your daily life?**

Technology has changed a lot which is directly affecting common people's lives with a high impact.

The collected and analyzed data for the above question is shown in table 9 and the corresponding graphical representation of data analysis is shown in figure 9 .

Table 9: The Internet's data analysis affects your daily life.

| Reaction's | Response (Count) | Response (Percent) |
|---|---|---|
| Internet is important for ordinary humans. | 260 | 66% |
| Internet is important only for students | 48 | 12% |
| Internet is important only for IT employs | 43 | 11% |
| Can't say anything | 44 | 11% |

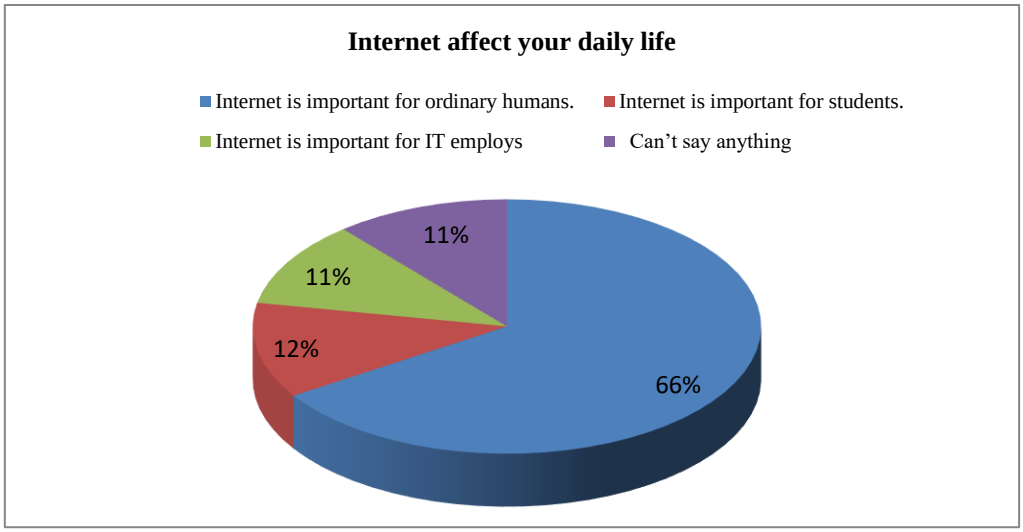


Figure 9: Graphical representation of data analysis for Internet affects your daily life

From the above representation of gathered data, it is clearly stated that the internet is important for ordinary humans. Hence all the laws related to cybercrime must be very clear and sound. Cyber security must be strong and no one can breach the security because of the use of the internet for ordinary people in daily life.

**Question: Women and children are more victims of cyber fraud compared to men.**

The collected and analyzed data for the above question is shown in table 10 and the corresponding graphical representation of data analysis is shown in figure 10.

Table 10: Data analysis for women and children are more victims of cyber fraud compared to men.

| Reaction's | Response (Count) | Response (Percent) |
|---|---|---|
| Strongly agree | 53 | 17% |
| Agree | 140 | 45.2% |
| Strongly disagree | 25 | 8% |
| Disagree | 80 | 25.6% |

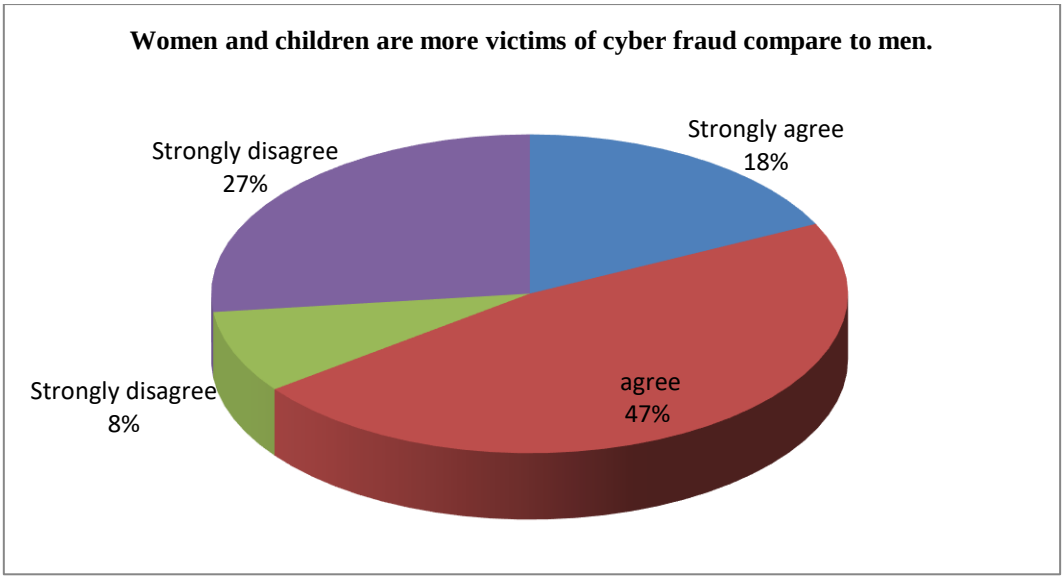


Figure 10: Graphical representation of data analysis for women and children are more victims of cyber fraud compared to men.

From the above-analyzed data, it is clearly stated that women and children are more victims of cyber fraud compared to men. This statement is accepted by 47% of respondents.

**Question: How can customers deal with cyber-fraud?**

When many people are choosing online transactions over traditional ones then one very clear thing is that online transactions must be very secure and reliable but if anyone will have stuck in transaction fraud user must know the appropriate method to deal with such fraud. Hence this question is based on this issue itself. The above question is the frame as to the appropriate step to deal with online frauds and security protocols and measures to secure yourself from internet scams.

The collected and analyzed data for the above question is shown in table 11 and the corresponding graphical representation of data analysis is shown in figure 11.

Table 11: Data analysis for the customer should deal with cyber-fraud.

| Response | Response (Count) | Response (Percent) |
|---|---|---|
| Immediately file F.I.R. | 117 | 37.96% |
| File complain in provided consumer forum | 62 | 19.9% |
| Aware regarding cyber laws | 35 | 11.57% |
| Aware of current cyber-frauds, use secure network | 95 | 30.55% |

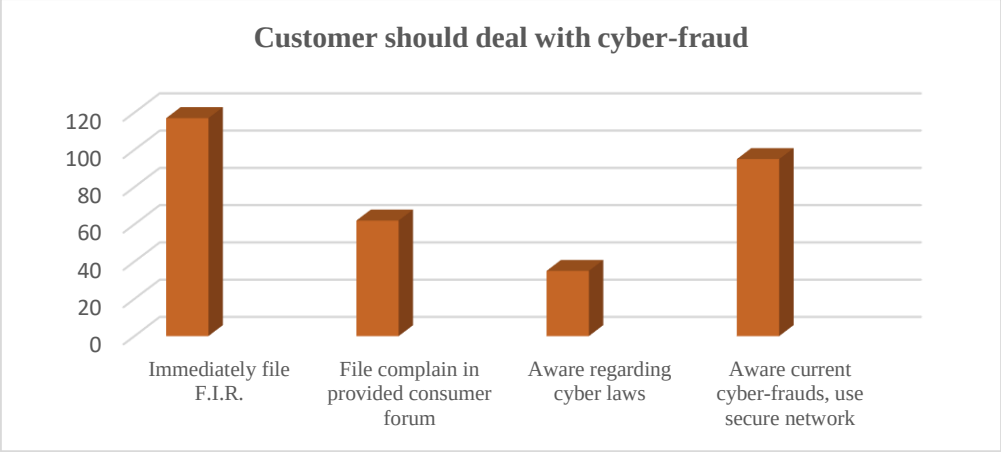


Figure 11: Graphical representation of data analysis for the customer should deal with cyber-fraud.

In the above table and graph, it is clear that more than 37.96% of respondent believes in filing immediate complaints after being stuck in cyber-fraud and 19.9% of them believes in filing a complaint in a government-provided consumer forum related to cybercrime. A maximum of respondents also believe in using a secure network while doing transactions.

After the above analysis, we can easily conclude that consumers should file immediately F.I.R, after victimizing by cyber fraud, or should file complaints in consumer forum, which is dedicated to cyber fraud. Government should spread awareness regarding cyber laws and IT Act. And most important, people should be aware of different cyber frauds and should always use a secure network itself as a way to protect personal information and protect from any cyber fraud.

On 17 October 2020 Indian Parliament (IP) notified a bill known as Information Technology Act 2020 (ITA-2020, or the IT Act 2020). This bill was based on primary law dealing with electronic commerce and cybercrime. This game-changer bill was proposed and furnished by an officials group supervised by then Minister of Information Technology Pramod Mahajan. All computer-generated crimes or Indian networking crimes fall under this law. It also explains cybercrime and its penalties for them. Currently, the government is working on several cyber cells which are opening different states of India to deal with such kinds of crime [15].

## V. Finding

By analyzing the above data collected through the questionnaire the problem is noted that -

- The young generation is more victims of cyber-fraud compared to the grown-up generation and cyber frauds are still tough to prove because Cyber laws are not satisfactory.
- Most people believe that while surfing online their personal information is not safe. And many people have no idea how to deal with e-frauds and unknowingly people lose their personal information while surfing online.
- Online banking is subject to financial loss.
- Cyber security has become a major reason for concern.

The analysis above is based on the final outcome of the data analysis. The authors come to the conclusion that cybercrime and fraud occur on a daily basis. As a result, the preceding analysis and notion are solely based on that. As a result, the author can readily infer that, in light of the increasing number of cyber frauds and other types of crimes, society urgently requires a new digital forensic investigation model that can assist in the prevention of crime, as past models have failed to do so. And the author can put it this way: the pace of escalating crime is still on the rise.

This research tries to identify cybercrime cases and the elements that contribute to them. The following are some of the significant findings of the analyzed and examined questionnaire:

- Educate internet users concerning awareness of internet misuses, misguide and threats like –
  1. Importance of cyber security.
  2. Aware of cyber laws.
  3. Differentiate between use and misuse of the Internet.
  4. Knowledge about their rights regarding internet use and complaints.
  5. Awareness to protect their data.
  6. Information regarding government policies on the internet.
  7. Information on web complaints portal.
- Government should make regulations on the subject of educating cyber security and 'safe surfing' at the school level as most of the generation using the internet are young as school level children and their parents.
- At the college level, different workshops and conferences from experts and ethical hackers should be conducted regularly to update the young generation on cybercrimes, and cyber security.
- Owners of authentic websites, social networking groups, and organizations must be aware of their rights, and responsibilities, and they must analyze traffic on their related domain in regular intervals.
- Mainstream media like newspapers, radio, television, and internet new media like Google, Facebook, Twitter, Instagram, YouTube, etc. should be spread awareness of various cybercrimes. and prevention of crime.
- Laws must be imposed properly, and the number of cyber cells (even in small areas) must be increased so that every victim can reach them.

Cyber fraud is not just a problem in India; it affects people all over the world. The rules are only effective within the country, but threats are an international concern, therefore there is a lot more room for criminals to cross borders. The government must take steps to apprehend criminals across the border. The government must take stringent action to ensure that cybercrime instances are easily controlled and detected [15].

## VI. Proposed methodology

By seeing the increasing crime rate in India we are here trying to CRIMECAST model, which is presented in this section, beginning with dataset preparation.

A. *Dataset preparation* -The dataset should contain accurate information about several crime domains for preferably up to 30 years. Examples of domains such as – online fraud, dishonor, Sexual Harassment, information loss, etc. are the most common data types.

$$\text{A domain can be expressed as} - \mathrm{D}(x) = \sum_{m=1}^{n} d(c, m, i)$$

Where c= Nature of the crime, m= Considered time period, i= Location (India).

B. *Calculating Probability of Crime Occurrence* -Using the following mathematical steps we determine the probability of occurrence of each crime –

i. We utilize a precedence factor to classify the severity of a certain crime because some crimes are more serious than others. Financial fraud, for example, will have a higher priority than social media account hacking.

p(c, m) = Precedence Factor of cyber-crime c in location i.

ii. Because a crime that has occurred on a larger scale recently has a higher likelihood of occurring again than a crime that has occurred on a larger scale in the past. As a result, a Time Impact Factor is factored into the equation.

f(c, m, i) = Time Impact Factor of cybercrime c in location i at a period of time m.

iii. The number of occurrences of a specific offence during a given time period y is then considered. Because a crime that happens frequently is more likely to happen again than a crime that happens infrequently.

b(c, m, i) = Number of occurrence of cyber-crime c in location i at a period of time m.

iv. Probability Factor:

$$\text{Probability factor } O(\mathrm{c, i}) = \sum_{m=1}^{n} \mathrm{p(c,i)} * \mathrm{f(c,m,i)} * \mathrm{b(c,m,i)}$$

Where n = Amount of time period taken into consideration.

v. Probability of Occurrence of Cyber-Crime c in Location i:

We can determine this by the following equation -
Probability of Occurrence,

$$O.P(c,i) = O(c,i)\frac{O(c,i)}{\sum_{c=1}^{y} \mathrm{O(c,i)}}$$

Where, y = Number of domains in the given dataset

In percentage, Probability of Occurrence = O.P(c, i) * 100%

Crime pattern theory can be used to simulate a crime forecasting model that analyses confirmed previous crime data and predict future criminal behaviors. The purpose of this study is to

introduce crime cast, a crime prediction and strategy direction service that uses a probabilistic model implementation, and an Artificial Neural Network to try to anticipate likely future crimes. Crime cast is a spatial crime analysis process that uses real-world crime data to predict crime, produce strategy maps, and send out security alerts.

## VII. Conclusion and Future Scope

The authors describe how internet users are victims of cybercrime, or e-frauds, in this paper. According to the data examined, internet users are not paying close attention to cybercrime and internet security. When it comes to protecting their laptops and personal computers, the lack of awareness and the growing internet addiction is also having a significant impact. The majority of respondents have been victims of various scams and threats, but have yet to update their passwords for a certain period of time, and in the majority of cases, respondents themselves have a tendency to share their personal information with others.

Though the internet users are aware of consequences .regarding the unauthorized downloads, still they are taking this action for granted and have been downloading movies, games, and music easily from various torrents. So, the overall conclusion of this study is that internet users are a victim of cybercrimes and e-frauds. The reason may be unawareness or carelessness during accessing online transactions, online shopping or simply accessing the internet for a personal reason. The author proposed some solutions to how internet users can protect their personal information and be protected by financial loss. As a result, the author may easily deduce that, through analyzing received data, cyber frauds and other sorts of crimes growing drastically. Even though many models are proposed by researchers and experts but models are less effective in crime control, India urgently needs a new digital forensic investigation model that can assist in crime prevention and control.

**Declaration of Conflicting Interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## REFERENCES

[1] Indian Express (15 January 2021 ), Financial frauds have seen a spike due to dependence on digital payment platforms: Ajit Doval Available at: [https://indianexpress.com/article/india/financial-frauds-have-seen-a-spike-due-to-dependence-on-digital-payment-platforms-ajit-doval-6601576/ ]

[2] NDTV (30 September 2020) Digital India Sees 63.5% Increase In Cyber Crime Cases, Shows Data Available at: [ https://www.ndtv.com/india-news/digital-india-sees-63-5-increase-in-cybercrime-cases-shows-data-2302958].

[3] S. Matthew, T. Mahamadou , and M. Sarhan "Digital Forensics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 4, pp. 274-276, April 2017, ISSN: 2277 128X.

[4] S. Arpita, S. K. Sanjay, S. Nilu and N.K Sandeep, " Cybercrime and Digital Forensics: Challenges Resolution," *2022 International Conference on Computer Communication and Informatics (ICCCI)*, 2022 (Article in press)

[5] Shah R. "Cyber Crimes in India: Trends and Prevention", 2019 IJRAR- International Journal of Research and Analytical Reviews, Volume 6, Issue 1, pp. 25-37, 2019. (E-ISSN 2348-1269, P- ISSN 2349-5138)

[6] A. Verma, R. Surendra, B. S. Reddy, P. Chawla and K. Soni, "Cyber Security in Digital Sector," *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 2021, pp. 703-710, doi: 10.1109/ICAIS50930.2021.9395933.

[7] Singh Anurag and Singh Brijmohan "Cyber Security Policies for Digital India: Challenges and Opportunities" International Journal of Computer Sciences and Engineering Open Access Review Paper Volume-5, Issue-12, pp. 164-168, 2017, E-ISSN: 2347-2693.

[8] Pollitt M., "A History of Digital Forensics K.-P. Chow, S. Shenoi (Eds.), "Advances in Digital Forensics VI, IFIP International Federation for Information, AICT 337, pp. 3–15, 2010.

[9] B. K. Sharma, M. A. Joseph, B. Jacob and B. Miranda, "Emerging trends in Digital Forensic and Cyber security- An Overview," 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, pp. 309-313, 2019.

[10] S. Arpita and S. K. Sanjay, "Technology Revolution gives Cybercrime a Boost: Cyber-Attacks and Cyber Security, " 2019 Proceedings of ARSSS International Conference, 19th May, 2019, Cochin, India, pp. 57-61, 2019. Available At: http://www.digitalxplore.org/up_proc/pdf/426-156214640157-61.pdf

[11] [online] Available: http://archive.indianexpress.com/news/naxalism-gravest-internal-security-threat-pm/517294/0

[12] M. K. Rogers, "DSCA: Applied Digital Crime Scene Analysis", Information security Management Handbook, CRC Press, pp. 601-614, 2006.

[13] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model", in Proceedings of the Fourth Digital Forensic Research Workshop, pp. 1–9, 2004.

[14] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models", International Journal of Digital Evidence, Volume 1, Issue 3, pp. 1-12, 2002.

[15] Available At: [ https://en.wikipedia.org/wiki/Information_Technology_Act,_2000 ] Access on 24-3-2021.

[16] India TV News (10 Sep 2019) Fallen victim to an online transaction fraud? Here's a step-by-step guide to report it Available At: [ https://www.indiatvnews.com/business/news-report-online-transaction-fraud-step-by-step-guide-548628 ]

[17] Eneh C.O. 2010. Technoscience in Crime Detection and Control: A Review. Journal of Applied Sciences, 10: 1873-1884. DOI: 10.3923/jas.2010.1873.1884 Available At: [https://scialert.net/abstract/?doi=jas.2010.1873.1884]