CYBER CRIME INVESTIGATION: INVESTIGATION PROCESSES AND METHODS

Ram Eswar D, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

Everything in this world is based on computers and computer networks, and due to this, cybercrimes have also increased. India is a growing nation in which technology also develops day by day. In India, along with technology day by day cybercrimes are also developing like a weed. According to statistics, cybercrime is on the rise in India as technology and the internet advance. Along with that, the pendency of cases also increases due to the outdated method of investigation we are using. So we proposed a model for the process of cybercrime investigation that aims to coordinate with digital forensic officials and cybercrime experts right from the start of a cybercrime investigation.

Keywords: cybercrime, investigation, investigation process, methods, forensics, cyber forensics.

Introduction:

"Technology is a servant but a dangerous master -(Christian Lous Lange,1921)"

Day by day, everything in the world is developing. Everything in this world is growing, from acorns to halos. Like these, technology is also advancing day by day. For the past 20 years, there has been an enormous advancement in technology that has been beyond our imagination. In the past, computers were owned only by companies and rich people, but due to technological development, now literally everyone in this world owns a computer in the form of a smart phone. We can almost do everything using a smartphone, including buying groceries and vegetables. Without smartphones, we can't do anything in this technological world. The internet's role is also crucial in this case. The increasing usage of the internet over the past 15 years is also a cause for these developments. While discussing something, we have to take into account both the positives and negatives of the concept under consideration. Due to emerging developments in technology, offences relating to these kinds of things have also increased. These are called cybercrimes. Cybercrime means offences which are occurred with the involvement of computer. These crimes are more vulnerable in nature than physical crimes, as the offender cannot be easily found out. Nowadays, mostly all the money transactions are digitalized, and even though we can make transactions through mobile, many offences relating to e-transactions are increased and most of the cyber crimes are based on this only. Day by day, like with technology, new crimes are also arising, and there is a need to curtail and control them. As said in the above quote, we can use computers and the internet both in positive way and in negative way. In India, cybercrimes are prevailing since 10 years only, as all the computer and internet related activities were increased for the past 10 years. Covid-19 pandemic is also a cause for this increase, as it forced all the people to stay at home and to do all activities through computer network. Cyber crimes were prevailed before the pandemic, but after pandemic due to increased usage of computer network for day to day activites is the main cause for increment of cybercrimes after the pandemic. In India there are laws which tries to prevent cybercrime like Information Technology Act, 2000 and Indian Penal Code, 1860 etc. However, there is a need for proper investigation and adjudication of these crimes. So, here is a research analysis that is related to the investigation of cybercrimes, challenges faced by police officers, and a new model for the process of investigating cybercrime.

Literature Survey:

Cybercrimes are offences that are committed using computers and computer networks. The ultimate aim of this paper is to discuss cybercrime investigation, its effects, challenges, etc. But it was surprising that only a very few knew about this cybercrime investigation in India; let's see it and also how people other than India handled this concept.

A Framework for Cyber Crime Investigation, Ayşe Okutan et al.(2019), the author attempted to discuss cyber crime investigation and cyber laws in Turkey in this work. He says that the major cause of cybercrime is the development of communication and informatics (IT). He says this was the major reason for rape in intellectual property, identical thefts, child pornography, and hacking became inevitable. Added to that, he says that malware, phishing, trojans, cyberstalking, cyberterrorism, cyberstalking, cyberfraud, worms, cyberbullying, cyberlaundering, man-in-the-middle attacks, denial-of-service attacks, screen loggers, keyloggers, EvilTwin, botnets, and social engineering are the most common crimes in Turkey. Several of the crimes on this list were new and unknown to us. They are,

Man in the Middle (MitM) Attack is a type of crime in which the attacker intercepts between the messages between sender and respondent. He says that Military people can also use this to confuse the enemies.

Screen logger is something like a virus which captures only the screenshots of the computer. They don't attack the computer and capture the files, just it captures the screenshot.

Key logger is also like screen logger, but the difference is it monitors the key stroke by users while using an website. It is generally used to capture the passwords and user ids from users and use them for illegal purposes like money theft, fake identity etc.

EvilTwin is a kind of attack which particularly attacks the WPA/WPA2 security based internet and attaint the data of the users who uses that Wireless Network.

Botnet is a kind of malware which is used to take the control of the computer when the user visits a website.

Social Engineering is a word which describes a range of attacks made through psychological interactions with the users and get the users data.

While talking about steps to detect a crime, they mostly rely on evidence that has been collected, but not on the possible ways to collect the evidence and investigate. For example, steps include: security of evidence, detection of evidence, collection of evidence, protection, extraction, reporting, and detection. Collection of evidence means copies of details taken from devices, but not all cybercrimes will leave evidence as data on the computer itself. So it is not possible to detect the crime and locate the offender. For punishments, they follow the Turkish Penal Code of 2004. The author has only covered the articles that discuss the crime, but not the punishments mentioned in the articles. Since the aim of the paper is to provide a framework for cyber crime investigation, the author doesn't give much importance to the punishment for the crimes that occur.

Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, Cecelia Horan, Hossein Saiedian, 2021, in this article, the author says that cybercriminals use new technology to commit crimes, so the investigators should also use new technology to find them. Added to that, the internet also plays a major role, as all these crimes are done through the internet only. These crimes can be uncovered by digital forensics. Digital forensics is the process of collecting and organising information for the investigation of cybercrimes. The author says that investigation using digital forensics can be done in three ways.

Host Forensics means collection of evidence in a computer device such as systemdate, time, applications used etc. The main challenge in this operating system as each operating system works differently and data can be in different locations.

Mobile Forensics, these kind of investigation is more common nowadays as all the crimes are based on smartphones only. Also it the easiest way of investigation as everyone in this has a smartphone which become an essential part of our life. So the data in smartphones can be easily be taken out. This Mobile Forensics has four investigation phases,

- Preservation
- Acquisition

- Analysis
- Reporting

Network Forensics, this is also like host forensics. Instead of taking computer data, in the details about the evidence is taken from internet host like browsing history, logs and website traffic etc.

Cloud Forensics, is the process of getting information about evidences from cloud services. Due to its emerging development it will also become an inherent evidence in future. Now also it is used to collect evidences.

He insisted new generation like Artificial Intelligence to investigate cybercrime. But it can be used both as a tool and as a target for crime. Also covered, the issues for investigating the crimes like technical issues, legal issues, ethical issues etc. It is important to talk about legal issues as the author says that the main issue is to prove the integrity of the evidence which is collected before the court. The author concludes by saying that the AI automation and machine learning techniques of investigation will have a great future especially in cybercrime and in physical crimes also.

The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics, AineMacDermott, Thar Baker (2020), the author of this article discussed the difficulties that investigators face in cybercrime investigations. In this article, they define cybercrime as criminal activities carried out by computers or the internet and say that it consists of three components. One is the computer as a tool. The second is that computers serve as a repository for criminal information. The third and most important target is the information in the computer.

The criminals are using newly emerged technologies to commit a crime, so the collection of evidence is so difficult that commonly used forensic processes will not be applicable. Nowadays, the world is based on IoT and IoA, and crimes committed using this technology are more stringent because data acquisition and imaging are not possible. Due to certain difficulties like Data Integrity Checking (DIC), Encryption, Cloud computing, VPN technology were became a burden. At last, the author concludes by saying that due to the tremendous development of IoT devices, there is a

need to develop a new process to investigate cybercrimes. Due to the challenges of investigating the crimes and the lack of practical study in this field, it is difficult to investigate cybercrimes.

Cyber-crime Investigation, Shruti Gupta (2020), in this article the author tried to discuss how cybercrime is investigated in India. The author says that between 2012-2018 there were 90,000 cybercrime complaints registered and bitter truth that 63% of Indians do not know that their identities are stolen and says that cybercrimes in India are the serious national issue which questions our security of the nation. Generally, in India common cybercrimes like child pornography, cyber bullying, cyberstalking, phishing, ransomware, Trojans, worms are happened. But specifically there are crimes like Online Job Fraud, Online Sextortion, Vishing, Ransomware, Cyber-squatting, Crypto jacking and espionage are occurred in India.

Ransomware, a type of malware which steals the sensitive information from the users and the offenders threaten the owner and demand money from them.

Cyber-squatting, is a kind of IP crime, in which someone creates a fake website like the true one using their Trade Mark to gain money.

Crypto jacking, is something which is related to cryptocurrencies. In this, the user can be influenced to mine cryptocurrencies using illegal methods.

Online Job Fraud, is common nowadays in India. In this, the offenders will issue notices to public stating that they will earn more in online and promising them to use the application/website.

Online Sextortion, in this the offenders threatens the user to post obscene, sensitive, private images using electronic medium.

Vishing, in this crime, the offender randomly calls people and asks debit or credit card information.

These crimes are investigated by persons who are higher in grade than an Inspector. It is given under Section – 78 of Information Technology Act. According to Section-80(1) of IT act, any police officer, not below the rank of Inspector can arrest any person without any warrant for suspecting or commission of cybercrime. After the arrest, they should present him before a

magistrate having jurisdiction without any delay. It is given under Section-80(2) of IT act. Added that the author described about the process of filing a complaint against cybercrime. So, any person who is an victim of Cybercrime can file an complaint in www.cybercrime.gov.in and also they can give complaint physically by writing to police stations which comes in their jurisdiction. The author in this article, says process of investigation in a simple way,

- Preservation of digital scene
- Survey of digital evidence
- Document Evidence and Scene
- Search for Physical Evidence
- Digital Crime Scene Reconstruction
- Presentation of Digital Scene Theory

About applicability of act for the offences,

- Online hate comments- Section-66A of IT act + Section -153A&153B of Indian Penal code, 1860.
- Email Hacking – Section-43 of IT act.
- Web Defacement – Section – 43,66F,67,70 of IT act.
- Cyber Terrorism - Terrorism laws + Section – 66F,69 of IT act.
- Phishing and email scams – Section – 66,66A and 66D of IT act + Section – 420 of IPC.

The author did not describe punishments and did not explain further how the investigation is done in detail or about the tools that were used by officials in India for the investigation of a cybercrime. More specific statistical data about cybercrimes and their persistence rate, as well as the challenges faced by Indian officials during cybercrime investigations, were also not provided. So, this paper will give an answer to all the portions that were left out.

Methodology:

We are using the statistical method to explain how cybercrime investigation has been done in previous years and its disposal rate. Before that, we shall first know the number of cybercrime cases reported between 2012 and 2021. The table below describes the total number of cases that were reported in India in all of the states between 2012 and 2021.

No. of Cybercrime Cases Reported Between 2012 to 2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
No. of Cases Reported	3,477	5,693	9,622	11,592	12,317	21,796	27,248	44,546	50,035	52,974

According to the above table, the difference in the number of cybercrime cases reported between 2018 and 2019 is 22,750. It results in a 63.5% increase in cybercrime cases in 2019 as compared to the previous year, 2018. The difference between the number of cases reported in 2020 and 2021 is 2939. It resulted in a 5% increase in cybercrime cases as compared to 2020. This describes India as a whole. Let's see the number of cybercrime cases that were registered in each state between 2012 and 2021. The below table describes the top ten states that contribute a high number of cybercrime cases compared to all other states in India.

Top 10 leading states in contributing cybercrime cases in India from 2014 to 2021

Year State	2014	2015	2016	2017	2018	2019	2020	2021

Telangana	703	687	593	1,209	1,205	2,691	5,024	10,303
Uttar Pradesh	1,737	2,208	2,639	4,971	6,280	11,416	11,097	8,829
Karnataka	1,020	1,447	1,101	3,174	5,839	12,020	10,741	8,136
Maharashtra	1,879	2,195	2,380	3,604	3,511	4,967	5,496	5,562
Assam	379	483	696	1,120	2,022	2,231	3,530	4,846
Andhra Pradesh	282	536	616	931	1,207	1,886	1,899	1,875
Rajasthan	697	949	941	1,304	1,104	1,762	1,354	1,504
Bihar	114	242	309	433	374	1,050	1,512	1,413
Tamil Nadu	172	142	144	228	294	385	782	1,076
Jharkhand	93	180	259	720	930	1,095	1,204	953

By observing the table, we can say Uttar Pradesh state has contributed the most number of cybercrime cases between 2014-2021. In 2021, Telangana state contributed 10,303 cases, which is the highest rate in 2021. The ultimate aim of this paper is to discuss cybercrime investigation in

India, so let's see about the cases that were registered, the cases that were disposed of, and the cases that were pending in each year from 2014 to 2018. The table below summarises the cases that were registered, disposed of, or are currently pending between 2014 and 2018.

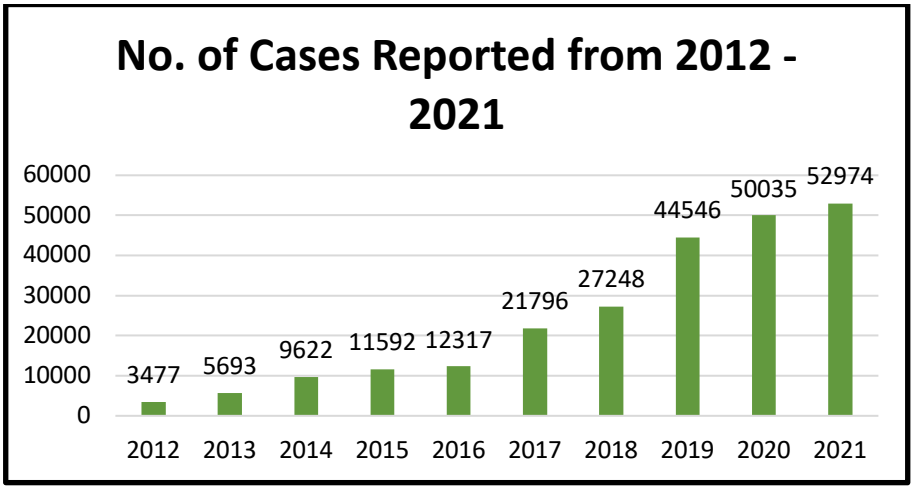
Cyber crimes registered and disposed during the year 2014-2018

Year	Cases Registered	Cases Disposed	Pending Cases
2014	9,622	4,196	8,049
2015	11,592	7,634	11,789
2016	12,317	3,009	14,973
2017	21,796	13,996	22,608
2018	27,248	17,378	32,482

According to the above table, the pendency rate rises each year, and more cases are registered, because the pendency rate is calculated by adding the pending cases from the previous year and the pending cases from the current year. As we can see, in 2014, pending cases were 8,049, and in 2015, they were 3,958. As a result, there are 11,789 pending cases. In 2018, the pendency rate was 65.8 in 2018, which was an increase of 4.1% compared to 2017. So, using the data described above, let's analyse them in detail.

Result and Analysis:

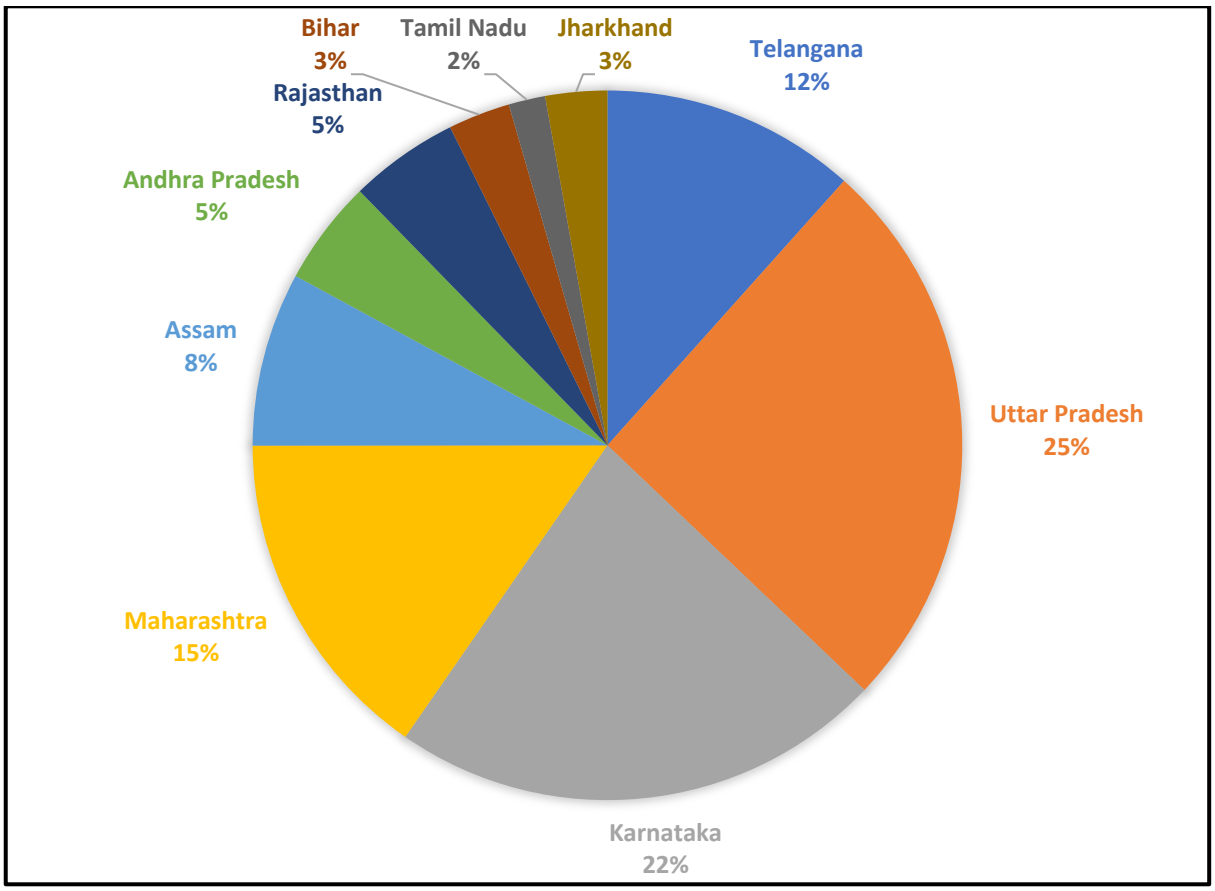
India is an growing country in which technological development is occurring step by step. Like a weed, the number of cyber crimes also increases. So, there is an need to research and analyse it. In this part, we will analyze from the data which were discussed in previous part. First, we shall discuss about the Number of Cases reported between 2012 and 2021.



As we can see that every year, the number of cases increases. This may be due to increasing usage of computer and computer network as the phase of digitalization of all things using internet is also a major reason for it. And another thing which is notable is 63.5% increase in cybercrime cases in the year 2019. According to experts, the increase was due to the digitisation of activities of government. Another notable thing in 2020, the difference in number of cybercrime cases between previous year was 5,489 and it was an increase of 11.8% as compared to previous year. The main reason in 2020 was Covid-19 pandemic, during which all the activities were made online right from education everything were made through computer and computer network. So, the increase in number of cases was due to Covid-19.

To understand better, let's see the analysis of top ten states which contributed more number of cybercrime cases between 2014 and 2021. We took into consideration only the top ten states, so that we can understand which state contributes the most cases and find a reason as well as a solution for the increase in a particular state by analysing state contribution in cybercrime cases.

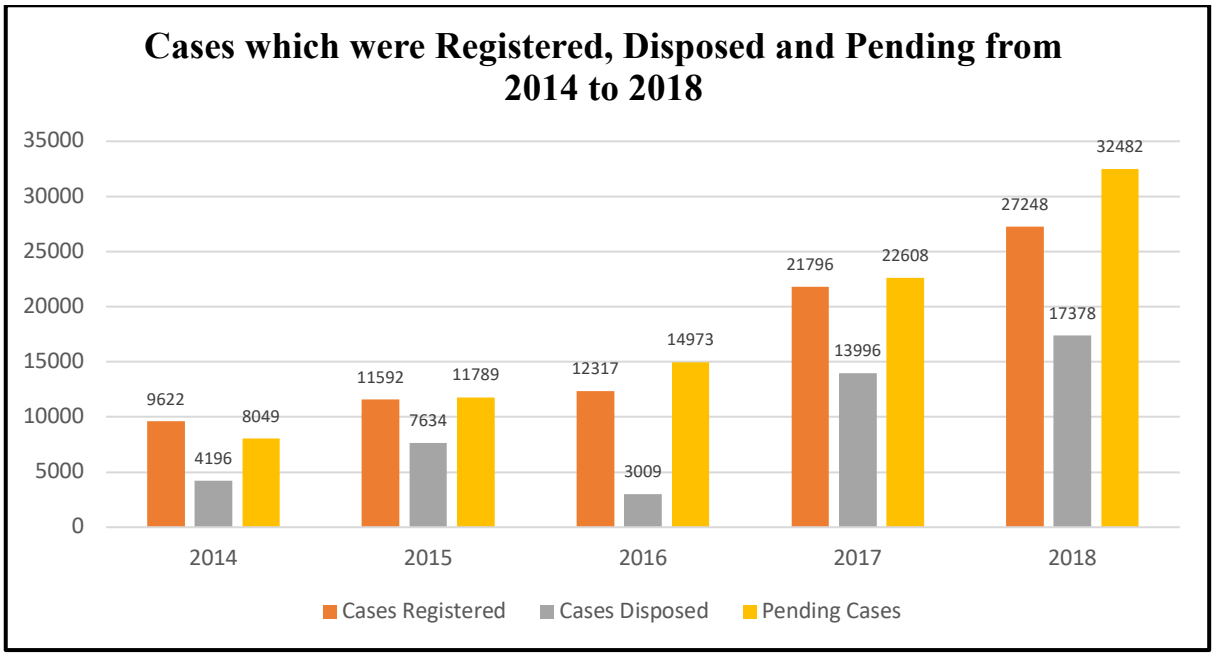
Leading states which contributed more number of cybercrime cases between 2014 and 2021



By seeing the pie chart, we can definitely say that Uttar Pradesh contributes more and the number one state in cybercrime rate. Due to this, it is called as Cybercrime Capital of India. According to experts, the increment in cybercrime in Uttar Pradesh was due to unemployment and due to 4G services which were given free by service providers in during 2017 and 2018. So, due to free internet, the jobless youngsters found way to earn money through online in illegal ways. The other reason for this are unemployment and high population in the state. Next to that, Telangana. Everyone believed that Telangana is the new state and the possibility of cyber crime will be very low. But surprisingly, in 2020, it was the top most state in cybercrime rate as it recorded 10,303 cases in 2020. Other states like Kerala, Tamil Nadu, Assam, Andhra Pradesh, Bihar, Jharkhand, Rajasthan had considerably low rates compared to other states. But, the cybercrime rate doesn't lowered in these states. It is increasing year by year but not tremendously like Uttar Pradesh,

Karnataka and Maharashtra.

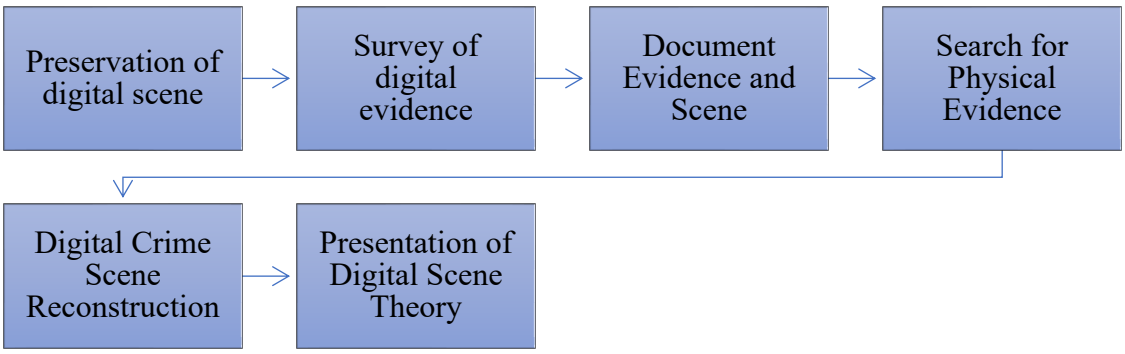
Till now, we have seen about cyber crimes in India as a whole and in leading states. Let's see about cases which were registered, cases which were disposed and cases which were pending during the period of 2014 to 2018 in India. By analysing this, we can find the result of all the questions which were arisen in previous circumstances.



After analysing the above bar chart, it's clearly understood that the number of pending cases in every year is increasing, while the number of cases that were disposed of is very low. In 2018, the total number of pending cases was 32,482. It is the total number of pending cases in each year. From 2014-2018, the total number of disposed cases was 46,213. In 2017, there was an tremendous increase in the disposal as it was the time internet in India got boom. Here internet services which were made free and low by certain service providers is a main cause for it. In 2018, also there was a increase in the disposal rate. But, the pendency rate didn't reduce like increment in disposal rate. Approximately more than 60% of cases registered in each year remain undisposed. What's the reason behind this? The reason behind this is the method our officials follow to investigate cybercrimes. In cybercrime investigation, they follow the regular methods of investigating physical crimes. These methods are outdated, and there is a need to bring some updates to investigation methods. So let's discuss about them.

Discussion:

As we already said the main reason for increment in cyber crime is development of technology. After analyzing the statistical data, we observed that every year the cases of cybercrime increases as well as the pendency of cyber crime cases also increases year by year. As said, the main reason for this is, investigation methods followed by our police officials are not effective and outdated. so it takes more time to dispose a case. Commonly used investigation method is as follows,



This investigation method is of 6 steps, they are, preservation of Digital Scene. In this phase, first the crime scene in which cybercrime was happened will be preserved. It means making restriction to use the crime scene by others as the evidence may disappear. Next is Survey of Digital Evidence, in this phase, the evidences which are in the device from which the cybercrime happened will be taken. Next is Document Evidence and Scene, in this phase, a report will be drafted from the crimescene references and digital evidences which were collected. Next is Search for Physical Evidence, in this phase, the crimescene is put into investigation for collection of any physical evidences which were left out by the criminal. Next is Digital Crime Scene Reconstruction, in this phase, based on the evidences collected, the officials reconstruct the crimescene based on the evidences. Next is Presentation of Digital Scene Theory, in this Phase, the crimescene happening based on theories by officials shall be presented before the higher officials. While investigating there are challenges faced by our officials. So, let's discuss about challenges faced by our officials while investigating the cybercrime in India.

Challenges in investigating a cybercrime:

- Lack of Knowledge

The cybercrimes are done by persons who have a wide knowledge about computers. Since, these crimes are investigated by police officers, they will not have much knowledge about these crimes.

- Lack of Technology

As already said, they don't have much knowledge about the computers, using the existing technology, they will find it difficult to investigate. So, the disposal rate decreases. Nowadays Artificial Intelligence based investigation techniques are there to investigate the crime. But, the officers were not aware of that.

- Loss of evidences

As already said, they officials are not aware of new techniques, there are chances for loss of evidences. So, they may found it difficult to locate the criminal.

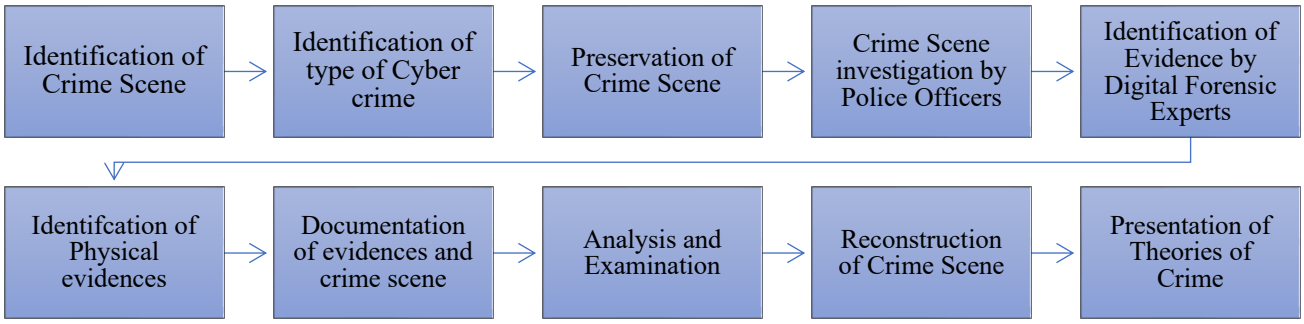
- Lack of awareness

This is the main challenge in cybercrime investigation. As both the people and officials were not aware about the cybercrimes and so the criminals may easily manipulate and steal money from people.

- Adjudication of Cybercrime

Though, we have IT act, 2000, which provides punishment and IPC which also provides punishment for cybercrimes. But they are not effective. There are so much loopholes in these laws and so the criminal escapes from punishment.

Due to these challenges faced by our police officials, the investigation of a cybercrime takes longer time than physical form of crimes and also process of investigation is the main cause for lower disposal rate of cases in every year as this process takes more time to investigate. This is based on the statistical data which we have collected. Instead of this process of investigation, we made a model for process of investigation of cybercrime. Let's see it.



Our model for the investigation includes 10 steps, let's discuss about them in detail.

1. Identification of Crime Scene

   This is the very first phase in the investigation process. In this phase, the complaint from the victim will be recorded and the crime scene where the crime scene occurred is identified. And the data from the crimescene is collected.

2. Identification of Cyber Crime

   After identifying the crime scene, the officials should recognise which type of cyber crime is happened. Mostly in India, Phishing, Vishing, Online Job Fraud, Online Sextortion, Money laundering, Cyber Stalking etc. are common types of cyber crimes which are happening in India. It will be identified by police officials or if they found it difficult Digital Forensic Experts will identify the type of crime.

3. Preservation of Crime Scene

   The crime scene should be preserved. If not, the evidences will be manipulated, destroyed, damaged. After collecting the data in the crimescene, we need to preserve them. So, the crimescene and the device should be secured. First, the data collected from the device should be copied to another storage device, so that the data loss couldn't be occured. There are three popular methods for preserving the crime scene data. They are:

- **Drive Imaging,** in this method the drive in which the data is stored shall be copied bit-by-bit. It

means taking carbon copy of the drive.

- **Hashing,** in this method the the investigator creates an image of the evidence through generating cryptographic hash value. It is the process by which the huge data will mapped into small tables using hashing value.

- **Chain of Custody,** it is the process of validating the evidences which were collected by arraning them in sequential order.

4. Crime Scene Investigation by Police Officers

   In India, generally police officer who is not below the rank of an Inspector will investigate cybercrime. It is given under Section – 78 of IT act, 2000. So, first the police officers will investigate the crime scene.

5. Identification of Evidence by Digital Forensic Experts

   After, investigation by police officers, the digital forensic experts will investigate and search for digital evidences in the crime scene.

6. Identification of Physical Evidences

   Even though it is a cybercrime, sometimes physical evidences also help in finding the criminal who did the cybercrime. So, after identification of digital evidences, the police officers shall search for physical evidences related to the crime scene.

7. Documentation of Evidences and Crime Scene

   After identification of evidences, all the crime scene evidences will be documented. Which means the evidences collected from crime scene shall be noted in form of document as the investigator will recall all the instances of the crime.

8. Analysis and Examination

   In this phase, all the evidences collected will be examined and analysed. The Digital Forensic

Expert will analyse the evidences using the tools like Sleuth Kit(is an software used to analyse storage devices, smartphones etc.), Wireshark (is an software used to analyse website traffic and capture network files for analysis).

9. Reconstruction of Crime Scene

   After analysing the evidences, the investigators will know how this crime is happened. After that they will reconstruct the crime scene which was happened.

10. Presentation of Theories of Crime Scene

    After reconstructing the crime scene, the theories will be constituted and will be presented before the higher officials and the process of arresting and prosecution will be done.

This is our model for cybercrime investigation process. Though it has more steps than the conventional process, normal police officer can't investigate themselves without the help of Digital Forensics Experts and Cyber Crime experts. So, by interference of these experts along with police officers, the investigation will be done faster than the conventional method of investigation.

Future Enhancements:

As already said, even if we use various methods to investigate cybercrime, the criminals will easily elude us as our laws and legal system have many loopholes. So, in my opinion, we should impose harsh penalties for cybercrime as well as a wide range of other crimes that are prevalent in our society. For example, for hacking, the punishment under Section 66 of the IT Act is imprisonment up to 3 years with a fine up to Rs 2 lakh. For an eminent hacker, 2 lakh is not a big amount, and after 3 years, it is not sure that he will not again do hacking. So, if there is a rigorous punishment that reforms the criminal to deviate from his evil mind, it is needed. So I will conclude by saying that more and more punishment will reduce the crime, even if we follow different modes of investigation for cybercrime.

Conclusion:

As technology advances, the number of cyber crimes also increases. By analysing statistical data,

we discovered that cyber crime is increasing year over year, as is the number of pending cases. The pendency of cybercrime cases increases year by year due to an outdated investigation process by police officers. In India, these crimes are investigated by police officials, but due to this outdated process and other challenges they face, they find it difficult to dispose of the cases in a shorter period of time. As our aim is to discuss the process of investigation, challenges, we proposed a new model for the process of cybercrime investigation that mainly aims to coordinate with digital forensic and cybercrime experts from the initial process to the investigation of the case. Though we can define various models for investigation, our Indian legal system has many loopholes, so a criminal can easily be exempted from punishment. So, if there is a strict legal system and adjudication of these crimes, the crime rate will decrease; otherwise, it will increase every year, and the pendency will also increase. So, I conclude by saying that lack of awareness among people is the main cause for these crimes, and it will be more helpful if the government provides basic awareness about cybercrimes in India in the future.

Bibliography:

- Marcella, A. J. (2008). *Cyber forensics: A Field Manual For Collecting, Examining, And Preserving Evidence Of Computer Crimes.* (pp. 98–107). , Auerbach.
- Yatindra Singh,(2016). *Cyber Laws* (6th Edition). (pp. 174)., Universal Law Publishing.
- Rahul Matthan.(2000). *The Law Relating to Computers and the Internet*. (pp. 19-21)., Butterworths.

Webliography:

- https://www.sciencedirect.com/science/article/pii/S1877050919312141
- https://www.mdpi.com/2624-800X/1/4/29
- https://www.igi-global.com/article/the-internet-of-things-challenges-and-considerations-for-cybercrime-investigations-and-digital-forensics/240648
- https://blog.ipleaders.in/cyber-crime-investigation-conducted/
- https://community.nasscom.in/communities/cyber-security-privacy/cyber-forensics/how-to-investigate-cyber-crime-and-be-cyber-secure.html
- https://www.statista.com/statistics/309435/india-cyber-crime-it-act/
- https://factly.in/in-5-years-more-than-fourfold-increase-in-the-number-of-pending-cyber-crime-cases-in-courts-the-police/