THE LEGALITES LEXSCRIPTA
ISSN 3108-2416 (ONLINE)
Editor-in-Chief: - Prof. (Dr.) Aryendu Dwivedi
Volume II Issue I (Jan-March 2026) Page No.: - 485 to 500

REFORMING INDIA LEGAL FRAMEWORK FOR DIGITAL FORENSIC: ADDRESSING CYBERCRIME, DIGITAL VIOLENCE AND PRIVACY CHALLENGES

SHANIKA SHUKLA
Student at Amity Law School, Amity University, Lucknow

ABSTRACT

In the recent time, cybercrime has emerged as a major and serious global threat, mainly due to the rapid growth of internet-based crimes. With rapid advancement in the technology and cyber tools, criminals now have access to various tools and social platforms such as social media, online marketing, e-commerce, messaging application. These tools provide them with a convenient and anonymous way to communicate and coordinate for omission of such offences. As a result, today the world at large is getting more subjected to serious offences of cybercrimes, online harassment, privacy infringement, human trafficking, and terrorism.

In the digital era, crime has expanded far beyond traditional boundaries, becoming more organized, widespread, and technologically advanced. Criminal operate across border without physical presence, targeting victim globally. Techniques like phishing, hacking, Ransome attacks, and online scams have become more complex due to artificial intelligence, data manipulations, automation. This shift has not only increased the volume of crime but also changed their nature which is now more focused on data theft, system disruption and financial fraud.

The paper deals with how the rapid advancement of cybercrime have led to the development of digital forensic science as a crucial field in criminal investigation. Digital forensic involves the identification, collection, and analysis of electronic evidence from devices such as phones, computers, networks. Its plays an important role in tracing criminal activity, recovering deleted data, and identifying suspects of internet-based crime. As cyber crimes continues to grow, digital forensic helps the law agency to provide reliable evidence for investigation and court proceedings. Its importance has grown significantly in solving modern crime and ensuring that offender can be brought to light and justice is served.

Keywords: Digital Forensic, Cybercrime, Digital Violence, Artificial intelligence, Privacy infringement.

INTRODUCTION

Since the starting of the decade, there have been an increase in the number of crimes that is committed online. Internet has become a content dependency for people to not only to stay connected but also, conduct their business and profession. This has become a major aspect for the cybercrime. Cyber-crime in general term is defined as any unlawful activity where communication of computer device or computer network is used to commit or facilitate the commission of crime. The technological advancement has made it more convenient for the offenders to have various tools and opportunity to access a larger information and data for the commission of the cybercrime. Platforms like social media, encrypted messages, online calling/texting, e-commerce, e-banking have become a great medium for the offenders to defraud people into such situation.

After the recent covid pandemic, digital and cyber technology and digitalisation has emerged as a new dimension today. it is led to people quarantined in their homes, with internet and online platforms being the sole means for connecting and conducting business. From making calls, filing online forms, to making payments these platforms have now became a necessity. The digitalisation has not only impact and but also change the societal nature. While the widespread adaptation of technology facilitates a large group of people, its also provides antisocial elements with a platform to develop a new and sophisticated method to fraud. These law breakers are more rapidly upgrading themselves with these new technologies and so to use it for their advantage and thus making innocent people more vulnerable and target of such illegal actions.

All this have caused a create impact to the current criminal justice system as now the old way of investigation becomes pointless. The transition in the digital era has changed the nature of criminal investigation system. Historically the evidence used to be testimony and document based but now it prioritises digital evidences and digital footprints. These footprints include data left behind, networks, texts, IP logs, meta data which are far more evident and verifiable.

DIGITAL FORENSIC

DEFINITION

Digital forensic or digital criminal investigation in a new age investigating procedure which involves several applications of computer. Its preserve and identify digital evidence to facilitate the investigating procedure[1]. Digital criminal investigation involves gathering and examining data from electronic devices so that it is properly used in legal matters. It helps in understanding the past events which in turn helps in preventing possible future crimes, while also ensuring that privacy and security is maintained.

EVOLUTION OF DIGITAL FORENSIC

The emergence of digital forensic dates to 1980s when the use of network was increased. This made it a necessary for investigator to recognise the value of digital network in solving crimes. This need led to the development of computer forensic as a different category such as FBI's Magnetic media program (1984), computer analysis and response team an early forensic software tools in the era of 1990s the personal computer network started dominating the society and it resulted in the need of digital forensic s for enlarging everything related to networks and Internet

Later in 1995 The International Organisation on computer evidence brought a rapid growth in digital forensics. These organisations standardise protocols and expanded Networks beyond computer devices. As we move into 2000 The increasing use of laptops mobile phones and other smart devices created new challenges for investigators. This device store huge amount of data and are often connected to cloud platforms and advanced technologies like artificial intelligence. Because of these digital forensic experts had to continuously improve their techniques to develop new tools to extract Analyse preserve digital Information In an effective way

In India the legal recognition of digital evidence began with the introduction of information Technology Act 2000. This is an important step in addressing cybercrime and regulating digital activities. Overtime, the legal framework has been strengthened through new laws such as

[1] Raed S.A.Faqir, Digital Criminal Investigation in the Era of Artificial Intelligence: A comprehensive overview, Vol 17 Issue 2 Open Access, 77, page 78, (2023)

Bhartiya Naye Sahitha and the Bharti Saksh Adhiniya which includes important provisions related to electronic evidence and cyber offences

Furthermore, the Bhartiya Nagar Suraksha Sahita BNSS 2023 Emphasis the use of modern technology in law enforcement Stop. It highlights the role of audio video recording during police investigation especially in process like search and seizure this improves transparency and helps ensure proper handling of evidences.

Overall digital forensic is a constantly involving field. As technology continues to advance new challenges will rise. But at the same time better tools and method will also develop. It pays a vital role in model investigation by helping authorities solving crime and present accident digital evidences in court

BRANCHES OF DIGITAL FORENSIC

- Computer forensic: a type of digital forensic. It includes the investigation and collection of evidences related to crime and incident from devices such a computer, laptops, servers
- Mobile forensic: this deal with accessing data and information from smart devices, tablets, and another portable device. In this the evidence may include text, image, video, call logs, app usage, etc.
- Cloud forensic: the investigator analyses the cloud storage and its activity to determine if any illegal activity or evidence.
- Network forensic: this type of forensic indulge in analysing network traffic to identify security infringement, unauthorised access to determine its is used for any illegal act or omission.
- Memory forensic: this includes examining the computer or devices memory software like RAM.
- Forensic data analysis this type of investigation involves examination of large amount of data and identifying the patterns, trends, inconsistency in data to track illicit activities.
- Malware analysis: in this aspect, analyst examine the corrupt malware.

PROCESS OF DIGITAL FORENSIC

The National institute od standard and technology (NIST) highlights four main steps of process of digital forensics. These are as follows:

- Data collection: The investigation begins with gathering important digital information from various sources like devices and storage systems. Investigator identifier useful data along with its details and make proper copies to keep the route evidence safe for further use.
- Examination: Once the data is collected it is closely checked and reviewed. This may include looking at browsing history, messages, cloud data, deleted files, system storage and corrupted files. Only duplicate copies are examined to protect the original data. This step helps ensure that the evidence is accurate and can be thrusted in legal cases
- Data Analyst: In this stage Experts study the data using different techniques and forensic tools. They tried to uncover hidden details Track suspicious activities, and understand the sequence of events various tools Including open sources once can be used to identify possible threads or criminal actions.
- Reporting: After completing the analysis investigator prepare a detailed report this report clearly explains the findings, outlines what happened and may indicate who was responsible. It is the final step and is used as supporting evidence in court.

DIGITAL FORENSIC VS COMPUTER FORENSIC

digital forensic and computer forensic are often used interchangeably. However, there are some crucial differences between them. Digital forensic includes the examination of data from any digital device such as smartphones, digital camera, tablets, and network traffic. While computer forensic emphasis on investigation through computer devices such as laptops, and desktops and servers.

In brief, computer forensic is a type of digital forensic. Both of methods are applied to extract information and data from devices for legal proceedings.

Digital forensic and Incident Response (DSIR) is a growing area in cyber security that brings about the process of investigation digital evidence and responding to cyber incidents. Its main goal is to quickly handle ad fix security threats while making sure that any digital evidence collected stay safe and unchanged.

ROLE OF DIGITAL FORENSIC

In recent years, artificial intelligence has become an important tool in facilitating in identifying of risk and predicting behaviour of criminals and preventing further crimes. It works through advanced algorithms that are design to detect security threats, cybercrime, and analyse

evidence effectively and efficiently. Technologies like machine learning and deep learning are also used for surveillance purpose such an observing crowd through CCTV footage and enabling facial recognition. Compared to the traditional methods, AI driven investigation focuses more on analysing digital data and how it can be accepted in court. These systems also strengthen and improve real time monitoring and can also interpret intention through facial expression and body movements.

Various advance tools and technique linked with AI helps in extracting important digital evidence such an emails, chat histories, and metadata. Such evidence is generally reliable and accepted in legal proceedings. AI supported digital investigation reply on modern technologies to provide accurate and through analysis across different types of digital evidence while following legal standard. However, these advancements also come with important ethical and legal responsibilities. Maintaining the integrity of evidence, protecting privacy, and ensuring fairness are essential. Strong data protection, transparency and proper documentation play a key role in ensuring a just and trustworthy investigation process

COMBATING DIGITAL VIOLENCE

Forensic examination plays an important role in dealing with cyber bullying and online threats, especially because digital investigation can be complex. It includes carefully collecting, preserving and studding digital evidence to find out who is responsible and make sure they are held accountable. Investigators need to understand how different online platform and communication system works. They also have to follow legal and ethical rules so that the evidence can be accepted in the court.

To find the source of online threats, investigators use methods like IP tracking, studying network logs, using open-source intelligence to connect to online activity to individuals. But tools like VPN and proxy server have made it more challenging for investigator due to which only through advance technique, they are able to trace from where the threats comes from.

ROLE OF META DATA

Meta means underlying description. Meta data together mean any information in a form of data that gives description for another data. It is commonly called as “data about data”. In the digital forensic metadata is very useful, especially if it provides access to information which is difficult to extract. Because it gives more crucial information to investigators then just content of files or computer hardware, it becomes extreme useful.

In the field such as a legal investigation and information management, instructing digital forensic experts to conduct a metadata analysis can serve an invaluable resource. They support in verifying authenticity, tracing data origin and ensuring the integrity of digital evidence whilst reducing manual efforts and minimising the risk of errors[2]

ROLE IN PREVENTING DIGITAL ARREST

Digital arrest is a cybercrime involving scammers posing as law enforcement or governmental authorities like officials from Reserve bank of India, central bureau of investigation or directorate of enforcement, etc and scams and defrauding innocent individual and extort huge sum of money from them. These scammers mostly isolate the victim on the pretext of subsequent arrest or imprisonment. This has been on the rise in India, not only due to the technological advancement but also cause of digital illiteracy.

As per the reports of the world cybercrime index, India is ranked 10th among nations facing alarming cyberattacks and cybercrime related cases.[3] According to a report published by The Times of India in 2023, innocent Indians targeted by cybercriminals lost ₹17,000 crore in wealth. Around 4,50,000 bank accounts were identified as being involved in the rotation and circulation of cybercrime proceeds, transferring funds from victims' bank accounts to overseas accounts. In 2024 alone, approximately 29,000 cyber fraud cases were reported in India. Alarmingly, less than 10% of the total fraud amount was recovered by law enforcement agencies.[4]

The government of India have put proactive measure in preventing such crimes and to combat digital arrest and make it safer for the people. Though digital forensic is a critical for investigation the conviction rate of criminal of digital arrest remains low. The conviction has approximately bee 1.6% between 2020 and 2022

[2] Cyfor Forensic, https://cyfor.co.uk/what-is-metadata-how-does-it-work/.
[3] Shailesh kumar Pandey and Ansh Parashar, Navigating digital arrest under Indian's cyber forensic framework, Vol 4 issue 1, NFSU journal of forensic justice, page 80, 80, 2025.
[4] Id, at 80.

LEGAL FRAMEWORK OF DIGITAL FORENSICS

UNITED STATES

In united state the admissibility if digital evidence is governed by the federal rule of evidence 1975. In it the most important factor is the authentication of evidence. after the authentication the evidences come from the federal rule of evidence section 401 and 402.

Section 401[5] states that, the evidence is only admissible when it is considered relevant and has the potential to influence the facts stated and that fact is important in deciding the case.

Rule 402[6] state that relevant evidence is admissible unless there is specific reason for exclusion. The reason includes provision in the united state constitution, federal statute, and rules specific in the document or laws as establish by supreme court.

The only challenge united state faces in admissibility of evidence are their dealing with hearsay evidence. rule 801 and 802 state that the court determine whether the evidence given is direct evidence or a statement to prove a fact.

EUROPE

In the European union, the electronic identification authentication and trust service (eIDAS) through EU regulation regulates the electronic transaction in European union. It sets standard for digital and electronic signature, electrical seals, and time stamps. It gives significance to digital evidence.

AUSTRALIA

In Australia, the uniform evidence act governs the admissibility of digital evidence. section 146 and section 147 state that admissibility of computer-generated evidences.

Section 146[7] explain that when a document or item is produced using a device or process that are normally give a particular result when operated properly it is presumed that the outcome is accurate.

[5] Federal rule of evidence, rule 401, Act of parliament, 1975(USA)
[6] Id at rule 402.
[7] Evidence (National uniform legislation) act, section 146, act of parliament, AUS, 1995.

Section 147[8] work in a similar way but applies to record created during business activity. It assumes that the document made is in the ordinary course of business are trustworthy. These provision helps in accepting electronic evidence in courts.

LEGAL FRAME WORK IN INDIA

In India, the introduction of the three new criminal law i.e. BNS, BNSS, BSA has played a crucial role in recognizing the legal admissibility of digital as well as electronic evidences. These laws put emphasis on digital forensic in modern law enforcement. Some of the main provisions are as follows

BHARTIYA NYAYA SANHITA 2023

In BNS, which is the new substantive criminal law in India, include provision regarding digital as well as electronic evidences. This evidence may be used as relevant evidence in court.

Section 2(8) of BNS[9], defines "document" to specifically include digital and electronic records. this provision brings in the digital evidences in operation and makes them admissible as evidence

Moreover, section 241[10] of BNS makes it punishable in causing destruction or hinderance in production of digital or electronic records. this punishment extends to 3 years or imprisonment with fine or both.

Section 151[11] of the act, defines the act that harms the honour and sovereignty and integrity of the India, whether knowingly or purposefully either through words, written or by signals, or by electronic communication, excites or attempts to excite separatist activity will be punishable. Therefore, this provision state that any act or omission that give rise to enmity between people or group of people, through electronic records or communication shall be liable. The Bhartiya Nyaya Sanhita, also includes provision for extortion and forgery which if done through sending mails, or messages or through false records shall be punishable.

BHARTIYA NAGARIK SURAKSHA SANHITA

The Bhartiya Nagarik Suraksha have modernized the Indian criminal procedure by inculcating the electronic and digital evidence. key changes include police to record examination parade

[8] Id, at section 147.
[9] Bhartiya Nyaya Sanhita, section 2(8), act 45, Act of parliament,2023, IND.
[10] Id at section 241.
[11] Id at section 151.

through audio video devices, recording the whole investigation, inquiry, examination of witnesses which gives transparency and accountability of the evidences specially in case of digital and electronic records

Further Bhartiya Nyaya Sanhita, also give significance to various forensic samples like voice notes, biometrics, digital fingerprints, electronic signature etc.

The reliability and admissibility of the evidence in India is largely affected by how much the digital evidence is authentic. Bhartiya sakshya adhiniyam 2023, state the process to proof such evidences.

BHARTIYA SAKSHYA ADHINIYAM

Section 63[12] sub section 4 of BSA, state the provision for the certification of the electronic records. this section includes how electronic evidence is made, the identification of the devices and declaration by the person making it.

In the seminal case of NCT of Delhi vs Navjot Sandhu[13] 2005 the supreme court held that the reliability and admissibility of electronic records, ruling can be accepted without the certification under provision. Later the supreme court reversed its ruling in the case of Anwar P.V. vs P.K. basher[14] 2004 and highlighted the need for certification under section 65b of Indian evidence act.

In a subsequent landmark case of K.L. Nagadev v State of Karnataka, the Karnataka high court revisited the earlier judgments and set aside and dealt with the important aspect of the admissibility of the electronic judgement. The court stated how digital evidence is collected and handled by investigators, when procedure where not strictly followed under code of criminal procedure and section 79 of information technology act 2000

The section 79[15] of information technology act provides the need for the governmental recognised digital experts to test the electronic evidences. These provisions aim to reduce the risk associated with improper seizure, handling or presentation of digital material in court.

the act plays a crucial role in widening the scope of the internet related crimes such as cyber threats, online frauds, counterfeit activities, identity theft, cyber harassment, cyber stalking etc.

[12] Bhartiya sakshya adhiniyam, section 63, act 47, act of parliament,2023, IND
[13] NCT Delhi vs Navjot Sandhu (2005) 11 SCC 600.
[14] Anvar P.V. vs P.K. Basheer and Ors (2014) 10 SCC 473.
[15] Information Technology act 2000, section 79, act 21, act of parliament, 2000, IND.

NEW AMENDMENTS IN FRAMEWORK AND ADMISSIBILITY OF EVIDENCE

The increasing social media platform and specially WhatsApp has totally changed the communication style in the recent years. With the rising cybercrimes this platform becomes an integral part of criminal proceeding as well. WhatsApp end to end encryption has made it easier for the people to share sensitive information. The admissibility of WhatsApp chats in Indian courts, is governed by Bhartiya sakshya adhiniyam 2023. Though these evidence raises legal and ethical issues regarding the credibility of the evidence. the supreme court in the case of K.S. Puttuswamy vs Union of India (2017)[16], recognised the right to privacy as a fundamental right. This landmark judgment highlights the tension between using private communication as evidence and protecting individual from unwarranted intrusion into their personal lives, including the right against self-incrimination.

Section 65B of the evidence act makes it necessary to provide a certificate confirming the authenticity of electronic records since digital data can be easily manipulated. However, Indian courts not always followed a uniform approach. In state vs Navjot Sandhu[17] (2005) electronic evidence was accepted even without strict adherence to certificate requirements. This position was later reversed in Anvar P.V. vs P.K. Basheer (2014) [18]where the supreme court clarified that compliance with section 65B is compulsory.

The legal position shifted once more in Shafi Mohammad vs state of Himachal Pradesh (2018)[19] where the supreme court observed that a section 65B certificate is not always compulsory. It pointed out that such a requirement maybe unnecessary in certain cases. First when a party does not have the possession or control of the device from which the electronic record is obtained, it cannot reasonably be expected to produce a certificate. Secondly since

[16] K.S. Puttaswamy vs Union of India (2017) 10 SCC 1.
[17] Supra note 13.
[18] Supra note 14.
[19] Shafi Mohammad vs State of Himachal Pradesh (2018) 2 SCC 801.

authentication is a procedure requirement courts have the discretion to relax it when the interest of justice demand.

To remove the uncertainty caused by these conflicting views the supreme court later constituted a larger bench in Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal (2020)[20]. In this ruling the court clarified that the section 65 B certificate is generally a mandatory condition for admitting electronic evidence. it also distinguished between original electronic records (primary evidence) and computer-generated copies (secondary evidence). the court states that the certificate may not be enquired if the original devices where it is necessary. It is further emphasized that secondary electronic evidence is admissible only when it complies strictly with section 65B.

In another case of Ambala Sarabhai Enterprise ltd vs KS Infraspace LLP Limited (2020)[21] the court dealt with the evidentiary value of the virtual communication. The supreme court held that WhatsApp messages are a form of virtual verbal communication and stated that if WhatsApp chats may be admissible (if authenticated and meet the requirements of section 65b) it does not mean it is something that can be automatically relied upon as substantial evidence. the veracity will be depended upon the devices and the ease with which chats can be manipulated or altered.

In several cases high court have also examine d the evidentiary value of WhatsApp chats. For example, in Rakesh Kumar Singla Vs Union of India (2021)[22] he Punjab and Haryana high court relied on WhatsApp chats while granting bail but clarified that without a proper certificate they cannot be treated as valid evidence. likewise in C.D. Sulekha vs State of Gujarat[23], high court referred to WhatsApp chats while deciding a bail application.

These contrasting decision highlights the difficulty of maintaining a balance between the reliability of evidence and fairness in legal procedure. At the same time courts have begun to recognize the growing role of digital communication with WhatsApp chats being used in situation, like legal notice and bail proceeding.

[20] Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal, AIR 2020 SC 641.
[21] Ambala Sarabhai Enterprise LTD vs K.S. Infraspace LLP LTD, (2020) 15 SCC 585.
[22] Rakesh Kumar Singla vs Union of India (2020), CRM 23220 of 2020 (O&M)
[23] C.D. Sulekha vs state of Gujarat, 18834 of 2020.

CHALLENGES

1. Technical Challenges: A major challenge in digital investigation is handling the enormous amount off data involved. Investigators, prosecutors and police officers are often required to go through vast and complex dataset, which can be overwhelming without the support of advanced tools like artificial intelligence. These tools help in decoding information, identifying patterns and even retrieving encrypted data that could otherwise be difficult to access.
2. Investigation challenge: Another layer of difficulty comes from the fat that digital evidence is not stored in a single location. It is scattered across both physical as well as online environment. Useful information can be found on hard drives, CDs, DVD, USB, memory card, computer system, cloud storage, internet storage, and various social media platform. Popular platforms such as Instagram, twitter, Facebook, OneDrive and Microsoft services often contain crucial evidence in the form of chats, photos, video, and documents. Because this data is widely distributed collecting and analysing it becomes very tough, time consuming, and technical. It requires proper tools, skilled professionals, and wide range of resources. As a result, digital investigation teams frequently collaborate with the technical experts who specialize in recovering and examine the data from different devices and system to ensure nothing crucial is missed.
3. Jurisdictional hinderance: Every country has their own law that governs their cyber security and data privacy. By the rise in technologies, cross border crimes have seemingly increased. Thus, it gets difficult for the investigator and experts to fetch those data and evidences, since it requires special permission from authorities of other state, which creates delay in investigation.
4. Lack of Infrastructure: the lack of facilities and experts' personnel and limited access is a sever challenge for the digital forensic. Digital evidence and their procedure require high tech tools and software to decode and get access to such information.
5. Deep fakes effects digital forensic: deep fake is a new concept that recently surfaced. It's an advance artificial technique through which people create highly realistic content by the use of image, audio and videos. that looks like real people. Though it has been widely used for entertainment purposes, the misuse of the same technology can cause

immense amount of misinformation, commit cybercrime, frauds and manipulate people. It makes it challenging for the investigator to separate the real content from these fakes one.

6. Privacy challenge: At the same time, protecting individual privacy remains a critical concern in digital investigations. These investigations must be carried out in a way that respects legal, constitutional, and ethical standards. Since investigators often deal with large volumes of personal and sensitive information, there is always a risk of invading someone's privacy if proper safeguards are not followed. In comparison to traditional investigations, digital methods involve deeper access to a person's private life, making it more challenging to strike a balance between collecting evidence and respecting personal rights. To address this issue, investigators must ensure that every step they take is legally justified and ethically sound. For example, they should avoid searching or seizing electronic devices without obtaining proper legal authorization, such as a warrant. They should also be careful to collect only relevant and necessary data instead of gathering excessive or unrelated information. Furthermore, strong data protection measures, including encryption, secure storage, and password protection, should be used to prevent unauthorized access and misuse. By following these practices, investigators can maintain both the integrity of the investigation and the trust of the public.

AI IN REFORMING DIGITAL FORENSIC

Artificial intelligence is a transformative force that have recently emerged and have revolutionized how the digital evidences are tested and analysed. AI provides many enhanced and advance technologies, and methodologies each contributing to more effective, accurate and an insightful forensic investigation. AI can help digital forensic in the following ways

- Al can enhance the data analysis by the help of machine learning and deep learning algorithm to interpret large volume of data. Traditional forensic approach finds this difficult to analyse and keep up with the modern digital world where data is scattered and enormous. Therefore, AI powered data can analyse such data at a faster pace and better accuracy helping to spot patterns and uncover important details that might otherwise go unnoticed
- Ai ability to recognise pattern can be a crucial role in digital forensic. Ai tools recognise malware and code structure and other attributes. It can analyse user activity logs and

network to determine malicious and unauthorised actions. This capacity is particularly valuable in detecting insider threats or sophisticated cyberattacks that may not trigger traditional security alerts[24]

- AI powered anomaly detention system can monitor network traffic in real time to spot irregularities, such as unexpected data transfer or unusual access pattern. This detention can be used for investigation helping forensic expert to uncover potential security breach and fraudulent activities.
- Ai also helps a lot in automatically finding and recovering digital evidence. in many cases investigators have to deal with data stored in damaged, corrupted or encrypted devices which can be difficult to access. Traditional method takes a lot of time and does not always recover complete data. However, ai based tools can help in this task quickly and efficiently increasing the chance of successfully recovering useful evidences.

Ai with the help of tools like machine learning (ML), deep learning, natural language processing (NLP) and block chain technology can help digital forensic in getting administrating cyber crime more effectively. For law enforcement agencies, using ai helps clear pending cases faster and speeds investigation which ultimately leads to quicker justice and safer society. In the corporate world ai make it easier to detect and respond to cyber incident in less time reducing losses and protecting a company reputation from the damage caused by the system failure or data breaches.

Although ai can save time and money it also has some drawbacks that's needs attention. One major issue is bias, as AI system learns from human made data that may already contains error and unfair patterns, which might result into error. Secondly privacy is also an important factor when talking about AI. As investigation involves use of sensitive data, any misuse can create more complications for the investigator and the victims. Moreover, heavily relying on ai for investigation can to hamper the procedure. so, to avoid risk and any misinformation investigator should themselves do a proof reading. Overall, al can be an extremely crucial technology for investigator is used in a caution way and with full transparency.

Conclusion

[24] Rohot Tahsildar Yadav, AI – driven digital forensic, Vol 10 Issue 4, International Journal of scientific research and engineering trends (IJSRET), 1673, 1676, (2024).

Digital forensics has strong potential to improve criminal investigation in India. With a proper legal procedural framework, it might make investigation more reliable, authentic, and efficient. A structure forensic process also helps ensure that the electronic evidence is collected in a way that is acceptable in Indian courts. For digital evidence to be valid it must be accurate, verified, and legally admissible. This study also discussed various forensic tools used to detect cyber frauds and security breaches usually by analysing data from digital devices. These tool not only helps in collecting and identifying data but also assist investigation in uncovering important to solve complex cases.