ARTIFICIAL INTELLIGENCE IN INDIAN CYBER FORENSICS

Cruz Joshna I[1] & Layasri B[2]

ABSTRACT

Artificial Intelligence (AI) is rapidly evolving in many sectors including the judiciary and law enforcement in India. AI is now a powerful tool in crime investigation helping the police and forensic experts solve digital crimes faster and more accurately. Methods like machine learning, deep learning, and natural language processing allow investigators to process huge amounts of data quickly, which was nearly impossible using traditional manual techniques. The paper highlights successful AI applications in India's law enforcement, such as facial recognition for identifying suspects and AI tools that speed up analyzing crime data. It compares India's situation with the European Union AI Act, a law that classifies AI by risk levels and sets out duties for AI providers to ensure liability and accountability. However, India's current legal framework, primarily governed by the Information Technology Act, 2000, lacks explicit provisions for AI's legal status, liability, and ethical deployment. This legal gap raises concerns about misuse, liability and accountability. To fix this, the paper recommends India adopts a risk-based, transparent regulatory framework, inspired by global standards like the EU AI Act. Such a framework should clearly define who is responsible for harm, require human oversight, and protect people's rights. This will help India benefit from AI innovation in cyber forensics while ensuring safety, justice, and trust for all citizens. The paper concludes that developing a robust legal framework for AI is necessary to ensure ethical deployment, liability, accountability and advancing India's leadership in AI governance globally.

Keywords: Artificial Intelligence, Cyber Forensics, Jurisdiction, Recognition, European Union.

[1] Cruz Joshna I, 5th year BBA LLB.,(Hons.), SASTRA University
[2] Layasri B, 5th year BBA LLB.,(Hons.), SASTRA University.

INTRODUCTION:

This paper explores the transformative impact arising from the use of Artificial Intelligence (AI) in Indian cyber forensics, presenting a comparative analysis with the European Union AI Act. AI technologies, including machine learning, deep learning, and natural language processing are increasingly utilized by Indian law enforcement and the judiciary to automate evidence collection, enhance pattern recognition, and speed up forensic investigations. The integration of AI promises greater efficiency and accuracy in tackling complex digital crimes, such as facial recognition and advanced data analytics in recent Indian investigations. However, India's current legal framework, mainly governed by the Information Technology Act, 2000 lacks explicit provisions defining AI's legal status, fixing accountability, and ensuring ethical deployment, leaving significant liability and governance gaps. The paper examines the legal gaps through a doctrinal research methodology, referencing global best practices and the EU AI Act's risk-based regulatory model. The Act classifies AI systems based on risk, mandates human oversight, and imposes robust obligations for data governance, transparency, and accountability serving as an inspiration for Indian reforms. While AI has the potential to revolutionize India's investigative and forensic processes, its unregulated deployment poses significant risks. To ensure legal certainty, ethical compliance, India must amend its foundational cyber laws particularly the IT Act, 2000 and to expressly recognize AI systems, define their operational boundaries, and establish accountability mechanisms grounded in human oversight.

LITERATURE REVIEW:

Rohit Tahsildar Yadav,AI - Driven Digital Forensics,Volume 10, Issue 4, July-Aug-2024, International Journal of Scientific Research and Engineering Trends- highlights that the integration of AI into cyber forensics has emerged as a transformative development, addressing the escalating complexity of cyber threats and the exponential growth of digital data. It highlights the pivotal role of AI technologies- such as machine learning , deep learning, and natural language processing in enhancing the efficiency, accuracy and scalability of forensic investigations. It also emphasizes the growing adoption of AI in automating routine forensic tasks, improving threat detection and supporting real – time monitoring.

Hareesh Kumar C, Trisha B, Cyber Forensic Analytics with AI, Volume 6, Issue 6, November-December 2024,International Journal for Multidisciplinary Research

(IJFMR)- this paper explains the role of AI in cyber forensics, highlighting its transformative impact on investigating and analyzing cybercrimes. The paper identifies future directions including the enhancement of AI capabilities through advanced algorithms and quantum computing, the importance of interdisciplinary collaboration between AI experts, and forensic investigations. AI is recognized as a pivotal force in evolving cyber forensics analytics to respond effectively to increasingly sophisticated cyber threats while calling for cautious ethical integration to maintain justice and reliability.

Gauhar Suhail Jilani Advancing Cyber Forensics with AI: Revolutionizing Digital Investigations and Threat Mitigation,2024, International Journal of Science and Research (IJSR)- it highlights the AI's developing role in cyber forensics. It explains how AI tools such as machine learning, deep learning, and natural language processing are automating threat detection and complex data analysis, thereby modernising forensic procedures. In order for forensic practitioners to stay up to date with increasingly complex cyberattacks, the review emphasises the necessity of ongoing innovation and AI literacy.

Janani J, Ensuring AI Accountability: The Need for Expedited Oversight

Frameworks Based On EU,Vol 01 Issue 02; Apr-2024, Journal of Law and Legal Research Development, - this paper captures the current state of AI in cyber forensics, highlighting its technological potential, regulatory challenges, and emerging governance frameworks for responsible use. While India is advancing AI policy development through initiatives like the National Artificial Intelligence Mission and collaborations with industry, its current legislative environment is fragmented and lacks comprehensive AI-specific laws.

Bandr Fakiha,Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification,Vol. 13, No. 4, August, 2023,International Journal of Safety and Security Engineering- it explains the increasing challenges posed by the rising frequency of cyberattacks, which necessitates effective cyber forensic investigation techniques. It identifies the gap between the recognised potential benefits of AI and Machine Learning and their adoption in cyber forensics.

STATEMENT OF THE PROBLEM:

The attribution of liability and accountability for harms arising from the integration of Artificial

Intelligence (AI) within cyber forensic investigations is ambiguous in India. The current statutory framework, including the Information Technology Act, 2000 does not address responsibility when AI systems operate independently. This study addresses the need to establish a standard legal framework to govern AI use in cyber forensics, balancing technological innovation with legal responsibility.

RESEARCH OBJECTIVES:

1. To analyse the existing International and Indian legal framework governing AI and identify gaps concerning liability and accountability.

2. To assess the contribution of AI in cyber forensics and judicial procedures.

3. To suggest a comprehensive risk- based regulatory framework for AI in India, drawing lessons from international models like the EU AI Act.

RESEARCH QUESTIONS:

1. Whether the developers, users, owners or the AI system itself can be held responsible for the harm caused by the AI system?

2. How can India use ideas from International AI laws like the EU AI Act, but change them so they fit India's own laws and technology needs?

SCOPE AND LIMITATIONS OF THE STUDY:

1. Focuses on AI's role in cyber forensics and judicial processes.

2. Comparative insights are drawn from EU AI act.

3. AI regulation is still developing globally and in India, many laws and policies discussed may change rapidly. Therefore, the findings are based on the current legal scenario, which could soon become outdated as new laws emerge.

RESEARCH METHODOLOGY:

This study employs a doctrinal research methodology, relying on an extensive review of

existing literature. A systematic and comprehensive analysis of academic journals, policy documents, case studies and reputable online sources will be conducted to gather data. It also includes comparative methods to examine global frameworks such as the EU AI Act.

AI JURISPRUDENCE:

There is no universally accepted or standardized definition of AI. The Oxford English Dictionary defines Artificial Intelligence to mean "the capacity of computers or other machines to exhibit or simulate intelligent behaviour." Indian law has yet to evolve regarding the legal implications of self-governing AI systems. No decision has been recorded that responds directly to one of the questions of whether AI can be held liable or whether the harm caused by AI would call for tort or criminal law principles to be revisited. AI behaviour becomes more increasingly common in various areas of the Indian economy, the law treats AI as an object. Indian legislation, norms are all anthropocentric, which deal with only human actors or statutorily recognised legal entities such as businesses or corporations.

Under Tort law, if an AI system causes harm, civil courts will assess liability based on negligence, product liability or failure to exercise reasonable care determining who owns, builds, manages or deploys the AI. Where foreseeability and causation can be reasonably established, human and corporate entities involved in training data and deployment plans may be held liable under the doctrine of vicarious liability of developers and employers.When discussing the responsibility in Artificial Intelligence, especially Machine Learning algorithms, responsibility is the role of an individual in response to AI systems. It does not pertain to the fact that computer software of any kind should be made responsible. Rather the organisation and the employee within the organisation should be made accountable. With respect to the Indian policy landscape, NITI Aayog's National Strategy on Artificial Intelligence (NSAI) recognizes the Principle of Accountability and Responsibility in AI decision-making systems. The national policy for Ethical AI, as promoted by NITI Aayog's NSAI uses proportionate liability to guarantee accountability and responsibility. Second, when making high-risk decisions. Human conformation should be sought before any action is taken. This is known as the "human is the loop" and it is already being used in a number of Indian Industry sectors that use automated AI.[3]

[3] Kushagra Vats, *Beyond Human Hands – "Rethinking Legal Status and Responsibility for AI in India,"* Int'l J. Legal Stud. & Soc. Sci. 3 no. 4, at 115 (July 17, 2025).

INFORMATION TECHNOLOGY ACT, 2000:

Under Sec 2(1)(k) of the IT Act, 2000 "computer resource" means computer, computer system, computer network, data,computer data base or software;[4]

As per Cambridge Dictionary, Software is defined as, *"the instructions that control what a computer does;"*

Words are given their ordinary meaning if they are clear and unambiguous. Since "computer resource" includes software and databases, and AI operates as software or algorithms running on a computer system, it arguably falls within the plain meaning by way of Ejusdem generis(general words follow specific ones in a statutes, the general words should be confined to the same kind and nature as the specific ones) and liberal interpretation.

Therefore, an amendment to the IT Act, 2000 is necessary to expressly include Artificial Intelligence and algorithmic decision-making systems within its definitional and regulatory scope. Such clarification would ensure that the law does not hinder the legitimate use of AI in cyber forensics, while simultaneously providing a legal basis for oversight, data governance, and accountability in AI-assisted investigations.

AI IN CYBER FORENSICS:

Cyber-forensics, is defined as the acquisition, preservation, and analysis of electronically stored information in such a way that ensures its admissibility for use as evidence, exhibits, or demonstratives in a court of law. It is the science of collecting, analysing, and reporting evidence from data found on electronic media, combining computer science and investigative procedures to investigate criminal activity involving electronic devices or malicious activity targeting computer systems and networks. The process involves several key stages: identification of relevant media or data, preservation of integrity, technical examination and extraction of information, logical correlation of findings, and comprehensive reporting. These procedures are essential for incident response, enabling investigators to identify, preserve, recover, analyze, and present facts and opinions regarding evidence stored on or transferred between digital devices. The gathering, examination, and preservation of electronic evidence for use in criminal investigations, cybersecurity incidents and court proceedings is known as

[4] Information Technology Act, 2000, sec 2(1)(k).

Cyber Forensics. By automating data processing, improving pattern recognition, and identifying hidden threats that human investigators might overlook. AI powered forensic tools use machine learning, deep learning, natural language processing and predictive analytics to analyse vast amounts of digital evidence, including emails, logs, metadata, network traffic and multimedia files. Manual data analysis is necessary for traditional forensic investigations, and it can be time consuming and prone to mistakes. AI expedites the process by automating the collection, classification and analysis of data from a variety of sources, including mobile devices, cloud storage, and hard drivers. Biometric analysis and facial recognition are helpful for tracking criminal behaviour, identifying suspects and verifying the legitimacy of evidence. AI is faster than human professionals in processing large amounts of surveillance footage.

IT Act, 2000:

The Information Technology Act, 2000 (IT Act) in India contains several provisions relevant to cyber forensics, primarily in the context of legal recognition, evidence handling, and offences related to cybercrime. All these provisions can be amended to include the aspect of AI.

1. Section 43 provides penalty and compensation for damage to computer, computer system, etc. It relates to cyber forensics as investigations often begin with detecting and proving unauthorized system access or data breaches. It can be extended to the AI driven forensic tools used to detect unauthorised damage or data damage.

2. Section 65 deals with tampering computer source documents. AI tools could be deployed in software to check the integrity and detect tampering.

3. Section 66 to 67B deals with cyber offences. AI forensics tools enhance detection and analyzing suspicious activities. The AI tools are used in tracing and blocking unlawful transmission.

4. Section 69 to 69B deals with government powers for interception, monitor, decrypt or block data for security reasons. AI tools support automated monitoring and data analysis while preventing misuse. AI decisions on blocking or interception must be transparent and legally accountable.

TRADITIONAL CYBER FORENSICS AND AI- INTEGRATED CYBER FORENSICS:

Conventional forensics depends on human specialists to thoroughly inspect evidence, such as fingerprints, DNA, crime scenes, or digital logs, often adhering to rule- based or sequential procedures. Whereas, AI integrated Cyber Forensics leverages automated evidence review, machine learning, NLP, and pattern recognition to investigate data from numerous sources simultaneously. Traditional methods are typically slower and may be limited in scope due to data volume constraints, while AI tools process information much faster and scale efficiently with big data. Human analysis in traditional forensics often increases risk of error, whereas AI methods can improve accuracy by detecting hidden patterns, reducing both false positives and negatives. While both traditional and AI- based cyber forensics require meticulous chain of custody and documentation to ensure evidence integrity, AI approaches often extend this rigor to recording digital system logs, model parameters, and processing steps, enabling audibility and explainability. In traditional forensics the chain of custody is well- understood and practiced. Whereas in AI, it requires enhanced tracking for automated data handling to maintain evidentiary integrity. In traditional forensics, the human role is central and experts lead analysis and interpretation. In AI it is shifted towards supervision, validation, and complex decision-making with AI supporting. The traditional forensic techniques remain fundamental physical evidence and have established legal acceptance. AI forensic techniques revolutionize speed and data complexity handling in modern investigations. However, AI introduces challenges around data integrity bias and legal admissibility that must be carefully managed.

AI TECHNIQUES:

Artificial Intelligence (AI) techniques have revolutionized digital forensics by introducing sophisticated methods for analyzing complex datasets, detecting anomalies, and automating routine tasks. The application of AI in digital forensics encompasses a range of techniques, including machine learning (ML), deep learning, natural language processing (NLP), and blockchain integration.

1. Machine Learning (ML:) Machine Learning (ML) is a subset of AI that focuses on developing algorithms that can learn from and make predictions based on data. In digital forensics, ML techniques are employed to identify patterns and anomalies in large datasets, which can be crucial for detecting fraudulent activities or identifying malicious behavior.

2. Unsupervised Learning: Unlike supervised learning, unsupervised learning algorithms work with unlabeled data and aim to identify hidden patterns or groupings. Clustering algorithms such as K-means or hierarchical clustering can be used to group similar forensic artifacts or network traffic patterns, which helps in identifying abnormal behavior or unknown threats.

3. Anomaly Detection: Anomaly detection techniques, such as Isolation Forests or Autoencoders, are employed to identify deviations from normal behavior. In digital forensics, these methods can be used to detect unusual activities in network traffic or system logs that may indicate a security breach or a cyberattack.

4. Deep Learning: Deep Learning, a specialized subset of machine learning, uses neural networks with multiple layers to analyze complex data representations. Deep learning techniques have shown remarkable success in digital forensics due to their ability to handle large volumes of unstructured data, such as images, videos, and text.

5. Natural Language Processing (NLP) Natural Language Processing (NLP) involves the interaction between computers and human language. NLP techniques are employed in digital forensics to analyze textual data from various sources, such as emails, social media posts, and chat logs. [5]

AI IN INDIAN INVESTIGATIONS:

NAGPUR: The Nagpur Police have launched an AI-powered technology, SIMBA (System Integrated for Monitoring and Big-data Analysis), to enhance the city's law enforcement capabilities. The tool was developed by Staqu Technologies, India's premier artificial intelligence (AI) implementation enabler, in collaboration with the Nagpur police department. SIMBA is an advanced generative AI tool that delivers swift information from various data sources, such as CCTV feeds, images, and audio related to crime and criminals. Integrated into a digitized database of 1,50,000 criminals, it offers customized information based on specific prompts and features such as facial recognition and speaker identification. Crime GPT, a key feature of SIMBA, utilizes an extensive criminal database to provide results from video, document and audio data. Criminal information can be searched using Facial recognition, audio

[5] Rohit Tahsildar Yadav, *AI-Driven Digital Forensics*, 10 Int'l J. Scientific Res. & Eng'g Trends 4 (July-Aug. 2024), https://ijsret.com/wp-content/uploads/2024/07/IJSRET_V10_issue4_353.pdf.

input or natural language query in written form. The tool promptly accesses the database and delivers the required information.[6]

DELHI: In Jan 2024 Delhi Police used artificial intelligence (AI) to reconstruct the face of an unidentified murder victim. The incident unfolded when the body was discovered near the Geeta Colony flyover on January 10. The victim's lack of identification documents posed a significant challenge for investigators. Following the autopsy, which revealed the cause of death as strangulation, Delhi Police initiated a 72-hour AI-driven facial reconstruction process to establish the victim's identity. They employed the image on posters to seek information about his identity. The novel approach not only led to the victim's identification but also played a crucial role in apprehending the perpetrators, according to police sources. The integration of AI in criminal investigations marks a significant advancement in law enforcement techniques, showcasing the adaptability of technology in solving complex cases.[7]

KERALA: Kerala police solved a 19-year-old murder case involving a mother and her twins, using AI technology. In 2023, the Technical Intelligence Wing of the Kerala Police began using artificial intelligence to re-examine cold cases. Trying to locate Ranjini's killers, they enhanced old photographs of the two accused to generate an estimation of how they might look after 19 years. These images were then compared against photographs on social media. After sifting through social media, a wedding photo provided a breakthrough. The photo bore a 90% similarity to the suspect Rajesh who was located in Puducherry. With his help, police traced the other suspect, Divil. The two men were arrested by the CBI in Puducherry on January 4, almost 20 years after the crime.[8]

ACCOUNTABILITY AND AI:

The accountability debate on AI, which in most cases today is aimed at ascertaining the liability, needs to be shifted to objectively identifying the component that failed and how to prevent that in the future.

[6] "AI-Powered 'SIMBA' to Aid Nagpur Police in Fighting Crime," INDIA ai (July 24, 2024), https://indiaai.gov.in/article/ai-powered-simba-to-aid-nagpur-police-in-fighting-crime.
[7] How AI Helped Delhi Police to Solve a Blind Murder Case, ECON. TIMES (Jan. 24, 2024), https://economictimes.indiatimes.com/news/new-updates/how-ai-helped-delhi-police-to-solve-a-blind-murder-case/a rticleshow/107122601.cms?from=mdr.
[8] 19 Years, 1 Wedding Photo, and AI: Kerala's Chilling Triple Murder Mystery Solved, Hindustan Times (Jan. 5, 2025), https://www.hindustantimes.com/trending/19-years-1-wedding-photo-and-ai-kerala-s-chilling-triple-murder-mystery -solved-101736408070616.html.

One possible framework that can be mooted involves the following components:

a) Negligence test for damages caused by AI software, as opposed to strict liability. This involves self-regulation by the stakeholders by conducting damage impact assessment at every stage of development of an AI model.

b) As an extension of the negligence test, safe harbours need to be formulated to insulate or limit liability so long as appropriate steps to design, test, monitor, and improve the AI product have been taken.

c) Framework for apportionment of damages needs to be developed so that the involved parties bear proportionate liability, rather than joint and several liability, for harm caused by products in which the AI is embedded, especially where the use of AI was unexpected, prohibited, or inconsistent with permitted use cases.

d) Actual harm requirements policy may be followed, so that a lawsuit cannot proceed based only on speculative damage or a fear of future damages.[9]

The DPDP Act introduces obligations of consent, purpose limitation, and data minimisation that have direct bearing on AI model training and deployment. It prohibits processing of personal data without consent, requires safeguards against misuse of sensitive data, and empowers the Data Protection Board to investigate harms caused by misuse of AI-driven profiling. These provisions create accountability pathways for AI developers and deployers handling personal data at scale.[10]

Forensic AI systems must deliver Explainable AI human readable, transparent explanations for their output. A shared liability framework where accountability is allocated proportionally that distributes responsibility across developers, deployers and data providers for ensuring that AI systems are designed with transparency and ethical safeguards. Entities and individuals who deploy the AI systems for decision making must be held accountable when they use AI in a way that facilitates fraudulent acts or fails to monitor and control.

[9] NITI Aayog, National Strategy for Artificial Intelligence (2023), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.
[10] "India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation," Government of India (Nov. 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.

LIABILITY AND AI:

Under the India AI Governance Guidelines, the graded liability system proposed is a risk- and function-based framework that assigns responsibility proportional to the function performed, the level of risk anticipated and the degree to which due diligence is undertaken. The committee recommends the following approach:

a) Clarify how different entities in the AI value chain (e.g. developers, deployers, end-users) are governed under the existing regulations.

b) Recommend principles for attributing liability and responsibility for the concerned entities that is proportionate to their function and the risk of harm (e.g. transparency reporting, audits, grievance redressal)

c) Developing suitable accountability frameworks to mitigate harm.[11]

Under the eyes of law, AI is not considered a legal person. Hence liability should be fixed on developers, users, owners for the harm caused by the AI system.

EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT:

This act came into force in the EU from 1st August 2024. Though it has not been fully enforced, it has an impact on organisations that develop, use, distribute or import AI systems in the EU. This act governs the development, deployment and use of AI in the EU. It has risk based obligations and clear guidelines for different types of AI. The Act assigns applications of AI to three risk categories. First, applications and systems that create an unacceptable risk, such as government-run social scoring of the type used in China, are banned. Second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements. Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.[12]

1. Art 5 of EU AI act includes prohibited AI systems:

a) deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair

[11] Supra 6.
[12] EU Artificial Intelligence Act, 2024, https://artificialintelligenceact.eu/.

informed decision-making, causing significant harm

b) biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.

c) assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.

d) compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.

e) 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when:

- a) searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited;
- b) preventing substantial and imminent threat to life, or foreseeable terrorist attack; or
- c) identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).

2. **Art 6** includes classification of high risk AI systems. High risk AI systems are those:

a)used as a safety component or a product covered by EU laws in Annex I AND required to undergo a third-party conformity assessment under those Annex I laws; or

b)listed under Annex III use cases (below), except if:

- the AI system performs a narrow procedural task;

- improves the result of a previously completed human activity;
- detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; or
- performs a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

c)AI systems listed under Annex III are always considered high-risk if it profiles individuals, i.e. automated processing of personal data to assess various aspects of a person's life, such as work performance, economic situation, health, preferences, interests, reliability, behaviour, location or movement.

d) Providers whose AI system falls under the use cases in Annex III but believes it is not high-risk must document such an assessment before placing it on the market or putting it into service.

3. **Art 8 - 17** provides requirements for providers of high-risk AI systems. High risk AI providers must:

a) Establish a risk management system throughout the high risk AI system's lifecycle;

b) Conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose.

c) Draw up technical documentation to demonstrate compliance and provide authorities with the information to assess that compliance.

d) Design their high risk AI system for record-keeping to enable it to automatically record events relevant for identifying national level risks and substantial modifications throughout the system's lifecycle.

e) Provide instructions for use to downstream deployers to enable the latter's compliance.

f)Design their high risk AI system to allow deployers to implement human oversight.

g) Design their high risk AI system to achieve appropriate levels of accuracy, robustness, and cybersecurity.

h)Establish a quality management system to ensure compliance.[13]

India's Takeaway from EU AI Act:

The act classifies application of AI based on the risk factor involved. It imposes stringent rules on those affecting core rights of the people such as biometric identification, evidence automation, etc. India should assess the risk levels of forensic AI tools and frame legislations according to it. It is also required to have strict human supervision, traceability and accountability in the cyber forensics to avoid misuse. Like EU AI act, India also should enforce strong standards for data integrity, privacy and robust data governance in cyber forensics. Post-market monitoring and reporting of failures of AI in cyber forensics. Impose strong penalties for non-compliance.

CHALLENGES OF USING AI TOOLS IN CYBER FORENSICS:

1. Legal and Regulatory gaps: India currently lacks legislation governing use of AI tools in cyber forensics and regulation of automated investigation tools. Amendment should be made to the IT Act, 2000 and add relevant provisions in DPDP Act, 2023 to govern AI deployment in cyber forensics and fitting AI liability and accountability provisions inspired by EU AI Act.

2. Data privacy: a large amount of personal data may be collected and analysed to train and run AI. This affects the Right to privacy of individuals under Art 21 of the Indian Constitution. Also ethical issues arise as people would be unaware that their data is being used in forensic investigation.

3. Admissibility of evidence: Courts would question the accuracy, reliability and transparency of AI driven forensic evidence as in India AI evidences are not recognized.

[13] *High-Level Summary of the AI Act*, EU Artificial Intelligence Act, Feb. 27, 2024, updated May 30, 2024, https://artificialintelligenceact.eu/high-level-summary/.

An amendment has to be made in BSA to include the AI evidence and provide required guidelines for them to be accepted by the court.

4. Transparency: Use of AI tools in cyber forensics leads to difficulty in understanding, explaining and verifying the decision making processes. Many AI algorithms operate as a 'black box' which refers to the invisibility of their internal workings and how conclusions are arrived at. Explainable AI initiatives should be introduced and establish accountability measures to make it reliable.

5. Algorithm bias: AI tools might perpetuate existing biases if they are trained on prejudiced data. It results in unfair targeting and raises ethical questions like discrimination and equity in cyber forensics investigations. To remove this challenge algorithm auditing standards can be set for AI tools which includes bias testing, impact assessments and human monitoring.

SUGGESTIONS:

India should enact a specific AI law that explicitly defines AI's legal status, liability and set ethical standards for AI design and deployment drawing inspiration from EU AI act and other international norms. It should have regulatory authority to monitor AI compliance, enforce transparency and oversee the AI mechanisms in judiciary and cyber forensics. Vicarious liability should be given to developers, deployers or owners to ensure victims receive redress. A graded liability framework should be adopted, assigning responsibility based on the level of control and risk involved. To ensure fairness and transparency, all high-risk AI systems used in cyber forensics must operate under human supervision. To protect data privacy, ensure data quality and prevent bias legal policies are required. AI forensic tools must comply with standards for data integrity and undergo post-deployment monitoring to detect failures or misuse. India should foster international cooperation for AI governance and harmonize standards to address cross-border AI challenges.

CONCLUSION:

The integration of Artificial Intelligence (AI) into India's legal and judicial systems, especially in cyber forensics, presents both great opportunities and significant regulatory challenges. While AI tools enhance the speed, accuracy, and effectiveness of cybercrime investigations,

India currently lacks a specific legal framework that clearly recognizes AI's status, liability, and accountability. India has made important policy advances like the National Strategy on AI and the IndiaAI Mission, which emphasize ethical AI and accountability. However, to fully harness AI's potential responsibly, India needs comprehensive legislative reforms. Such reforms would establish clear legal recognition for AI, enforce strong data governance, promote transparency, and fix liability for harms caused by AI systems. This legal framework must balance technological progress with constitutional safeguards, protecting fundamental rights and public trust. Without proper regulation, risks like algorithmic bias, data misuse, privacy breaches, and wrongful outcomes could undermine social values and the fairness of the judicial process. India can learn from the EU AI Act's risk-based regulatory approach, demanding strict controls on high-risk AI and human supervision. Overall, the paper stresses that India must enact AI-specific laws with accountability mechanisms, data integrity standards, and post-deployment monitoring, alongside fostering international cooperation for harmonized AI governance. This will position India as a global leader in ethical and effective AI regulation, benefiting its growing digital and legal ecosystem.

REFERENCE:

1. *The EU AI Act: A Quick Guide*, Simmons & Simmons (July 12, 2024), https://www.simmons-simmons.com/en/publications/clyimpowh000ouxgkw1oidakk/the-eu-ai-act -a-quick-guide.
2. Vaishnavi, *AI in Digital Forensics | A Revolutionary Breakthrough or a Risky Gamble?*, Web Asha Technologies (Feb. 28, 2025), https://www.webasha.com/blog/ai-in-digital-forensics-a-revolutionary-breakthrough-or-a-risky-ga mble.
3. Yuri Gubanov, *Revolutionizing Investigations: The Impact of AI in Digital Forensics*, Cyber Def. Mag., Jan. 26, 2025, https://www.cyberdefensemagazine.com/revolutionizing-investigations-the-impact-of-ai-in-digita l-forensics/.
4. Amiya K. Padhi & Samir K. Shah, *AI-Driven Cyber Forensics: Enhancing Digital & Cyber Investigations*, 12 J. Eng'g & Tech. Innovation Res. (July 2025), https://www.jetir.org/papers/JETIR2507215.pdf.
5. *Implementation Guidelines for eProcurement Roll-out in States as a Mission Mode Project*, National Informatics Centre, July 15, 2011, https://eprocure.gov.in/cppp/sites/default/files/implementation_guidelines_states.pdf
6. Ministry of Electronics & Information Technology (MeitY), *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)* (Aug. 11, 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.
7. *AI and ML in Digital Forensics: The Future of Forensic Investigations*, EC-Council (Feb. 27, 2025), https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/ai-and-ml-in-digital-forensics-thefuture-of-forensic-investigations/.

8. Dipo Dunsin, Mohamed C. Ghanem & Karim Ouazzane, *The Use of Artificial Intelligence in Digital Forensics and Incident Response (DFIR) in a Constrained Environment*, 16 Int'l J. Info. & Commun. Eng'g 280 (2022), https://repository.londonmet.ac.uk/id/eprint/8678.
9. *What Is Artificial Intelligence (AI)?*, Google Cloud, https://cloud.google.com/learn/what-is-artificial-intelligence.
10. *What Is Cyber Forensics? A Beginner's Guide for Cybersecurity Students: Skills, Tools and*

    Career Paths, GISMA (Berlin) (June 3, 2025), https://www.gisma.com/blog/what-is-cyber-forensics-a-beginners-guide-for-cybersecurity-student s-skills-tools-and-career-paths.
11. Accountability By Design: Shared Liability In AI Fraud Under Indian Cyber Law, Virtuosity Legal, https://virtuositylegal.com/accountability-by-design-shared-liability-in-ai-fraud-under-indian-cyb er-law/.
12. Saleem Akhtar, Cyber Forensics in the Age of AI: Investigating Cyber Crimes with Advanced Multi-Factor Authentication and Adaptive Threat Mitigation, available at https://www.researchgate.net/profile/Saleem-Akhtar-14/publication/383498564_Cyber_Forensics_in_the_Age_of_AI_Investigating_Cyber_Crimes_with_Advanced_Multi-Factor_Authentication_and_Adaptive_Threat_Mitigation/links/66d045f2bd201736675d7c14/Cyber-Forensics-in-the-A ge-of-AI-Investigating-Cyber-Crimes-with-Advanced-Multi-Factor-Authentication-and-Adaptive -Threat-Mitigation.p.