VOLUME 5 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

USE OF AI DIGITAL FORENSIC

- Jaspreet Kaur[1] & Dr. Gargi Bhadoria[2]

ABSTRACT:-

The application of Artificial Intelligence (AI) in digital forensics has revolutionized the field of criminal investigation, evidence examination, and computer security. AI boosts forensic capability through machine-based data analysis, pattern identification, and increased precision. Application of AI, nevertheless, relies on legal and ethical factors mainly based on the admissibility of evidence generated by AI and adherence to privacy law. The paper provides a general perspective on the future of AI towards transforming digital forensics, emphasizing the optimistic future directions and the particular issues that have to be ironed out. It offers recommendations on greater utilization of AI, promoting fairness, transparency, and compliance with legal parameters, and anticipating directions of research in the new field.

KEYWORDS:-

Artificial Intelligence (AI), Digital Forensics, Machine Learning (ML), Cybercrime, Data Recovery, Evidence Admissibility, Malware Analysis, Natural Language Processing (NLP), Forensic Investigations, Pattern Recognition, Legal Implications, Data Integrity, AI Algorithms, Ethical Considerations, Anomaly Detection, Digital Evidence, Privacy Concerns, Forensic Tools, Automation in Forensics, Cybersecurity, Legal Frameworks.

INTRODUCTION:-

Digital forensic is the process of identification, preservation, analysis, and presentation of digital evidence. With digital information expanding exponentially, AI-powered solutions are needed to work with and analyse complex forensic evidence in a cost-efficient way. AI assists in image recognition, predictive analytics, and anomaly detection. However, its authenticity and admissibility in the court of law are questionable.

With greater dependence on digital evidence during legal proceedings, law enforcement agencies, business organizations, and cybersecurity professionals are using AI to speed up forensic analysis.

[1] Student at Amity Law School, Noida
[2] Assistant Professor at Amity Law School, Noida

AI-based digital forensic software assists in tracing digital footprints, detecting cybercriminals, and retrieving deleted or encrypted data. However, although AI is followed by tremendous benefits, its use needs to be subjected to strict scrutiny to maintain legality and justice in criminal justice systems.

DIGITAL FORENSIC:-

Digital forensic is a sub discipline of forensic science addressing the identification, collection, analysis, and preservation of digital evidence to be presented during court hearings. It is an important discipline employed to examine cybercrimes, financial scams, intellectual property theft, unauthorised data access, and corporate disputes. It begins with the protection and collection of digital evidence from a variety of sources, such as computers, mobile phones, cloud storage, and network records, and the preservation of the integrity of the data to ensure that it is not altered. Forensic tools and techniques are employed to recover deleted data, examine metadata, decrypt encrypted data, and identify digital footprints left behind by the criminals.

As cybercrime and data breach were in vogue, digital forensics was an important tool employed by law enforcement agencies, cybersecurity firms, and corporate investigators. Digital forensics in India is governed by laws like the Information Technology Act, 2000, which provides a legal framework for investigating cybercrime to ensure digital evidence is collected and presented to judicial standards. As there has been increasing dependence on technology, digital forensics has become an important discipline to establish justice in the digital age.

AI IN TRADITIONAL FORENSIC DISCIPLINES:-

With continuous growth and development in digital forensic science, conventional forensic science has been an integral part of society's functioning for decades. The significant areas of forensic science include DNA analysis, fingerprint analysis, and forensic pathology, and forensic scientists work in numerous diverse environments like criminal justice agencies, medical examiner offices, private industry, and research institutions.

Even in these traditional fields, AI is proving to be a useful partner. AI technology is revolutionising the way evidence is collected and analysed, both giving forensic scientists the time and the ability to better interpret the information that they are dealing with.

DNA ANALYSIS

Forensic DNA analysis has revolutionized the criminal justice field over the last several decades. The ability to collect and analyze DNA evidence has allowed criminal justice professionals and law enforcement officials to improve the results of their investigations, and in some cases, they have been able to reverse wrongful convictions.

The National Institute of Justice explains how AI can dramatically speed up the analysis of DNA because it can automate processes, forecast DNA profiles and aid in complicated kinship analysis. Forensic scientists are discovering a blend of a human investigator and machine learning processes, where human investigators are augmented with machine learning processes, enabling them to enhance the analysis of DNA samples and the outcome of their investigations.

FINGERPRINT ANALYSIS

Fingerprint analysis has also been a long-standing traditional technique in computer forensics, but, like any other traditional technique, human experts were constrained by their own limitations in interpreting and analyzing. In the majority of instances, human fingerprint analysis has produced errors and mistakes that invalidate the integrity of the investigation. It is noteworthy that artificial intelligence technology has the potential to enhance both the precision and efficiency of fingerprint analysis through several mechanisms, including the automation of fingerprint matching, the improvement of latent print quality, and the identification of distinctive characteristics. Furthermore, AI technology can mitigate the likelihood of human error, while concurrently accelerating the investigative process.

Forensic pathology

Forensic pathology is a pathology subfield where examiners target the examination and analysis of unnatural death case medical evidence. Forensic pathologists conduct autopsies in a systematic way to determine the cause and timing of death. The autopsy results can be quickly examined using AI, which finally makes the results more precise and helps in the investigation of the death.

ARTIFICIAL INTELLIGENCE(AI) IN DIGITAL FORENSIC:-

Artificial Intelligence (AI) is now a revolutionary digital forensics force, with new features which bypass the limitations inherent in traditional forensic methods.AI is a wide range of technologies that include Machine learning, deep learning, and natural language processing, which all contribute substantially to improving forensic examinations. For example, machine learning Algorithms possess the capability to independently recognize patterns and abnormalities in large data, and typically discovering subtleties which can escape human observers when inspected manually.

The main driving force behind the use of artificial intelligence in Digital forensics possesses the ability to handle large huge volumes of data. Traditional forensic methods often exhibit laborintensive and time-consuming, particularly when confronted using large datasets or intricate digital environments. AI-powered tools, however, are capable of processing and analyzing data on an enormous scale, granting forensic specialists accelerated and amplified accurate findings. For instance, AI can quickly scan network traffic logs to identify unusual patterns that suggest cyber attacks, or it can search through terabytes of data to identify relevant evidence. This skill is especially vital in advanced persistent inquiries threats (APTs) or sophisticated cybercrimes that result in huge amounts of electronic evidence.

Additionally, artificial intelligence enhances the precision of forensic investigations by reducing human error and enhancing evidence analysis reliability. Computer systems can embrace uniform analytical procedures to all data, thus reduce the possibility of surveillance or personal inclination that would occur in manual analysis. For example, AI-powered tools can use pattern recognition techniques to detect mild symptoms of forgery or manipulation of electronic documents—abnormalities that can escape the attention of human examiners. This in court cases, more specificity is needed, since integrity of evidence can significantly influence the outcomes of investigations and prosecutions.

The Application of Artificial Intelligence in Digital Forensics:-

1) Machine-based Evidence Analysis

- Artificial intelligence algorithms can rapidly analyze big data, sifting out applicable information that would be much more time-consuming for human analysts to consider.
- Natural Language Processing (NLP) programs enable the inspection of emails, chat logs, and other forms of electronic communication to search for possibly suspicious activity.
- Machine learning processes enable the detection of irregularities in financial transactions that may represent fraud.

2) Facial Recognition and Biometrics

- Artificial intelligence technologies enable the detection of suspects by facial recognition and biometrics.
- Automated fingerprint identification, voice pattern matching, and gait recognition strengthen forensic capacity.
- Artificial intelligence forensic facial reconstruction assists in the identification of unknown persons from skeletal remains.

3) Cybersecurity and Threat Detection

- AI boosts forensic capacity in the detection of cyber attacks, malware, and network anomalies.
- Deep learning algorithms have applications in intrusion detection systems (IDS) for the detection of unauthorised access to network infrastructure.
- AI facilitates rapid detection and response to zero-day attacks and advanced cyber-attacks.

4) Predictive Policing and Crime Mapping

- Artificial intelligence aids law enforcement authorities in predicting criminal activity and efficiently allocating resources.
- Analytics predictive models utilize historical crime data to identify areas of risk and potential offenders.
- Artificial intelligence-based surveillance systems employ behavioral analytics to identify suspicious behaviour in real-time.

Benefits of AI in Digital Forensic:-

Artificial Intelligence has numerous benefits if employed in the field of digital forensicswhich greatly improves the effectiveness of inquiryprocess. Computer forensic analysis is currently undergoing achange as a consequence mostly of artificial intelligence-based tools. Algorithms that greatly improve speed and efficiencyas these can take some timeuse of human analysis of big data, AI algorithmsare highly effective in rapidly scanning and filtering information, whichspeeds up initial stages of inquiries. This speeded-upspeed is required because it allows investigators to stay awaketo remain current with the ever-evolving digital evidence environment,especially given how quickly cyber threats are emerging.

AI in digital forensics introduces a huge surge inAnalytical precision and rigor.The capacity of artificial intelligence toidentify minute details results in forensic findings that aremore accurate and more balanced, representing a substantialimprovement of investigation capacity.The vast amount of data that digital researchers. The process it has to go through is one of the toughest.obstacles. AI meets this difficulty by being exceptionallyexperienced in managing and analyzing big data, whichmakes it possible for investigators to quickly sort throughlarge amounts of data. The researchers can focus onkey features of the case, as computer-aided data classification. Classification accelerates the process of recognising relevantevidence. With the exponentialevolution of data creation in the modern digitalecosystem, such competence grows in significance

for efficient information retrieval new technologiesare needed.The subject is experiencing aparadigmchange with the combination of AI with digital forensics,which will increase the overall effectiveness andthe responsiveness of investigative procedures in the ever-evolvingthe changing character of cyber threats.

Laws governing AI in India with respect to digital forensic:-

1) The Information Technology Act,2000

- Governs cybercrime, electronic evidence, and digital transaction.

- Sections 43, 66, 67 and 72 deals with unauthorised access, hacking and data privacy violations.

2) Indian Evidence Act, 1872

- Section 65B deals with the admissibility of electronic evidence. AI- driven forensic tools play a role in ensuring compliance.

3) The Personal Data Protection Bill, 2019

- Aims to regulate data privacy and security, impacting AI-driven forensic investigations.

4) The Criminal Procedure(Identification) Act, 2022

- Allows law enforcemnt agencies to collect and store biometric and digital evidence, including AI-powered facial recognition data.

5) Cybersecurity Guidelines by CERT-In

- The Indian Computer Emergency Response Team(CERT-IN) issues advisories for digital forensic best practices.

Case Laws Involving AI and Digital Forensics in India

1. **Shafhi Mohammad v. State of Himachal Pradesh** [3] The Supreme Court held that electronic evidence does not necessarily require a certificate under Section 65B of the Indian Evidence Act if collected by a reliable source. AI-powered forensic tools have been instrumental in authenticating such evidence.

2. **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**[4]This case reinforced the requirement of Section 65B certification for electronic records, emphasizing AI's role in verifying the authenticity of digital evidence.

3. **Anvar P.V. v. P.K. Basheer**[5]The court ruled that secondary electronic evidence must comply with Section 65B of the Indian Evidence Act. AI forensic tools assist in ensuring such compliance by verifying metadata and timestamps.

4. **State (NCT of Delhi) v. Navjot Sandhu** [6] Digital forensics, including call detail records (CDRs) and email tracking, played a significant role in convicting the accused. AI tools now enhance such forensic investigations.

[3] Shafhi Mohammad v. State of Himachal Pradesh (2018) 5 SCC 311.

[4] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

[5] Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.

[6]State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.

The future of AI in Digital Forensic:-

The future of Artificial Intelligence (AI) in digital forensics isprepared for significant advancement, fueled by flourishingtechnologies and new research areas. Since digital forensicsremains sensitive to the larger scope and complexity ofdata, and artificial intelligence will play a central part in enhancingforensic techniques are applied. This section examines the main areas whereArtificial Intelligence will bear an influence, e.g., technological progress.advances, incorporation with other advanced technologies,and longstanding research problems.

1. Artificial Intelligence Technology Developments

One of the main areas of development is the developmentof artificial intelligence technologies. Recent advances in machinelearning algorithms, especially deep learning and neuralnetworks, in an effort to further improve the abilities of AI indigital forensics.For example, the application of advanced neural networkarchitectures such as Transformers and GenerativeAdversarial Networks (GANs), can improve the accuracy ofdata analysis and pattern recognition. These developmentswill facilitate better identification and categorization of digital objects by AI systems.evidence, even in uncertain and complex circumstances .

2. Integration with Quantum Computing

Quantum computing is a revolutionary advancement incomputational might that can rattle AI-poweredDigital forensics. Quantum computing, which holds the potentialprocess massive data in parallel, would speed upAI algorithms and allow real-time examination of huge data sets.This ability is most applicable for forensiclarge-scale investigations involving large amounts of electronic evidenceor advanced encryption. Quantum AI maypotentially resolve issues that are now intractable withconventional computational methods, offering new promise fordecrypting data, anomaly detection, and revealingconcealed structures.

3. Enhancing Data Privacy and Security

With artificial intelligence tools becoming more integrated into digital forensics,the guarantee of data privacy and security becomesbecome increasingly relevant. Future AI innovations will have totackle data privacy issues and ethical considerations. Methods like federated learning, which

enables AI models to be trained on a number of decentralizeddevices that don't reveal raw data can significantly contribute tokeeping information private. Also, developments incryptography techniques, such as homomorphic encryption,will ensure secure data processing and analysis, which will ensure thatsensitive information is saved safe through theForensic methodology.

4. Enhanced Interdisciplinary Partnerships

The future of digital forensics AI will be assisted byexpanded inter-disciplinary cooperation with artificial intelligenceforensic science students and legal practitioners.The convergence of these fields is essential to guaranteeing thatForensic software is built with an intimate understanding of forensic principles.requirements and legal norms. For instance, artificial intelligence modelsIn digital forensics, tools must be created to yield efficient results.which can be translated and held in court. Ongoingdiscussions between developers of AI and forensic practitioners willhelp bridge the gap between technological capabilities andpractical forensic requirements.

5. Resolving Ethical and Legal Issues

As AI develops, it is responding to ethical and legalchallenges will continue to be a top priority. Providing equity andTransparency of artificial intelligence algorithms is important to counteract biases.that could impact forensic outcomes. Further, the legalframework for the use of AI in forensicinvestigations need to adapt to new challenges pertainingto ownership, privacy, and accountability. Future researchit will be forced to find ways of integrating ethical considerationsAI development and establish standards for itsuse in forensic environments.

Challenges and Ethical consideration:-

The use of AI in digital forensics brings inthe possibility of algorithmic prejudice, where the inherent models inadvertently perpetuate and validate preconceptionsidentified in the training data. Biased algorithms can discriminate unfairlytarget specific audiences or groups in the contextof digital forensics, where it may result in wrongful accusation. It is necessary to recognize and oppose prejudice in order to providethe objectivity and fairness of analysis made possible through artificial intelligence. Thisdemands ongoing monitoring, improvement, and openness inthe development and application of artificial intelligence algorithms, with afocus on removing all the biases.Because of its nature, digital forensics examinespersonal information, privacy issues are of critical importance. When AIalgorithms are used on large sets of data, people's privacy suspects being investigated may unintentionally becompromised. Getting a balanced agreement is not easy between need for seeking online evidence and retaining peopleprivacy. Secure data processing procedures,privacypreserving practices, and rigid adherence to legaland ethical requirements become essential considerations. Digital forensicprofessionals have to tread carefully in thisethical footing to protect the rights and privacy ofthose who are concerned.

In digital forensics, interpretability and explain-ability arefaced with the inbuilt complexities of artificial intelligence systems. Forensic specialists, lawyers, and interested parties need an understandinghow conclusions are reached when AI systems generateinsights or inform decision-making. Transparency has the potential to create encouragingtrust and suspicion, which will hinder the discipline'sacceptance and uptake of AI. Developing AI models withintegrated interpretability features is an approach toovercome this challenge and enable practitioners to comprehend andvalidate the decision-making process. In the field of digitalforensics, for explainable AI not only enhancesresponsibility while simultaneously facilitating the work of human expertsand artificial intelligence systems to work together.

Conclusion:-

The field of cyber investigations has grown as a result ofAI integration into digital forensics. AI has evolvedinto a forensic tool of investigators, capable of automatingrepeat processes and providing advanced analyticalsolutions. The effectiveness of digital forensic techniques hashas been greatly helped by its function of establishing the tempo forinvestigations and further analysis. Utilization of AI indigital forensics is still in its infancy stage. AI toolsabilities will grow with technology. A dynamic new approach is called for by the continuing development, whichchallenges and prompts specialists to keep up with evolvingtechnological developments, approaches, and best procedures. Demonstrating flexibilityand flexibility will be required as the profession evolves andfaces new challenges.The application of AI to digital forensics will probably result inground-breaking advancements provided that technology continuesdeveloping. Machine learning's subset, deep learning, isare bound to be crucial. Digital forensic analysis willbe more precise and efficient as the complexity increasesalgorithms that utilize contextual analysis and subtle patternsrecognition skills are formed. In addition, the volume of data to be processed will increase with theintegration of natural language and computer visionprocessing into AI technologies. This will enable researchersto derive meaning from non-structured data sources andmultimedia content.

References:-

1) https://marymount.edu/blog/the-role-of-ai-in-forensics/

2) https://ijsret.com/wp-content/uploads/2024/07/IJSRET_V10_issue4_353.pdf

3) Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairnessand Machine Learning: Limitations and OpportunitiesMIT Press.

4) https://www.lawjournals.net/assets/archives/2023/vol5issue4/5130-1701684595237.pdf