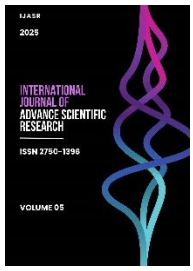
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135



Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Ensuring The Reliability Of Digital Evidences Through The Application Of Artificial Intelligence (Ai)

Submission Date: May 12, 2025, **Accepted Date:** May 30, 2025,
Published Date: June 18, 2025
Crossref doi: https://doi.org/10.37547/ijasr-05-06-04

Shomaxsudov Shoakrom Shomuratovich
Digital Forensics Research Institute of the Law Enforcement Academy of the Republic of Uzbekistan Head of Digital Forensics Laboratory, Uzbekistan

Gallyamov Marsel Gabtulxayevich
Digital Forensics Research Institute of the Law Enforcement Academy of the Republic of Uzbekistan Digital forensics laboratory Senior prosecutor-criminalist, Uzbekistan

Abdiaxatov Jakhongir Ravshan o'g'li
Digital Forensics Research Institute of the Law Enforcement Academy of the Republic of Uzbekistan Digital forensics laboratory prosecutor-criminalist, Uzbekistan

Dadaboyeva Guzal Akbarjonovna
Teacher (ESP), Uzbekistan

Abstract

The author concentrates on the recommendations aimed at ensuring the reliability of digital evidence by using (AI) artificial intelligence technologies. This article investigates the utilization of artificial intelligence in the automation of the analysis of digital evidence. The authors explore contemporary methodologies regarding the application of AI technologies for the processing, classification, and analysis of digital traces within forensic practice. The paper evaluates the advantages associated with the integration of AI into the processes of cybercrime investigation, which encompass the enhancement of processing speed for extensive data sets, the identification of concealed patterns, and the automation of routine tasks. Particular emphasis is given to machine learning, neural networks, and computer vision algorithms within the framework of digital evidence analysis. Furthermore, the article addresses the challenges concerning the

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

reliability of results derived from AI systems, issues of legal regulation and ethical aspects of the use of automated solutions in criminal proceedings.

KEYWORDS

Digital evidence, artificial intelligence (AI) technologies, cybercrime.

INTRODUCTION

Digital evidence, encompassing items such as electronic mail, SMS messages, and online browsing records, is progressively regarded as vital in legal inquiries and judicial proceedings. It is imperative to manage digital evidence meticulously to preserve its authenticity and guarantee its acceptability within the judicial system. So far, identifying and ensuring reliability of digital evidence is not always simple meaning sometimes it requires accuracy and carefulness and time to comprehend. This article suggests using AI (artificial intelligence) approach in ensuring the dependability of digital evidences. By exploring the interface between AI and digital evidences, these studies promote cross-disciplinary collaboration and innovation and help to count on future characteristics and instructions within the field. There are some questions to discuss for understanding the topic deeply, thus this article gives answer to the following questions.

HYPOTHESIS AND AIM

What is digital evidence? How it can be helpful to maintaining forensic procedure? Digital evidence refers to any electronic data stored or accessible, including information from computers, mobile devices and cloud services. It may include e-mails, text messages, web browsing history, documents, images, audio/video recordings and social media content. Metadata (data on data such as time and location) can also be valuable digital evidence.

2. The importance of digital evidence digital evidence is used in a wide range of investigations, from cybercrime to traditional crime. It can provide crucial information on the location, communication and intention of the suspect. It can also help to reconstruct events, identify perpetrators and build a strong case for prosecution. However, there are little challenges to regulate digital technologies in modern world.

1.Difficulties in Managing Digital Proof Data Volatility: It's critical to rapidly safeguard digital data because it can be easily lost or altered Technological Complexity: Gathering and evaluating digital evidence can be difficult due to the quick advancement of technology. Data Overload: It may be challenging to locate pertinent evidence due to the overwhelming amount of digital data. Security and Privacy: One of the main challenges is maintaining the integrity of digital evidence

while upholding privacy. 4. Best Practices for Managing the Preservation of Digital Evidence: To

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

guarantee that evidence is admissible in court, it should be gathered and stored utilizing recognized

forensic techniques. Documentation: It is essential to keep thorough records of the entire evidence gathering and processing procedure. Chain of Custody: Preserving a straightforward chain of custody guarantees that the evidence hasn't

been altered. Use of Certified Tools: The dependability of the evidence is increased by using digital forensics tools that have been verified and certified.Examples of Digital Evidence in Action Cybercrimes: When it comes to the prosecution of cybercrime such as fraud, phishing, and hacking, digital evidence is essential.

Financial Crimes:Fraudulent financial transactions can be found and the offenders can be identified using digital proof. Conventional Crimes: In traditional crimes, digital evidence can reveal important details about the conversations, whereabouts, and intentions of suspects.

What is happening to digital evidence in crime at a global level?

According to the Cyber Security Incident Management Guide in the private sector, there are particular protocols that must be followed in order to contain, investigate, and/or resolve cyber security incidents (such as distributed denial of service attacks, unauthorized access to systems, or data breaches) (Cyber Security Coalition, 2015). Recovering swiftly or gathering evidence are two main approaches to managing a cyber-security incident (Cyber Security Coalition, 2015): The first strategy, "recover rapidly," focuses on containing the incident to reduce damage rather than on data collecting or preservation. Crucial evidence may be lost due to its emphasis on quick response and recovery. The second strategy keeps an eye on the cyber security event and concentrates on digital forensic tools to collect data and proof about the incident. The recovery from the cyber security issue is delayed due to its major focus on gathering evidence. The commercial sector is not the only one using these strategies. The private sector's strategy differs depending on the organization and its aims.

Problem statement. Disruptive technologies like artificial intelligence (AI), the Internet of Things, drones, and crypto currencies, which can be extremely dangerous instruments in the hands of criminals, have made it possible for new crimes to arise quickly. As a result, we constantly encounter new types of digital crimes, hybrid crimes, crime-as-a-service, cyber-attacks, political advocacy campaigns, and cybercrime for war crimes, to name a few. These crimes have a significant impact on our society and, consequently, how we live our lives. Therefore, in order to safeguard organizations and individuals, our society needs a significantly greater ability to detect and investigate illegal conduct. Therefore, while utilizing the potential of digital technology, it is imperative that we deepen our understanding of how these tools can be used against our society and consistently make it more difficult for criminals to use them successfully.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

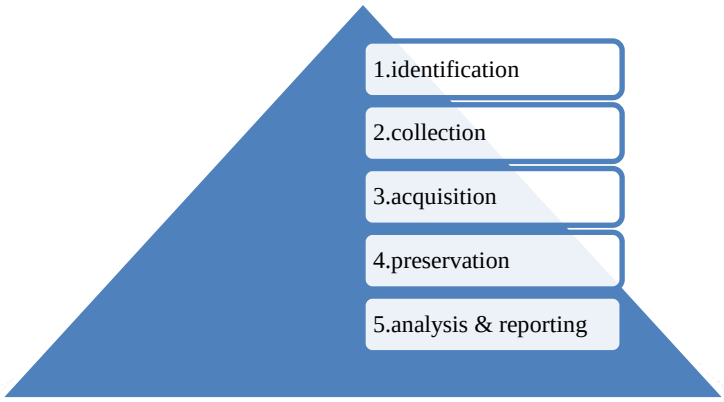


Fig.1. Handling of digital evidence

LITERATURE REVIEW

The role of AI in forensic science

Without a doubt, artificial intelligence plays a part in forensic sciences, which suggests that we need to learn more about its effects.For instance, the European Forensic Science Area 2030 strategy for2030 includes AI and future technologies , albeit given the rate of digitalization now, 2030 seems a little far off. Although certain ideas and observations are discussed in this section, Geradts and Franke, who provide state-of-the-art implementations, offer a more thorough analysis.Numerous instances demonstrate how quickly technology is developing. The evolution of airplanes from the first wooden models over a century ago to the modern jets serves as an example. Similar to this, forensic science has evolved, and new techniques for analysis keep opening doors to maximize both digital and physical evidence of crimes. AI techniques come in a variety of forms, with more to follow. AI-based techniques, however, still fall short of what our human brains are capable of. According to Kahneman, the human brain can be divided into two distinct systems: a quick, unconscious system and a slower, conscious system that distributes attention as needed. It is fair to assume that the AI systems of today merely replicate the unconscious portion of the human brain.1 Driving a car serves as a basic illustration. Autonomous driving AI techniques are "non-conscious." They are unable to manage unforeseen circumstances for which they are not prepared. Conversely, we have the ability to activate our conscious system, process the novel circumstance, and take action right away. However, we may find ourselves using the non-conscious brain function to drive to our old workplace rather than to our new one if we are fatigued or distracted. We must therefore be conscious of AI systems' limits. AI systems outperform humans in other domains, such as processing and retaining vast amounts of diverse data that are beyond the capacity of human brains. These days, AI techniques outperform humans in several forensic domains, such language and image recognition. This suggests that man-machine interaction has to be reviewed. We shouldn't undervalue the

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

application of AI, for example, to handle the massive volume of data. One example is the difficulty of managing the 40 billion IP addresses in the globe and their potential permutations while searching the internet for criminal activity. We also shouldn't overestimate AI because forensic scientists will always be needed in the wake of digital transformation, for example, to handle reports and discoveries and employ AI-based technologies. To improve the effectiveness and precision of investigations, forensic science optimization entails utilizing the advantages of both computer-based and human-based methodologies.

In order to find matches in databases that can identify a certain person or object, we analyze traces, turn them into vectors of digital information, and feed these strings—derived from things like fingerprints and DNA—into different classification algorithms. Using labeled datasets to train algorithms to reliably classify data or anticipate outcomes, predictive AI, such as supervised learning, involves adding logic and training the system to recognize the desired outcome. By inverting the process and feeding the system results instead, generative AI enables us to produce new material based on the input we provide. We will probably be inundated with generative AI content related to crimes as well. Generative AI is extensively used, for example, to generate code, create graphics and videos from text, and create big language models. Systems like ChatGPT are trained to respond in-depth to our prompts by following our directions. However, we must understand that generative AI creates knowledge based on the input we provide. This suggests that we cannot completely rely on the response to be honest or accurate if it has received little training on a particular topic. The creation of specialized "ChatGPTs" for usage in particular applications is another issue we currently face. The same is true for criminals, such as WormGPT, which is made to help criminals with their programming and hacking activities and enable them to engage in destructive actions. Since the cost of training is still too expensive, ChatGPT and related technologies are being used extensively. The dependability of software is questioned. For example, how can we understand the error rate in code produced by AI? The transition from AI apps to AI assistants, which combine the capabilities of generative AI in novel ways, is anticipated to be the next big advancement. AI-enabled discussions are one example, which combines a number of AI approaches, including voice-activated big language models, digital twins, and visualization tools. We must pay attention to the ethical issues raised by the application of AI. We must have faith that AI-based systems are safe, deliver real outcomes, and haven't had any of their parts compromised in order to use them. We must comprehend and take into account prejudice in AI systems just as we do with traditional approaches because bias in all its manifestations is significant. One example is bias in training data, since AI systems are capable of reproducing human prejudices. The majority of training databases depict reality rather than the ideal state of our society, such as in terms of gender equality, explains ability, and justice. This suggests that in order for us to trust AI systems as much as we do more traditional tools and instruments, we

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

must provide training and education, as well as conduct regular assessments and monitor AI systems for biases. Furthermore, we must discuss when computer-based techniques ought to be verified based on the demographic characteristics of the populations involved in the cases under consideration, rather than a representative distribution of these characteristics in the broader community.

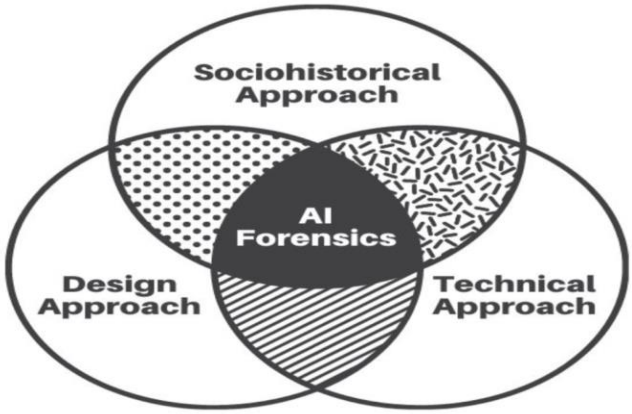


Fig.2. Artificial Intelligence and the Society of the Future

https://www.cdh.cam.ac.uk/research/projects/ai-forensics/

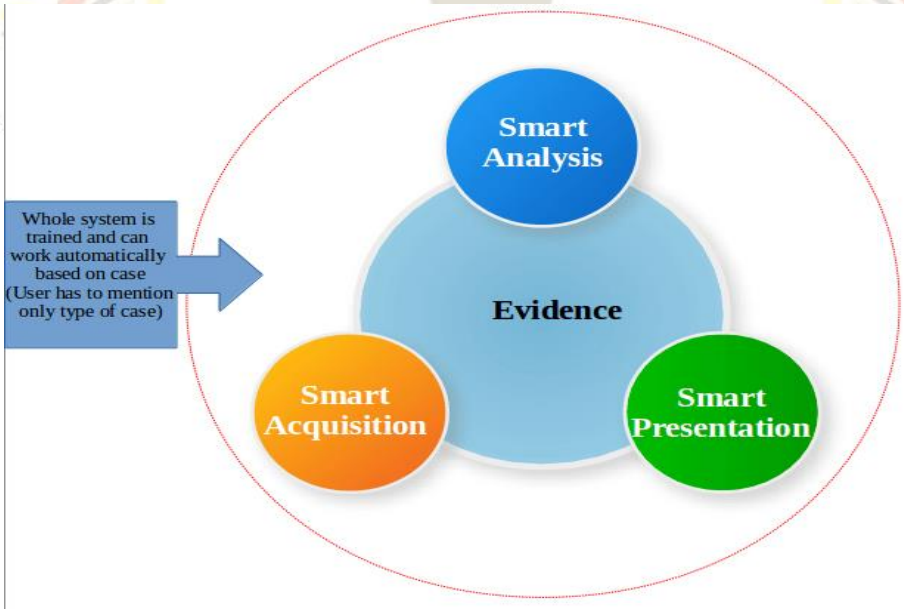


Fig.3. Proposed Digital Forensic Framework

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

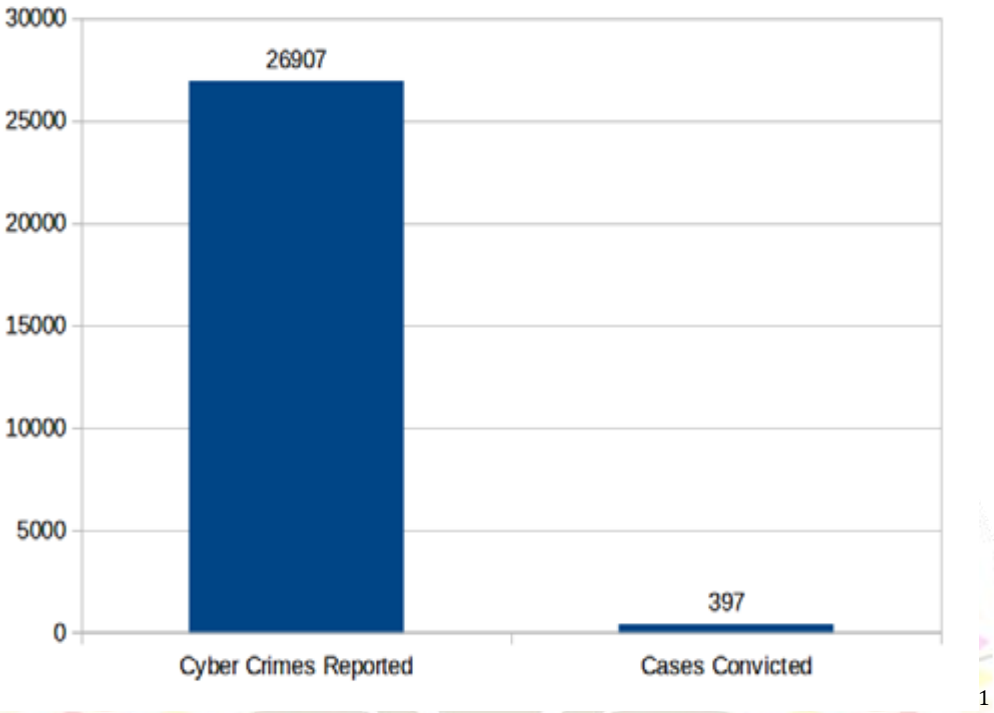


Fig.4. Cyber Crime Conviction Rate in India between 3013-15

Key features AI technologies in investigations

Numerous AI technologies are leading the way in automated evidence processing, such as machine transcription and translation, automated redaction, tracking persons of interest in videos, and AI-driven metadata tagging. Below is an explanation of how each contributes to investigations: Machine transcription and translation: evidence is available in multiple formats and may be in languages that are not familiar to the investigation team. The processes of transcription and translation can significantly delay an investigation. Locating a service for these tasks is challenging, and once found, obtaining the results can take several days. Additionally, if a substantial amount of evidence requires this processing, the time frame can extend even further. AI can greatly expedite this process, enabling investigators to uncover evidence that may have otherwise gone unnoticed.

Automated redaction: in numerous instances, certain individuals may be present in evidence files that require redaction. In the past, this necessitated a labor-intensive manual process that diverted

6.Rughani, P. H. (2017). ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK. International Journal of Advanced Research in Computer Science, 8(8), 10–14. https://doi.org/10.26483/ijarcs.v8i8.4571

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

valuable resources from other critical tasks. AI can significantly streamline the redaction process, substantially decreasing the time required.

Person-of-interest and vehicle tracking: facial recognition technology has limitations in scenarios where video footage includes large crowds. While there are appropriate contexts for its use, some individuals express hesitation due to concerns regarding the safeguarding of personally identifiable information (PII). However, recent advancements in AI technology that categorize humans as objects can assist investigators in identifying key features of a potential suspect (such as a logo on a shirt, a specific type of hat or backpack they are wearing, etc.) to monitor that individual across video files on a large scale, thereby greatly minimizing the time needed to analyze video evidence. This same technology can also be employed by investigators to track vehicles within the footage.

AI-driven metadata tagging: when analyzed using AI, digital evidence generates a substantial amount of data that can be utilized to assist investigators in comprehending the materials at their disposal. From highlighting only pertinent files to identifying moments within files that may contain crucial evidence capable of altering the case, AI offers automated evidence processing to equip investigators with the insights necessary to locate that needle in a haystack.

Ethical considerations in the responsible deployment of AI As artificial intelligence increasingly influences investigations and law enforcement, it is essential that ethical considerations remain paramount in its implementation. Concerns such as algorithmic bias, data privacy, and other related issues necessitate that AI leaders adhere to standards designed to safeguard individuals from potential harm. While legislation is still striving to keep pace, there are proactive measures that companies can undertake immediately. Veritone has established a framework of AI for Good principles that directs all our efforts to ensure that our technology is transparent, reliable, secure, and compliant. Furthermore, it enhances the capabilities of individuals, including investigators, enabling them to perform their duties more effectively.

Research methodology introduction

This is the main part of the research work that shows the procedures and methods used in this study. The chapter is organized into subheadings representing the steps of the study. These sub-headings include: the digital forensic material to be studied, research design, research instruments, methods that are used to collect data and methods which are used to analyze data.

Research design

Qualitative research method used in the form of graphs, and charts which includes well-structured some questions which show strategies are necessarily give answers and 1 of them was open question where participants are free to answer.

Population of the study

This study is based on secondary data materials, basically taken from different articles and web

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

pages written by international scholars and scientists.

Method of data analysis

Descriptive statistics were used to understand the preference of the criminals on application of AI in analyzing digital evidence.

Hypothesis 1

The role of digital evidence and its' importance to maintaining forensic procedure.

Digital evidence refers to electronic data used in legal proceedings. It includes emails, texts and more. Modern law enforcement relies heavily on digital evidence to solve crimes and ensure convictions. This article deals with the collection, legal considerations and investigative role of digital evidence. Digital evidence, which includes data from various electronic sources, is crucial to modern law enforcement, often surpassing DNA evidence in the context of investigation. Special methods and legal considerations are crucial to the collection and analysis of digital evidence in order to ensure its integrity and its admissibility to court, including the maintenance of a strict chain of custody. Technological advances, such as cloud computing and artificial intelligence, have had a major impact on digital law enforcement, requiring constant updates to the tools and methodologies used by investigators. Digital evidence refers to all electronic data or information that can be used in legal cases. This includes a wide range of digital data, including: logging emails multimedia file databases various forms of software record Digital evidence plays a central role in investigations, providing insight essential to the resolution of crimes and the assurance of convictions.

Hypothesis 2

Utilizing the potential of AI technologies in digital evidence analysis, and how these tools can be used against our society and consistently make it more difficult for criminals to use them successfully.

One of the primary benefits of artificial intelligence in the management of digital evidence is its capability to swiftly and accurately process extensive amounts of data. Investigations frequently require the examination of a vast array of digital evidence from multiple sources, including social media, surveillance videos, and emails. The ability of AI to analyze these files and highlight pertinent data enables investigators to concentrate on the most essential aspects of the case without being overwhelmed by manual data review tasks. By employing machine learning algorithms and natural language processing (NLP), AI tools can quickly extract relevant information, assist teams in recognizing patterns, and deliver crucial insights. By implementing this approach, AI introduces an additional level of accountability aimed at minimizing human error, which tends to occur more frequently in manual evidence analysis procedures. AI addresses this risk by automating repetitive tasks and examining evidence with unwavering precision. Machine learning models that have been trained on extensive datasets can reveal and detect elements that might be overlooked by human analysts. This improvement boosts the accuracy of data analysis and accelerates the investigation process, ultimately

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

resulting in more dependable and favorable outcomes. So that, this article helps to identify key features of using AI approach in two ways first for its quickness for finding materials and second for the effectiveness of AI approach using.

DATA INTERPRETATION AND FINDINGS

How AI approach may foster the work of investigators?

1.Case In India, financial crime has developed to fit a complicated ecosystem. For example, several payment banks may encounter regulatory consequences after the Financial Intelligence Unit (FIU) found that nearly 50,000 accounts do not have adequate Know Your Customer (KYC) verification. These accounts are believed to be linked to dubious transactions and possible money-laundering activities. Of these accounts, approximately 30,000 are associated with payment banks excluding Paytm Payments Bank. Over the last ten years, the Enforcement Directorate (ED) documented its peak number of money laundering and foreign exchange violation cases in 2021 and 2022, with 1,180 and 5,313 complaints, respectively. Between FY 2012-13 and 2021-22, the agency filed a cumulative total of 3,985 criminal complaints under the Prevention of Money Laundering Act (PMLA) and 24,893 under the civil law of the Foreign Exchange Management Act (FEMA). In the previous three years, the ED has received more than 12,000 complaints regarding alleged foreign exchange violations. Furthermore, the adjudicating authority of the PMLA verified proceeds of laundering totaling INR 2,214.92 crore over the last three years.

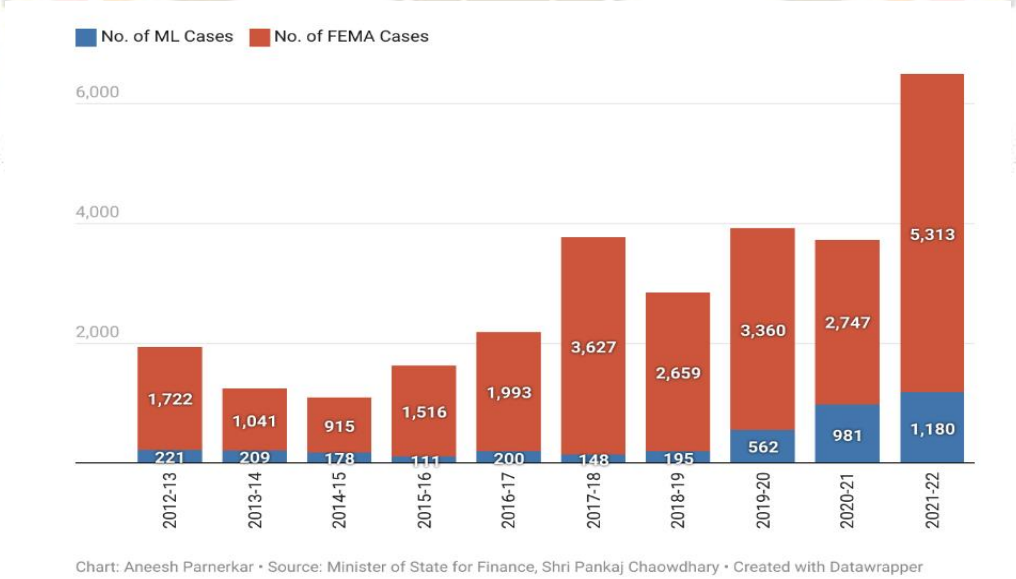


Fig.5. Money Laundering and Foreign Exchange Management Act (FEMA) Cases in India

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

As illustrated in Fig.6 below, supervised learning is the most commonly employed method in crime prediction, accounting for 31% of the research papers. Additionally, since some studies implemented multiple machine learning algorithms, 22% of the collected papers utilized both supervised and unsupervised methods. In contrast, only 10% of the papers focused on unsupervised learning. Interestingly, a mere 1% adopted the semi supervised approach, indicating that this method is rarely used in the realm of crime prediction. Lastly, 36% of the papers did not clarify which approach they adopted.

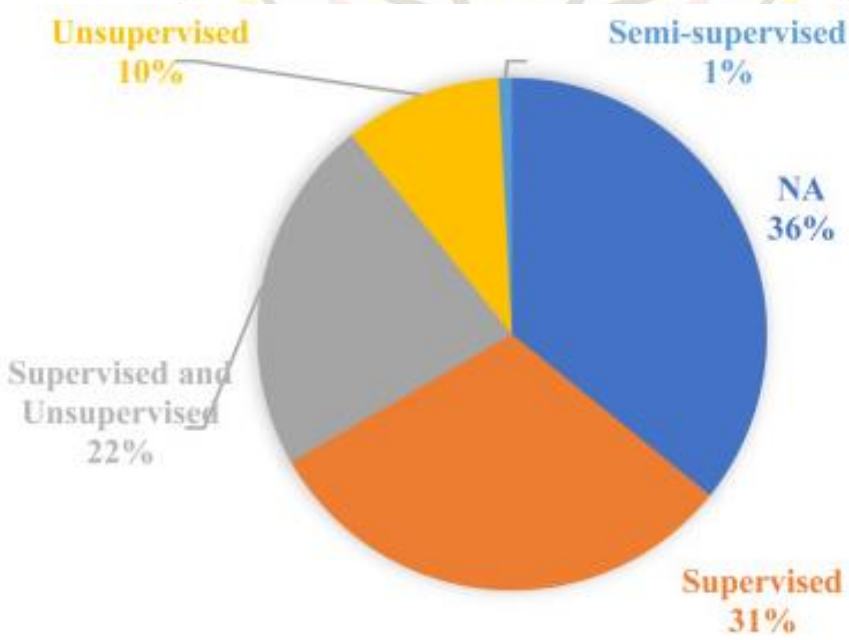


Fig.6. Learning methods percentages

CONCLUSION

This research underscores the transformative potential of Artificial Intelligence (AI) in enhancing the reliability and efficiency of digital evidence analysis for forensic investigations. Key findings demonstrate that AI technologies—including machine learning, neural networks, computer vision, and natural language processing—significantly accelerate the processing of large-scale digital datasets, automate labor-intensive tasks (e.g., transcription, redaction, metadata tagging), and uncover hidden patterns imperceptible to human analysts. These capabilities are critical in combating evolving cybercrimes, financial fraud, and hybrid threats.

REFERENCES

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 24-35
OCLC – 1368736135

1. AI IN DIGITAL FORENSICS Manasi Pritam Zirpe1, Shravani Santosh Potdar1&, Harshali Rohit Kadaskar. (n.d.). International Journal of Scientific Research in Modern Science and Technology.
2. Artificial intelligence & crime prediction: A systematic literature review. (n.d.). Social Sciences & Humanities Open Volume 6, Issue 1, 2022, 100342.
3. Muhammad Arjamand1, Areeba Saleem1 , Abdul Basit1 , Subha Iftikhar1 , Muhammad Sharif2 , Muhammad Shahid Cholistani1 , Muhammad Farhan1 , Shumail1 , Bakht Ameer Khan1 , Zeeshan Ali1 , Bilawal Shahid1 , Muhammad Hasnain1. (n.d.). International Journal of Multidisciplinary Research and Publications.
4. Mitchell, F. (2014). The use of Artificial Intelligence in digital forensics: An introduction. Digital Evidence and Electronic Signature Law Review, 7(0). https://doi.org/10.14296/deeslr.v7i0.1922
5. Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. Forensic Science International, 362, 112133. https://doi.org/10.1016/j.forsciint.2024.112133
6. The role of AI in forensic science. (n.d.). Wiley.
7. Rughani, P. H. (2017). ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK. International Journal of Advanced Research in Computer Science, 8(8), 10–14. https://doi.org/10.26483/ijarcs.v8i8.4571
8. SAURADEEP BAG, Use of AI in Arresting Financial Crime. (n.d.). Published on Aug 19, 2024.