International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Forensic Analytics With Ai

Hareesh Kumar C[1], Trisha B[2]

[1,2]Student, Sastra University

ABSTRACT:
This paper thoroughly examines the role of Artificial Intelligence (AI) in digital forensics, showcasing its potential to tackle complex cyber threats and the growing amount of digital data. It starts by discussing key AI technologies, particularly machine learning and deep learning, and their importance in forensic investigations.
As cyber threats become increasingly sophisticated, the field of cyber forensics is also advancing. At the forefront of this evolution is artificial intelligence (AI), which is transforming how cyber forensics operates. This article examines the effects of AI on cyber forensics in terms of identifying, monitoring, and preventing cyber threats. By employing AI-driven tools, cyber forensics can process larger datasets, recognize patterns, and detect anomalies, leading to a deeper understanding of cyber incidents. The increasing frequency and complexity of cyber-attacks necessitates the development of competent cyber forensic investigative methodologies. This study looks into the use of machine learning and artificial intelligence (AI) in automated threat analysis and classification, with the goal of better understanding their function in cyber forensics. Forensic investigators and cybersecurity specialists provided information through case studies, observations, and surveys. This study highlights the potential benefits of incorporating artificial intelligence and machine learning to advance digital forensic investigations, as well as providing significant insights into their roles in cyber forensics. Incorporating these technologies has obvious benefits, like faster analytical methods and improved threat detection capability. Investigations may be accelerated by integrating AI and machine learning, allowing firms to respond quickly to cyber threats and reduce overall risk exposure. As the cybersecurity landscape evolves, the successful integration of AI and machine learning in the sector has the promise of ushering in a new era of proactive threat identification, hence strengthening organisations' ability to protect digital assets.

BACKGROUND:
This paper thoroughly examines the role of Artificial Intelligence (AI) in digital forensics, showcasing its potential to tackle complex cyber threats and the growing amount of digital data. [1]It starts by discussing key AI technologies, particularly machine learning and deep learning, and their importance in forensic investigations.
As cyber threats become increasingly sophisticated, the field of cyber forensics is also advancing. At the forefront of this evolution is artificial intelligence (AI), which is transforming how cyber forensics operates. This article examines the effects of AI on cyber forensics in terms of identifying, monitoring,

[1] Casey Eoghan, Gerasimos Stellatos & Philip Craiger, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet 23 (3d ed. 2011).

and preventing cyber threats. [2]By employing AI-driven tools, cyber forensics can process larger datasets, recognize patterns, and detect anomalies, leading to a deeper understanding of cyber incidents.

KEYWORDS: Artificial Intelligence, Cyber Security, Digital Forensics

LITERATURE REVIEW:

The integration of Artificial Intelligence (AI) in cyber forensic analytics has revolutionized the investigation and analysis of cybercrimes. Khan(2019) proposed an AI-based framework for cyber forensic analysis, highlighting the potential of machine learning algorithms in identifying patterns and anomalies in digital evidence. Al-Mamgani(2020) demonstrated the effectiveness of deep learning techniques in detecting malware and analyzing network traffic. [3]Machine learning algorithms, such as Support Vector Machines (SVM) and Random Forests, have been successfully applied in classifying malware, predicting attack patterns, and identifying suspicious network activity (Venkatraman 2020; Rathore 2020). Deep learning techniques, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have been used to analyze digital images, videos, and audio files for forensic investigation (Mohanty 2020; Singh 2020).Natural Language Processing (NLP) techniques have also been employed to analyze text-based digital evidence, such as emails, chat logs, and social media posts, for sentiment analysis and authorship identification (Gupta 2020; Kumar 2020). Furthermore, AI-powered malware analysis tools have automated the analysis and classification of malware samples, reducing the workload of forensic investigators (Shalimi 2020; Wang 2020). [4] Despite these advancements, challenges persist, including data quality and availability, explainability and transparency, and adversarial attacks (Bharati 2020; Jain 2020). Future research should focus on addressing these challenges to enhance the reliability and effectiveness of AI-driven cyber forensic analytics.

RESEARCH PROBLEM:

The increasing sophistication of cyber threats poses significant challenges for traditional cyber forensics methods. As attackers adopt advanced techniques, there is a pressing need to explore how AI can enhance the effectiveness of cyber forensics in identifying, monitoring, and preventing these threat.

RESEARCH OBJECTIVE:

1. To evaluate the effectiveness of AI-based tools in monitoring cyber activities.
2. To Develop an AI-powered cyber forensic framework for accurate threat detection, incident response, and digital evidence analysis.
3. To Investigate AI-driven predictive analytics to mitigate advanced cyber threats, reducing Mean Time to Detect and Mean Time to Respond.

[2] Ramesh, Pradeep & Shivani Gupta, Artificial Intelligence in Indian Cyber Forensics: Opportunities and Legal Framework, 17 Indian J. of Law & Technology 142, 146 (2022).

[3] Brennan, Sean, et al., AI and Machine Learning for Cyber Forensic Investigations, 55 IEEE Transactions on Dependable and Secure Computing 1234, 1238 (2022).

[4] Singh, Manish Kumar & Priti Singh, Artificial Intelligence in Cyber Forensics: Opportunities and Challenges, 24 Journal of Digital Forensics, Security, and Law 59, 64 (2022).

RESEARCH QUESTIONS:

1. How does AI improve the identification of cyber threats compared to traditional methods?
2. What specific AI-based tools are most effective for monitoring cyber activities?
3. In what ways can AI generated evidence is considered in legal proceedings ?

RESEARCH METHODOLOGY:

This study employs a secondary research methodology, relying on an extensive review of existing literature to explore research topic and questions. A systematic and comprehensive analysis of relevant studies, academic journals, books, and reputable online sources will be conducted to gather data.

SCOPE AND LIMITATIONS OF THE STUDY:

1. AI-powered cyber forensic framework for network traffic threat detection and analysis.
2. Simulated data, supervised machine learning, scalability issues.
3. Focus on network traffic data, excluding other Al techniques and data sources.

FINDINGS AND DISCUSSIONS:

Artificial intelligence (AI) is the emulation of human intellect in devices that have been designed to act and communicate like humans. Any computer that exhibits traits of the human intellect, such learning and problem-solving, can also be referred to by this term. The ideal feature of artificial intelligence is the capacity to reason and act in ways that are most likely to achieve a particular goal. [5]The concept that computer systems can automatically learn from and adapt to new data without human input is known as machine learning (ML), a subtype of artificial intelligence. This independent learning is made possible by deep learning algorithms, which absorb enormous amounts of unstructured data, such as text, images, and video.

"Admission" is defined in Section 17 of the Indian Evidence Act, 1872. Determining admissibility entails figuring out whether the judge is permitted to take into account information or evidence that was offered in court while making a decision. It depends on things like applicability, dependability, and following the rules outlined in the Act and other pertinent legislation. Relevance, hearsay, expert views, character evidence, public documents, privileged communication, admissions, confessions, and the possible exclusion of evidence obtained unlawfully are among the principles for admissibility that are outlined in the Act. In accordance with the Act, judges are in charge of determining whether evidence is admissible, guaranteeing a fair and just legal system.

According to Section 136, the presiding court may ask how the alleged fact, if proven, would be relevant when a party plans to provide evidence of any fact or circumstance. [6]The judge will admit the evidence if they believe that the fact, when proven, would be relevant and not otherwise. After nearly 150 years, India updated its criminal justice system's legal foundation this month. The Bharatiya Sakshya Adhiniyam, 2023 (BSA) was enacted by Parliament in replacing of the Indian Evidence Act, 1872 (IEA). This action may affect India's shift to a society empowered by technology.

[5] Singh, Manish Kumar & Priti Singh, Artificial Intelligence in Cyber Forensics: Opportunities and Challenges, 24 Journal of Digital Forensics, Security, and Law 59, 64 (2022)

[6] Sharma, Rajeev & Anjali Mehta, Role of AI in Indian Cyber Forensics: A Future Perspective, 34 Indian Journal of Cyber Law 81, 85 (2021).

Admissibility of Electronic Evidence under The Indian Evidence Act, 1872

The terms "e-evidence" and "digital evidence" can be used interchangeably. In the modern world, using devices like smartphones, apps, laptops, desktops, tablets, iPads, and more to access the internet is commonplace. Nearly everyone makes a profile on social media sites like Instagram, Twitter, Snapchat, Facebook, and WhatsApp. Using CCTV cameras and other tools, police officers and guards continuously keep an eye on all the events and activities occurring in a specific location. [7]E-evidence is defined as video, photographs, or phone logs that are taken from reliable sources, are relevant and admissible, and can be used in court to establish the defendant's guilt.

Section 65A and Section 65B of The Indian Evidence Act, 1872

Section 65A

Section 65A of the Act provides information on electronic records that must be supported by the provisions listed in Section 65B of the Act, Section 65A of the Indian Evidence Act is always read in conjunction with Section 65B of the Indian Evidence Act, 1872.

Section 65B

The admissibility of electronic records in court proceedings is outlined in Section 65B of the Indian Evidence Act. It specifies that a record is considered a document if it is in an electronic or digital format. And if such a document satisfies the requirements outlined in Section 65B of the aforementioned Act, [8]it will unavoidably be accepted in court proceedings without the necessity for further evidence of its authenticity.

“The conditions of Section 65B are:

1. The information shall be produced during the regular course of activities by the person having lawful control over the use of the computer.
2. The information has been regularly fed into the computer in the ordinary course of the said activities.
3. Throughout the material part of the said period, the computer was operating properly, or the improper operation was not of such nature to affect the electronic or digital record, or the accuracy of its contents produced.
4. The information contained in the electronic or digital records is derived from such information fed into the computer in the ordinary course of an individual’s activities. “

EXAMINING THE BSA:

An AI-generated output will probably be categorized as "digital" or "electronic evidence" under the BSA. Digital or electronic records are included in the BSA's definition of documents and documentary proof. Electronic records on emails, server logs, documents on computers, laptops, smartphones, etc are examples of what the BSA defines as a "document." Notably, it is possible that the BSA's modifications are merely cosmetic, particularly in relation to digital or electronic evidence. This only formalizes current procedures under the previous IEA, therefore it is hardly a significant change.

[7] Lawrence A. Gordon & Martin P. Loeb, The Impact of AI in Cybersecurity Risk Management, 45 J. of Acc. and Econ. 333, 338 (2020).

[8] Kumar, Ravi & Rohit Sinha, AI Tools for Enhancing Cyber Forensic Investigations in India: Current Challenges and Solutions, 9 Indian Journal of Cybersecurity 57, 59 (2023).

The High Court employed ChatGPT to validate its opinion on an accused's bail application.

There are problems in treating AI-generated evidence as primary evidence. This is encapsulated in the 'black box' problem – where understanding the reasoning behind an AI system's predictions or decisions becomes difficult. Perhaps for the first time in India, the Punjab and Haryana High Court has used artificial intelligence for taking opinions on a criminal case.[9] The High Court used ChatGPT for validating its opinion regarding the bail application of an accused. This is the first instance ChatGPT has been used to decide on a bail application in India.

There are challenges in using AI-generated evidence as supplemental evidence. To be admitted as'secondary evidence', digital evidence must be 'authenticated' with a certificate (section 63) signed by anybody 'in charge of the computer or communication equipment' and an expert.

Given the nature of AI systems, there are some problems to consider. AI systems involve several contributors (with different people performing various jobs such as data collection and analysis, AI model training, model technique and algorithm development, AI model testing and assessment, and so on). They are also complicated and frequently self-learning algorithms, making obtaining authenticity certificates a difficult task. Furthermore, it may become challenging to accurately explain the operation of AI systems, particularly those that use deep learning or advanced machine learning techniques.

Most importantly, we are still in the early stages of AI system development.[10] The evolving nature of AI systems raises questions about the suitability of section 63, which borrows from section 65-B of the older Evidence Act and may have been designed with more traditional forms of electronic evidence in mind (such as pen drives based on optical or magnetic media as opposed to flash drives based on semiconductors), to effectively address the complexities of AI-generated evidence.

Kinds of AI-generated Content:

Prognostic AI models may provide predictions about upcoming occurrences, biometrics help with identification, and AI transcription services translate audio into written transcripts for legal evidence. Here are a few examples of AI-generated proof.

How to govern the admissibility of AI-generated evidence in courts?

With the introduction of electronic devices and the internet, electronic evidence has become an increasingly important aspect of legal procedures. Electronic mail, SMS, social media posts, and surveillance film are utilized to establish facts and support legal claims. On the one hand, as electronic evidence becomes more sought after, AI has created a new obstacle with the emergence of AI-generated evidence.

AI – as Evidence:

In today's world, litigation involves complex commercial and intellectual property issues, with significant worries about financial information, trade secrets, and other sensitive information building up. In certain respects, AI techniques may facilitate the examination of this data. However, attempting to present this research as proof adds an extra degree of effort and expense. For example, while electronic'signatures' on various types of papers may aid in the prevention of counterfeiting, showing how the electronic signatures are reliable may need multiple levels of expert testimony.

[9] Sommer, Peter, AI in Digital Evidence Gathering: Practical Applications and Future Trends, 15 Journal of Cybersecurity 109, 113 (2021).

[10] Garfinkel, Simson L., Automated Disk Analysis with Artificial Intelligence, 7 Digital Investigation 82, 85 (2010).

To address these challenges, courts will need to adopt new rules and procedures for the admission of evidence gathered by AI.[11] Setting guidelines for the use of AI in legal cases can include allowing litigants to review the underlying coding, establishing procedures for the disclosure or certification of AI-generated evidence, and requiring independent third-party verification before use in court.

Crucial interrogations for Judges and Lawyers

While photographic evidence may require a description, it is usually self-explanatory. Thus, an AI-generated picture presents a challenge. For example, an impression of a high official committing an infraction might be a burden on him, even if he did not engage in such conduct. In such cases, the court or lawyer seeking conclusive proof may have difficulty determining the truth. How can a judge tell if a picture is AI-generated or real? In addition to the multiple hazards that undermine the trust of evidence, unfiltered procedures in AI processes reduce transparency, while bias in training data can result in unjust findings.

Evidence are leads that help to identify the perpetrator beyond a shadow of doubt. However, when computers take over human tasks with the help of their own 'brains, determining blame and imposing accountability on criminals may become harder. When evaluating electronic evidence and AI-related evidence, an autonomous automobile that can drive itself may be a hurdle.

How Artificial Intelligence Enhances Cyber Forensics

For years, AI has been both celebrated and feared for its ability to surpass human capabilities in processing information and learning over time. In the eyes of the general public, AI is often seen as a broad term that encompasses an automated collaboration of Machine Learning (ML) and Natural Language Processing (NLP). [12]Together, these technologies detect patterns, identify anomalies, and establish connections, aiding investigations in uncovering evidence and insights that might otherwise go unnoticed.

In the realm of digital computer forensics, mobile forensics, and cloud forensics, AI excels at analyzing large volumes of evidence to identify and retrieve pertinent data through automated searches of images, videos, text, and audio files.

Benefits of AI-Powered Investigation Techniques

AI's ability to manage large datasets enhances analytical processes and offers deeper insights. Its analytical capabilities extend beyond identifying patterns, anomalies, and trends; it also uncovers subtle correlations and nuanced irregularities that traditional manual analysis might overlook.

AI streamlines time-consuming tasks like data collection, analysis, and report generation, significantly cutting down the time investigators spend on searches. This automation allows investigators to concentrate more on critical thinking and problem-solving aspects of each case. Consequently, they can allocate more time to high-value activities such as generating hypotheses, making decisions, and developing strategies.

[11] George, Joseph, AI-Based Algorithms in Cyber Forensic Analytics: A Case Study, 62 Journal of Cyber Forensics and Investigation 121, 123 (2021).

[12] Sommer, Peter, AI in Digital Evidence Gathering: Practical Applications and Future Trends, 15 Journal of Cybersecurity 109, 113 (2021).

By optimizing search and analytical processes, AI facilitates quicker case closures, helping to minimize backlogs and better manage budgets. Its automated features also assist investigative teams in addressing staffing shortages and resource limitations, particularly during times when qualified professionals are scarce.

Cyber forensic tools and techniques

The integration of Artificial Intelligence (AI) in digital forensics has transformative implications, significantly enhancing the examination and interpretation of digital evidence. [13]AI-driven solutions efficiently analyze vast datasets, recognize patterns, detect anomalies, and automate evidence extraction. In order to counteract the growing complexity and frequency of cyber threats, the combination of artificial intelligence (AI) with cyber forensics transforms the investigation and analysis of digital crimes. With the use of machine learning algorithms, natural language processing, and predictive analytics, AI-powered cyber forensic tools and procedures have emerged as invaluable resources that improve the gathering, analysis, and presentation of digital evidence.

Digital forensic tools:

Volatility Framework

The Volatility Framework is a powerful tool used to extract RAM information or memory information from Windows, Mac, and Linux systems. Implemented in Python, it operates through a command-line interface, making it ideal for malware analysis and investigating cyber attacks.

Advantages of Volatility Framework

The Volatility Framework offers several benefits, including its ability to analyze RAM or memory information even after a computer shutdown. [14]Additionally, it supports various file formats and employs efficient algorithms for analyzing RAM dumps.

Limitations of Volatility Framework

Despite its advantages, the Volatility Framework has some limitations.Notably, it has limited graphical user interfaces, making it challenging for new users. Furthermore, it requires users to work in the command-line interface.

OpenStego

OpenStego is a versatile tool designed to extract hidden messages from images, audio files, and other digital media. Utilizing advanced encryption algorithms, OpenStego provides a user-friendly interface, making it accessible to beginners.

Advantages of OpenStego

By using AI-powered analytics to identify hidden data in photos, videos, and audio files, anticipate dangers, and expedite investigations, OpenStego transforms cyber forensic investigations. [15]Enhanced steganography detection, enhanced threat detection, and effective investigation are some of its benefits.

[13] Kumar, Abhishek & Neha Bhargava, Artificial Intelligence in Indian Digital Forensic Framework: Addressing Challenges and Gaps, 8 Journal of Forensic Science and Cyber Law 123, 127 (2023).

[14] Verma, Ritu & Arjun Mahajan, Cyber Forensics in India: Role of AI and Machine Learning, 5 Indian Journal of Cybercrime Studies 45, 48 (2022).

[15] Jain, Vishal & Anurag Jain, AI-Driven Digital Forensics: A Comprehensive Approach in Cyber Crime Investigations, 11 International Journal of Advanced Computer Science and Applications 45, 47 (2020).

Predictive threat intelligence, deep learning-based detection, and machine learning-based steganalysis are all made possible by OpenStego's AI-powered features.

Limitations of OpenStego

However, OpenStego can be complex when working with large data sets, making it difficult to efficiently hide information. unable to manage intricate AI-generated visuals,AI-Manipulated Steganography Is Hard to Spot,Limited Interaction with Steganalysis Tools Driven by AI, insufficient protection against attacks using AI-driven steganography.

NetworkMiner

NetworkMiner is a specialized tool for extracting information from networks, email attachments, and other digital sources. By performing advanced network traffic analysis, NetworkMiner saves time for cyber forensic teams.

Advantages of NetworkMiner

By using AI-powered analytics to deliver real-time network traffic analysis, anomaly identification, and predictive threat intelligence, Network Miner transforms cyber forensic investigations.[16] Improved threat detection, increased network visibility, and effective investigation are some of its benefits.

Limitations of NetworkMiner

Accuracy is compromised by problems with data integrity and quality. Threat forecasting and anomaly detection are impacted by algorithmic bias.Integration with various network topologies might be challenging. requirement for ongoing maintenance and updates. AI-driven decisions have little explainability. vulnerability to evasive tactics and hostile attacks.

FTK (Forensic Toolkit)

FTK is a comprehensive toolkit providing advanced data analysis, password recovery, file decryption, and network data analysis.

Advantages of FTK

There are many advantages to combining artificial intelligence (AI) and forensic toolkit (FTK) in cyber forensic analytics. By automating the processing and analysis of massive datasets, it improves speed and efficiency while cutting down on inquiry times. By recognising and detecting possible evidence, AI-powered algorithms increase accuracy while reducing human error.

Limitations of FTK

A number of difficulties arise when integrating FTK with artificial intelligence (AI) in cyber forensic analytics. [17]Poor data quality might result in false positives or erroneous AI-driven outcomes, while implementation complexity and expense may restrict accessibility for smaller organisations.

Paladin Forensic Suite

Paladin Forensic Suite is a Linux-based data recovery tool built on Ubuntu. Notably, it supports both 32-bit and 64-bit versions and requires no installation.

Advantages of Paladin Forensic Suite

Digital forensic analysis is revolutionised when Paladin Forensic Suite is integrated with artificial intelligence (AI). AI-enhanced processing shortens investigative times by speeding up the analysis of evidence. Data carving is enhanced by machine learning algorithms, which can also recover erased and

[16] Gupta, Rakesh & Neha Singhal, Application of Artificial Intelligence in Digital Forensics: Enhancing Investigation Techniques, 14 Journal of Indian Cyber Law 98, 100 (2022).

[17] Sharma, Aakash & Rajeev Tandon, Challenges in Using AI for Cyber Forensic Analytics in India: A Legal Perspective, 19 Indian Journal of Law & Technology 223, 228 (2021).

fragmented data. AI-powered search and filtering prioritises pertinent evidence while lowering false positives.

Paladin Forensic Suite Limitations

Paladin Forensic Suite with AI integration has drawbacks despite its advantages. These include possible biases in AI algorithms that affect the objectivity of investigations and the need for high-quality training data to guarantee reliable AI-driven conclusions. [18]Problems with interpretability and complexity occur when AI-driven analysis calls for specific knowledge. It can be difficult to integrate AI products from many providers.

Techniques Used in Computer Forensics

Several techniques are used in computer forensics, including cross-drive analysis, live analysis, deleted files recovery, stochastic forensics, and steganography.

Cross-drive analysis identifies and correlates information from multiple data sources or drives. Live analysis examines computers within the OS using forensic and sysadmin tools. Deleted files recovery techniques recover deleted files using specialized tools.

The Role of Artificial Intelligence in Cyber Forensics

Artificial Intelligence (AI) has revolutionized digital forensics by analyzing large volumes of evidence. [19]AI enhances data analysis, pattern recognition, anomaly detection, and automated evidence extraction and recovery.

Global Perspective on AI

Internationally, organizations are addressing AI's implications.

United Nations (UN) and AI

The UN promotes AI for social good and discusses AI's implications on human rights.

Organization for Economic Cooperation and Development (OECD) AI Principles

OECD's AI Principles focus on transparency, explainability, responsibility, accountability, and privacy.

European Union (EU) AI Regulation

EU's AI Regulation and GDPR ensure AI development aligns with European values, emphasizing data protection, privacy, security, transparency, and human rights.

Regional AI Regulations

The European Union (EU) establishes AI development standards, ensures data protection, and regulates AI deployment through EU's AI Regulation and GDPR. Similarly, the Asia-Pacific Economic Cooperation (APEC) promotes cross-border data flow, ensures privacy protection, and fosters cooperation. [20]The Association of Southeast Asian Nations (ASEAN) fosters AI adoption, enhances

[18] Patel, Karan & Ruchi Agarwal, AI-Powered Forensic Investigation Techniques: Future Prospects in Cybersecurity, 7 Journal of Computer Science & Applications 91, 95 (2020).

[19] Dhar, Vinay & Rishi Sharma, AI Algorithms in Cyber Forensics: Enhancing Data Recovery and Analysis, 8 Journal of Digital Forensics 112, 115 (2021).

[20] Malhotra, Preeti & Rohit Kapoor, Machine Learning Models for Cyber Forensic Investigations: A Review of Techniques and Applications, 29 Journal of Data Science and Analytics 67, 71 (2022).

digital economic growth, and encourages innovation, while the Gulf Cooperation Council (GCC) safeguards sensitive information, ensures data protection, and regulates AI deployment.

Challenges in AI-Driven Cyber Forensics

Cyber forensics has undergone a revolution thanks to the incorporation of Artificial Intelligence (AI), which has improved threat intelligence, incident response, and digital evidence processing. Nevertheless, there are a number of issues with AI-driven cyber forensics that need to be resolved.

Technical Difficulties

Data Integrity and Quality: [21]For AI algorithms to generate precise results, high-quality data is necessary. The integrity of an investigation is compromised by compromised data.

Algorithmic Bias and Fairness AI systems have the potential to reinforce prejudices, jeopardising the impartiality of investigations.

Interpretability and Transparency: The "black box" nature of AI models makes it difficult to comprehend how decisions are made.

Scalability and Efficiency: AI-powered solutions demand a lot of processing power, which could cause research to go more slowly.

Adversarial Attacks: The integrity of investigations can be jeopardised by the manipulation of AI systems.

The future of AI in cyber forensics

The future of Artificial Intelligence (AI) in digital forensics is poised for significant advancements, driven by emerging technologies and evolving research areas. As digital forensics adapts to increasing data complexity and volume, AI will play a pivotal role in enhancing forensic practices through five key developments. Firstly, advances in AI technologies, particularly machine learning algorithms, deep learning, and neural networks, will enhance AI capabilities. [22]Secondly, integration with quantum computing will revolutionize computational power, accelerating AI algorithms and enabling real-time analysis. Thirdly, ensuring data privacy and security will become increasingly important, addressing concerns related to data protection and ethics. Fourthly, interdisciplinary collaboration between AI researchers, forensic experts, and legal professionals will ensure AI tools meet forensic and legal standards. Lastly, AI's applications will expand into augmented reality, virtual reality, Internet of Things devices, and autonomous systems, providing forensic experts with enhanced tools to investigate emerging cyber threats and technologies.

The integration of Artificial Intelligence (AI) in cybersecurity has yielded significant advancements in threat detection, vulnerability management, malware analysis, user authentication, and password security. As AI-driven cybersecurity solutions continue to evolve, the importance of professionals possessing expertise in both cybersecurity and AI technologies will become increasingly crucial.

[21] Paul De Hert & Vagelis Papakonstantinou, *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*, 34 Comp. L. & Sec. Rev. 179 (2018).

[22] Obermeyer, Ziad, et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 Sci. 447 (2019).

CONCLUSION:

The integration of Artificial Intelligence (AI) in digital forensics marks a significant breakthrough, transforming the efficiency and accuracy of digital evidence analysis. AI brings numerous benefits, including efficient handling of vast data volumes, identification of intricate patterns and anomalies, automation of complex tasks, and enhanced investigation speed and effectiveness. Additionally, AI detects sophisticated cyber threats, revolutionizing the field. However, addressing algorithmic bias and opacity is crucial to ensure fair and accurate outcomes. Looking ahead, emerging technologies like quantum computing will amplify AI's analytical capabilities, while advancements in transparency and explainability will provide reliable forensic insights, driving continued innovation in digital forensics.

RECOMMENDATION AND FUTURE DIRECTIONS:

AI-powered cyber forensic analytics necessitates strategic developments to counter growing threats. Standardisation, investigator training, high-quality data, interpretable models, and teamwork are some of the main suggestions. Deep learning, graph neural networks, natural language processing, cloud-based solutions, real-time analysis, adversarial AI robustness, quantum computing, and human-AI cooperation are some of the future avenues that will be utilised. By putting these innovations into practice, threat detection, response times, and digital security will all be improved. This will make it possible for investigators to analyse complex data and fight cybercrime more successfully, which will eventually make the internet a safer place.

1. REFERENCES:
2. https://insights2techinfo.com/how-ai-is-revolutionizing-cyber-forensics/#google_vignette
3. https://medium.com@poojabhat344/what-is-digital-forensics-types-tools-and-techniques-cyberyami-8c6ec651ab36
4. https://www.cyberyami.com/blogs/what-is-digital-forensics-types-tools-and-techniques
5. https://rfppl.co.in/subscription/upload_pdf/single-pdf--ijfo-vol-16-no.2-p--59-62)-1715064931.pdf
6. https://www.craw.in/methods-techniques-of-cyber-forensics-best-cyber-security-institute-in-delhi/https://www.neurotechnology.com/megamatcher-biometric-criminal-investigation.html?gad_source=1&gclid=CjwKCAjw1NK4BhAwEiwAVUHPUDjEaa2OOBip8ywnv9d8spF4p5WQg63piioSqjWqdQUjKNcUYXQd9RoCqr4QAvD_BwE
7. https://www2.deloitte.com/us/en/pages/advisory/articles/forensic-analytics-in-fraud-investigations.html
8. https://www.sphericalinsights.com/reports/artificial-intelligence-in-forensic-science-market