International Journal of Scientific Research in Modern Science and Technology
ISSN: 2583 -7605 (Online)
© IJSRMST | Vol. 3 | Issue 5 | May 2024
Available online at: https://ijsrmst.com/
DOI: https://doi.org/10.59828/ijsrmst.v3i5.208

AI IN DIGITAL FORENSICS

Manasi Pritam Zirpe[1*], Shravani Santosh Potdar[1&], Harshali Rohit Kadaskar[2$]

[1]Department of Computer Science, Sarhad College Arts, Commerce, Science, Katraj Pune-411046

[2]Assistant Professor, Departmentof Computer Science, Sarhad College Arts, Commerce, Science, Katraj Pune-411046

Email: zirpemanasi@gmail.com[*] | shravanipotdar05@gmail.com[&] | harshalikadaskar@sarhad.in[$]

ABSTRACT

Writing a research paper on AI in digital forensics is important because it has the potential of emerging technologies in forensics.

AI and machine learning can transform digital forensics by increasing productiveness and perfection, allowing automated analysis of vast and complex data sets, which is essential as digital evidence grows in volume and complexity. Moreover, AI integration brings new challenges, which includes algorithmic biases and the want for robust validation strategies, which require cautious exam to ensure dependable and honest forensic practices. This research can also delve into the legal and ethical implications of AI, including privacy concerns and the effect of automatic choice-making, contributing to the improvement of pointers and standards. Additionally, it serves as an educational resource, selling know-how among practitioners, researchers, and college students. By exploring the intersection of AI with digital forensics, the studies foster move-disciplinary collaboration and innovation, and helps count on future traits and instructions inside the field.

Keywords: Future Proofing Forensic Practices, Intigration, Process, Benefits, Types, Tools.

Introduction:

Digital Forensics is a section of forensic science that relates to the identification, collection, examination, and revealing of any digital information hidden in different kinds of electronic devices usable using personal laptops, etc. as an investigation evidence against computer crimes, cyber - crime & cyber - related crime. In simple words Both Artificial intelligence (AI) and machine learning (ML), have started revolutionizing in the world of digital forensics. This software can analyze large data volumes, find trends, and predict future risks with better precision at a much faster rate.

Increasingly we are seeing large numbers of rapid threats linked to the capabilities offered by advanced threat development technologies. New malware threats are being developed constantly through these advancements, taking advantage of how easily they bypass the current threat detection systems. Examples of common cyber threats include Phishing Attacks and Social Engineering.

IJSRMST | Received: 10 May 2024 | Accepted: 16 May 2024 | Published: 18 May 2024

Phishing Attacks: In phishing attacks, cyber attackers send masquerade email messages to users to obtain financial or other significant credentials such as internet banking, Credit/Debit card numbers, and more.

Social Engineering: Attacks that use psychological manipulation to trick users into giving this vital info. These specialized social engineering practices are difficult to identify and therefore protecting users from them is a major challenge.

To successfully conduct their investigations, digital forensics experts must adhere to specific ethical codes. This includes keeping confidential information, avoiding conflicts of interest and maintaining ethical standards in their work. In the investigation process forensic analysts must remain unbiased. The examination and interpretation of evidence should not be influenced by any prejudiced or biased factors. Sometimes it is necessary to obtain consent for the collection as well as examination of digital evidence.

Future proofing forensics practices

Digital forensics, on the other hand, faces challenges in keeping up with the expanding volume and complexity of advanced prove. As more criminal exercises are conducted carefully, agents require to be prepared with the apparatuses and methods to collect, analyze, and protect computerized prove viably. This incorporates remaining overhauled on the most recent advances and understanding the lawful and moral perspectives of advanced investigations.

The future of advanced forensics will moreover be formed by headways in encryption and protection advances. As encryption gets to be more predominant, agents may confront challenges in decoding information and extricating prove. On the other hand, privacy-enhancing advances can make it more troublesome for agents to get to and analyze computerized prove. Striking the right adjust between security and the require for compelling computerized examinations will be a key challenge for the future.

Objective

They can really help by analyzing their digital trails to identify the perpetrators of a crime. It also helps trace the origin of the cyber attack to find a leaking source and connect the suspect to the crime scene. It supports law enforcement investigations and closes the book on criminal cases.

Digital Forensic Investigators have a keen interest in artificial intelligence, AI in general. This allows researchers to focus on other areas of research that require intelligence.

Automated AI searches enable more powerful deeper engagement with evidence. It can also improve file or content filtering and classification. Generative AI tools can quickly scan and display large libraries of images and videos.

BODY:

Future practices includes:

AI and Machine Learning: These technology play an essential position in cybersecurity by figuring out and stopping threats in actual time. Machine mastering can analyze large quantities of statistics for styles and anomalies, permitting companies to take instantaneous movement on capacity safety breaches

Internet of Things : As the quantity of IoT devices increases, so does the want for sturdy security measures to defend those connected gadgets and the records they generate Digital forensics plays a key position in detecting and addressing cyberattacks concerning IoT devices

Cloud security: The transition to cloud computing brings both challenges and possibilities in terms of safety. The need for stable cloud infrastructures and information safety keeps to develop, consisting of advances in encryption, authentication and get admission to control techniques.

Mobile Security: With smartphone utilization at the upward push, cell safety will remain a first-rate challenge. As cellular phones talk more and accumulate greater sensitive records, they'll come to be more frequent targets for hackers. Future problems will cognizance on robust safety features designed specially for cellular gadgets, together with advanced authentication techniques and steady app improvement practices

Two Step Verification: Traditional username-password combinations aren't sufficient to make sure protection. Biometric methods of authentication, such as fingerprints and facial detection, play an important role in finding a person's identity. Multifactor verification which combines exclusive authentication mechanisms (e.g., consumer-acknowledged, owned, and possessed), becomes more commonplace to decorate protection.

Cyber Reporting: Proactive risk reporting could be vital in figuring out and mitigating capability cyber threats. Organizations have increasingly depended on threat intelligence structures that use big data analytics and device learning to aggregate and examine risk intelligence from a couple of sources, providing early warning and perception into emerging threats around

These trends suggest that the cybersecurity and virtual forensics industry will evolve hastily to deal with the ever-growing cyber threats. Organizations and experts in this zone ought to be aware about those factors and adopt advanced technologies and quality practices to protect virtual belongings.

In end, cybersecurity and virtual forensics face many demanding situations in an increasingly more interconnected virtual world. Future traits in those regions could be fashioned with the aid of the evolving hazard surroundings.

Role of AI in Digital Forensic

Natural Language Processing (NLP): NLP techniques help extract meaningful information from textual content. AI can analyze chat logs, emails, or documents to identify sentiment, extract relevant content, and summarize content, making it easier for researchers to analyze large amounts of data

Threat analysing and protection : Agile digital forensics can use AI to identify and react to potential threats before they are compromised Machine learning models can analyze system behavior and network traffic over time internally to identify signs of malpractice or security breaches.

Propose new AI based Forencis technics

Increased accuracy and performance

1. **Automated analysis:** AI can automate common and time-consuming tasks, such as data sorting and preliminary analysis, to improve efficiency and reduce the chance of human error.

2. **Pattern recognition:** AI excels at identifying complex patterns and correlations in data, which increases the accuracy of forensic analysis by identifying correlations and anomalies that can be detected through manual analysis.

3. **Improve judgment**

Advanced Techniques: AI can use superior strategies along with deep gaining knowledge of for photo and video analysis, herbal language processing for statistics evaluation, and predictive analytics for predicting future threats grade.

Improved statistics restoration: AI can improve data recovery from corrupted or deleted files and reconstruct segmented facts, which is vital for keeping proof

4. **Scalability Flexibility**

Scalable answers: AI structures can scale to deal with increasing volumes of records and adapt to new forms of proof and evolving forensic necessities. Adapting new demanding situations: As virtual forensics faces new challenges, along with encrypted communications and incoming files, AI-based totally strategies may be advanced and adapted to better meet those challenges.

The Digital Forensics Process

Digital forensics is the process of relating, conserving, assaying and presenting digital substantiation.

Substantiation Identification

This includes relating substantiation of digital crimes on storehouse media, tackle, operating systems, networks and/ or operations. This is the most important and basic step.

Preservation: The first step is to preserve the found digital evidence so that it does not get lost over time. The maintenance of digital proof is very important.

Analysis: This includes the collection of digital evidence related to cybercrime that has been analyzed in order to determine the crime and the possible method by which the system was breached

Documentation: This includes proper documentation of the entire digital investigation, digital evidence, loopholes in the attacked system etc. so that the case can also be studied and analyzed in the future and successfully prosecuted.

Uses of AI in Digital Forensics

For years there has been interest in AI and fears that it is beyond human ability to process information and learn along the way. A.I. These combined capabilities recognize patterns, sort out anomalies, and contribute to insights to identify evidence and insights that might otherwise have been missed.

However, challenges such as lack of skills, interpretive capacity, and legal considerations need to be addressed.

AI’s ability to sift through large amounts of data can also enhance analytics and provide better insights into that data. The power of AI in analytics lies not only in identifying the aforementioned patterns, anomalies and trends, but also in the presence of subtle interactions and irregularities that traditional manual analytics can break ignored as well.

The automation and learning of AI simplifies time-consuming tasks such as data collection, analysis, and report generation, reducing the amount of time analysts have to devote to research If AI is used for simple common tasks a, researchers can spend more time discussing complex reasoning and problem solving aspects of each. More time can be spent on more valuable “big picture” activities such as hypothesis generation, decision-making, and planning.

A streamlined search and inspection process closes searches faster, reducing backlogs and budgets. Automated AI capabilities can help analytics teams resolve staffing challenges in the absence of trained personnel or restrictions.

AI applications in Digital Forensics

Artificial intelligence (AI) is transforming virtual forensics with its capacity to go looking, analyze and interpret complex digital evidence. One of the most essential features is that of a multimedia seek engine. Traditional forensic methods may be time eating and hard work extensive, specifically while coping with large datasets from more than one gadgets or cloud sources AI-powered tools can fast sift thru terabytes of records, pick out patterns, anomalies and proof of it applies a ways better than guide for instance , gadget getting to know algorithms s classified and prioritized, It can flag touchy records which include suspicious connections.

Another crucial use case is to decorate forensic photograph and statistics acquisition. A.I. Techniques along with deep studying permit you to reconstruct a corrupted file via studying from patterns inside the information, for this reason developing a clearer photo of what turned into inside the unique files Thus this functionality is specially beneficial in instances in which digital evidence has been intentionally destroyed or tampered with.

AI additionally enhances the ability to carry out predictive analytics and danger evaluation in virtual forensics. By studying historical facts and identifying tendencies, AI fashions can predict capability protection breaches or fraudulent activity. This proactive method lets in forensic investigators to implement preventive measures and respond efficaciously to threats. Additionally, AI can automate court reviews, supplying a comprehensive list of summaries of findings that facilitate quicker choice-making and support legal complaints.

Digital Forensic tools

In the early days of the development of digital forensics, experts had very little tools for analyzing digital evidence. It sparked several accusations that such an investigation could alter and destroy evidence. Disk and data capture tools can detect encrypted data and capture and preview information on physical drives;

File managers work with file analysis tools to extract and analyze disparate files;

Registry analysis tools obtain information about the user and their activities from the Windows Registry;

Internet and web analytics tools provide detailed information about traffic and monitor Internet user activity;

Email analytics tools are designed to analyze email content;

Mobile device analytics tools help extract data from mobile devices and from external memory;

The Mac OS analysis tool provides metadata retrieval and disk imaging from the Mac operating system;

Database forensics tools can analyze and process data and provide reports on activities performed.

Conclusion:

Digital forensics plays an important role in preserving evidence, detecting criminals, protecting corporate interests, helping in investigating cyber crime and facilitating legal proceedings As technology continues to evolve, digital forensics will only become more important in today's day to day life.

Digital forensics is an important tool for investigating potential incidents in today's digital landscape. But digital forensic professionals must be prepared to meet the challenges associated with this area, including the complexity and volume of digital data, rapidly advancing technologies, and the ethical and legal issues surrounding the collection and about preservation -By adhering to best practices for data and its handling, digital forensics professionals can help organizations protect their digital assets and prevent cyber crime.

References:

[1] Digital Forensics-Interpol. Retrived from https://www.interpol.int/en

[2] Wikipedia-Digital Forensics. Retrived from https://en.wikipedia.org/wiki/Digital_forensics

[3] Simple Learn-DIgital Forensics. Retrived from https://www.simplilearn.com/what-is-digital-forensics-article

[4] ResearchGate-Future Proofing. Retrived from https://www.researchgate.net/publication/350690159_The_imp

[5] ICSS India-Cybersecurity and Digital Forensics. Retrived from https://icssindia.in/blog/future-trends-in-cyber-security-and-digital-forensics

[6] BlueVoyant-Techniques. Retrived from https://www.bluevoyant.com/knowledge-techniques-and-tools

Cite this Article:

Manasi Pritam Zirpe, Shravani Santosh Potdar, Harshali Rohit Kadaskar, "AI IN DIGITAL FORENSICS" *International Journal of Scientific Research in Modern Science and Technology (IJSRMST), ISSN: 2583-7605 (Online), Volume 3, Issue 5, pp. 01-06, May 2024.*

Journal URL: https://ijsrmst.com/

DOI: https://doi.org/10.59828/ijsrmst.v3i5.208