AI-Assisted Digital Forensics for Automated Incident Investigation

Manya Parikh[1], Parth Talaviya[2], Deep Solanki[3] ,Jigar Gajjar[4]

Lok Jagruti Kendra University, Ahmedabad,India[1]
Lok Jagruti Kendra University, Ahmedabad,India[2]
TechD Cybersecurity Limited, Ahmedabad, India[3]
TechD Cybersecurity Limited, Ahmedabad, India[4]

manyaparikh23@gmail.com[1],talaviyaparth07@gmail.com[2],deepsolanki5799@gmail.com[3],cyberian.jg@gmail.com[4]

Abstract: Digital forensics has emerged in the scene as a necessary area in the present scenario of cybersecurity, due to the rising trend of dependence on digital infrastructure that is vulnerable to complex cyber-attacks. The rising level of digital evidence and its complexity has made it challenging for traditional methods of investigation to be efficient and scalable. In this context, Artificial Intelligence has emerged in the scene as a promising solution that can assist in enhancing forensic practices by facilitating fast data analysis, complex pattern analysis, and efficient analysis of large datasets. This will assist in the efficient identification of potential security incidents and will assist in enhancing forensic practices as a whole. However, the application of AI in digital forensics also has some critical points to be considered. The concerns of data integrity, transparency, privacy, and admissibility of evidence in courts imply that the developments in technology are not sufficient to ensure the accuracy and integrity of the same. The requirement of human intelligence in interpreting the findings, understanding the context, and ensuring that the forensic evidence is credible and defensible is required in this context. This paper explores the effects of AI on the evolution of digital forensic methods and also explores the challenges that are associated with the use of AI in digital forensic analysis. This paper explores the importance of achieving a balance where intelligent technology can support human expertise, leading to more efficient and accountable forensic processes in the digital era.

Keywords: Digital Forensics, Artificial Intelligence, Cybersecurity, Automated Investigation, Digital Evidence, Machine Learning, Threat Detection

I. INTRODUCTION

Digital forensic is a department of forensic science that focuses on the identification, maintenance, analysis and presentation of digital evidence in such a way that protects its integrity and admissibility in court. As the digitization of society is speeding up, electronic devices like smartphones, computers and cloud computing services have become the primary warehouse of information, and digital evidence has become a crucial component of modern investigations. According to Casey[1], sound forensic practice is essential for ensuring that evidence remains of security incidents in organizations, insider threats, and regulatory compliance activities. As noted by Garfinkel [3], digital forensics can be used to recreate events from a complex digital environment, allowing investigators to take informed legal and business actions. However the sheer volume of data and refinement of cyber-attacks have made traditional forensic practices time-consuming and hard to scale or identify the incident.

Artificial Intelligence (AI) has emerged as a transformative technology capable of addressing these limitations. By automating data analysis, detecting patterns and speeding up investigative workflows, AI-assisted digital forensics improve both the speed and accuracy of the incident investigators to manage large amounts of datasets efficiently while focusing on high value evidence.

A. Usage of Digital Forensics in Real Life

Digital forensics can be defined as the procedure of examining and featuring electronics evidence. It ensures that digital evidence is managed in an identical valid manner so that it can be accepted by a court law. According to Casey[1], it is crucial

to protect the integrity of evidence during forensic analysis. Carrier[2] describes structured forensic processes that help in the analysis of evidence.

http://doi.org/10.63766/spujstmr.26.000097

Fig. 1. AI Enhanced Digital Forensics Lifecycle

In practical applications, digital forensics helps the police in investigating cyber crimes like ransomware attacks, phishing attacks, malware attacks, identity theft, financial fraud and many more attacks. Organizations use digital forensics to investigate data breaches and insider threats. Garfinkel[3], states that digital forensics helps in the rebuilding of digital timelines, which helps in understanding the flow of events that happened in a network of interconnected systems. With the increasing use of digital devices in communication and business, digital forensics has become a crucial tool in both criminal and business justice.

B. Benefits of Artificial Intelligence

Artificial Intelligence (AI) is a kind of technology that enables machines and computers to simulate machine learning, and AI has ability to perform tasks which require human intelligence, such as learning, problem solving, decision making, predictions and awareness. According to Russell and Norvig[4], AI is the study of intelligent agents that explain their environment and act to achieve specific goals. Machine learning is a significant part of AI that enables systems to improve their performance through experience, as opposed to programming.

The benefits of AI are that several advantages exist, especially its ability to analyze large amounts of data in a short time and recognize patterns that are impossible for humans to recognize. According to Goodfellow et al.[5], deep learning is a significant breakthrough that enables accurate classification and prediction. Domingos[6], states that AI is essential in discovering hidden patterns in data, while According to Mitchell[7], states that adaptive learning models continually improve the accuracy of analysis. According to Jordan and Mitchell[8], they state that AI enables automation, which decreases human labor and errors.

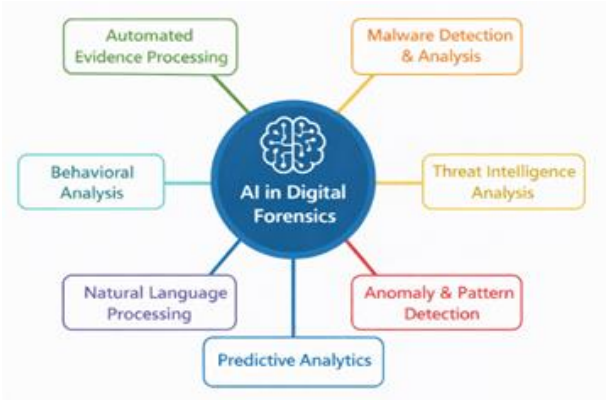

Fig. 2. Use of AI in Digital Forensics

C. Integration of AI into Digital Forensics Process

AI can be incorporated at various stages of the digital forensic process, such as data gaining, analysis, examination, and reporting. Standard digital forensic analysis involves the manual filtering of large amounts of datasets, but AI-based solutions can automatically classify files, detect anomalies, and point out areas of interest. As stated by Carrier and Spafford[9], the systematic nature of digital forensic work can be significantly assisted through automation in large scale digital environments.

Machine learning can be applied in the detection of unusual patterns in network traffic, while deep learning helps in malware detection and image processing. Singer and Friedman[10], state that AI enhances forensic preparedness by allowing for fast digital evidence triage. Quick and Choo[11], further clarify that intelligent automation enables faster response and investigation efficiency during cyber attacks. Moreover, AI can assist in providing a timeline. Such analysis is achieved by correlating data from various resources for visualization. of attack patterns.

However, such successful integration needs to be validated for forensic integrity and legal acceptability. Raghavan[12] highlights the need for AI generated results to be interpretable to enable the justification of conclusions in a court of law. When done correctly, AI-based solutions can help digital forensics shift from a relative field to a proactive investigative approach.

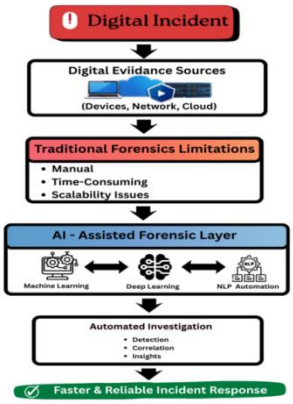

Fig. 3. High-Level AI-Assisted Digital Forensics Workflow

D. Benefits of using AI in Digital Forensics Compared to Traditional Methods

AI-powered digital forensics greatly enhances the efficiency and level of analysis of investigations compared to the standard approach. The traditional approach is largely dependent on human knowledge and expertise. However, this approach is time-consuming when dealing with large amounts of data. AI can process terabytes of data in a matter of minutes, thus reducing the backlogs of cases. Russell and Norvig [4] highlight that intelligent automation of tasks improves decision-making by reducing analytical overload.

Another important benefit of AI is accuracy. Machine learning algorithms identify hidden patterns and exceptions that human investigators may not be able to identify. Singer and Friedman [10] highlight that AI improves the ranking of evidence, ensuring that key evidence is analyzed first. Moreover, predictive analysis enables organizations to predict threats before they become major incidents. AI also allows for consistency in the forensics process. Quick and Choo highlight the aspect in their article[11], stating that the algorithmic analysis reduces the variability associated with the various human analyses. Moreover, AI facilitates the scalability of the forensics process in the cloud and distributed systems, which can be difficult to handle through conventional processes. Though AI processes need to be overseen by a human, it can add speed, accuracy, and scalability to the forensics process.

E. Concerns of using AI for Investigative Purpose

Although AI improves forensic analysis, it also presents a number of challenges. First, there is the problem of bias in algorithms, which can produce erroneous results if trained on incomplete data. Raghavan[12], suggests that such errors could compromise the validity of evidence. Another problem is the lack of transparency in many AI systems, which operate as “black boxes”, thereby hiding the logic used to arrive at certain concussions. Goodfellow et al.[5], highlight the need for understandability in many AI systems, especially in forensic analysis. There is also the problem of privacy in AI systems that handle personal information.Moreover, there is the risk of human forensic analysis being overshadowed by automation, which could lead to errors going undetected. Garfinkel[3], suggests that human forensic analysis is still necessary to verify the findings of automated systems.

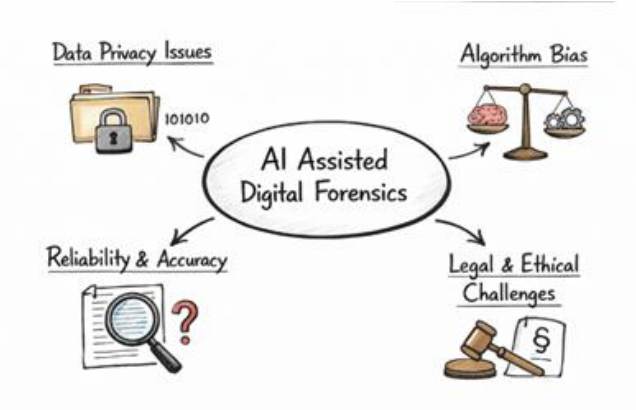

Fig. 4. Key concerns in AI assisted Digital Forensic Investigations

F. Analysis

The introduction implies that the AI technology is revolutionizing the aspect of digital forensics since it is able to improve the speed of the investigation, increase the accuracy of the analysis, and make the process quite efficient. However, there are underlying issues of transparency, objectivity, privacy, and some aspects of legal soundness. The above statements, therefore, suggest an argument that for there to be efficacious digital forensics, there is a need to integrate ethics into the investigation process. Essentially, digital forensics facilitated by AI technology is quite advantageous, but there is a need for the integration of accompanying expertise.

II. LITERATURE SURVEY

A. History of Digital Forensics and Evolution

Digital forensics started gaining its shape as a discipline in the 1980s due to the rapid spread of personal computers and the escalation of various cyber crimes. Investigations concentrated on recovering deleted information and examining individual computers for evidence. With the advancement of technology, investigators encountered increasing challenges of large amounts of information, different storage media, and complex systems. The contributions of Carrier [2] organized the frameworks of digital forensic investigation, which standardized the processes of investigation and made them reliable.

In the years that followed, computer forensics evolved to accommodate other devices, issues of cloud storage, IoT, and the vast and extensive enterprise systems. Casey [1] explains that modern computer forensics is based on the development and implementation of methods that preserve the integrity of the collected data and ensure their admissibility in court. The field continues to advance and develop to accommodate the changing technology and the evolving smarter cyber attacks.

B. Integration of AI for Digital Forensics and its Benefits

The concept of Artificial Intelligence in digital forensics is the talk of the town today, owing to the rate at which cybercrime is advancing and the amount of digital evidence we have to go through. Traditional forensic methodologies, although robust, are not efficient enough to keep up with the pace of the current world, particularly when dealing with massive amounts of data spread all over the place. AI comes to the rescue by using smart automation, filtering, and the speedy identification of the most relevant evidence.

A key advantage of using machine learning algorithms in any investigation process is that they are effective in detecting suspicious behavior. Through the use of machine learning algorithms, AI has made it significantly easier to reduce the workload of those in the investigation process. Quick and Choo [11] explain that the advantage of using AI in any investigation process is that it enhances forensic readiness. The usage of sophisticated attacks, however, makes it necessary for firms to be proactive in their approach as opposed to relying on reactive approaches.

Deep learning will enhance forensic work through sharpening the classification of malware, the verification of the biometric, and the analysis of multimedia content. According to Goodfellow and colleagues, neural networks can find complex patterns in high-dimensional data, and the forensic field can greatly benefit from this since every connection must be traced. Furthermore, Domingos introduced predictive modeling as an avenue where the investigator can make predictions concerning the various potential attacks.

Another important benefit of AI is that it can assist decisions. Intelligent systems are able to sift through key evidence to provide organized analyses instead of bombarding investigators with information. According to Russell &Norvig[4], this technology improves situational awareness, allowing investigators to make speedier decisions.

Although the benefits exist, the academic press cautions that we must approach AI-based interventions in forensics with caution. According to Raghavan [12], the "urgency" for "interpretable" AI builds on the "need for machine learning results that can be intelligently presented as evidence." Moreover, the "expertise of human analysts" would be required "to interpret the results that these algorithms compute." Nevertheless, the consensus in academic circles is that AI represents a "truly transformative" shift for digital forensics, which "speeds and broadens the reach of investigation in this increasingly complex digital world."

AI can enhance the scope of examination by allowing the investigator to peruse data across dispersed systems, including those found in the cloud environment, while allowing for ease of search. This is important due to the massive amounts of both organized and unorganized data being generated by organizations. The evolution of smart forensic investigation software has the capability to connect information from numerous sources, thus enabling the observer to view potential associations that were not initially recognized. This is not only important for ensuring the precision of investigation results but also makes the investigation process faster.

C. Comparison Table: Traditional vs AI Assisted Digital Forensics

TABLE I

EVOLUTION FROM TRADITIONAL TO AI-ASSISTED DIGITAL FORENSICS

Aspect	Traditional Digital Forensics	AI-Assisted Digital Forensics
Investigation Speed	Time-consuming and manual	Rapid automated analysis
Data Handling	Difficult to scale	Efficient handling of massive datasets
Analytical Capability	Limited pattern recognition	Advanced behavioral analytics
Accuracy	Dependent on examiner skill	Improved through machine learning
Error Probability	Higher risk of oversight	Reduced through automation

D. Real Life Use cases

Digital forensics has played a great role in the investigation of notable cyber incidents in the recent past. Notable is the Sony Pictures Entertainment 2014 breach, which involved the breach of internal networks and the leak of confidential and sensitive information. There was also a breach of operations on an across-the-board scale. To draw a picture of the breach and attempt to establish how it was conducted, various digital investigation techniques, such as malware analysis and network forensics were employed. As Casey in [1] puts it, a systematic digital approach was critical in the construction of a timeline.

At the same time, there was another parallel major event in the case of the Target Data Breach, which took place in 2013 when the attackers accessed the point-of-sale systems, thereby releasing millions of customer payment records. The detailed and thorough investigation into the breach led to the identification of the point where the breach was initiated and where the vulnerabilities were in the company's security system. According to Garfinkel, such a process not only revealed the events of the case but also taught the way forward in the process of defense.

Collectively, these cases underscore the growing reliance on advanced forensic capabilities within contemporary cybersecurity environments. As cyber threats continue to increase in sophistication and scale, the integration of AI-supported analytical tools is increasingly recognized as an important progression in strengthening investigative effectiveness.

E. Concerns of Using AI for Digital Forensics

Although there are a number of probable advantages to the use of AI in furthering forensic investigations, there are also some notable limitations and difficulties in adopting AI. There are many chances that AI might end up giving very erroneous leads if there is any bias in the algorithms used in the process. Raghavan in his paper highlights the need for continuous validation and testing.Explainability is another significant challenge to be overcome. For instance, explainability has to be provided in legal

investigations involving digital data, and many AI systems are "black boxes," as they cannot be easily interpreted. According to Goodfellow et al. [5], interpretable models should be developed to increase explainability and trust of AI systems.

The issue of privacy creates a new dimension to the complexities of applying AI in forensics. Analyzing various data has the potential to reveal personal information, thereby raising a number of questions about the usage of this information. Carrier highlights the importance of developing strict evidence-handling protocols to avoid any kind of abuse.On another note, overdependency on technology may lead to a loss of value in human expertise. It may also lead to a situation where crucial factors are ignored if one is over dependent on computer-generated data. As Garfinkel puts it, human experience should always be used to validate the outcome and ensure fair and reliable conclusions.

As a result, it is the consensus opinion of a significant number of researchers that there is a need to employ AI in a cooperative mechanism. That is to say, the AI assists the investigator as opposed to replacing the investigator. This therefore guarantees the requirement to 'align technological innovation with ethical governance' in AI use. AI can be effectively used to enhance the efficiency of the forensic process without compromising the admissibility of the digital evidence.

TABLE II

KEY ADVANTAGES OF AI-ASSISTED DIGITAL FORENSICS

Feature	Traditional Approach	AI-Assisted Approach
Evidence Analysis	Manual and time-intensive	Automated and faster processing
Pattern Detection	Limited by human capability	Identifies hidden patterns efficiently
Investigation Speed	Slower due to large data volumes	Accelerates investigative workflow
Decision Support	Based mainly on examiner judgment	Provides data-driven insights

III. ANALYSIS

TABLE III

IMPACT OF AI ON DIGITAL FORENSIC INVESTIGATION PROCESSES

Investigation Stage	Traditional Forensic Approach		Investigative Advantage
Evidence Identification	Manual device examination	Automated data discovery	Faster recognition of relevant evidence
Data Collection	Time-intensive acquisition	Intelligent filtering	Reduces unnecessary data handling
Evidence Analysis	Human-driven interpretation	Machine learning pattern detection	Improves analytical accuracy
Incident Reconstruction	Sequential review of logs	Automated timeline generation	Enhances event clarity
Threat Detection	Reactive investigation	Predictive analytics	Supports proactive response
Decision Support	Based on examiner experience	Data-driven insights	Strengthens investigative judgment
Reporting	Manually compiled findings	AI-assisted documentation	Accelerates case preparation

From the table above, it is clear that the integration of Artificial Intelligence in digital forensics helps a lot in speeding up the accuracy and speed of the investigations. With the ability to handle the boring and repetitive work of identifying complex patterns, Artificial Intelligence allows investigators to focus on the critical analysis part of the work rather than being tied down to the handling of the data. This helps in speeding up the timelines and making the reconstructed events more reliable. However, as we rely more on these automated systems, it is important to retain human review to preserve context and the value of the results.

TABLE IV

BENEFITS VS RISKS OF AI-ASSISTED DIGITAL FORENSICS

AI Capability	Investigative Benefit	Potential Risk
Automated Analysis	Speeds up evidence review	Overreliance on algorithms
Pattern Recognition	Detects hidden relationships	False positives/negatives
Predictive Modeling	Anticipates threat behavior	Model bias
Large-Scale Data Handling	Manages massive datasets	Privacy concerns
Decision Support	Enhances investigator efficiency	Reduced human interpretation

What the table above shows is that Artificial Intelligence is indeed changing the game when it comes to digital forensics. It is a technology that can speed up processes, increase accuracy, and expand our capabilities when it comes to data analysis. Automation is also a great help to investigators who have to deal with massive amounts of digital evidence. However, despite all the advantages that come with Artificial Intelligence, human oversight should still be at the forefront.

IV. LIMITATIONS

Artificial Intelligence has made a big difference in digital forensics, but its application is not without controversy. The quality of the results that you obtain using Artificial Intelligence is highly dependent on the training data that you are using. If the data is flawed, then the results are likely to be flawed as well. The other problem is the who and why of the algorithms. Lack of transparency in the algorithms can make it difficult to understand the reasoning.

The move towards AI in the forensic field requires a great deal of technical expertise and financial resources, which not all forensic departments have access to. On the other hand, the management of large amounts of sensitive digital data continues to raise privacy and data protection concerns. There is also the problem of automated systems failing to detect or failing to properly identify sophisticated, novel cyber threats, which may result in false positives or false negatives that can cast doubt on the results. In addition, AI software may not interpret evidence in the same context as a human forensic investigator, and the admissibility of AI-generated results in court may be raised.

V. CONCLUSION

Digital forensics has now become an integral part of the current cybersecurity landscape as organizations are faced with an ever-increasing number of complex and data-driven cyber events. The integration of Artificial Intelligence has greatly enhanced the process of investigation as it allows for faster analysis of data, facilitates pattern analysis, and helps experts handle large amounts of digital evidence. The power of technology has made the process of forensic analysis simpler and enabled investigators to focus more on high-level analysis and less on details.However, the growing application of AI also emphasizes the need for cautious application of technology. The issues of data integrity, explainability, privacy, and admissibility in courts indicate that technology alone is not sufficient to ensure the accuracy of results for the investigation process. The application of human expertise is of utmost importance to understand the results, the nuances of the context, and the integrity of the forensic process.The future of digital forensic investigation will be based on the complementary application of intelligent technology and human expertise. AI can be a useful tool in the process of investigation that can enhance accuracy and ensure trust, accountability, and integrity in the context of an increasingly digital world.

REFERENCE

[1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Amsterdam, Netherlands: Academic Press, 2011.
[2] B. Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley Professional, 2005.
[3] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.
[4] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Upper Saddle River, NJ, USA: Prentice Hall, 1995.
[5] I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
[6] P. Domingos, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. New York, NY, USA: Basic Books, 2015.
[7] T. M. Mitchell, *Machine Learning*. New York, NY, USA: McGraw-Hill, 1997.
[8] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.
[9] B. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, no. 2, pp. 1–20, 2003.
[10] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, U.K.: Oxford University Press, 2013.
[11] D. Quick and K. K. R. Choo, "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT + OSINT)," *Future Generation Computer Systems*, vol. 78, pp. 558–567, 2018.
[12] S. Raghavan, "Digital forensic research: Current state of the art," *CSI Transactions on ICT*, vol. 1, no. 1, pp. 91–114, 2013.
[13] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
[14] M. A. Ferrag, L. Maglaras, S. Moschoyiannis and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1347–1380, 2020.
[15] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.
[16] J. A. Kroll *et al.*, "Accountable algorithms," *University of Pennsylvania Law Review*, vol. 165, no. 3, pp. 633–705, 2017.
[17] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN Computer Science*, vol. 2, no. 3, pp. 1–21, 2021.
[18] H. Chen, R. H. Chiang and V. C. Storey, "Business intelligence and analytics: From big data to big impact," *MIS Quarterly*, vol. 36, no. 4, pp. 1165–1188, 2012.
[19] S. Mohurle and M. Patil, "A brief study of WannaCry threat: Ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.
[20] Digital Forensic Research Workshop (DFRWS), "A roadmap for digital forensic research," *Digital Forensic Research Workshop*, 2001.
[21] A. Behl and K. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, U.K.: Oxford University Press, 2017.
[22] S. Shinde, A. Kulkarni and S. Bhosale, "Cyber threat intelligence: Survey and research directions," *International Journal of Computer Applications*, vol. 179, no. 46, pp. 20–24, 2018.