International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Artificial Intelligence in Digital Forensics and Cyber Security

Vaishnavi Aher[1], Sujata Katkade[2], Tejaswi Jagtap[3], Sapna Bhusare[4]

[1]Ashoka Center for Business and Computer Studies, Savitribai Phule Pune University
Email: *ahervaishnavi24[at]gmail.com*

[2]Assistant Professor, Ashoka Center for Business and Computer Studies, Savitribai Phule Pune University
Email: *sujatak.acbcs[at]aef.edu.in*

[3] Assistant Professor, Ashoka Center for Business and Computer Studies, Savitribai Phule Pune University
Email: *tejaswij.acbcs[at]aef.edu.in*

[4] Assistant Professor, Ashoka Center for Business and Computer Studies, Savitribai Phule Pune University
Email: *sapana.acbcs[at]aef.edu.in*

Abstract: ***The rapid growth of digital technologies has led to a significant increase in cyber-crimes, making traditional digital forensic and cyber security methods insufficient to handle the volume, complexity, and speed of modern attacks. Artificial Intelligence (AI) has emerged as a powerful tool to enhance digital forensics and cyber security by enabling automated data analysis, intelligent threat detection, and efficient incident response. This paper explores the role of AI techniques in strengthening cyber security systems and improving digital forensic investigations. The study also discusses the applications of AI in intrusin detection systems, network security monitoring, malware analysis, and forensic evidence examination. Furthermore, the paper highlights key challenges associated with AI adoption, including data privacy concerns, model transparency, bias, and legal admissibility of AI-generated evidence. By examining current trends, applications, and limitations, this research emphasizes the potential of AI to transform digital forensics and cyber security while underlining the need for ethical frameworks and regulatory guidelines to ensure its responsible use.***

Keywords: AI-Driven Cyber Security, Automated Forensic Analysis, Malware Detection, Network Security Monitoring, Anomaly Detection, Incident Response, Ethical and Legal Issues in AI

1. Introduction

The rapid growth of digital technologies has led to an increase in cyber crimes and security threats, creating challenges for traditional digital forensic and cyber security methods. The large volume and complexity of digital data make manual and rule-based analysis time- consuming and less effective against modern cyber attacks. As cyber threats become more sophisticated, there is a growing need for intelligent and adaptive security solutions.

Artificial Intelligence (AI) has emerged as a powerful tool in digital forensics and cyber security by enabling automated data analysis, threat detection, and efficient incident response. AI techniques such as machine learning and deep learning help identify patterns, detect anomalies, and analyze digital evidence more accurately and quickly. Despite its advantages, the use of AI also raises concerns related to data privacy, transparency, and legal admissibility. This study focuses on understanding the role of AI in enhancing digital forensics and cyber security while addressing its challenges.

2. Literature Review

Recent studies highlight the growing role of Artificial Intelligence (AI) in strengthening digital forensics and cyber security frameworks. Researchers emphasize that AI has become essential due to the increasing complexity and volume of cyber threats and digital evidence. Traditional forensic and security methods are often slow and ineffective when dealing with large-scale data, whereas AI enables faster processing, automation, and intelligent decision- making. Several scholars note that AI improves the efficiency of cyber crime investigations by assisting in evidence identification, classification, and analysis.

A significant portion of existing literature focuses on the use of AI techniques such as machine learning and deep learning for detecting cyber threats and analyzing digital evidence. Studies show that machine learning algorithms are widely applied in intrusion detection systems, malware detection, and anomaly-based network monitoring. Deep learning models have been found effective in identifying complex attack patterns and zero-day threats. In digital forensics, researchers report successful use of AI in log analysis, memory forensics, and image and video forensics, where automated pattern recognition helps investigators reduce manual effort and investigation time.

Despite the advantages, many researchers discuss the challenges and limitations associated with AI in digital forensics and cyber security. One major concern identified in the literature is the lack of transparency and explainability of AI models, which affects trust and legal acceptance of AI-generated forensic evidence. Data privacy issues, biased training datasets, and high computational requirements are also highlighted as key limitations. Additionally, studies warn that cyber criminals may exploit AI technologies to develop more advanced and evasive attacks. Overall, the literature suggests that while AI significantly enhances digital forensics and cyber security, addressing ethical, legal, and technical challenges is crucial for its effective and responsible implementation.

3. Research Methodology

- Research is based on secondary data sources only.
- Data is collected from research journals, academic papers, books, conference proceedings, and trusted online sources related to digital forensics and cyber security.
- Relevant literature is systematically reviewed to understand concepts, tools, and applications in the field.
- Qualitative analysis is used to study the role of Artificial Intelligence in cyber security and digital forensic investigations.
- A comparative analysis is carried out to identify benefits, challenges, and limitations of existing techniques. Ethical, legal, and security issues related to digital evidence and AI usage are also examined.
- Findings are organized and interpreted to draw conclusions and suggest future research directions

4. Data Analysis

The collected literature was systematically reviewed to identify patterns, trends, and recurring themes concerning the application of AI in cyber threat detection and forensic investigations. The analysis reveals that Artificial Intelligence techniques, particularly machine learning and deep learning, are extensively applied in intrusion detection systems, malware detection, and anomaly-based network monitoring. Multiple studies indicate that AI- driven systems outperform traditional rule-based approaches by enabling faster detection of cyber threats and reducing false positives. AI models were also found to be effective in identifying complex attack patterns and zero-day threats through automated pattern recognition and predictive analysis.

In the domain of digital forensics, the analysis highlights the growing use of AI in log analysis, network traffic examination, memory forensics, and image and video forensics. The reviewed data shows that AI-assisted forensic tools significantly reduce manual effort and investigation time while improving the accuracy of digital evidence analysis. Automated classification and correlation of large volumes of forensic data were identified as key advantages of AI adoption.

The analysis further identifies critical challenges associated with the use of AI in digital forensics and cyber security. Recurrent concerns across the literature include lack of transparency and explainability of AI models, data privacy risks, biased training datasets, and legal issues related to the admissibility of AI-generated forensic evidence. These limitations highlight the need for ethical guidelines, regulatory frameworks, and human oversight in AI- based forensic and security systems.

Overall, the data analysis demonstrates that while Artificial Intelligence plays a transformative role in strengthening digital forensics and cyber security, its effective implementation depends on responsible use, transparency, and alignment with legal and ethical standards.

5. Findings

- Artificial Intelligence plays a significant role in enhancing digital forensics and cyber security by automating data analysis and improving the speed and accuracy of investigations.
- AI-based systems help security professionals identify suspicious activities and cyber threats more effectively than traditional rule-based methods.
- Machine learning and deep learning techniques are widely used in intrusion detection systems, malware detection, and anomaly-based network monitoring.
- In digital forensics, AI assists in analyzing large volumes of digital evidence such as logs, network traffic, images, and videos, thereby reducing manual effort and investigation time.
- The use of AI improves proactive threat detection and supports faster incident response in cyber security operations.
- Despite its advantages, the adoption of AI faces challenges such as lack of transparency in AI models, data privacy concerns, and biased training datasets.
- Legal and ethical issues related to the admissibility and reliability of AI-generated forensic evidence remain a major limitation.

6. Conclusion

This study concludes that Artificial Intelligence plays a vital role in enhancing digital forensics and cyber security by enabling faster, more accurate, and automated analysis of cyber threats and digital evidence. AI techniques such as machine learning and deep learning have proven effective in detecting complex cyber attacks, identifying anomalies, and supporting efficient cyber-crime investigations. The integration of AI has significantly improved the capability of security systems to respond proactively to evolving cyber threats.

The findings also indicate that AI-assisted digital forensic tools reduce manual effort and investigation time while improving the accuracy of evidence analysis. However, the study highlights several challenges associated with the use of AI, including lack of transparency in AI models, data privacy concerns, biased datasets, and legal issues related to the admissibility of AI-generated evidence. These limitations emphasize the need for careful implementation and human oversight.

Based on the findings and suggestions, it can be concluded that while AI offers significant benefits to digital forensics and cyber security, its effective use depends on ethical practices, proper training, robust legal frameworks, and transparent AI systems. Overall, the study underscores the importance of responsible adoption of Artificial Intelligence to strengthen cyber security measures and support reliable digital forensic investigations in an increasingly complex digital environment.

References

[1] Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.
[2] Jain, A. K., Flynn, P., & Ross, A. A. (2008). *Handbook of biometrics*. Springer.

[3] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[4] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cyber security: An overview, security intelligence modeling and research directions. *SN Computer Science, 2*(3), 173. https://doi.org/10.1007/s42979-021-00557-0

[5] Quick, D., & Choo, K. K. R. (2018). Digital forensic intelligence: Data reduction and data mining frameworks. *Digital Investigation, 24*, 1–15. https://doi.org/10.1016/j.diin.2018.01.003

[6] Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it*. Oxford University Press.

[7] Raghavan, S., & Parthiban, L. (2014). The effect of cyber crime on a bank's finances. *International Journal of Current Research and Academic Review, 2*(2), 173–178.

[8] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[9] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

[10] National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). NIST.