What are the major benefits and challenges of using artificial intelligence to automate and enhance the accuracy of digital forensics investigations in cloud environments?

Jasmyn Wilhelm

Writing Workshop 2

A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response

- Author:
  - Dunsin, Granem, Ouazzane, and Vassilev
- Discipline/Discipline Perspective:
  - Digital Forensics
- Thesis:
  - Notably, the use of AI in criminal investigations is essential, especially given the increasing prevalence of technology and cybercrime. (p. 1)
- Assumption:
  - AI and machine learning can improve the efficiency and accuracy of digital forensics investigations by identifying patterns that humans do not easily detect.
- Theory Name:
  - None mentioned.
- Key Concept(s):
  - AI and Machine Learning
  - Malware Classification
  - Memory Analysis Tools
- Method:
  - Feature Engineering
  - Classifier algorithms
- Phenomena Addressed:
  - Challenges of accurately classifying malware, limitations of current classifier tools, and memory analysis.
- Bias (If any):
  - Possible bias towards specific classifier tools.
  - Many benefits are discussed, but the limitations mentioned are minimal.

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International. Digital Investigation, 48, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges

- Author:
  - Malik, Bhatti, Park, Ishitaq, Ryou, and Kim
- Discipline/Discipline Perspective:
  - Information Technology and Cloud computing
- Thesis:
  - Not mentioned.
- Assumption:
  - Cloud computing exposes companies to security threats despite its multiple advantages.
- Theory Name:
  - Not mentioned
- Key Concept(s):
  - Cloud computing
  - Security in cloud-based digital forensics
  - Data management
- Method:
  - Analysis of surveys and platforms compared to offered cloud-based software.
- Phenomena Addressed:
  - The risks and benefits of cloud computing to analyze the safety of the information being held.
- Bias (If any):
  - None mentioned

Malik, A. W., Bhatti, D. S., Park, T., Ishtiaq, H. U., Ryou, J., & Kim, K. (2024). Cloud Digital Forensics: Beyond tools, techniques, and challenges. Sensors, 24(2), 433. https://doi.org/10.3390/s24020433

The Use of Artificial Intelligence in Digital Forensics and Incident Response (DFIR) in a Constrained Environment

- Author:
  - Dunsin, Ouazzane, and Ghanem.
- Discipline/Discipline Perspective:
  - Digital forensics or cybersecurity.
- Thesis:
  - Not clearly stated.
- Assumption:
  - Utilizing multiple tools and techniques can improve the effectiveness of forensic investigations.
- Theory Name:
  - Not clearly stated.
- Key Concept(s):
  - MADIK systems
  - Tool integration software (i.e. Wireshark, Volatility, Access-data, Scapy)
- Method:
  - Many integrations of tools to create a focused framework.
- Phenomena Addressed:
  - The complexity and volume of data in investigations along with the need for automated solutions to effectively manage the data.
- Bias (If any):

The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment | London Met Repository. (n.d.). https://repository.londonmet.ac.uk/7708/

What are the major benefits and challenges of using artificial intelligence to automate and enhance the accuracy of digital forensics investigations in cloud environments?

- Author:
  - Dunsin and Ghanem
- Discipline/Discipline Perspective:
  - Digital Forensics
- Thesis:
  - None mentioned
- Assumption:
  - Developing a framework using intelligent software agents (ISA) to assist in proof-related concerns in criminal courts.
- Theory Name:
  - None mentioned
- Key Concept(s):
  - AI
  - Digital forensics in criminal investigations
- Method:
  - CBR technique
  - Java Development Framework
- Phenomena Addressed:
  - The lack of evidence to determine sources in investigations relating to fewer convictions using the technology.
- Bias (If any):
  - None mentioned

The use of Artificial intelligence in Digital Forensics and Incident Response (DFIR) in a constrained environment. (n.d.). ResearchGate. https://www.researchgate.net/publication/361241108_The_Use_of_Artificial_Intelligence_in_Digital_Forensics_and_Incident_Response_DFIR_in_a_Constrained_Environment

An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data Heterogeneous Big Data

- Author:
  - Mohammed, Clarke, and Li
- Discipline/Discipline Perspective:
  - Digital Forensics
- Thesis:
  - An automated approach for analyzing heterogeneous data in digital forensics.
- Assumption:
  - The integration of tools and techniques can increase the capability to handle and analyze large volumes of data.
- Theory Name:
  - Not mentioned
- Key Concept(s):
  - Automation
  - Heterogeneous big data analysis
- Method:
  - A variety of computational tools and techniques for data extraction and analysis. Specific tools and details are not mentioned.
- Phenomena Addressed:
  - The challenges posed by the large volume of digital data and the need for more efficient and accurate tools.
- Bias (If any):
  - Not displayed.

Mohammed, H., Clarke, N., & Li, F. (n.d.). An automated approach for digital forensic analysis of heterogeneous big data. Scholarly Commons. https://commons.erau.edu/jdfsl/vol11/iss2/9/?utm_source=commons.erau.edu%2Fjdfsl%2Fvol11%2Fiss2%2F9&utm_medium=PDF&utm_campaign=PDFCoverPages