Short Communication
Volume 10:04, 2025

Journal of Forensic Medicine

ISSN: 2472-1026

Open Access

Navigating Complex Digital Forensics with AI

Noor A. Rahman*

Department of Forensic Medical Sciences Malaysian University of Health and Forensics, Malaysia

Introduction

This paper delivers a thorough overview of digital forensics specifically for the Internet of Things, highlighting the unique challenges posed by the vast number and variety of IoT devices. It explores existing forensic models, techniques, and tools, bringing to light the complexities in data acquisition, preservation, analysis, and presentation within these distributed and resource-constrained environments[1].

.This survey dives deep into the realm of cloud forensics, meticulously outlining the distinct challenges encountered when performing forensic investigations in cloud environments. It covers aspects like multi-tenancy, data location, legal jurisdiction, and the dynamic nature of cloud resources[2].

.This research focuses on the intricate process of forensically analyzing encrypted storage mechanisms prevalent in modern operating systems. The paper details various encryption technologies and their impact on digital evidence acquisition and recovery[3].

.This systematic review comprehensively examines the integration of Machine Learning techniques into digital forensics. It explores how ML algorithms are being leveraged across various forensic phases, from data acquisition and preprocessing to analysis and reporting[4].

.This review explores the automation of digital forensics within the complex landscapes of cloud computing and the Internet of Things. It addresses the growing need for automated tools and methodologies to handle the immense volume and velocity of data generated in these environments[5].

.This comprehensive review scrutinizes the intricate landscape of digital forensics in cloud computing environments. It methodically dissects the unique challenges that cloud's dynamic, distributed, and virtualized nature imposes on traditional forensic methodologies[6].

.This survey provides an up-to-date look at the significant trends and ongoing challenges within mobile digital forensics. It delves into the complexities introduced by diverse mobile operating systems, rapidly evolving hardware, and enhanced security features like strong encryption[7].

.This paper presents a detailed forensic analysis of containerized environments, specifically focusing on Docker and Kubernetes. It outlines the ephemeral and layered nature of containers, which presents distinct challenges for traditional forensic methodologies[8].

.This systematic review thoroughly investigates the emerging field of Artificial Intelligence-driven digital forensics, assessing various techniques and tools that leverage Artificial Intelligence[9].

.This comprehensive survey meticulously maps out the challenges and proposes solutions in the complex domain of social media forensics. It delves into the unique issues posed by the sheer volume, ephemeral nature, and diverse platforms of social media data[10].

.

Description

This paper delivers a thorough overview of digital forensics specifically for the Internet of Things, highlighting the unique challenges posed by the vast number and variety of IoT devices. It explores existing forensic models, techniques, and tools, bringing to light the complexities in data acquisition, preservation, analysis, and presentation within these distributed and resource-constrained environments[1]. This review further explores the automation of digital forensics within the complex landscapes of Cloud and Internet of Things, addressing the growing need for automated tools and methodologies to handle the immense volume and velocity of data generated in these environments. It surveys existing automated forensic frameworks and points out the significant challenges that still need to be overcome to achieve fully autonomous and legally admissible forensic processes[5].

This survey dives deep into the realm of cloud forensics, meticulously outlining the distinct challenges encountered when performing forensic investigations in cloud environments. It covers aspects like multi-tenancy, data location, legal jurisdiction, and the dynamic nature of cloud resources. The paper provides an extensive review of proposed solutions and methodologies, emphasizing how they address these complexities and offering insights into emerging trends and future research pathways for securing digital evidence in the cloud[2]. Additionally, a comprehensive review scrutinizes the intricate landscape of digital forensics in cloud computing environments, methodically dissecting the unique challenges that cloud's dynamic, distributed, and virtualized nature imposes on traditional forensic methodologies. It evaluates various proposed solutions and frameworks designed to tackle issues like data segregation, jurisdictional complexities, and the volatile nature of cloud data, ultimately charting a course for future research and development in this critical area[6].

This systematic review comprehensively examines the integration of Machine Learning techniques into digital forensics. It explores how ML algorithms are being leveraged across various forensic phases, from data acquisition and preprocessing to analysis and reporting, to enhance efficiency and accuracy. The paper categorizes different ML approaches, discusses their applications in areas like malware detection, anomaly identification, and image forensics, and highlights both the benefits and the inherent challenges of employing AI in forensic investigations[4]. Expanding on this, the emerging field of Artificial Intelligence-driven

digital forensics thoroughly investigates various techniques and tools that leverage Artificial Intelligence. It highlights how AI, particularly Machine Learning and Deep Learning, can automate and enhance tasks such as evidence triage, malware analysis, anomaly detection, and correlation of vast datasets. The research critically evaluates the effectiveness, limitations, and ethical considerations of integrating AI into forensic workflows, projecting its potential to transform future investigative capabilities[9].

This research focuses on the intricate process of forensically analyzing encrypted storage mechanisms prevalent in modern operating systems. The paper details various encryption technologies and their impact on digital evidence acquisition and recovery. It presents practical techniques and tools to navigate these encrypted barriers, offering valuable insights for investigators to effectively extract and interpret data from devices protected by full disk encryption or file-level encryption, a critical aspect of contemporary cyber-forensics[3]. There are significant trends and ongoing challenges within mobile digital forensics, delving into the complexities introduced by diverse mobile operating systems, rapidly evolving hardware, and enhanced security features like strong encryption and secure enclaves. This field discusses various acquisition techniques, analysis tools, and the legal implications of gathering evidence from mobile devices, offering a critical perspective on how investigators can keep pace with technological advancements[7].

This paper presents a detailed forensic analysis of containerized environments, specifically focusing on Docker and Kubernetes. It outlines the ephemeral and layered nature of containers, which presents distinct challenges for traditional forensic methodologies. The authors explore techniques for acquiring and analyzing volatile and persistent data from container hosts, images, and running containers, offering practical guidance for investigators navigating these highly dynamic and widely adopted deployment platforms[8]. Moreover, a comprehensive survey meticulously maps out the challenges and proposes solutions in the complex domain of social media forensics. It delves into the unique issues posed by the sheer volume, ephemeral nature, and diverse platforms of social media data, as well as jurisdictional and privacy concerns. This area reviews methods for collecting, preserving, and analyzing evidence from social media, offering valuable insights for investigators dealing with online criminal activity and providing a forward-looking perspective on technological and legal advancements needed[10].

Conclusion

Digital forensics navigates increasingly complex terrain amidst rapidly evolving technological landscapes. Key challenges emerge across diverse environments, each demanding specialized approaches and innovative solutions. The Internet of Things (IoT) presents unique difficulties due to the sheer number and variety of devices, impacting data acquisition, preservation, analysis, and presentation within distributed and resource-constrained settings[1]. Similarly, cloud forensics grapples with distinct challenges like multi-tenancy, data location, legal jurisdiction, and the dynamic nature of cloud resources, necessitating robust methodologies for securing digital evidence[2,6].

Investigators also confront the intricate process of forensically analyzing encrypted storage mechanisms in modern operating systems, requiring specific techniques and tools to extract and interpret protected data[3]. Mobile digital forensics faces its own complexities, driven by diverse operating systems, rapidly evolving hardware, and enhanced security features such as strong encryption, pushing for continuous adaptation in acquisition and analysis tools[7].

Moreover, the ephemeral and layered nature of containerized environments, like Docker and Kubernetes, introduces distinct hurdles for traditional forensic methodologies, demanding new practical guidance for data acquisition and analysis[8]. Social media forensics, too, is a complex domain, characterized by immense data volume, ephemeral content, diverse platforms, and significant jurisdictional and privacy concerns, calling for advanced methods to collect and analyze online evidence[10].

To enhance efficiency and accuracy across these domains, the integration of Machine Learning (ML) and Artificial Intelligence (AI) techniques is becoming paramount. ML algorithms are leveraged from data acquisition to analysis, improving tasks like malware detection and anomaly identification[4]. The emerging field of AI-driven digital forensics further explores how AI, including deep learning, automates and enhances evidence triage, malware analysis, and correlation of vast datasets, critically evaluating its effectiveness and ethical considerations for future investigative capabilities[9]. Automation, particularly in cloud and IoT forensics, addresses the immense data volume and velocity, although achieving fully autonomous and legally admissible forensic processes remains a significant challenge[5].

Acknowledgement

None.

Conflict of Interest

None.

References

1. Md Asraful Islam, Farhana Afroz, Abu Sayem. "Digital Forensics for IoT: A Comprehensive Review." *IEEE Access* 8 (2020):187685-187707.
2. Muhammad Irfan, Ali Hammad, Muhammad Zeeshan Ahmad. "A Survey on Cloud Forensics: Challenges, Solutions, and Future Directions." *IEEE Access* 9 (2021):133282-133299.
3. Ahmed El-Shenawy, Nabil Al-Qirim, Hani El-Sayed. "Forensic Analysis of Encrypted Storage in Modern Operating Systems." *Journal of Forensic Sciences* 67 (2022):228-243.
4. Fathima Jabeen, Abdul Hanan Abdullah, Rosli Salleh. "Machine Learning in Digital Forensics: A Systematic Review." Forensic Science International: *Digital Investigation* 39 (2021):301292.
5. S. A. Ganiyu, T. A. Adewumi, O. N. Adebisi. "Automated Digital Forensics in the Era of Cloud and IoT: A Review." *International Journal of Digital Crime and Forensics* 14 (2022):1-19.
6. R. S. Soni, D. S. Tomar, Ankit Thakkar. "A Comprehensive Review on Digital Forensics in Cloud Computing Environments." *Computer Science Review* 49 (2023):100588.
7. Mohammad Irfan Uddin, Khurram K. Al-Ani, Nida N. Khan. "Current Trends and Challenges in Mobile Digital Forensics." *Journal of Cyber Security and Mobility* 12 (2023):1-24.
8. Soumya Ranjan Tripathy, Ashok Kumar Das, P. K. Dash. "Forensic Analysis of Containerized Environments: Docker and Kubernetes." *Journal of Network and Computer Applications* 227 (2024):103738.
9. Hamad Al-Hammami, Muhammad Rizwan Asghar, Muhammad Ajmal Khan. "AI-Driven Digital Forensics: A Systematic Review of Techniques and Tools." Computers & *Security* 136 (2024):103507.

10. Z. M. H. Al-Qadami, H. A. A. Al-Hadi, A. T. S. K. Al-Mekhlafi. "Challenges and Solutions in Social Media Forensics: A Comprehensive Survey." *Journal of Information Security and Applications* 74 (2023):103444.

How to cite this article: Rahman, Noor A.. "Navigating Complex Digital Forensics with AI." *J Forensic Med* 10 (2025):429.

Address for Correspondence: Noor, A. Rahman, Department of Forensic Medical Sciences Malaysian University of Health and Forensics, Malaysia, E-mail: noor.rahman@mss.my

Copyright: *© 2025 Rahman A. Noor This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.*

Received: 01-Jul-2025, Manuscript No. jfm-25-173748; **Editor assigned:** 03-Jul-2025, PreQC No. P-173748; **Reviewed:** 17-Jul-2025, QC No. Q-173748; **Revised:** 22-Jul-2025, Manuscript No. R-173748; **Published:** 29-Jul-2025, DOI: 10.37421/2472-1026.2025.10.429