Chapter 7
AI-Powered Behavioral Analysis in Digital Investigations

ABSTRACT

Behavior analysis, a discipline traditionally associated with psychology and criminology, involves studying patterns in behavior to understand and predict actions. In the realm of digital forensics, behavior analysis has gained significant traction due to the increasing complexity of cybercrimes and the vast amounts of data involved. This chapter delves into the role of AI-powered behavioral analysis in digital investigations, exploring its methodologies, applications, and implications for cybersecurity and forensic science.

1. INTRODUCTION

The exponential growth of digital data and the complexity of cyber threats have necessitated advanced tools and methodologies in digital investigations. Traditional methods of forensic analysis often fall short when faced with large-scale, dynamic, and multifaceted digital environments. To bridge this gap, Artificial Intelligence (AI) has emerged as a transformative force, particularly in the realm of behavioral analysis.

Behavior analysis, a discipline traditionally associated with psychology and criminology, involves studying patterns in behavior to understand and predict actions. In the realm of digital forensics, behavior analysis has gained significant traction due to the increasing complexity of cybercrimes and the vast amounts of data involved. This chapter delves into the role of AI-powered behavioral analysis

DOI: 10.4018/979-8-3693-2960-3.ch007

Copyright © 2025, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

in digital investigations, exploring its methodologies, applications, and implications for cybersecurity and forensic science.

2. EVOLUTION OF DIGITAL INVESTIGATIONS

Digital investigations have evolved significantly since the early days of computer forensics. Initially focused on data recovery and system reconstruction, the field has expanded to address complex cybercrimes and sophisticated attacks. The advent of AI has further revolutionized this domain, offering new paradigms for analyzing and interpreting vast amounts of digital evidence.

- **From Manual Analysis to Automation:** Traditional digital investigations were labor-intensive and required forensic experts to manually sift through data. This process was slow and prone to human error, limiting the ability to handle large datasets or respond in real-time. These methods are typically reactive, focusing on evidence recovery and analysis after an incident has occurred. The introduction of automated tools and scripts represented a significant leap forward, allowing for more efficient data processing and analysis. However, these tools were still limited by their reliance on predefined patterns and rules.
- **The Role of AI in Transforming Investigations:** AI has revolutionized digital investigations by introducing advanced capabilities for analyzing large volumes of data, identifying patterns, and predicting future behavior. Unlike traditional methods that rely heavily on human intervention, AI-powered systems can process and analyze data at large scale, uncovering insights that would be challenging or impossible to detect manually.

AI-enhanced techniques provide proactive capabilities, enabling real-time monitoring, threat detection, and predictive analytics.

- **Integration of Behavior Analysis and Digital Forensics:** Integrating behavior analysis with digital forensics offers a deeper understanding of the motives and actions behind digital crimes. By analyzing patterns of behavior, investigators can gain insights into the intentions of cybercriminals, identify potential threats, and improve the accuracy of forensic investigations. This integration enhances the ability to interpret digital evidence and link it to specific behaviors and intentions.

32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/ai-powered-behavioral-analysis-in-digital-investigations/370613

Related Content

Web-Based Child Pornography: Quantification and Qualification of Demand
Chad M.S. Steel (2009). *International Journal of Digital Crime and Forensics (pp. 58-69).*
www.irma-international.org/article/web-based-child-pornography/37425

A Study of Forensic Imaging to Evaluate “Unsanitized” Destination Storage Media
Gregory H. Carltonand Gary C. Kessler (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 329-335).*
www.irma-international.org/chapter/a-study-of-forensic-imaging-to-evaluate-unsanitized-destination-storage-media/252697

A Conceptual Methodology for Dealing with Terrorism “Narratives”
Gian Piero Zarri (2012). *Crime Prevention Technologies and Applications for Advancing Criminal Investigation (pp. 274-290).*
www.irma-international.org/chapter/conceptual-methodology-dealing-terrorism-narratives/66845

Tampering Localization in Double Compressed Images by Investigating Noise Quantization
Archana Vasant Mire, Sanjay B. Dhok, Naresh J. Mistryand Prakash D. Porey (2016). *International Journal of Digital Crime and Forensics (pp. 46-62).*
www.irma-international.org/article/tampering-localization-in-double-compressed-images-by-investigating-noise-quantization/158901

Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics
George Grispos, Tim Storerand William Bradley Glisson (2012). *International Journal of Digital Crime and Forensics (pp. 28-48).*
www.irma-international.org/article/calm-before-storm/68408