Chapter 5
Machine Learning in IoT and Mobile Device Forensics

Mahmoud Basharat
https://orcid.org/0009-0000-1859-5485
Capitol Technology University, USA

ABSTRACT

The increasing integration of the Internet of Things (IoT) and mobile devices in everyday life has led to significant advancements in the field of digital forensics. However, the complexity and volume of data generated by these devices pose challenges for traditional forensic methods. Machine learning (ML) has emerged as a powerful tool to address these challenges by enabling the automation of data analysis, anomaly detection, and pattern recognition in IoT and mobile device forensics. This chapter explores the role of machine learning in enhancing forensic investigations, with a focus on its application to IoT devices and mobile phones. It highlights various machine learning techniques, including supervised and unsupervised learning, deep learning, and reinforcement learning, and examines their potential in solving complex forensic cases. The chapter also discusses the ethical and legal considerations surrounding the use of machine learning in forensics, as well as its limitations and future prospects in the evolving landscape of digital forensics.

1. INTRODUCTION TO IOT AND MOBILE DEVICE FORENSICS

In recent years, the proliferation of Internet of Things (IoT) devices and mobile technologies has radically transformed how individuals and organizations interact with the digital world. With the increasing integration of smart devices into daily

DOI: 10.4018/979-8-3373-0857-9.ch005

life, ranging from smartphones and wearables to IoT-enabled appliances, the volume and complexity of digital data generated have expanded significantly. These developments present new challenges and opportunities in the field of digital forensics, particularly in the investigation of cybercrimes, data breaches, and other illegal activities. IoT and mobile devices serve as both sources and targets of digital forensics investigations, making it imperative to understand their unique characteristics and how they influence the forensic process.

IoT forensics pertains to the collection, analysis, and interpretation of digital evidence from interconnected devices that communicate over networks. These devices, which include smart home systems, industrial sensors, wearable health devices, and vehicles, often store and transmit sensitive data such as user behaviors, location information, and communication logs. Mobile device forensics, on the other hand, focuses on smartphones, tablets, and other portable devices that are commonly used for personal and business purposes. These devices hold critical evidence such as call logs, text messages, multimedia content, and application data, which are valuable in criminal investigations. Both IoT and mobile device forensics require specialized techniques for data extraction, preservation, and analysis, considering the proprietary nature of many devices and the constantly evolving technologies used in their design.

The complexities of IoT and mobile device forensics are compounded by issues such as encryption, data storage across cloud systems, and the sheer variety of devices and operating systems involved. Additionally, the sheer volume of data generated by IoT devices, combined with the frequent lack of standardization, makes it difficult for forensic experts to apply traditional digital forensics methodologies. For instance, IoT systems often lack the same level of logging and evidence-collection capabilities that are common in computer systems, necessitating the development of new tools and techniques for forensic investigation (Zangana et al., 2024; Zangana & Omar, 2020).

Recent advancements in artificial intelligence (AI) and machine learning (ML) have shown great potential in transforming IoT and mobile device forensics. AI techniques, such as machine learning-based anomaly detection, can help forensic investigators identify suspicious activities, correlate disparate data sources, and predict potential areas of interest for deeper investigation (Dunsin et al., 2024). These AI-powered tools can also automate tedious tasks such as data parsing, pattern recognition, and the extraction of valuable evidence from raw data, significantly reducing the time required for investigation and increasing accuracy.

The application of AI in digital forensics is not without challenges. Issues such as data integrity, the privacy of individuals, and the ethical implications of using AI-based tools in sensitive investigations must be considered (Bhawna & Mahajan, 2024; Jarrett & Choo, 2021). Furthermore, as AI and ML algorithms become