Chapter 12
Navigating Emerging AI Technologies and Future Trends in Cybersecurity and Forensics

Pranjal Khare
https://orcid.org/0000-0002-9937-9588
O.P. Jindal Global University, India

Vishambhar Raghuwanshi
https://orcid.org/0009-0009-1365-1850
Manipal University, India

ABSTRACT

Artificial Intelligence (AI) has transformed digital forensics and cybersecurity, enhancing efficiency and accuracy in combating cybercrime and analyzing evidence. This chapter will explore AI's capabilities in handling vast data, identifying patterns, reconstructing crime scenes, and detecting anomalies that have revolutionized investigations.. However, these technologies also pose challenges, including ethical concerns, algorithmic bias, privacy issues, and potential misuse. In cybersecurity, AI facilitates real-time threat detection, fraud prevention, and cross-border cooperation against cyberattacks. Despite these advancements, addressing challenges like international legal inconsistencies, transparency, and ethical implications is critical. As AI evolves, its integration into forensic science and cybersecurity holds immense potential to uphold justice and security, demanding balanced governance to ensure ethical and lawful applications.

DOI: 10.4018/979-8-3373-0857-9.ch012

INTRODUCTION

A specialized branch of forensic science known as digital forensics is a subspecialty that involves analysis of digital media in gathering, acquiring, examining, and through documented and authenticated methods, putting into evidence such digital information. Originally developed in the late 20th century to handle cybercrimes using very basic technology, digital forensics is proven to be a necessary course for managing the expansive field that contains technologies, methods and processes that are involved in crime investigation. In its simplest terms, digital forensics seeks to provide methods that make the evidence collected more residual and credible, and that's why it plays a central role in both justice and defense systems.

The roots of computer forensics date back to the early 1980s when personal computers started to become popular thereby accompanying new forms of computer related crime. During the early years of computing and computer crime investigation, the concepts of digital evidence and scientific investigation of the digital environment were in their infancy, and the two main branches of digital forensic tools, computer forensics and network forensics, consisted of little more than rudimentary techniques and methods for data recovery from hard drives and more basic structures like email systems and rudimentary networks. Nevertheless, the constant increase of digital storage space, mobility of technology devices, and the appearance of cloud-based technology have made digital forensics become broader and much more intricate. Today, it includes subdomains like computer forensics, network forensics, digital communications forensics, or mobile device forensics and multimedia forensics. This evolution is due to the emergence of novelties in the digital environment not only in technology but also in the ability of methodologies to incorporate developments of criminal practice (Gaona, 2024).

The distributed computing environment provided by the use of the internet and shift from separate systems that are difficult to connect make up a new age in digital forensic practice. Fraud including identity theft, hacking and espionage were on the rise and detectives had to design equipment for data mining. At the same time, the use of encryption technologies and anonymization tools around the world was a new problem, which forced forensic specialists to develop constantly. Digital forensics functions in an extremely diverse community, which requires investigators to detect secured communication, work with numerous terabytes of data, and consider the differences in the legal treatment of digital evidence among states.

Artificial Intelligence (AI) has become a revolution in cybersecurity and forensic science because it solves many problems related to the scale, complexity, and constant changes in the digital environment. For instance, in cybersecurity, machine learning and deep learning are employed to provide predictions of attacks in real time and thereby reduce risks significantly from the norms applied in legacy systems.