Chapter 8
Exploring Effective Strategies for Combatting Cybercrime and Intersection of IoT, Deep Learning:
Legal Standpoints on Progressive Data Analytics

Bhupinder Singh
https://orcid.org/0009-0006-4779-2553
Sharda University, India

Christian Kaunert
https://orcid.org/0000-0002-4493-2235
Dublin City University, Ireland & University of South Wales, UK

ABSTRACT

The Internet of Things (IoT) represents a network of interconnected devices that collect and exchange data, while deep learning, a subset of artificial intelligence involves algorithms that model high-level abstractions in data through neural networks. The fusion of these technologies has transformed various sectors, from healthcare and agriculture to smart cities and autonomous vehicles. However, this convergence has also created new avenues for cybercrime, posing significant challenges to data security and privacy. The combination of deep learning and the Internet of Things has resulted in new vulnerabilities that hackers may take advantage of in addition to creative uses. This chapter looks at legal approaches to

DOI: 10.4018/979-8-3693-9235-5.ch008

enhanced data analysis as well as practical methods for fighting cybercrime in the context of new technologies. With a focus on deep learning, legal frameworks and forward-thinking solutions, this study attempts to convey a thorough knowledge of the confluence of deep learning, cybercrime, and IoT.

1. INTRODUCTION AND BACKGROUND

The vast network of devices with sensors or actuators that are linked by wired or wireless networks is referred to as the Internet of Things (IoT) (Ziwei et al., 2024; Kumar, 2024). This technology has a significant influence on daily life since it integrates easily with a number of industries, such as healthcare, smart homes, and smart cities (Thapaliya & Sharma, 2023). Internet of Things (IoT) security encompasses the tools and strategies used to safeguard cloud-connected devices and the networks they utilize for communication (Djenna et al., 2023). Its primary objectives are to protect user data, prevent cyber-attacks, and ensure the seamless operation of devices (Awajan, 2023). The recent data breaches have highlighted the importance of prioritizing IoT security for manufacturers and developers (Attaran & Deb, 2018). The quick growth of IoT applications and devices brings substantial security and privacy issues, notwithstanding its advantages (Brotcke, 2022). Major problems now include node spoofing, illegal data access, and cyberattacks such as denial of service (DoS), eavesdropping, and intrusion detection (Abebe et al., 2020). Lately, significant developments in deep learning (DL) and machine learning (ML) have offered reliable ways to improve IoT device security (Elluri et al., 2023; Hagendorff, 2019; Singh & Kaunert, 2024). The term "Internet of Things" (IoT) describes a network in which different intelligent gadgets and things exchange data via the Internet (Thapaliya & Sharma, 2023; Dash et al., 2022). Globally, there are already 17 billion linked devices; of them, 7 billion are Internet of Things (IoT) devices not including computers, smartphones, or tablets. By 2025, it is predicted that there will be 75.44 billion IoT devices globally (Barocas et al., 2023; Narayana & Sreedevi, 2023; Mhlanga, 2021).

There are many applications in industries including healthcare, home automation, agriculture, transportation, and education that are greatly advanced by IoT technology (Pocher et al., 2023; Chen et al., 2018). As a result of ongoing technical developments and the expansion of application fields, IoT has grown into a suite of specialized solutions made to meet particular requirements (Tyagi et al., 2020; Cao et al., 2021). Within artificial intelligence, deep learning is a subfield of machine learning (Alazab et al., 2023). Artificial Neural Networks, which are intended to mimic the connection and functioning of neurons in the human brain, are used in it (Zhang et al., 2022; Singh, 2023; Lee & Shin, 2020). So, compared to other AI