Chapter 2
Impact of Artificial Intelligence and Machine Learning in Cloud Security

I. Eugene Berna
https://orcid.org/0000-0002-3066-6511
Bannari Amman Institute of Technology, India

K. Vijay
Rajalakshmi Engineering College, India

S. Gnanavel
https://orcid.org/0000-0003-2344-0482
Department of Computing Technologies, SRM Institute of Science and Technology-Kattankulathur, India

J. Jeyalakshmi
https://orcid.org/0000-0001-7545-6449
Amrita VishwaVidhyapeetham, India

ABSTRACT

The rapid advancement of artificial intelligence (AI) and machine learning (ML) technologies has had a significant impact on cloud security, as it has in many other sectors. This abstract examines how AI and ML are affecting cloud security, highlighting their major contributions, difficulties, and potential. Traditional approaches to cloud security provide improved threat detection, real-time monitoring, and adaptive defense mechanisms. These technologies are adept at processing enormous volumes of data, allowing them to spot trends, anomalies, and potential dangers that more traditional security measures would miss. In order to quickly identify and take appropriate action in response to unauthorised access, data

DOI: 10.4018/979-8-3693-1431-9.ch002

breaches, and other malicious activities, AI-driven systems can quickly analyse user behaviour, network behaviour, and system logs. It introduces complexity in the form of adversarial assaults, model interpretability, and data privacy issues. For users to trust AI-driven security systems and to comprehend their decision-making processes, openness of these systems is essential.

1. INTRODUCTION

An innovative tool called artificial intelligence (AI) has the potential to provide analytics and intelligence to defend against continuously evolving cyberattacks by quickly scanning millions of events and keeping an eye on a variety of cyberthreats in order to foresee issues and take appropriate action. As a result (K, 2023), there are numerous applications of AI that either assist human security personnel or completely automate them. There is an increasing trend towards using AI in cyber defence. Increased interest among academics in cybersecurity and AI has led to a plethora of studies addressing topics related to cyberidentification, cyberprotection, cyberdetection, cyberreaction, and cyberrecovery (Saini et al., 2023; Sudha & Akiladevi, 2022).

Cybersecurity policies, procedures, and technical measures are implemented to protect information and communication systems and the data they contain against compromise, unauthorised use or modification, and exploitation. Accelerating technical development and innovation, as well as the ever-evolving nature of cyber threats (K, 2023; Nassif et al., 2021), compound the difficulty of the challenge. In light of this hitherto unseen difficulty, AI-based cybersecurity tools have emerged to provide valuable assistance to security teams in efficiently mitigating threats and bolstering security. Due to the diversity of AI and cybersecurity, a standardised taxonomy is necessary for reviewing research on using AI to cybersecurity. Researchers and practitioners will benefit from having a shared knowledge of the technological processes and services that need to be enhanced using AI thanks to this standardised taxonomy shown in Figure 1.a.

Before AI and ML reach unfathomable levels of accuracy and efficiency, this special issue (Sarirete et al., 2022) is devoted to the study of them as aspects of data-driven innovation and digital transformation.An agenda and multidisciplinary research on AI and ML are required because of rising user expectations for technology and the benefits it provides to society (Lytras et al., 2021; Visvizi et al., 2020; Chui et al., 2020). The five main issues listed above should form the basis of any study proposal of this kind (Figure 1.b).

By DominikSowinsk state that, Cloud computing has been transformed by AI and machine learning (ML), which has improved performance, scalability, and