Chapter 5
Role-Based access Control (RBAC) and Attribute-Based Access Control (ABAC)

Javed Akhtar Khan
Gyan Ganga College of Technology, India

ABSTRACT

This chapter explores the profound impact of artificial intelligence (AI) and machine learning (ML) on the realm of cloud security. As organizations increasingly migrate their operations and data to cloud environments, ensuring robust security measures becomes paramount. The integration of AI and ML technologies introduces novel ways to enhance threat detection, prevention, and response in the cloud. This chapter delves into various aspects of this synergy, discussing the benefits, challenges, and future prospects of utilizing AI and ML for safeguarding cloud infrastructures. This chapter also presents the benefits, challenges, and future directions. This abstract underscores the transformative potential of AI and ML in fortifying cloud infrastructures and safeguarding sensitive information in the digital age.

1. INTRODUCTION

In the rapidly evolving landscape of modern technology, the integration of Artificial Intelligence (AI) and Machine Learning (ML) has proven to be a catalytic force, reshaping industries and redefining conventional paradigms. One such domain that has witnessed a profound transformation is cloud security. As organizations increasingly migrate their operations and data to cloud environments, the need to ensure robust protection against a spectrum of evolving cyber threats has become an imperative

DOI: 10.4018/979-8-3693-1431-9.ch005

of paramount importance. In this context, the symbiotic relationship between AI, ML, and cloud security emerges as a potent solution, capable of revolutionizing the way we safeguard digital assets in an interconnected world.

n this exploration, we delve into the impact of AI and ML on cloud security, investigating their multifaceted roles in fortifying the integrity, availability, and confidentiality of data and applications. From advanced threat mitigation to automated incident response, the potential of these technologies is vast. As we embark on this journey through the intersection of AI/ML and cloud security, we uncover the transformative potential that promises a safer and more resilient digital landscape.

1.1 Cloud Security Landscape

The "Cloud Security Landscape" presents a panoramic view of the challenges, considerations, and evolving dynamics surrounding the protection of data, applications, and services in the cloud. The cloud, by its very nature, involves data traversal across diverse networks and geographical boundaries, necessitating a comprehensive reassessment of traditional security measures.It encompasses:

I. **Shared Responsibility Model:** A fundamental pillar of cloud security, this model delineates the distribution of security responsibilities between cloud service providers and their clients.
II. **Threat Vectors and Attack Surfaces:** The expansive reach of cloud computing introduces novel threat vectors and widens the attack surfaces that malicious actors can exploit. This section dissects the potential entry points for threats and the techniques employed to exploit vulnerabilities.
III. **Data Confidentiality and Privacy:** Entrusting data to third-party cloud providers necessitates stringent measures to preserve confidentiality and privacy. Encryption, access controls, and data residency regulations play pivotal roles in safeguarding sensitive information.
IV. **Identity and Access Management (IAM):** As cloud environments host a multitude of users, devices, and applications, effective IAM is pivotal in ensuring authorized access and preventing unauthorized breaches.
V. **Cloud-Native Security Tools:** Cloud-native security solutions are designed to protect cloud environments specifically, often offering features like cloud configuration scanning and native integration with cloud providers' security tools.
VI. **AI and ML in Cloud Security:** Artificial intelligence and machine learning are being used for threat detection, anomaly detection, and automated response in cloud security.