IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, December 2025

Impact Factor: 7.67

AI-Driven Threat Identification and Response: Implications for Secure and Scalable Telecom Infrastructure

Shiva Kumara
Independent Researcher
University of Washington
reachkumaras@gmail.com

Abstract: *Identity Threat Response and Detection based on AI has become a crucial facilitator in the case of secure and scalable telecom infrastructure as networks progress to 5G, B5G, and highly virtualized networks. The growing popularity of cloud-native architectures, the scale of connecting a large number of devices, and the evolving pattern of access have greatly increased the attack space of identity-based threats. In this paper, a detailed overview of AI-driven Identity and Access Management (IAM) models in telecom ecosystems is provided based on authentication, authorization, and adaptive access control. It discusses how machine learning (ML) methods, supervised, unsupervised, and reinforcement learning (RL), can be used to identify identity abuse, insider threats, and abnormal behavior using user and entity behavior analytics (UEBA). The survey also examines AI-based identity threat response, mitigation, such as anomaly detection, automated incident response, privacy-preserving monitoring, federated learning and integration with identity governance and administration (IGA) systems. The paper presents the role of AI-enhanced IAM in enhancing real-time threat detection, operational risk reduction and resilience and confidence in next-generation telecom networks.*

Keywords*:* AI-Driven Identity Threat Detection, Identity and Access Management (IAM), Telecom Security, 5G/B5G Networks, Machine Learning Privacy-Preserving Security, User and Entity Behavior Analytics (UEBA).

DOI: 10.48175/IJARSCT-30567