An Autonomous AI/ML Framework for Threat Detection and Automated Response in Multi Cloud Environments

Research Area:

Artificial Intelligence, Machine Learning, Cloud Security, Cyber Threat Intelligence

Abstract / Proposal Summary:

The rapid adoption of multi-cloud architectures has increased the complexity of enterprise security management, leading to challenges in detecting and responding to evolving threats across diverse cloud environments. Current solutions rely heavily on manual monitoring, rule-based systems, and static configurations, which are inadequate for handling large-scale, dynamic workloads.

This research proposes the development of an autonomous AI/ML-driven framework for real-time threat detection and automated response across multi-cloud infrastructures (AWS, Azure, GCP). The framework will leverage unsupervised and reinforcement learning algorithms to identify anomalies within vast volumes of logs, telemetry, and API call data, while a response orchestration layer will autonomously mitigate detected threats through intelligent action policies. Evaluation will be conducted using multi-cloud datasets (e.g., CloudTrail, Azure Activity Logs). Metrics such as detection accuracy, false positive rate, and response latency will assess system performance.

This study will contribute a novel, explainable, and automated AI-based defense architecture, setting the foundation for autonomous cloud security operations (AutoSecOps).