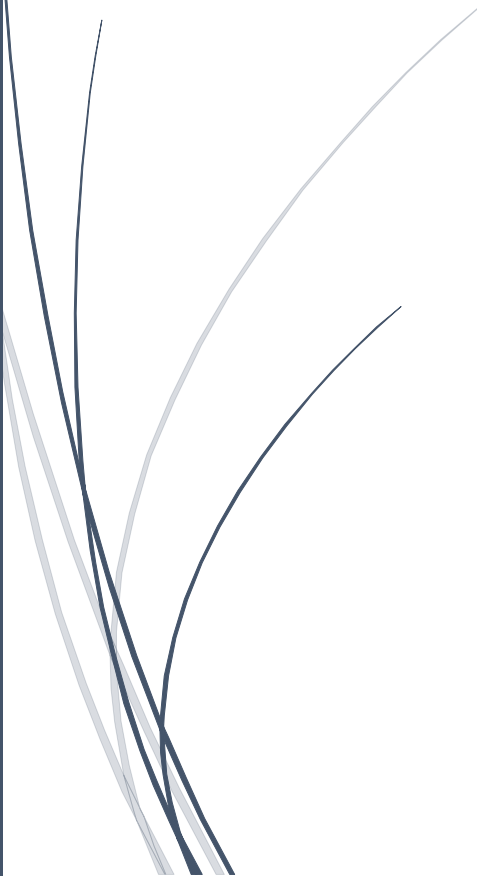


The logo consists of a dark blue vertical bar on the left and a blue arrow pointing right, containing the text "RADemics".

RADemics

End-to-End Integration of Reinforcement Learning and Deep Q-Networks for Autonomous Cyber Threat Remediation

Abstract line art consisting of several thin, curved lines in dark blue and light grey, originating from the bottom left and extending upwards and to the right.

A Suresh Kumar, S Mohan

RATHINAM TECHNICAL CAMPUS, NEHRU
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End-to-End Integration of Reinforcement Learning and Deep Q-Networks for Autonomous Cyber Threat Remediation

¹A Suresh Kumar, Assistant Professor, Department of Computer Science and Engineering, Rathinam Technical Campus, Coimbatore, Tamil Nadu, India. suresh.aacet@gmail.com

²S Mohan, Assistant Professor (SG), Department of ECE, Nehru Institute of Engineering and Technology, Coimbatore - 641105, Tamil Nadu, India. smohan2507@gmail.com

Abstract

This book chapter explores the end-to-end integration of Reinforcement Learning (RL) and Deep Q-Networks (DQN) for autonomous cyber threat remediation. It highlights the evolution of cybersecurity challenges and the potential of artificial intelligence to address these issues in real-time environments. By combining RL's decision-making capabilities with DQN's deep learning architecture, the chapter introduces a novel framework for detecting, analyzing, and mitigating cyber threats autonomously. The discussion covers the design, development, and deployment of RL-DQN systems, focusing on the scalability, generalization, and performance evaluation of such models in dynamic cybersecurity landscapes. Key challenges, including adversarial attacks and integration with existing security infrastructures, are critically analyzed. Ethical, regulatory, and societal implications of adopting AI-driven cybersecurity solutions are examined. This comprehensive analysis provides a strategic perspective on the future of autonomous security systems.

Keywords: Reinforcement Learning, Deep Q-Networks, Autonomous Cyber Defense, Cybersecurity, Threat Remediation, AI Integration.

Introduction

The rapidly evolving landscape of cyber threats continues to challenge traditional cybersecurity mechanisms, which often struggle to keep pace with increasingly sophisticated and dynamic attacks [1-4]. The rise of automated and AI-driven attack techniques has significantly enhanced the complexity of cyber threats, requiring more advanced and adaptive defense strategies [5]. In response to these emerging challenges, there was growing interest in leveraging artificial intelligence (AI) and machine learning (ML) to autonomously detect, analyze, and remediate cyber threats [6]. Traditional methods, which rely heavily on predefined rules and human intervention, often lack the agility and scalability needed to address the fast-changing nature of cyberattacks [7,8]. This chapter focuses on the integration of Reinforcement Learning (RL) and Deep Q-Networks (DQN) as an innovative approach to autonomous cyber threat remediation, providing an intelligent, adaptable, and self-optimizing solution [9].

Reinforcement Learning (RL) was a branch of machine learning that enables systems to learn from interactions with their environment to maximize long-term rewards [10]. In cybersecurity,

RL algorithms can autonomously learn optimal policies for detecting and responding to cyber threats by trial and error, enhancing their decision-making capabilities over time [11-13]. When coupled with Deep Q-Networks (DQN), which combine the strengths of deep learning and RL, this approach can significantly improve the ability of systems to handle complex, high-dimensional data and make real-time decisions [14,15]. DQNs utilize neural networks to approximate Q-values, enabling them to handle large-scale, dynamic environments where traditional RL methods struggle [16]. This integration forms a robust framework for autonomous threat detection and mitigation, capable of learning from past experiences and adapting to new, unknown attack patterns [17-21].

Autonomous cyber threat remediation refers to the use of intelligent systems to not only detect potential threats but also respond to them without human intervention [22]. This was particularly crucial in an era where cyber threats are not only more frequent but also more sophisticated, often outpacing human response times [23]. Autonomous systems equipped with RL and DQN can continuously monitor network traffic, identify vulnerabilities, and take preemptive or reactive measures to prevent attacks from succeeding [24]. The ability to make decisions in real-time, based on historical data and the evolving threat landscape, allows these systems to maintain high levels of security while minimizing the need for manual oversight [25]. By automating response actions, organizations can reduce the burden on cybersecurity teams and mitigate potential damage from emerging threats.