Chapter 2
Reinforcement Learning Approaches in Cyber Security

Ehtisham Safeer
UIIT, Pakistan

ABSTRACT

Reinforcement learning (RL) allows defense mechanisms to adapt to changing threats and has shown promise in tackling cyber security issues. This study presents a thorough introduction which includes foundations, uses, and difficulties to RL in cyber security. The efficacy of RL in making decisions is also emphasized in the introduction. Then the foundation for comprehending RL's use in cyber security, the fundamentals of the technology, and algorithm classifications is clarified. The study then delves into a number of RL applications in cyber security. Then a number of RL applications in cyber security and issues in RL is discussed. Along with prospects for improving cyber security safeguards through the application of RL methodologies, to successfully manage increasing cyber threats, future research directions are proposed with the integration of blockchain technology and generative adversarial networks (GANs). This work emphasizes the importance of RL in supporting cyber security and research to improve cyber defenses.

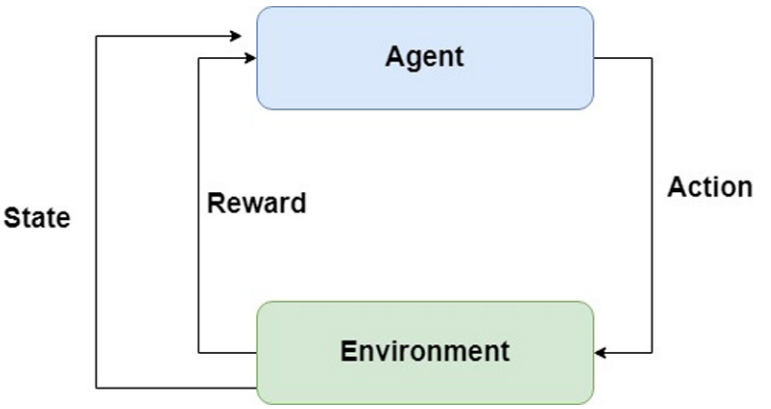
DOI: 10.4018/979-8-3693-5415-5.ch002

I. INTRODUCTION

A. Overview of Reinforcement Learning in Cyber Security

RL in machine learning makes decisions that refer to strategies for enhancing performance via trial and error (Qi et al., 2022). RL techniques have shown to be quite successful in the last few decades in resolving challenging issues in a variety of industries, such as vision in computers, robotics, and gaming. Rejuvenation in RL is superior to that of human performance. The agent's capacity to automate features acquisition and complete end-to-end learning is credited with this method's effectiveness. RL is goal-oriented and hypothesis-based, and it occurs when events, observations, and incentives are employed as inputs (Nguyen et al., 2020).

Figure 1. Representation of the RL Model



As modern civilization becomes more dependent on Information Technology (IT) systems including autonomous ones malicious actors also aggressively take advantage of these systems. Indeed, cyber risks are always changing, and as per Gartner, attackers will possess the necessary skills to cause injury or even death to humans. Defense mechanisms must be able to quickly respond to the changing settings and dynamic threat landscape in order to prevent such accidents and reduce the multitude of hazards that can target present and future IT systems (Süzen, 2020).

RL is a unique kind of machine learning in which a collection of observations, actions, and incentives provides the input. RL stands for goal-oriented interaction-based learning. RL picks up knowledge from, and while interacting with, the outside world. It makes use of agents, or systems, that enhance performance in response to their interactions with the surroundings. Through interactions with their sur-