Chapter 4
Quantum Cryptography-Enhanced Cyber Security Intrusion Detection System APTs Attacks in Blockchain

Senthil G. A.
https://orcid.org/0000-0001-7442-5499
Agni College of Technology, India

R. Prabha
Sri Sairam Institute of Technology, India

P. Priyanga
RNS Institute of Technology, India

S. Sridevi
https://orcid.org/0000-0003-2227-4371
Vels Institute of Science, Technology, and Advanced Studies, India

ABSTRACT

The novel proposed in this paper aims to revolutionize cybersecurity within Blockchain systems by integrating Quantum Cryptography with federated deep reinforcement learning intrusion detection systems (IDPS). This pioneering fusion of cutting-edge technologies o ers a multifaceted defense mechanism against advanced persistent threats (APTs) while preserving the decentralized nature of Blockchain networks. Complementing Quantum Cryptography, federated deep reinforcement learning

DOI: 10.4018/979-8-3693-5961-7.ch004

enhances cybersecurity by deploying AI-driven intrusion detection systems across decentralized Blockchain nodes. This decentralized learning paradigm empowers Blockchain networks to adapt dynamically to evolving cyber threats, ensuring timely and e ective responses to malicious activities. Quantum Cryptography and federated deep reinforcement learning, the proposed framework defines strategy against sophisticated cyber-attacks, bolstering the resilience of Blockchain systems. Markov Decision Process is the reinforcement learning algorithm used in the proposed system that detects cyber-attacks and threats.

1. INTRODUCTION

The continually growing technological landscape raises a major concern: cyber-attacks. As our dependence on technology grows, so will the complexity and regularity of attacks. Standard security methods strain to stay ahead of Advanced Persistent Threats (APTs), which are stealthy breaches meant to gain long-term access to systems. This needs to take place toward a proactive and flexible cybersecurity approach (Shiri I et.al., 2022). This quantum leap in encryption is accompanied by the notion of the Federated Deep Reinforcement Learning Intrusion Detection System (IDS), a powerful cyber threat protection mechanism. This approach enables devices to interactively build intrusion detection models while maintaining data privacy, which is critical in today's hyperconnected environment. With its capacity to adapt and change in real-time, the Federated DRL IDS provides a powerful line of protection for Advanced Persistent Threats (APTs) as well as complex intrusions that traditional security measures frequently fail to detect.

Likewise, the use of blockchain technology strengthens the system by offering a safe platform and sharing information about threats among enterprises (Hasan K. F et. al., 2024). This multi-layered approach strengthens digital communication channels while also laying the framework for an anticipatory and proactive cybersecurity ecosystem. In this dynamic landscape where cyber threats loom large and traditional defences fail, the coming together of Quantum Cryptography, Federated Deep Reinforcement Learning IDS, and blockchain technology provide a beacon of hope—a beacon that reveals the path to a subsequent where digital communication is not only secure but unbreakable.

This article investigates the combined use of quantum cryptography, federated deep reinforcement learning intrusion detection system (FDLR-IDs), and blockchain technology can be coupled to create a revolutionary cybersecurity architecture (Abou El Houda et.al., 2022). Quantum cryptography ensure unbreakable communication channels, whereas FDLR-IDS uses distributed learning to improve threat detection while protecting user privacy. Furthermore, Blockchain enables organizations to