Chapter 14
Integration of AI and Quantum Computing in Cybersecurity: A Comprehensive Review

Shyamalendu Paul
https://orcid.org/0009-0008-1028-4867
Department of Computer Science and Engineering, Brainware University, West Bengal, India

Nobhonil Roy Choudhury
https://orcid.org/0009-0009-1046-7492
Brainware University, West Bengal, India

Bipradash Pandit
https://orcid.org/0009-0009-5076-1418
Swami Vivekananda University, West Bengal, India

Avrodeep Dawn
Brainware University, West Bengal, India

ABSTRACT

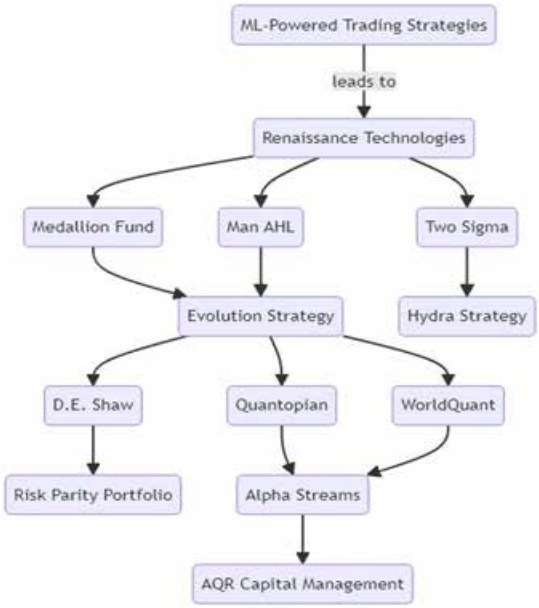
The rapid development of cybersecurity threats in the digital age has advance approaches to safeguarding critical assets and infrastructure. This review chapter research the integration of artificial intelligence (AI) and quantum computing like the transformative paradigm for magnifying cybersecurity resilience. There are countless opportunities for further study and development in the field of AI quantum cyber security, including the creation of quantum-safe AI algorithms. The importance of interdisciplinary collaboration, ethical deliberation, and transparency in advancing security is emphasized by the visualization of quantum communication protocols, ethical frameworks, and executive structures for AI quantum research, real-world applications, and successful implementations of AI quantum cyber security solutions. Overall, this review chapter bring out the transformative in the making of integrating AI and quantum computing in cybersecurity, offering insights into the challenges, opportunities, and ethical implications of AI-quantum cybersecurity solutions.

DOI: 10.4018/979-8-3693-7076-6.ch014

1. INTRODUCTION

In the rapidly evolving landscape of cybersecurity, the integration of artificial intelligence (AI) and quantum computing make an appearance as a promising approach to address the ever-growing complexity of threats and vulnerabilities. As organizations increasingly rely on digital systems and networks for evaluating performance, the need for robust cybersecurity measures has become paramount. Traditional cybersecurity approaches are often not enough in combating knowledgeable cyber threats, prompting the exploration of innovative technologies such as AI and quantum computing.

Figure 1. Overview of AI and quantum computing in cybersecurity



1.1 Background and Motivation

The development of digital technologies has revolutionized how people, organizations, and governments function, enabling previously unattainable levels of connectedness and efficiency. But there are also new difficulties brought about by this digital uprising, especially with regard to cybersecurity. Ransomware, phishing assaults, malware, and data breaches are just a few examples of cyberthreats that can seriously jeopardize the availability, confidentiality, and integrity of vital infrastructure and quickly accessible data.

The conventional paradigm for cybersecurity places a heavy emphasis on preventative measures like perimeter protection and signature-based detection. Although these strategies have shown some degree of success, they frequently find it difficult to keep up with the ever-evolving threat landscape. Cyber-