Chapter 9
Advancements in Quantum Machine Learning for Intrusion Detection:
A Comprehensive Overview

Esteban Payares
Universidad Tecnologica de Bolivar, Colombia

Juan Carlos Martinez-Santos
https://orcid.org/0000-0003-2755-0718
Universidad Tecnologica de Bolivar, Colombia

ABSTRACT

This chapter provides a comprehensive overview of the recent developments in quantum machine learning for intrusion detection systems. The authors review the state of the art based on the published work "Quantum Machine Learning for Intrusion Detection of Distributed Denial of Service Attacks: A Comparative View" and its relevant citations. The chapter discusses three quantum models, including quantum support vector machines, hybrid quantum-classical neural networks, and a two-circuit ensemble model, which run parallel on two quantum processing units. The authors compare the performance of these models in terms of accuracy and computational resource consumption. Their work demonstrates the effectiveness of quantum models in supporting current and future cybersecurity systems, achieving close to 100% accuracy, with 96% being the worst-case scenario. The chapter concludes with future research directions for this promising field.

DOI: 10.4018/978-1-6684-8422-7.ch009

INTRODUCTION

Quantum computing is a field of computing that promises remarkable results in solving complex problems like factoring and unordered search problems (Havenstein et al., 2019). Over the years, the progress made in quantum technologies has led to the beginning of a quantum revolution, opening up opportunities for numerous other applications. Among the exciting possibilities is the potential of quantum computers to enhance machine learning (Killoran et al., 2019). In addition, this technology has the potential to transform the way computers address previously intractable problems (Havl´ıˇcek et al., 2019).

Machine learning has become a powerful tool for discovering data patterns due to the increasing computing power and algorithmic advances. However, quantum systems can produce outlier patterns that are difficult for classical methods to detect efficiently. This fact leads to the assumption that quantum computers may outperform classical computers in machine learning tasks (Biamonte et al., 2017). Therefore, quantum machine learning (QML) can improve applications of conventional machine learning (ML).

In the era of noisy intermediate-scale quantum (NISQ) computing, these technologies explore the potential of developing advanced quantum systems. With modern machine learning, we can access generative modeling techniques wellsuited for the emerging landscape of NISQ hardware (Torlai and Melko, 2020). For example, quantum technologies can develop robust security systems against computer threats. However, the emergence of quantum technologies also poses a significant cybersecurity threat that requires us to rethink how we encrypt our data (noa,). Two decades ago, we learned that practically all public-key cryptography would be compromised by quantum computers (Mosca, 2018). Therefore, studying the behavior of various quantum security systems is critical to prepare for this problem as the industry slowly transitions to using quantum technologies. Quantum computing holds immense promise in numerous areas, including medical research, artificial intelligence, weather forecasting, and more.

ADVANCEMENTS IN QUANTUM MACHINE LEARNING FOR INTRUSION DETECTION SYSTEMS

Cybersecurity has become a significant concern with the increasing use of technology in our daily lives. Intrusion detection systems (IDS) are a crucial component in ensuring the security of computer networks by detecting and alerting the presence of any unauthorized access or malicious activity. However, the sheer volume and complexity of data that IDSs process make it challenging to detect new and sophisticated attacks. It is where quantum machine learning (QML) comes into play. QML has the potential to revolutionize the field of cybersecurity by offering a new approach to the processing and analysis of data that is faster and more efficient than classical computing. In this section, the authors will explore the recent advancements in QML for IDS and their potential to enhance the security of computer networks.

The paper “Quantum-Assisted Activation for Supervised Learning in Healthcare-Based Intrusion Detection Systems” proposes a novel method for IDS using quantum-assisted activation for supervised learning. The proposed method uses a neural network with a new activation function based on quantum mechanics that successfully capture patterns in the dataset while having less architectural memory footprint than classical solutions. The authors of this work claim that their method improves the performance of IDS and can achieve an accuracy rate as high as 99.9% (Laxminarayana et al., 2022).

Also, the work titled “Security Intrusion Detection Using Quantum Machine Learning Techniques” proposes a novel method for intrusion detection using quantum machine learning techniques. The authors