RADemics

Quantum Inspired Neural Networks for Next Generation Cybersecurity Threat Prediction and Response

Sreejith Sreekandan Nair, Nivetha
LEADING FINANCIAL FIRM, DALLAS, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY.

15. Quantum Inspired Neural Networks for Next Generation Cybersecurity Threat Prediction and Response

1Sreejith Sreekandan Nair, Independent Research Scholar, Leading Financial Firm, Dallas, Texas, USA.hisreenair@gmail.com

2Nivetha I, Assistant Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.nivethavcet22@gmail.com

Abstract

The integration of Quantum-Inspired Neural Networks (QINNs) into cybersecurity frameworks represents a transformative approach for addressing modern cyber threats. As traditional methods struggle to manage the complexity and high-dimensionality of data in dynamic environments, QINNs offer advanced capabilities for threat detection, response, and adaptation. By leveraging quantum-inspired algorithms, these neural networks enhance the detection of sophisticated attacks, such as advanced persistent threats (APTs), zero-day vulnerabilities, and insider threats. This chapter explores the core principles of QINNs, highlighting their potential in cloud security, intrusion detection systems (IDS), and real-time cybersecurity analytics. It examines the comparative advantages of QINNs over classical machine learning models, showcasing their superior adaptability, optimization, and processing efficiency. The chapter also discusses hybrid quantum-classical approaches, emphasizing their applicability in enhancing the resilience of cybersecurity systems. This work provides a comprehensive analysis of QINNs and their future impact on next-generation cybersecurity strategies.

Keywords:

Quantum-Inspired Neural Networks, Cybersecurity, Threat Detection, Cloud Security, Intrusion Detection Systems, Hybrid Quantum-Classical Approaches

Introduction

As digital transformation accelerates, organizations are increasingly exposed to sophisticated and evolving cybersecurity threats [1]. The rapid growth in internet-connected devices, cloud infrastructure, and the expansion of digital services have expanded the attack surface, making traditional security measures insufficient [2-4]. Cybersecurity systems today must contend with various malicious activities, including data breaches, Distributed Denial of Service (DDoS) attacks, Advanced Persistent Threats (APTs), and insider threats [5-7]. These attacks are more complex and difficult to detect with conventional methods that rely on fixed signatures or static rules [8]. Consequently, there was a pressing need for adaptive, scalable, and intelligent security solutions that can address these challenges in real-time [9,10].

Traditional cybersecurity strategies largely depend on rule-based detection, predefined heuristics, and signatures to recognize threats [11]. While effective against known attacks, these methods are often ineffective when faced with novel or zero-day threats [12]. The inability to anticipate or quickly adapt to new attack vectors leaves organizations vulnerable [13,14]. Classical machine learning (ML) models, while offering some degree of automation and pattern recognition, are often overwhelmed by the high-dimensionality of data in modern networks and can struggle to identify more complex or hidden attack patterns [15,16]. These models typically require extensive training datasets and are limited in their ability to generalize to unseen data, which results in false positives and negatives [17]. These limitations highlight the need for more advanced approaches to detect and mitigate cyber risks, especially in high-speed, data-rich environments like cloud computing and large enterprise networks [18-20].

Quantum-Inspired Neural Networks (QINNs) represent a significant advancement in the field of artificial intelligence and cybersecurity [21,22]. These networks are based on principles derived from quantum mechanics, such as superposition and entanglement, to enable more efficient processing of complex datasets [23]. By leveraging quantum-inspired algorithms, QINNs can perform computations at a much faster rate and process high-dimensional data more effectively than traditional classical neural networks [24,25]. The ability to identify patterns and correlations across vast amounts of data in real time makes QINNs ideal for tackling sophisticated cybersecurity threats. The probabilistic nature of quantum mechanics enables QINNs to better handle uncertainty, which was a common challenge in cybersecurity analysis, allowing for more accurate and reliable threat detection.