Chapter 4
Guardians of the Grid: Navigating Ethical Dilemmas and Regulatory Frameworks in Cyber Threat Detection

Rajeev Kumar
https://orcid.org/0009-0002-1655-6807
Independent Researcher, USA

Meetu Malhotra
https://orcid.org/0009-0009-7495-4484
Harrisburg University of Science and Technology, USA

C. Kishor Kumar Reddy
Stanley College of Engineering and Technology for Women, India

ABSTRACT

The rise of quantum and edge computing presents significant cybersecurity challenges, requiring a reassessment of security frameworks and ethical considerations. This chapter examines the risks involved in quantum and edge computing, exploring their impact on cryptographic resilience, data protection, and security vulnerabilities. The chapter also addresses ethical concerns, including privacy risks and AI-driven cybersecurity decisions. Existing regulations such as GDPR, CCPA, and NIST are evaluated for their limitations in addressing quantum and edge security threats. Cryptographic solutions like lattice-based encryption, homomorphic encryption, and secure multi-party computation are explored as potential countermeasures. Additionally, real-world case studies highlight national security threats, the impact of quantum cryptanalysis on financial systems, and edge security risks in smart

DOI: 10.4018/979-8-3373-3551-3.ch004

cities. The chapter concludes with policy recommendations and future research directions, emphasizing the need for post-quantum security standards and AI-driven regulatory compliance.

1. INTRODUCTION

The rapid evolution of computing technologies has brought about unprecedented advancements in cybersecurity, but also advanced and complex threats. The idea of two brand new digital security paradigms reshaping the way we perceive digital security are quantum computing and edge computing (Shor, 1999). While quantum computing possesses the potential to revolutionize cryptography by breaking conventional encryption algorithms, edge computing increases the attack surface by decentralizing data processing, creating diverse security challenges across heterogeneous devices and networks. However, due to these advancements, an extensive review of ethical challenges and regulatory concerns is needed to make sure that security measures follow technological changes. Furthermore, it is important to differentiate the types of cooperatives (co-ops) involved in this digital transformation, such as traditional consumer and worker co-ops versus emerging platform co-ops, as each presents unique governance, operational, and ethical considerations relevant to cybersecurity.

The core problem addressed in this chapter is the lack of adequate cybersecurity frameworks and policies that effectively respond to the emerging threats posed by quantum and edge computing technologies. Existing encryption methods are vulnerable to quantum attacks, while decentralized edge environments present new risks that traditional security models cannot fully mitigate. Additionally, there is insufficient clarity and guidance on managing the ethical and regulatory challenges introduced by these technologies, including how different types of co-ops can govern and secure their digital operations.

This chapter explores the ethical dilemmas and regulatory gaps associated with cyber threats in the quantum and edge computing domains, highlighting the need for proactive policy development and governance frameworks (Alagic et al., 2019; Satyanarayanan, 2017a).