Chapter 4
Comparative Analysis of Traditional vs. AI-Driven Network Security

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

Shyamalendu Paul
https://orcid.org/0009-0008-1028-4867
Brainware University, India

ABSTRACT

The increasing sophistication of cyber threats has driven the evolution of network security mechanisms. Traditional methods like firewalls, IDS, and antivirus software, which rely on established guidelines and signature-based detection, are now limited in addressing new and unknown threats. AI has introduced a new paradigm in network security, utilizing machine learning, behavioral analytics, and automated threat detection. AI-driven methods offer improved efficiency, accuracy, response time, adaptability, scalability, and cost-effectiveness. They analyze large data sets to detect patterns, recognize anomalies, and respond to threats in real time. While AI systems are costly and complex, their advantages in reducing false positives and handling zero-day attacks make them essential. The integration of AI with traditional methods can enhance security, combining strengths for a proactive defense against evolving cyber threats.

DOI: 10.4018/979-8-3693-9235-5.ch004

INTRODUCTION

Network security has been an essential component of information technology since the inception of computer networks. Ensuring the safety and integrity of data as it traverses these networks is critical for both organizations and individuals. Traditional network security measures, such as firewalls, intrusion detection systems (IDS), and antivirus software, have served as primary defence mechanisms against cyber threats for decades. These approaches, relying heavily on predefined rules and signature-based detection, have proven effective in mitigating known threats. However, the landscape of cyber threats has evolved dramatically, exposing the limitations of these traditional methods (Anderson & Brown, 2018; Harris & White, 2020).

The rise of sophisticated attacks, such as zero-day exploits and advanced persistent threats (APTs), has highlighted the inadequacies of traditional security measures (Zhao et al., 2021). These threats often bypass conventional defences by exploiting unknown vulnerabilities that are not covered by existing rules and signatures. The growing complexity and frequency of these cyber-attacks necessitate more advanced and dynamic security solutions. In response to these challenges, the cybersecurity industry has increasingly turned to artificial intelligence (AI) and machine learning (ML) to enhance network security (Jones & Patel, 2019).

AI-driven network security leverages advanced algorithms to analyze vast amounts of data, identify patterns, and predict potential threats. Unlike traditional methods, AI-driven approaches can adapt to new threats in real-time, providing a more proactive and dynamic defence mechanism (Nguyen & Lee, 2020). AI technologies, including machine learning, deep learning, and behavioural analytics, enable systems to learn from data, improving their detection capabilities over time and reducing the reliance on human intervention. This evolution represents a significant shift in how organizations approach network security, moving from reactive to proactive strategies (Tripathi et al., 2024).

The primary objective of this paper is to explore the differences, advantages, and limitations of traditional and AI-driven network security methods. By examining various aspects such as efficiency, accuracy, response time, adaptability, scalability, and cost-effectiveness, this study seeks to provide a comprehensive understanding of these two approaches.

Traditional Network Security Methods

Traditional network security methods have long been the cornerstone of network defence strategies. Firewalls, IDS, and antivirus software are some of the most commonly used tools. Firewalls act as a barrier between trusted and untrusted networks, filtering traffic based on predefined rules. They are effective in blocking unauthorized