Chapter 4
Smart Economy Cybersecurity: AI-Driven Risk Management in Digital Markets

Ali Bakhshi Movahed
https://orcid.org/0009-0006-4463-6838
Iran University of Science and Technology, Iran

Amirhossein Ghasemi Abyaneh
Kharazmi University, Iran

Masoud Khakbazan
Iran University of Science and Technology, Iran

Aminmasoud Bakhshi Movahed
https://orcid.org/0000-0003-3259-5419
Iran University of Science and Technology, Iran

ABSTRACT

Integrating AI, IoT, and cloud computing into smart economies has boosted digital efficiency but introduced cybersecurity vulnerabilities like AI-driven phishing, deepfake fraud, and malware. This study explores AI-driven risk management in mitigating such threats through a meta-synthesis of existing literature. Findings reveal that traditional security models are insufficient against adaptive AI attacks, necessitating autonomous solutions like self-healing networks, AI threat detection, and behavioral analytics. Regulatory frameworks also lag, highlighting the need for global standards and ethical AI governance. Critical gaps include limited predictive AI models, regulatory oversight, and standardized policies. The study proposes an

DOI: 10.4018/979-8-3693-4369-2.ch004

integrated AI cybersecurity framework combining innovation, compliance, and public-private collaboration. It concludes that AI-driven solutions and robust governance are vital for cyber resilience, urging future research on AI ethics, predictive risk models, and global standards to counter emerging threats.

1- INTRODUCTION

Smart economies are built upon digital transformation, automation, and the integration of advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), blockchain, and cloud computing (Peter Boolm, 2020). These technologies have significantly enhanced efficiency, streamlined financial transactions, and facilitated the expansion of global digital markets, thereby creating new opportunities for businesses and digital services (Dana et al., 2022). However, the increasing dependence on digital technologies has also introduced significant cybersecurity challenges. In particular, smart economies are highly vulnerable to sophisticated cyber threats, which have the potential to compromise sensitive data, disrupt financial markets, and erode public trust in digital systems (Hossain et al., 2023).

In recent years, cyber threats have escalated in both frequency and complexity. Cybercriminals and advanced threat actors leverage AI-driven automation and big data analytics to develop intelligent and highly targeted cyberattacks (Guembe et al., 2022). Some of the most prevalent threats in smart economies include autonomous phishing attacks, deepfake-based identity fraud, AI-powered malware, and blockchain exploitation (Wongwas et al., 2024). These cyber-threats result in significant financial losses for corporations and governments and introduce substantial legal and security challenges that require immediate attention and regulatory intervention (Darem, 2023).

Artificial intelligence enhances cybersecurity by enabling advanced threat detection, predictive analytics, and automated incident response mechanisms (Laxmi and Kumar, 2024). Machine learning algorithms and artificial neural networks can analyze behavioral patterns and detect cyber threats before they materialize (Alaa Hammad et al., 2024). Furthermore, autonomous cybersecurity systems, which leverage AI and big data analytics, can effectively identify and neutralize cyber threats, ensuring the protection of digital infrastructures (Ameedeen et al., 2024). Technologies such as self-healing networks, advanced cybersecurity analytics, and automated surveillance systems have demonstrated great potential in strengthening the security of digital economies challenges (Alijoyo et al., 2024).