Chapter 2
Artificial Intelligence in Cryptographic Evolution:
Bridging the Future of Security

Abdelraouf Ishtaiwi
Data Science and Artificial Intelligence, University of Petra, Amman, Jordan

Mohammad A. Al Khaldy
https://orcid.org/0009-0009-7502-4668
University of Petra, Jordan

Ahmad Al-Qerem
https://orcid.org/0000-0003-2187-6194
Zarqa University, Jordan

Amjad Aldweesh
https://orcid.org/0000-0001-9358-1323
Shaqra University, Saudi Arabia

Ammar Almomani
https://orcid.org/0000-0002-8808-6114
Skyline University College, UAE

ABSTRACT

The combination of artificial intelligence (AI) methods like machine learning with cryptography is essential for more intelligent and adaptable security measures. This chapter of the book outlines the convergence of AI with cryptography in detail. It summarizes the foundations of cryptography and the major AI techniques such as machine learning, deep learning, and evolutionary algorithms. The merging of AI & cryptography to maximize the potential of automated cryptanalysis that comes

DOI: 10.4018/979-8-3693-5330-1.ch002

in terms of exposing the vulnerabilities, state of the art ciphers that follow an improved cryptographic design, enhanced intrusion detection in the form of anomaly recognition and advanced secure collaboration protocols for safe collaborative learning without sacrificing the secrecy of information. Applications in domains like finance, healthcare, and internet of things (IoT), among others, are further proofs of the benefits of program crypto-AI techniques. In addition, adversarial actions against the candidate and ethical issues are also the challenges.

INTRODUCTION

In the last few years, there have been a number of enhancements in the AI approaches including machine learning and deep learning and other in the field of cybersecurity and cryptography. The dynamic nature of cyber structures therefore requires that AI has the ability to build sophisticated cryptographic systems capable of adapting to the latest emerging threats. This integration of both AI algorithms and cryptography can create advanced campaigns that could fill the leaking gaps of cyber security.

Cryptography is the fundamental component of the cybersecurity industry encoding data and preserving the integrity of online operations. Nevertheless, conventional cryptography is based on pre-defined mathematical functions that can be easily compromised amid increasing threats. The use of AI algorithms provides the perfect environment for continued learning of new cryptographic models. The innovation of automated systems is imminent and thus, AI cryptography is the future (Farzaneh & Samragh, 2021).

The traditional approaches of computer security have significantly shifted with such trends such as cloud computing technology, the call for the Internet of Things, and constant connectivity. There are more incentives and opportunities for the attackers to act effectively with automated and rapidly propagating threats (Xu et al., 2020). Security controls that were used in legacy systems cannot provide enough protection. AI can help provide predictive threat modeling, threat prevention, and quick detection of emerging threats.

This chapter aims to assess the relationship between artificial intelligence and cryptography. It introduces basic concepts; it describes advanced methods motivated by machine learning and deep learning and defines applications. The two issues explored are those of scalability, security, and ethical considerations. Therefore, it is the primary goal of the chapter to identify future research directions and to become a source of reference and learning for future growth in the domain.