Chapter 2
Future Outlook:
Synergies Between Advanced AI and Cryptographic Research

Dankan Gowda V.
https://orcid.org/0000-0003-0724-0333
BMS Institute of Technology and Management, India

Joohi Garg
https://orcid.org/0000-0003-1008-0350
Mody University of Science and Technology, India

Shaifali Garg
https://orcid.org/0000-0002-5647-3347
Amity Business School, Amity University, Gwalior, India

K. D. V. Prasad
https://orcid.org/0000-0001-9921-476X
Symbiosis Institute of Business Management, Symbiosis International University, India

Sampathirao Suneetha
Andhra University College of Engineering, Andhra University, India

ABSTRACT

Artificial intelligence (AI) and cryptography have recently made rapid progress respectively, forming a surprising mutual relationship. With the development of AI, it is now evolving to a point where an AI can study and even design cryptography systems. Cryptographic researchers are continually bringing out new ways to protect AI infrastructures from the ever-changing nature of attack, however. So, in this area, the authors examine the future topography and consider various possible ways these two breaking fields of study could meet up. Meanwhile, quantum computing and neuromorphic technology could push advanced AI further than any computer has been able to go before. On the one hand, cryptographic methods also help keep AI models open, safe, and within legal privacy regulations even facing attack. In a nutshell, cutting-edge AI and cryptography research are together reinventing the frontier of internet security within artificial intelligence. What lies ahead? This chapter lays out the problems and prospects of this exciting intersection.

DOI: 10.4018/979-8-3693-1642-9.ch002

Copyright © 2024, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

1. INTRODUCTION

In the rapidly evolving field of technology, AI and cryptography are a good case for such interdisciplinary cooperation. The impact of AI and cryptography combined As well as being fascinating reading in their own right, the developments described here will have many interesting outcomes.

The twenty-first century has witnessed unprecedented progress in AI and cryptography, and their convergence represents a pivotal moment in technological history. Cryptography is a perfect fit for artificial intelligence because to AI's pattern recognition, intelligent decision-making, and capacity to analyze massive volumes of data. Cryptography, on the other hand, has long been the guardian of data privacy and security, ensuring that sensitive information remains shielded from prying eyes. Artificial Intelligence (AI) is a specialized field within computer science focused on creating rational agents. These agents are designed to perceive their environment, process this information internally, and then select the most suitable action from various possibilities. Improving the agent's function of objective is the goal of this decision-making procedure (N. Hussain, A. A. J. . Pazhani, and A. K. . N, 2023). Once the agent decides what to do, it modifies its internal model of the environment and goes to work. Some of the many kinds of agents that fall under the umbrella of artificial intelligence are learning agents, logical agents, planning agents, antagonistic search agents, and search agents. Learning agents stand out because of their data-driven decision-making capabilities and use of machine learning methods. A set of data pairs is used to infer these activities.

At the heart of artificial intelligence (AI) lie Artificial Neural Networks (ANNs). ANNs are defined by their structure, which includes the amount of cells or perceptual neurons in each layer, the specific activation processes used by the neurons, the cost function for training, and the number and setup of densely interrelated hidden layers (Figure 1). The weights of the interconnections are adjusted during ANN training using gradient descent and backpropagation, which are based on the slope of the cost function within the weight space (as shown in Figure 2). The three most important areas of interest for artificial neural networks (ANNs) are input categorization, sequence learning, and function approximation. An important AI tool, ANNs can easily represent complex nonlinear functions thanks to their use of the nonlinear activation functions such as Sigmoid, Tanh and RELU.

1.1 The Convergence of AI and Cryptography

The role of AI in cryptography is broad and profound. The most notable aspect of this convergence is the advent of AI-driven encryption. Traditional encryption is based on algorithms and mathematical structures, effective but by no means adapted to today's computer environment. This aspect is handled by AI,as it can learn to adjust encryption techniques to the very purpose of protecting data (Shivashankar, and S. Mehta, 2016). But the convergence between AI and cryptography is truly a fascinating phenomenon. The two are becoming ever more intertwined, with each promoting the other in turn. The application of AI in cryptography has completely transformed how we think about data security and information protection. In fact, AI is the motor that drives cryptographic innovation to its limits.

For instance, AI sifts through data-traffic patterns to increase encryption on the fly. In this way, important information is well protected even when in transit. It can also improve key generation procedures, lowering the workload and time spent on encrypting. These AI-based encryption algorithms are constantly learning and evolving, staying one step ahead of potential attackers. Another major area where AI and cryptography overlap is that of the targeted use known as cryptanalysis. Breaking codes is secret

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/future-outlook/340971

Related Content

Towards Parameterized Shared Key for AVK Approach
Shaligram Prajapatand Ramjeevan Singh Thakur (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 239-256).*
www.irma-international.org/chapter/towards-parameterized-shared-key-for-avk-approach/244917

A Novel Approach of Symmetric Key Cryptography using Genetic Algorithm Implemented on GPGPU
Srinivasa K. G., Siddesh G. M., Srinidhi Hiriyannaiah, Anusha Morappanavarand Anurag Banerjee (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 193-213).*
www.irma-international.org/chapter/a-novel-approach-of-symmetric-key-cryptography-using-genetic-algorithm-implemented-on-gpgpu/244915

Quantum Cryptography: Algorithms and Applications
R. Thenmozhi, D. Vetriselviand A. Arokiaraj Jovith (2024). *Innovative Machine Learning Applications for Cryptography (pp. 119-144).*
www.irma-international.org/chapter/quantum-cryptography/340976

A Methodological Evaluation of Crypto-Watermarking System for Medical Images
Anna Babuand Sonal Ayyappan (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 458-479).*
www.irma-international.org/chapter/a-methodological-evaluation-of-crypto-watermarking-system-for-medical-images/244933

Securing the IoT System of Smart Cities by Interactive Layered Neuro-Fuzzy Inference Network Classifier With Asymmetric Cryptography
B. Prakash, P. Saravanan, V. Bibin Christopher, A. Saranyaand P. Kirubanantham (2024). *Innovative Machine Learning Applications for Cryptography (pp. 242-268).*
www.irma-international.org/chapter/securing-the-iot-system-of-smart-cities-by-interactive-layered-neuro-fuzzy-inference-network-classifier-with-asymmetric-cryptography/340983