RADemics

Neural Cryptographic Protocols Using Secure Multi-Party Computation (SMPC) for Encrypted Data Processing in AI-Driven Security System

Shivi Dixit, A. Ramamoorthy, K.B. Anusha
ACHARYA INSTITUTE OF GRADUATE STUDIES & SOLDEVANAHALLI, ST. JOSEPH'S INSTITUTE OF TECHNOLOGY, ADITYA INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Neural Cryptographic Protocols Using Secure Multi-Party Computation (SMPC) for Encrypted Data Processing in AI-Driven Security System

[1]Shivi Dixit, Assistant Professor, Department of Computer Application, Acharya Institute of Graduate Studies & Soldevanahalli, Bangalore, Karnataka, shivi2760@acharya.ac.in

[2]A. Ramamoorthy, Assistant Professor, Maths, St. Joseph's Institute of Technology, OMR, Chennai 600119. ramzenithmaths@gmail.com

[3]K.B. Anusha, Assistant Professor, CSE, Aditya Institute of Technology and Management, Tekkali. anushakb91@gmail.com

Abstract

The integration of Secure Multi-Party Computation (SMPC) and neural cryptographic protocols presents a novel approach to safeguarding data privacy in AI-driven security systems. This chapter explores the synergistic potential of these two advanced technologies, focusing on their application in privacy-preserving computations for real-time, large-scale AI systems. SMPC ensures secure collaborative computation across multiple parties without revealing sensitive data, while neural cryptographic protocols leverage machine learning to generate adaptable and efficient encryption schemes. The chapter delves into the theoretical foundations of both protocols, examines their performance benchmarks, and highlights the challenges and opportunities of combining them in AI environments. Key topics include optimizing computational efficiency, addressing scalability issues, and enhancing adversarial resilience in encrypted AI systems. By investigating the practical implications and use cases in domains such as secure federated learning, anomaly detection, and secure cloud-based AI applications, this chapter provides a comprehensive analysis of the future potential of SMPC and neural cryptography in advancing secure AI technologies. The findings offer valuable insights into developing scalable, efficient, and robust privacy-preserving solutions for next-generation AI-driven security systems.

Keywords: Secure Multi-Party Computation, Neural Cryptography, AI-driven Security Systems, Privacy-Preserving Computations, Performance Optimization, Federated Learning

Introduction

The integration of artificial intelligence (AI) with security systems has introduced significant advancements in threat detection, anomaly identification, and overall cyber defense. However, these developments have also raised concerns regarding the privacy and security of sensitive data processed by AI systems. The need for secure AI systems capable of safeguarding confidential information while performing complex computations has never been greater. Traditional cryptographic methods, though effective in securing data, often impose significant computational overhead, making them inefficient for real-time applications. In this context, two emerging technologies Secure Multi-Party Computation (SMPC) and neural cryptographic protocols offer promising solutions to address these challenges. SMPC allows multiple parties to jointly compute

functions over their inputs without revealing their individual data, while neural cryptographic protocols leverage machine learning to enhance encryption techniques, providing dynamic, adaptable security mechanisms for modern AI applications.

SMPC, as a privacy-preserving protocol, ensures that computations on sensitive data can be performed in a collaborative yet secure manner. This method prevents the leakage of private information during computation by distributing the task across multiple parties, each of which only has access to a fraction of the data. While SMPC guarantees data privacy, it often results in high computational costs due to the communication overhead and the need for complex encryption schemes. On the other hand, neural cryptographic protocols combine cryptography with artificial intelligence, utilizing deep learning techniques to generate encryption functions that adapt based on data and threat models. This ability to evolve encryption schemes offers a more flexible and efficient approach to securing data, particularly in dynamic environments where threats are constantly changing.

In the realm of AI-driven security systems, the integration of SMPC and neural cryptographic protocols holds immense potential. By combining the strengths of both technologies, it becomes possible to develop privacy-preserving AI models that are secure, scalable, and efficient. For instance, federated learning, which involves training machine learning models across multiple decentralized devices without sharing raw data, can benefit significantly from SMPC. By using SMPC in federated learning, participants can collaboratively train models without compromising the privacy of individual datasets. Neural cryptographic protocols can further enhance this process by ensuring that the data being processed remains secure throughout the training process. This combination of SMPC and neural cryptography has the potential to revolutionize privacy-preserving machine learning in cybersecurity applications, enabling organizations to leverage the power of AI while maintaining strict data confidentiality.