RADemics

Neural Network Ensembles Combined with Statistical Models for Enhanced Encryption Algorithms

Shobana D, W.Nancy, P R.Therasa.
Rajalakshmi engineering college, Jeppiaar Institute of Technology , R.M.K. Engineering College.

6. Neural Network Ensembles Combined with Statistical Models for Enhanced Encryption Algorithms

1Shobana D , Department of Mechatronics, Rajalakshmi engineering college,shobana.d@rajalakshmi.edu.in

2W.Nancy , Assistant Professor ,Department of ECE, Jeppiaar Institute of Technology nanruban07@gmail.com

3P R.Therasa , Associate Professor, Department of Computer Science and EngineeringR.M.K. Engineering College , RSM Nagar, Kavaraipettai , Thiruvallur District, 601206. prt.cse@rmkec.ac.in

Abstract

The rapid evolution of cryptographic systems has driven the need for innovative approaches to enhance data security, particularly in the context of modern technological landscapes such as Internet of Things (IoT) and edge computing environments. This chapter explores the synergistic integration of neural network ensembles and predictive statistical models, offering a promising paradigm for strengthening cryptographic solutions. Neural network ensembles, known for their pattern recognition capabilities, provide an adaptive layer of security, while statistical models offer robust analytical insights that improve encryption robustness. Together, these technologies address the growing demands for secure, efficient, and scalable encryption in resource-constrained environments. Special attention is given to the optimization algorithms required to harmonize these approaches, as well as their practical applications in real-world cryptographic systems. Additionally, the chapter examines the critical role of entropy analysis in fortifying key robustness and the challenges posed by distributed, dynamic networks in IoT and edge computing. The integration of these methodologies aims to bridge the gap between traditional cryptographic techniques and emerging security needs, paving the way for more resilient, adaptive encryption systems.

Keywords: Neural Network Ensembles, Statistical Models, Cryptographic Systems, IoT Security, Edge Computing, Encryption Optimization.

Introduction

The rapid expansion of the Internet of Things (IoT) and the increasing reliance on edge computing have transformed the landscape of digital communication and data processing [1]. As more devices become interconnected, the volume of data exchanged across networks continues to grow exponentially [2]. These advancements, while offering numerous benefits in terms of efficiency and accessibility, also introduce significant security risks [3]. Traditional cryptographic systems, while effective in many use cases, are often inadequate when applied to the unique challenges posed by IoT and edge environments [4]. In particular, resource constraints, such as limited processing power, storage, and energy supply in IoT devices, complicate the implementation of robust encryption schemes [5]. As cyber threats evolve and become more sophisticated, the need for adaptive cryptographic systems that can handle these challenges is more pressing than ever [6].

To address these challenges, recent research has explored the integration of machine learning techniques, specifically neural network ensembles, with statistical models to create more robust encryption solutions [7]. Neural network ensembles consist of multiple individual neural networks working together to enhance prediction accuracy and system performance [8]. By leveraging their ability to learn from large datasets, neural network ensembles can detect complex patterns in data, offering the potential to identify threats and vulnerabilities in real-time [9]. On the other hand, statistical models provide a deeper understanding of data distributions and statistical relationships, making them particularly valuable for improving key generation, encryption strength, and threat detection capabilities [10]. The integration of these two powerful approaches offers the potential to enhance both the security and efficiency of cryptographic systems [11].

The integration of neural network ensembles with statistical models offers a multifaceted approach to enhancing cryptographic systems [12]. One key advantage of neural networks is their capacity to learn and adapt over time, making them well-suited to environments where attack patterns are constantly evolving [13]. In contrast, statistical models can be utilized to measure uncertainty and identify anomalies in data that might signal an attack [14]. By combining the strengths of these two methods, cryptographic systems can become more resilient, offering both predictive capabilities and real-time adaptability [15]. This combination enables systems to dynamically adjust encryption protocols based on the detected threat landscape, improving their overall effectiveness [16].

Combining neural network ensembles with statistical models presents a series of challenges that must be addressed to ensure optimal performance [17]. One significant challenge is the complexity of integrating machine learning techniques into traditional cryptographic frameworks [18]. Neural network ensembles typically require considerable computational resources, and their training demands large datasets to achieve optimal performance [19]. In resource-constrained environments such as IoT, ensuring that these models can be efficiently deployed without significant performance degradation is crucial [20]. The integration of statistical models into the neural network framework requires careful consideration of how to balance model accuracy and computational efficiency [21]. Effective optimization techniques are essential to ensure that the benefits of both methods are fully realized [22].

In addition to the computational challenges, ensuring the robustness of encryption systems when combining these techniques is critical [23]. Encryption algorithms are often designed to withstand specific types of attacks, such as brute-force or side-channel attacks. These attacks are constantly evolving, requiring adaptive cryptographic solutions that can adjust to new threats. The integration of neural network ensembles with statistical models can help identify emerging attack vectors and adjust encryption protocols accordingly. For instance, neural networks can detect patterns indicative of a potential attack, while statistical models can assess the likelihood of the attack’s success. This collaboration between machine learning techniques and traditional cryptography offers a promising direction for building more resilient encryption systems that can defend against a broader range of threats.

The role of entropy analysis in strengthening key robustness was a key area of focus when integrating neural network ensembles and statistical models. Entropy was a measure of unpredictability or randomness, and it plays a vital role in cryptography by determining the strength of encryption keys [24]. A high level of entropy ensures that the encryption key is difficult to predict, thereby enhancing the security of the cryptographic system. By applying statistical models to analyze the entropy of encryption keys and incorporating neural network ensembles to adaptively adjust key generation processes, it is possible to strengthen key robustness and improve the overall security of the system [25]. This combination of techniques will enable cryptographic systems to better resist attacks, ensuring data confidentiality and integrity in dynamic, decentralized environments.