RADemics

Scalable Neural Network Models for High Dimensional Data Analysis in Cyber Defense Applications

Thivya Rajkumar, Puneet Sapra
VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY. RAYAT BAHARA UNIVERSITY.

12. Scalable Neural Network Models for High Dimensional Data Analysis in Cyber Defense Applications

1Thivya Rajkumar, Assistant Professor, Department of Artificial Intelligence and Data Science, Velalar College of Engineering and Technology, Thindal, Erode, Tamilnadu, India. thivyarajkumarvcet@gmail.com

2Puneet Sapra, Associate Professor, Department of Computer Science Engineering, Rayat Bahara University, Mohali, Punjab, India. puneetsapra91@gmail.com

Abstract

This chapter explores the application of scalable neural networks in analyzing high-dimensional data within cyber defense frameworks. As cyber threats become more sophisticated, traditional security systems struggle to keep pace with the volume and complexity of data. Scalable neural networks, particularly deep learning models, offer promising solutions for real-time threat detection, anomaly identification, and predictive defense mechanisms. However, training these models on high-dimensional data presents significant challenges, including issues of computational efficiency, model accuracy, and latency. This chapter delves into the fundamentals of scalable neural networks, key techniques for optimizing training with large datasets, and strategies to address data scarcity and imbalance. Additionally, it highlights advanced training methods, including transfer learning, hyperparameter tuning, and hardware acceleration, as well as the integration of edge computing for low-latency decision-making in critical applications. The research identifies key strategies for overcoming existing limitations and optimizing performance in dynamic, real-world cyber defense environments.

Keywords:

Scalable Neural Networks, High-Dimensional Data, Cyber Defense, Deep Learning, Latency Optimization, Transfer Learning.

Introduction

In today's increasingly interconnected world, cybersecurity has become one of the most critical concerns for organizations across various sectors [1]. The rapid growth of digital systems and the advent of IoT devices have generated vast amounts of data, posing significant challenges for traditional security models [2-5]. These models often struggle to keep pace with the sheer volume, velocity, and variety of data being generated [6]. As cyber threats continue to grow in sophistication, a more robust and scalable approach to defense was required [7]. This was where scalable neural networks, particularly those utilizing deep learning techniques, offer significant potential [8]. By harnessing the power of machine learning and artificial intelligence, scalable

neural networks can process vast amounts of high-dimensional data in real time, identifying patterns and anomalies thatotherwise go undetected by conventional systems [9].

High-dimensional data refers to datasets with a large number of features or variables, which was typical in many cybersecurity applications, such as network traffic analysis, intrusion detection, and anomaly detection [10-12]. The complexity of this data poses significant difficulties in terms of processing, storage, and interpretation [13]. A key challenge in working with high-dimensional data was the "curse of dimensionality," where an increase in the number of features results in exponentially larger data spaces, making it harder for traditional algorithms to perform effectively [14,15]. In cyber defense, this issue was amplified by the need to quickly analyze vast amounts of data to detect real-time threats [16]. Scalable neural networks, designed to handle these large and complex datasets, offer a way to overcome this challenge [17]. These models are capable of learning intricate patterns in the data that can be indicative of potential security threats, such as cyber-attacks or system vulnerabilities [18,19].

Training neural networks with high-dimensional data was a complex and computationally intensive task [20]. High-dimensional datasets often suffer from data sparsity, making it difficult for machine learning models to learn meaningful patterns without overfitting [21-23]. Additionally, the large number of features present in such datasets can significantly increase the training time and resources required [24]. Traditional neural network architecturesstruggle to scale efficiently when faced with such challenges [25]. To address these issues, various techniques such as dimensionality reduction, feature selection, and data augmentation have been developed to make the training process more efficient. For instance, methods like Principal Component Analysis (PCA) and t-SNE help reduce the number of features while preserving the key characteristics of the data.