RADemics

Spatiotemporal Deep Learning Models for Monitoring Cyber Threats in Surveillance Data Streams

Govindarajan Lakshmikanthan, 2Nanthini M
LEADING FINANCIAL FIRM, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY.

7. Spatiotemporal Deep Learning Models for Monitoring Cyber Threats in Surveillance Data Streams

1Govindarajan Lakshmikanthan, Independent Research Scholar, Leading Financial Firm, Dallas, Texas, USA. govind.lkanthan@gmail.com

2Nanthini M., Assistant Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. nanthini.velalar@gmail.com

Abstract

Spatiotemporal deep learning models have emerged as transformative tools for monitoring and mitigating cyber threats in surveillance data streams. These models effectively capture complex spatial and temporal dependencies, enabling real-time detection and prediction of malicious activities. This chapter explores advanced architectures, including hybrid models, transformer-based frameworks, and graph neural networks, optimized for cybersecurity applications. Key challenges such as adversarial robustness, scalability, and resource efficiency on edge devices are critically examined. Innovative solutions are proposed, including ensemble techniques for enhanced reliability and capsule networks tailored for spatiotemporal data. The chapter provides a comprehensive evaluation of performance metrics and presents methodologies for integrating these advanced models into real-world cyber monitoring systems. This work contributes to the growing body of research on deploying deep learning for secure, adaptive, and efficient cyber threat management in dynamic data environments.

Keywords:

Spatiotemporal Deep Learning, Cyber Threat Detection, Surveillance Data Streams, Transformer Models, Graph Neural Networks, Ensemble Learning.

Introduction

Cybersecurity has become a critical priority across industries as the digital landscape expands, with increasingly sophisticated threats targeting vulnerable systems [1]. Surveillance data streams, characterized by high volumes of continuously evolving information, present unique challenges for threat detection [2]. Spatiotemporal deep learning models have emerged as essential tools to address these complexities [3]. Unlike traditional approaches, these models capture both spatial and temporal dependencies in data, enabling more accurate and timely threat identification [4,5]. Their capacity to process dynamic patterns in real-time makes them invaluable for monitoring diverse cybersecurity domains, including anomaly detection in networks and the prevention of malware propagation [6-8].

Recent advances in deep learning have significantly enhanced the capabilities of spatiotemporal models [9]. Architectures such as hybrid models combining convolutional neural networks

(CNNs) and recurrent neural networks (RNNs), transformers, and graph neural networks (GNNs) have proven effective in capturing intricate data relationships [10,11]. These advanced models not only improve predictive accuracy but also enable scalability across large-scale surveillance systems [12-14]. The integration of innovative techniques such as attention mechanisms and ensemble learning ensures robustness and adaptability, addressing the evolving nature of cyber threats [15].

Adversarial attacks, where malicious inputs manipulate the model's predictions, pose significant risks [16]. Additionally, ensuring scalability and resource efficiency, particularly in edge computing environments, was a pressing concern [17]. This chapter delves into these challenges, proposing novel strategies to enhance the robustness, reliability, and efficiency of these models [18-20]. Emphasis was placed on techniques such as adversarial training and optimization of model architectures to ensure practical deployment [21].

To meet the demands of real-world applications, spatiotemporal models must be seamlessly integrated into cybersecurity systems [22,23]. Techniques like hybridization of architectures and ensemble learning enhance their capacity to handle dynamic and heterogeneous data [24,25]. The adoption of resource-efficient implementations enables deployment on edge devices, making these solutions accessible in environments with limited computational resources. These advancements pave the way for the adoption of spatiotemporal models in critical systems requiring real-time threat detection.