Chapter 2
Deep Learning for Threat Detection and Analysis

Kiran Sree Pokkuluri
https://orcid.org/0000-0001-8601-4304
Shri Vishnu Engineering College for Women, India

S. S. S. N. Usha Devi N.
https://orcid.org/0000-0002-2292-7494
University College of Engineering-Kakinada, Jawaharlal Nehru Technology, Kakinada, India

Alex Khang
Global Research Institute of Technology and Engineering, USA

ABSTRACT

Deep Learning has revolutionary potential to improve cybersecurity threat identification and analysis. This system quickly and accurately analyses large datasets by using Deep Learning, spotting patterns and anomalies that more conventional approaches would miss. This ability is essential for identifying sophisticated cyberthreats that traditional rule-based systems find difficult to detect, such as advanced persistent threats (APTs) and zero-day assaults. Deep learning models are constantly adapting to the trends in cybersecurity threats since they are taught on a variety of

DOI: 10.4018/979-8-3693-6371-3.ch002

dynamic data sets. This flexibility lowers operational costs and speeds up response times by preserving the efficacy of cybersecurity measures without the need for frequent manual updates. Deep learning is also used to improve overall system reliability by lowering false positives, a typical cybersecurity concern and improve overall system reliability by lowering false positives, a typical cybersecurity concern.

1. INTRODUCTION

Using sophisticated neural network topologies, deep learning (DL) has become a game-changing technology for threat identification and analysis. It can be used to detect, evaluate, and reduce a wide range of dangers in the domains of cybersecurity, fraud detection, and physical security(Schuartz, Fábio César, Mauro Fonseca, and Anelise Munaretto, 2020) This strategy makes use of deep learning models' capacity to learn from and generalize large volumes of data, providing more sophisticated understanding and detection capabilities than those of conventional techniques.

Deep learning techniques are used in cybersecurity to detect new malware variants, spot unusual network traffic that can point to a breach, and identify phishing efforts and other security concerns. These models are especially good at managing the dynamic and evolving nature of cyber threats, which are getting more and more sophisticated and elusive. This is because of their hierarchical feature learning capabilities(Yuan, Shuhan, and Xintao Wu., 2021)While DL models improve physical security by instantly identifying suspicious activity or unauthorised access, they also aid in fraud detection by analysing transaction patterns to indicate fraudulent actions. Large, annotated datasets, reliable pre-processing techniques to prepare the input data, and the choice of suitable neural network architectures Convolutional Neural Networks (CNNs) for image-based analysis and Recurrent Neural Networks (RNNs) for sequential data like logs or financial transactions, for example—are all necessary for deep learning to be effective in these applications(Joloudari, Javad Hassannataj, Mojtaba Haderbadi, 2020). Significant obstacles must be overcome before deep learning can be used for threat detection. These include the necessity for enormous computational resources, the possibility of biased

AI Applications for Clean Energy and Sustainability: Utilizing Artificial Intelligence for Monitoring Marine Ecosystems

Babitha Hemanth, Preethi Prabhu, Kartik Maruti Shetti, Deeksha D. Shettyand Zhenkar T. M. (2024). *AI Applications for Clean Energy and Sustainability (pp. 16-31).*
www.irma-international.org/chapter/ai-applications-for-clean-energy-and-sustainability/354456