Chapter 11
Adaptive Transfer Learning for Robust Phishing Attack Detection Using Recurrent Layers:
Enhancing Cybersecurity Through Dynamic Defense Mechanisms

Alnoman Mundher Tayyeh
https://orcid.org/0000-0001-7651-0240
Institute of Technology, Middle Technical University, Iraq

Abdulsattar Abdullah Hamad
College of Education, University of Samarra, Iraq

Rana B. Yaseen
College of Education for Women, Tikrit University, Iraq

Khalid Saeed Lateef Al-Badri
https://orcid.org/0000-0003-3678-4954
College of Education, Samarra University, Iraq

Firas Tarik Jasim
Northern Technical University, Al-Dour Technical Institute, Iraq

Noor Mohammed Kadhim
College Education for Human Sciences, Wasit University, Iraq

Shafeeq K. S. Aldoori
https://orcid.org/0000-0001-7996-7051
University of Samarra, Iraq

Husam Abdulhameed Hussein
University of Samarra, Iraq

Ahmed Ibrahim Turki
University of Samarra, Iraq

Omar Azeez Abbas
College of Administration and Economics, University of Samarra, Iraq

DOI: 10.4018/979-8-3373-0330-7.ch011

ABSTRACT

This paper proposes a robust phishing detection framework the use of adaptive switch getting to know mixed with recurrent layers, such as Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs), and Gated Recurrent Units (GRUs). Phishing assaults pose a significant chance to cybersecurity, and conventional detection techniques have struggled to maintain pace with the dynamic nature of those assaults. The proposed framework leverages the strength of switch getting to know to conform to new phishing styles with out requiring widespread retraining. By integrating recurrent layers, the model captures temporal dependencies inherent in phishing emails and verbal exchange styles, making an allowance for more accurate detection of evolving threats. The framework is designed to enhance cybersecurity by way of dynamically adjusting to new phishing approaches, supplying a scalable and effective solution for phishing detection.

INTRODUCTION

Phishing assaults have emerged as one of the maximum good sized threats in today's digital ecosystem. These attacks commonly make the most human vulnerabilities, tricking users into divulging confidential information like passwords, credit card numbers, or other sensitive facts. The attackers often conceal their communications as valid entities which includes banks, authorities groups, or famous companies, making it tough for conventional detection systems to understand phishing tries. While traditional security answers, consisting of rule-based systems, blacklists, and signature-based strategies, were applied to combat phishing, those techniques are more and more becoming less effective in detecting contemporary phishing assaults because of their dynamic and evolving nature. As phishing strategies have emerged as greater sophisticated, leveraging superior machine getting to know (ML) and deep getting to know (DL) models for phishing detection has emerge as imperative.

Adaptive Transfer Learning (ATL) gives a promising approach to address the challenges posed via evolving phishing tactics. ATL permits a model to switch know-how from formerly learned tasks or domains and apply it to a brand new, however related, venture, improving performance without requiring enormous retraining. This method has been specifically useful in cybersecurity, wherein it's far frequently vital to fast adapt to novel attack vectors. By combining ATL with Recurrent Neural Networks (RNNs)Long Short-Term Memory networks (LSTMs), and Gated Recurrent Units (GRUs), phishing detection fashions can seize the temporal patterns inherent in phishing attacks and adapt to emerging threats dynamically.