GAS Model: A New Hybrid Deep Learning Method for Enhancing Phishing URL Detection

Hajara Musa
Department of computer Sciences, Gombe State University, Gombe, Nigeria

A.Y Gital
Department of Mathematical Sciences, Abubakar Tafawa Balewa University Bauchi, Nigeria

Ahmed Mohammed
Department of computer Sciences, Gombe State University, Gombe, Nigeria

Usman Ali A
Department of Computer Sciences, Federal collage of education technical Gombe, Nigeria

Abstract:

Technological advancements have transformed cyberspace into a hub for banking, shopping, education, and entertainment. However, as human activities increasingly shift online, cybercriminals, including phishers, are exploiting this space, and posing significant risks to users, businesses, global security, and the economy. Traditional methods for classifying and detecting phishing URLs often rely on content-based approaches, which struggle with generalizing to new, unseen URLs. To address these limitations, our approach leverages the ability to automatically capture the semantic and sequential patterns in URLs, achieving notable success. This research introduces a new method called GAS, which employs GRU (Gated Recurrent Units), an Attention mechanism, and a sigmoid activation function for phishing detection in cyber-attacks. This research utilizes benchmark datasets to enhance detection accuracy for various phishing URLs. Specifically, the phishing URL data is sourced from the University of California, Irvine (UCI) repository. The experimental dataset consists of 11,055 URL entries, with 4,898 legitimate URLs and 6,157 phishing URLs. The results indicate that the GRU-ATT-Sigmoid model outperforms previous methods, achieving an accuracy rate of 96.36% on the UCI Repository dataset.

Keywords:

Machine leaning algorithms, Deep learning algorithms, Nature inspired algorithms, hybrid deep learning algorithms and optimized algorithms.