Chapter 1
Harnessing the Power of Large Language Models for Cybersecurity: Applications, Challenges, and Future Directions

Hewa Majeed Zangana
https://orcid.org/0000-0001-7909-254X
Duhok Polytechnic University, Iraq

Marwan Omar
Illinois Institute of Technology, USA

ABSTRACT

The LLMs not only have changed the overall nature of NPL but have also helped a lot in setting standards in cyber security. Within the confines of this review, the authors discuss the benefits, progressions, difficulties, as well as the future paths aimed to be taken in the cybersecurity field of LLMs. They delve into how LLMs help companies process unstructured textual data for text dangers detections, vulnerability assessments, and incident responses. In addition, they investigate the ethical and societal consequences of using LLMs for cybersecurity, facing challenges like algorithmic bias, privacy, and data safety. Besides that, they find that critical research questions in the crossroads of LLMs and cybersecurity language include unique assessing techniques and the improvement of algorithms to clarify the information. Through the development of many-faceted interdisciplinary cooperation and ethics-based considerations, we can maximize the opportunities LLMs present in the cyber world and build a more resilient and secure environment for everyone.

DOI: 10.4018/979-8-3693-9311-6.ch001

INTRODUCTION

The field of large language models (LLMs) has been remarkably changed by the recent emergence of these models, in terms of various areas, such as NLP, cybersecurity, and more. LLMs like BERT (Bidirectional Encoder Representations from Transformers) and GPT (Generative Pre-trained Transformer) have shown proficiency in understanding how humans write and can generate realistic text in the process, leading to their reputation for being the best suitable for cybersecurity missions.

Recently, there have been comprehensive research programs devoted to using LLMs in cybersecurity, because cyber weapons and means are getting very sophisticated and the defensive one have to be more effective. LLMs not only bring the possibility of improvement of the cybersecurity, which may consist in threat detection, vulnerability assessment, incident response and others. There is no question that these tools ease the tasks for the cybersecurity professionals but at the same time, their integration into cyber workflows pose the challenges and brings up the issues like privacy, ethics and robustness models.

In this review article, we undertake an overview and a critical analysis of the literature concerning the stances and uses of LLMs in cyber security. We will look at how LLMs can benefit cybersecurity while also disclosing their weaknesses, obstacles, and future opportunities. The key to our success is this that we does synthesis of the different studies with a wide range of perspective, hence, helpful to those people looking for research, practitioner, and policy making.

Figure 1 depicts the evolutionary tree of modern Generation Loving Machines.