DEEP LEARNING MODELS FOR COMPUTER NETWORKS SECURITY, A SURVEY

Karari Kinyanjui[a], John Wandeto[b]

[a]School of Computer Science, Dedan Kimathi University of Technology, Private Bag, Nyeri, 10143, Kenya, E-mail: efantusk@gmail.com

[b]School of Computer Science, Dedan Kimathi University of Technology, Private Bag, Nyeri, 10143, Kenya, E-mail: john.wandeto@dkut.ac.ke

Keywords: deep learning, cyber security, intrusion detection, classification

---

Increased use of smart devices and affordability of the internet has resulted to rapid growth in nodes connected to the internet as indicated by the migration from IPV4 to IPV6 and evolution to internet of things. The positive results of this growth and the benefits associated with connection to the internet are being negated by cyber-attacks which have become increasingly costly. Ransomware attacks have in recent times cost organizations huge sums of money posing a threat to their existence and calling for determined effort to eliminate or minimize the impact such attacks have on systems. The situation is not helped by new entrants to the cyber space who do so with less care about cyber security. There are several fronts in which the battle to secure systems can be fought and key among them is in having effective and efficient algorithms capable of detecting and classifying such attacks. Deep learning is one of the techniques that can be used to develop such algorithms. This survey aimed at providing a curated reference for Deep learning techniques used in cyber security.

Systematic approach was used in this study to review research articles already published and available from the various journals [1]. Reviewed articles were mainly from IEEE and springer. The search terms considered were deep learning and related methods such as; Convolutional Neural Networks (CNN), Deep Belief Network (DBN), Recurrent Neural Networks (RNN) and Temporal Convolutional Networks (TCN); Computer security and related terms such as cyber security, information systems security, computer networks security and Intrusion Detection Systems (IDS). Certain terms related to security were excluded such as physical security. Relevant data was extracted from review articles to facilitate comparison in performance.

The survey formed a curated reference that is the resultant paper and revealed that ensemble or hybrid algorithms perform better than individual algorithms. This composite algorithms may include components of conventional machine learning algorithms. Deep learning algorithms will be crucial where patterns need to be discovered through multiple layers like in the case of multilayer perceptron [2]. Research into network security should focus more on ensemble algorithms with deep learning being among the composite.

[1] Tawfik, G. M., Dila, K. A. S., Mohamed, M. Y. F., Tam, D. N. H., Kien, N. D., Ahmed, A. M., & Huy, N. T. (2019). A step by step guide for conducting a systematic review and meta-analysis with simulation data. Tropical medicine and health, 47(1), 1-9

[2] Adeyemo, V. E., Abdullah, A., JhanJhi, N. Z., Supramaniam, M., & Balogun, A. O. (2019). Ensemble and deep-learning methods for two-class and multi-attack anomaly intrusion detection: an empirical study. International Journal of Advanced Computer Science and Applications, 10(9).