The State of the Art in Machine Learning-Based Information Security

Authors : Thobeka Langa, Hein S. Venter

Abstract : — Machine Learning (ML) has emerged as a constantly evolving and powerful technology with the potential to transform the field of information security. Its ability to handle enormous quantities of data at high speeds, detect abnormalities, and automate efficient responses to security risks makes ML very promising in this domain. However, its application in the field of information security has not been extensively investigated, and a comprehensive understanding of existing research gaps in ML-based information security is still lacking. To accomplish this objective, the authors use previous publications to conduct an analysis of the machine learning techniques that have been adopted or explored within the field of information security. The outcome is then used to produce a state-of-the-art paper, identifying areas where more research is required.