4TH IMITEC 2024 4th International Multidisciplinary Information Technology and Engineering Conference, Vanderbijlpark, South Africa, 27 - 29 November 2024

A review of AI/ML algorithms for security enhancement in cloud computing with emphasis on artificial neural networks

Rakgoale, DM; Kobo, Hlabishi I; Mapundu, ZZ; Khosa, TN

Abstract

Security in cloud computing is becoming increasingly important due to the scale and sensitivity of data handled. Artificial Intelligence and Machine Learning algorithms offer robust solutions for enhancing security measures in cloud environments. Traditional security methods often fail to safeguard private information and user anonymity against the ever-evolving cyber threats. As new attack methods and techniques continuously emerge, traditional approaches become inadequate. Embracing modern strategies can enhance resilience and better protect sensitive data. Utilising AI and machine learning for threat detection, automated responses, and predictive analytics can significantly improve contemporary security measures. The use of Artificial Intelligence and Machine Learning is essential in the current era of big data to handle and analyse enormous amount of cloud-based data quickly and accurately. In addition to the security challenges posed by cloud computing and Internet of Things (IoT) devices, the utilisation of AI by hackers remains an ongoing threat in the realm of cybersecurity. This paper review various Artificial Intelligence and Machine Learning algorithms, with a particular focus on the application of Artificial Neural Networks (ANNs). It further provides an analytical review of how ANNbased approaches contribute to an improvement of threat detection, anomaly detection in cloud computing, highlighting their Zamikhaya Z, Mapundu Tshwane University of Technology Pretoria,South Africa MapunduZ@tut.ac.za Artificial Intelligence (AI) enabled technologies empower security systems to identify patterns, anomalies, and potential threats across large datasets. By leveraging Machine Learning (ML) algorithms that analyse historical attack data, these systems can forecast future threats and enhance their defensive strategies proactively [1]. This capability not only improves the detection and response time to security incidents, but also enable organisations to adapt swiftly to evolving cyber threats. Moreover, AI enables security solutions to automate routine tasks, allowing human analysts to focus more on complex and strategic aspects of cybersecurity management [3]. Thus, integrating AI into security frameworks not only bolsters protection but also enhances overall operational efficiency and resilience against cyber threats. Furthermore, the convergence of Machine Learning and AI in cloud frameworks is expected to accelerate digital transformation and bring in an exciting period of efficiency and innovation [4]. effectiveness, potential challenges. Moreover, the advantages of artificial neural networks (ANNs) are discussed along with the current challenges encountered when applying these advanced models in cloud computing security.