DOI: doi.org/10.47363/JAICC/ICAIC2025/2025(4)15

International Conference on
Artificial Intelligence and Cybersecurity (ICAIC 2025)

Conference Proceedings November 27-28, 2025 (Virtual)

Artificial Intelligence in Cyber Defense: A Quantitative, Open-Source Approach

Mohammad Saifuzzaman

Department of Computer Science and Cybersecurity, College of Health, Science, and Technology, University of Central Missouri, USA

Abstract
This study investigates the role of artificial intelligence (AI) in improving cyber defense through the use of an open-source, quantitative approach, based on reproducibility, transparency, and comparison of models in terms of their performance. Due to a rise in the number and complexity of cyber threats, the study determines how AI models, known as supervised learning algorithms and unsupervised learning algorithms, can be used to analyze open datasets like CIC-IDS2017 and NSL-KDD to identify intrusions at a higher rate of accuracy and in real-time than existing systems. When using precision, recall, F1-score, and ROC-AUC as the performance measures, the study concludes that Random Forest and Convolutional Neural Networks (CNNs) have over 95 percent accuracy in detection, compared to traditional ones, which are much faster and reliable, especially when detecting zero-day attacks. It was also found that the results provided statistically significant improvement in detection time, resolution rates, and false positive reduction. Important contributions consist of a reproducible research design with the usage of open-source platforms and libraries like Scikit-learn, TensorFlow, and PyTorch, so it can be tested and adapted by other scientists. Other ethical issues discussed in the paper include adversarial attacks, bias, and lack of transparency of algorithms, which present responsible deployment of AI and regulatory alignment. The results of the given study could make a strong contribution to policy and practice, assuming that open-source, AI-driven systems can be not only technologically better, but also more just and flexible in diverse conditions of operation. The study has thus helped in realizing the interest of building inclusive, scalable, and resilient global application cybersecurity infrastructures through linking technical excellence with ethical responsibility.

Keywords: Artificial Intelligence, Cyber Defense, Open-Source Intelligence, Intrusion Detection, Machine Learning, Ethics, Quantitative Analysis.