ISSN: 2473-4901
v9 n5995

Network Intrusion Detection System with Machine Learning as a Service

Loma Kangethe
Lk07736@georgiasouthern.edu
Department of Information Technology
Georgia Southern University
Statesboro, GA 30460, USA

Hayden Wimmer
hwimmer@georgiasouthern.edu
Department of Information Technology
Georgia Southern University
Statesboro, GA 30460, USA

Carl M Rebman, Jr.
carlr@sandiego.edu
Knauss School of Business
Department of Supply Chain, Operations, and Information Systems
University of San Diego
San Diego, CA 92110, USA

Abstract

Cloud Computing and Big Data continue to be disruptive forces in computing. This has introduced threats and vulnerabilities. The paper seeks to demonstrate how an end-to-end network intrusion detection system can be built, trained, and deployed using Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). We determined the performance of these tools by building a network intrusion detection system (NIDS) and evaluating the performance of each based on precision, accuracy, F1 Score, recall, user experience, cost and computation time for training and predicting the model. Overall, all three platforms performed greater than 90% accuracy with Google Vertex AI having the highest accuracy using the decision tree and Microsoft Azure performing the best based on accuracy, precision, and computation time.

Keywords- Network Intrusion Detection, Machine Learning (ML), Microsoft Azure Machine Learning, Amazon Web Services (AWS), Sage Maker, Vertex AI

A full and updated version of this abstract may be found at https://jisar.org