INFORMATICS INSTITUTE OF TECHNOLOGY
In Collaboration with
UNIVERSITY OF WESTMINSTER

MACHINE LEARNING APPROACH TO ADDRESS SECURITY AND PRIVACY CONCERNS IN HEALTHCARE ORGANIZATIONS

A Project by

SARANYA ARULNATHAN

STUDENT NUMBER: IIT: 20211012 / UOW: 18699526

Supervised by
PROF. PRASAD WIMALARATNE

Submitted in partial fulfilment of the requirements for the MSc in CYBER SECURITY & FORENSICS degree at the University of Westminster.

15th May, 2023

Abstract

The research focuses on a problem in healthcare sectors regarding privacy and security issues. Some of the identified problem include; insecurities such as unauthorized persons accessing the patients' room, data leakage through cybercrime, falls which can be prevented through digital monitoring and immediate reporting, and accessing patients' data from physical areas such as in the registration office, and waiting room. Problems with existing models were discovered for example they are; costly, require training to use, occupy much space in android and windows device, slow down the device with low storage and RAM capacity, and high maintenance costs. Suggestions were made that a machine learning model can increase monitoring healthcare's' performance which would thus, increase privacy and enhance security on patient's data and wellbeing in the facility. Data was collected using case studies approach whereby, interviews were analyzed.

The results indicate that many healthcare organizations have been experiencing minimal privacy and security has been a significant issue which in some cases, worsen the patients' condition. Where monitoring in healthcare would be increased, there would be reduction in unauthorized persons accessing the patients' room, in addition, a monitoring tool can monitor patients' movement and create an alert to the management in time. In the study, CNN was not applied, however, to solve the problem a machine learning tool which would resemble datix model was suggested. The tool is an improved version of the existing machine learning tools. Confusion matrix was applied to make predictions on the accuracy and precision with the tool to test its reliability, functionality, and to test whether it can help healthcare organizations improve on privacy and security reporting in the facility.

Key Words: Machine Learning, Privacy, Security, differential privacy, NVIDIA, Microsoft Azure, and google cloud engine, XG Boost