2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS) | 979-8-3503-8145-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/PAIS60821.2023.10321979

Investigating Security and Privacy Concerns in Deep-Learning-based Pervasive Health Monitoring Architectures

Amine Boulemtafes
Division Sécurité Informatique
Centre de Recherche sur l'Information
Scientifique et Technique, Algiers, Algeria
Département Informatique, Faculté des Sciences exactes
Université de Bejaia, 06000, Bejaia, Algeria
aboulemtafes@cerist.dz, *0000-0002-1407-5295*

Abdelouahab Amira
Division Sécurité Informatique
Centre de Recherche sur l'Information
Scientifique et Technique, Algiers, Algeria
Département Informatique, Faculté des Sciences exactes
Université de Bejaia, 06000, Bejaia, Algeria
amira@cerist.dz, *0000-0002-2516-738X*

Mohamed Saddek Derki
Division Sécurité Informatique
Centre de Recherche sur l'Information
Scientifique et Technique, Algiers, Algeria
Ecole Nationale Supérieure d'Informatique, Algiers, Algeria
msaddek@cerist.dz, *0000-0003-2386-0225*

Samir Hadjar
Division Sécurité Informatique
Centre de Recherche sur l'Information
Scientifique et Technique, Algiers, Algeria
Département Informatique, Faculté des Sciences exactes
Université de Bejaia, 06000, Bejaia, Algeria
hadjar@cerist.dz, *0009-0006-7962-1724*

***Abstract*—Pervasive Health Monitoring (PHM) uses sensors and wearable devices and data analytics for real-time health monitoring. It enables early detection and personalized care interventions. This technology has the potential to revolutionize healthcare by improving proactive and preventive care.**

Besides, Deep learning (DL) based PHM is even more promising as it improves the discovery of complex patterns and correlations. This leads to precise health monitoring and personalized care, enhances diagnostics, and ultimately improves patient outcomes in the field of healthcare.

However, privacy and security considerations must be addressed for successful implementation. This paper investigates the security and privacy concerns in Pervasive Health Monitoring architectures. It discusses through an illustrative DL-based PHM architecture the potential threats and attacks during the inference and training phases, and identifies key security and privacy issues. It also gives insights on countermeasures and technological solutions that can address security and privacy concerns in PHM architectures.

***Index Terms*—Pervasive health monitoring, Security and privacy, Deep learning, PHM architectures**

I. Introduction

Pervasive Health Monitoring (PHM) has emerged as an innovative approach in healthcare. It uses sensors, wearable devices, and data analytics to continuously monitor people's health in real-time. This new way of healthcare delivery offers proactive and personalized care, early detection of health issues, and improved patient outcomes. By integrating these technologies seamlessly into daily life, PHM systems have the potential to transform healthcare by providing timely interventions, reducing hospital visits, and increasing patient involvement [1].

Deep learning (DL) plays a vital role in Pervasive Health Monitoring by exploring complex patterns and correlations for accurate health monitoring and personalized care. It leverages deep neural networks to analyze diverse data modalities and uncover valuable insights. With the ability to automatically learn and adapt, deep learning models enable early disease detection and personalized interventions. By enhancing diagnostics, they empower healthcare providers to make informed decisions and improve patient outcomes. Deep learning revolutionizes healthcare by harnessing vast health data for proactive and preventive care. The growing prevalence of chronic diseases, an aging population, and the increasing demand for remote and personalized healthcare services have propelled the development and adoption of PHM architectures. These architectures comprise various components, including sensors, wearable devices, communication networks, data storage, and analytics engines, working together to collect, transmit, analyze, and interpret health-related data. By leveraging the power of data analytics and machine learning algorithms, PHM systems can derive actionable insights and provide predictive models for effective health monitoring and prognostics [2].

However, PHM architectures continue to evolve, and several challenges and considerations need to be addressed to ensure their successful implementation and widespread adoption. One of the primary concerns is the security and privacy of sensitive health data collected, transmitted and processed within these systems. The continuous monitoring of individuals' health data raises questions about data protection, unauthorized access,

979-8-3503-8145-0/23/$31.00 ©2023 IEEE