A Privacy enhancing model using differential privacy for IoT wearable devices in healthcare

By
Rawan Mohammed AlHarbi

Supervised by:
Dr. Haya Almagwashi

Abstract

Nowadays, the wave of the internet of things has arrived with its pros and cons, and massive evolution has reached the most significant point in the way the humans and smart wearable devices interact. Users feel comfy using it to achieve several services through these technologies that improve their daily life quality. However, the wearable technologies bring a diversity of privacy concerns. Because many of critical data and details about an individual can be gathered while the person is not aware of who will use his data. Today, there are no specific methods or techniques that succeeded in solving this technology's privacy issues. This research aims to improve the privacy of wearable internet of things devices in the healthcare domain. Differential privacy is a method that guarantees the highest level of privacy for a collected record while delivering practical information about the dataset. This research will focus on identifying the privacy requirements for WIoT in healthcare

and priorities these requirements from the user's perspective, then use differential privacy hyper parameter to evaluates the effect of it on preserving the privacy of healthcare records at different algorithms accuracy. The proposed model was implemented on a patients' datasets using a variation of algorithms to achieve the desired level of privacy. The implementation included different algorithms such as naïve Bayes, linear regression and k-means to achieve the optimum accuracy while maintaining the least value of privacy loss. The proposed model achieved a good privacy level with accuracy on privacy epsilon equal=1. The results came through testing different epsilons showed that we can achieve a very higher privacy level with little decrees on data accuracy. Future work will be on testing differential privacy with other epsilons and more algorithms.