Abstract

As Machine Learning as a Service (MLaaS)-based deep learning (DL) solutions are increasingly used in the healthcare industry, concerns regarding personal data privacy have been raised. Consequently, the need for privacy-preserving methods enabling DL model development has grown significantly. Over the past few years, our research has addressed these concerns through various strategies, including homomorphic encryption, encoding, and image obfuscation. In our earlier work, we proposed a variation of a noise-free matrix-based homomorphic encryption scheme (MORE) to ensure privacy in computations within deep learning models. This approach was subsequently employed to create a privacy-oriented cloud-based platform for deploying machine learning algorithms tailored to wearable sensor data. For enhanced security, we integrated a homomorphic encryption scheme that uses modulo operations over integers, an encoding technique that enables computations on rational numbers, and a numerical optimization strategy that facilitates training within a fixed number of operations. To reduce the computational overhead in image-based applications, we proposed several image obfuscation approaches based on non-bijective functions, variational autoencoders, and matrix decomposition. Security assessments were conducted through analytical means and by simulating different attack scenarios. We evaluated the effectiveness of the proposed approaches by implementing them in diverse medical applications, achieving promising results.