Journal of Information Security and Applications 77 (2023) 103552

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

PRIviLY: Private Remote Inference over fulLY connected deep networks for pervasive health monitoring with constrained client-side

Amine Boulemtafes [a,b,*], Abdelouahid Derhab [c], Yacine Challal [d]

[a] Division Sécurité Informatique, Centre de Recherche sur l'Information Scientifique et Technique, Algiers, Algeria
[b] Département Informatique, Faculté des Sciences exactes, Université de Bejaia, 06000 Bejaia, Algeria
[c] Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia
[d] Laboratoire de Méthodes de Conception des Systèmes, Ecole Nationale Supérieure d'Informatique, Algiers, Algeria

ARTICLE INFO

Keywords:
Fully connected deep neural networks
Privacy
Constrained
Remote inference

ABSTRACT

Remote deep learning paradigm enables to better leverage the power of deep neural networks in pervasive health monitoring (PHM) applications, especially by addressing the constrained client-side environment. However, remote deep learning in the context of PHM requires to ensure three properties: (1) meet the high accuracy requirement of the healthcare domain, (2) satisfy the client-side constraints, and (3) cope with the privacy requirements related to the high sensitivity of health data. Different privacy-preserving solutions for remote deep learning exit in the literature but many of them fail to fully address the PHM requirements especially with respect to constrained client-side environments. To that end, we propose PRIviLY, a novel privacy-preserving remote inference solution, designed specifically for the popular Fully Connected Deep Networks (FCDNs). PRIviLY avoids the use of encryption for privacy preservation of sensitive information, in order to fully prevent accuracy loss, and to alleviate the server-side hardware requirements. Besides, PRIviLY adopts a non-colluding two-server architecture, and leverages the linear computations of FCDNs along with reversible random perturbation and permutation techniques in order to preserve privacy of sensitive information, while meeting low overhead requirement of constrained client-sides. At the cloud server, efficiency evaluation shows that PRIviLY achieves an improvement ratio of 4 to more than 15 times for communication, and a minimum improvement ratio of 135 times for computation overhead. At the intermediate server, the minimum improvement ratio is at least more than 10,900 for computation, while for communication, the improvement ratio varies from 5 to more than 21 times. As for the client-side, PRIviLY incurs an additional overhead of about 27% in terms of communication, and between 16% and at most 27% in terms of computation.

1. Introduction

Pervasive health monitoring (PHM) is one of the most interesting fields of e-healthcare. It enables anywhere and anytime patient monitoring towards improving medical quality while reducing costs, as well as improving the quality of patients' lives. With the advancements in sensing technologies and the emergence and increasing development of deep learning, PHM applications are nowadays able to target various health diseases like pneumonia, sleep apnea, heart health assessment, and Covid-19, as well as different well-being cases like helping elderly living independently [35,42,48].

Besides, in order to further take advantage of the power of deep learning, powerful infrastructures with high-power computation and massive storage such as clouds are nowadays used in order to run deep neural network models. This paradigm called remote deep learning, allows to better fit the increasing depth and computation requirements of powerful deep learning models, while it enables the access to proprietary deep models. Moreover, remote inferences were shown able to incur, in appropriate settings, shorter execution time in comparison to local inferences [17].

Remote deep learning is furthermore interesting when the client-side environment is constrained in terms of computation, energy, or storage. This is the case of PHM environment which generally relies on client devices with limited power and computation. In fact, because PHM can be particularly leveraged with powerful deep learning-based data analytics [49], but its environment is considered as constrained, remote deep learning paradigm represents an effective approach to better benefit from PHM potential.

However, by transmitting sensitive data from client devices to external infrastructures, the use of remote deep learning raises a number of privacy

* Corresponding author.
E-mail addresses: aboulemtafes@cerist.dz (A. Boulemtafes), abderhab@ksu.edu.sa (A. Derhab), y_challal@esi.dz (Y. Challal).

https://doi.org/10.1016/j.jisa.2023.103552

Available online 21 July 2023