2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA) | 978-1-6654-0969-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/AICCSA53542.2021.9686893

PReDIHERO – Privacy-Preserving Remote Deep Learning Inference based on Homomorphic Encryption and Reversible Obfuscation for Enhanced Client-side Overhead in Pervasive Health Monitoring

Amine Boulemtafes[1,2], Abdelouahid Derhab[3], Nassim Ait Ali Braham[4] and Yacine Challal[5]

[1] Division Sécurité Informatique, Centre de Recherche sur l'Information Scientifique et Technique, Algiers, Algeria
[2] Département Informatique, Faculté des Sciences exactes, Université de Bejaia, 06000 Bejaia, Algeria
aboulemtafes@cerist.dz
[3] Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudia Arabia
abderhab@ksu.edu.sa
[4] Remote Sensing Technology Institute (IMF), German Aerospace Center (DLR), Germany
en_ait_ali_braham@esi.dz
[5] Laboratoire de Méthodes de Conception des Systèmes, Ecole Nationale Supérieure d'Informatique, Algiers, Algeria
y_challal@esi.dz

Abstract*–Homomorphic Encryption is one of the most promising techniques to deal with privacy concerns, which is raised by remote deep learning paradigm, and maintain high classification accuracy. However, homomorphic encryption-based solutions are characterized by high overhead in terms of both computation and communication, which limits their adoption in pervasive health monitoring applications with constrained client-side devices. In this paper, we propose PReDIHERO, an improved privacy-preserving solution for remote deep learning inferences based on homomorphic encryption. The proposed solution applies a reversible obfuscation technique that successfully protects sensitive information, and enhances the client-side overhead compared to the conventional homomorphic encryption approach. The solution tackles three main heavyweight client-side tasks, namely, encryption and transmission of private data, refreshing encrypted data, and outsourcing computation of activation functions. The efficiency of the client-side is evaluated on a healthcare dataset and compared to a conventional homomorphic encryption approach. The evaluation results show that PReDIHERO requires increasingly less time and storage in comparison to conventional solutions when inferences are requested. At two hundreds inferences, the improvement ratio could reach more than 30 times in terms of computation overhead, and more than 8 times in terms of communication overhead. The same behavior is observed in sequential data and batch inferences, as we record an improvement ratio of more than 100 times in terms of computation overhead, and more than 20 times in terms of communication overhead.

***Keywords*–Deep Learning; Neural Network; Homomorphic Encryption; Random mask; Privacy; Sensitive data; Constrained; Inference**

I. Introduction

Deep learning is a an advanced approach of machine learning, which allows to overcome the dependency on hand-designed features encountered in traditional learning algorithms. The power of deep learning is particularly leveraged when performed on powerful cloud infrastructures providing high computational power and massive storage. This paradigm is called remote deep learning, and enables furthermore the access to proprietary deep models. However, transmitting sensitive data from the client devices to the external infrastructure in order to feed the remote deep learning model raises privacy concerns. These include for example the disclosure of private information, identification of individuals, or even unauthorized commercial sharing of confidential information.

In pervasive health monitoring (PHM) applications, the client-side generally relies on sensors, mobile devices, and cellular connectivity, which represents a constrained environment. In this context, the design of privacy-preserving solutions needs to take into consideration the requirements of the client-side. These comprise resource-limited devices in terms of power and computation, as well as unreliable network with possible high communication costs [1, 2].

One of the most promising techniques for privacy-preserving inference solutions is Homomorphic Encryption (HE). In fact, HE-based solutions are able to simultaneously provide high accuracy and privacy without trade-off. However, HE-based solutions are characterized by high overhead in terms of both computation and communication [1], which limits their adoption in PHM applications.

In this paper, we propose PReDIHERO (Privacy-preserving Remote Deep learning Inference based on Homomorphic Encryption and Reversible Obfuscation), a novel solution based on reversible obfuscation mask, allowing to significantly mitigate high client-side overhead in privacy-preserving homomorphic-encryption-based deep learning inference solutions. PReDIHERO employs a reversible obfuscation technique [40] that successfully protects sensitive information, and enhances the client-side overhead. To that end, PReDIHERO tackles three main heavyweight client-side tasks, namely, (a) encryption and transmission of private data, (b) refreshing encrypted data, and (c) outsourcing computation of activation functions. Compared to the conventional homomorphic encryption approach, the results of PReDIHERO show an increasing improvement ratio in terms of client-side computation and communication overhead during successive inferences, as well as during batch and sequential data inferences.

The remainder of this paper is organized as follows: Section 2 presents background on deep learning, homomorphic

978-1-6654-0969-8/21/$31.00 ©2021 IEEE