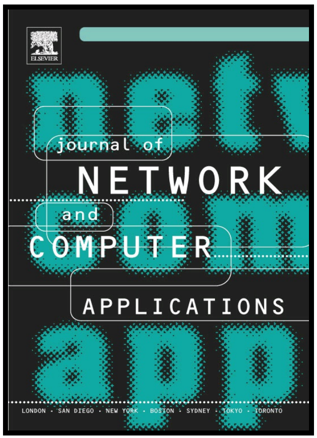
ELSEVIER
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

Efficient and Privacy-Aware Multi-party Classification Protocol for Human Activity Recognition

Zakaria Gheid, Yacine Challal, Xun Yi, Abdelouahid Derhab

PII: S1084-8045(17)30301-6
DOI: http://dx.doi.org/10.1016/j.jnca.2017.09.005
Reference: YJNCA1972

To appear in: *Journal of Network and Computer Applications*

Received date: 31 January 2017
Revised date: 10 August 2017
Accepted date: 14 September 2017

Cite this article as: Zakaria Gheid, Yacine Challal, Xun Yi and Abdelouahid Derhab, Efficient and Privacy-Aware Multi-party Classification Protocol for Human Activity Recognition, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2017.09.005

Efficient and Privacy-Aware Multi-party Classification Protocol for Human Activity Recognition

Zakaria Gheid[a,*], Yacine Challal[a,b], Xun Yi[c], Abdelouahid Derhab[d]

[a]*Laboratoire de Modes de Conception des Systs, Ecole Nationale Supeure d'Informatique, Algiers, Algeria*
[b]*Centre de Recherche sur l'Information Scientifique et Technique, Algiers, Algeria*
[c]*The School of Computer Science and IT, RMIT University, Melbourne, Victoria, Australia*
[d]*Center of Excellence in Information Assurance (COEIA), King Saud University, Riyadh, Saudi Arabia*

Abstract

Human activity recognition (HAR) is an important research field that relies on sensing technologies to enable many context-aware applications. Nevertheless, tracking personal signs to enable such applications has given rise to serious privacy issues, especially when using external activity recognition services. In this paper, we propose (Π-Knn): a privacy-preserving version of the K Nearest Neighbors (k-NN) classifier that is mainly built on (Π-CSP+): a novel cryptography-free private similarity evaluation protocol. As a sample application, we consider a medical monitoring system enhanced with a HAR process based on our privacy preserving classifier. The integration of the privacy preserving HAR aims to improve the accuracy of the clinical decision support. We conduct a standard security analysis to prove that our protocols provide a complete privacy protection against malicious adversaries. We perform a comparative performance evaluation through several experiments while using real HAR system parameters. Experimental evaluations show that our protocol (Π-CSP+) incurs a low increasing overhead (37% in Online classification and 50% in Offline classification) compared to PCSC, representative state-of-the art protocol, which incurs 3600% and 4800% in online and offline classification respectively. Besides, Π-CSP+ provides a stable and efficient response time (W=0.0x m.seconds) for both short and long duration activities while serving up to 1000 clients. Comparative results confirm the computational efficiency of our protocol against a competitive state-of-the-art protocol.

Keywords: Human Activity Recognition, k-NN Classification, Multi-Party Computation, Privacy Preserving.

1. INTRODUCTION

Data mining methods are gaining an increasing attention because of the wide proliferation of knowledge-based applications. Analyzing data from wireless and sensor networks has enabled developing new services, such as Human Activity Recognition (HAR). HAR consists of tracking environmental and personal sensed signs, then, analyzing them to provide accurate information about persons' daily activities. Nevertheless, the collection and analysis of personal private data, such as GPS location, raises concerns about users' privacy, especially when the analysis is performed through external service providers. External recognition aims to reduce the cost of computation and storage accrued by client devices. Additionally, it aims ensuring a high accuracy level in recognition results, which are built upon big data stores of activity patterns.

To face such a concern, several Privacy-Preserving Data Mining (PPDM) methods have been proposed. These include classification, clustering and other data mining tasks [1]. PPDM methods protect the privacy

[*] Corresponding author

Email addresses: z_gheid@esi.dz (Zakaria Gheid), y_challal@esi.dz (Yacine Challal), xun.yi@rmit.edu.au (Xun Yi), abderhab@ksu.edu.sa (Abdelouahid Derhab)