

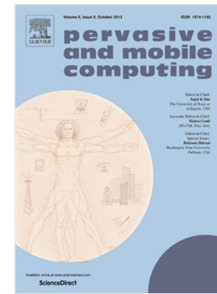
## Accepted Manuscript

Efficient data perturbation for privacy preserving and accurate data stream mining

M.A.P. Chamikara, P. Bertok, D. Liu, S. Camtepe, I. Khalil

PII: S1574-1192(17)30522-9  
DOI: <https://doi.org/10.1016/j.pmcj.2018.05.003>  
Reference: PMCJ 934

To appear in: *Pervasive and Mobile Computing*



Please cite this article as: M.A.P. Chamikara, P. Bertok, D. Liu, S. Camtepe, I. Khalil, Efficient data perturbation for privacy preserving and accurate data stream mining, *Pervasive and Mobile Computing* (2018), <https://doi.org/10.1016/j.pmcj.2018.05.003>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

# Efficient Data Perturbation for Privacy Preserving and Accurate Data Stream Mining

M.A.P. Chamikara<sup>a,b,\*</sup>, P. Bertok<sup>a</sup>, D. Liu<sup>b</sup>, S. Camtepe<sup>b</sup>, I. Khalil<sup>a</sup>

<sup>a</sup>*RMIT University, Australia*

<sup>b</sup>*CSIRO Data61, Australia*

---

## Abstract

The widespread use of the Internet of Things (IoT) has raised many concerns, among them the protection of private information. Existing privacy preservation methods cannot provide a good balance between data utility and privacy, and also have problems with efficiency and scalability. This paper proposes an efficient data stream perturbation method (named as  $P^2RoCAI$ ).  $P^2RoCAI$  delivers better data utility compared to its contenders, classification accuracies of  $P^2RoCAI$  perturbed data streams are very close to those of original data streams.  $P^2RoCAI$  also provides higher resilience against data reconstruction attacks.

*Keywords:* Privacy, privacy preserving data mining, data streams, Internet of Things (IoT), Web of Things (WoT), sensor data streams, big data.

---

## 1. Introduction

The Internet of Things (IoT) is becoming widely popular as it connects typical day to day devices such as kitchen appliances, cars, washing machines, headphones, wearables, etc. to the Internet to allow life activities be more intelligent, efficient and reliable [1]. IoT devices can forward a significant amount of data in streams from various sensors via long-lasting connections. IoT has revolutionized many fields including health-care, wellbeing applications, social life, environment monitoring, transportation, and energy. The availability of low-cost pervasive sensing devices has enabled IoT to grow in an ever-increasing manner, and IoT sensor streams have become a vital source of big data [1, 2].

The vast diversity of IoT devices introduces many challenges [3], among which the most important ones are (i) effective data collection, (ii) efficient data processing, and (iii) privacy protection and security [4]. The availability and increased accessibility of IoT sensors often introduce the risk of privacy

---

\*Corresponding author

*Email address:* pathunchamikara.mahawagaarachchige@rmit.edu.au (M.A.P. Chamikara)

Download English Version:

<https://daneshyari.com/en/article/6888595>

Download Persian Version:

<https://daneshyari.com/article/6888595>

[Daneshyari.com](https://daneshyari.com)