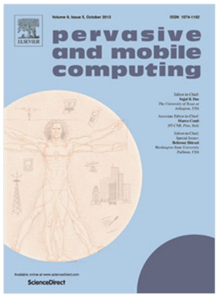
Accepted Manuscript



Wearable IoT data stream traceability in a distributed health information system

Richard K. Lomotey, Joseph Pry, Sumanth Sriramoju

PII: S1574-1192(17)30327-9
DOI: http://dx.doi.org/10.1016/j.pmcj.2017.06.020
Reference: PMCJ 860

To appear in: *Pervasive and Mobile Computing*

Wearable IoT Data Stream Traceability in a Distributed Health Information System

Richard K. Lomotey, Joseph Pry, Sumanth Sriramoju

Pennsylvania State University, Department of Information Sciences and Technology (IST), Monaca, PA 15061, USA

Abstract—With the soaring interest in the Internet of Things (IoT), some healthcare providers are facilitating remote care delivery through the use of wearable devices. These devices are employed for continuous streaming of personal medical data (e.g., vitals, medications, allergies, etc.) into healthcare information systems for the purposes of health monitoring and efficient diagnosis. However, a challenge from the perspective of the physicians is the inability to reliably determine which data belongs to who in real-time. This challenge emanates from the fact that healthcare facilities have numerous users who own multiple devices; thereby creating an *N x M* data source heterogeneity and complexities for the streaming process. As part of this research, we seek to streamline the process by proposing a wearable IoT data streaming architecture that offers traceability of data routes from the originating source to the health information system. To overcome the complexities of mapping and matching device data to users, we put forward an enhanced Petri Nets service model that aids with a transparent data trace route generation, tracking and the possible detection of medical data compromises. The results from several empirical evaluations conducted in a real-world wearable IoT ecosystem prove that: 1) the proposed system's choice of Petri Net is best suited for linkability, unlinkability, and transparency of the medical IoT data traceability, 2) under peak load conditions, the IoT architecture exhibits high scalability, and 3) distributed health information system threats such as denial of service, man-in-the-middle, spoofing, and masking can be effectively detected.

Index Terms—Internet of Things (IoT), Sensors, Mobile devices, Middleware, Wearables, Petri Nets, Privacy, Health Information System

1 Introduction

THE huge galaxy of interconnected "things" around us today is leading to the creation of new use cases and applications across several domains [1] [3]. Through networking capabilities, these devices are facilitated to sense, collect heterogeneous data types from different places, and deliver the collected data to other nodes (e.g., cloud facilities) for analytical transactions.

There are several use cases and applications of IoT and especially in healthcare, the list includes: Telehealth: remote or real-time pervasive monitoring of patients, diagnosis, and drug delivery. With wearable IoT for fitness tracking, sensors are able to read users' vitals and the information can be pushed to healthcare facilities.

However, the quest for sensor data streaming in an attempt to offer health monitoring services for instance, can be challenging for the physicians. Taking wearable IoT for example, smart watches and other sensors such as blood oxygen readers, gamma ray radiation detectors, and fitness trackers are facilitated to generate and/or collect personal records (including vitals, location, and dosage levels) which should be delivered to the healthcare information system. These devices therefore are constantly running to enable the data streaming process which can create certain problems at the physicians' end.

• *R.K. Lomotey, Department of Information Sciences and Technology (IST), Pennsylvania State University, Beaver Campus Monaca, PA 15061, USA. E-mail: rkl5137@psu.edu.,* ***Corresponding Author***

Firstly, medical facilities have several "users", say *N*, who may subscribe to real-time monitoring through wearable IoT services. But, a user can own more than one IoT device, say *M*, where device heterogeneity is due to varied conditions; and some devices can only sense and deliver specific data. This means the healthcare systems have to stream the IoT data in an *N x M* transactional view. Since the physicians mostly do not control what devices users purchase (because it's personal), the task is for the former to determine who owns what data — a requirement that can be tedious and limiting real-time diagnosis.

Moreover, the medical data streaming process can also be demanding on features such reliability, transparency, and user privacy preservation. This means the care facilities are not only dealing with the *N x M* data streaming sources but, must be able to track devices, maintain data source origination record, and data read points. This often leads to unbearable complexities.

Some researchers identified the aforementioned issues as well. For instance, Kang et al. [32] studied RFID-based traceability and its implication to IoT data storage systems. Also, there are some reported works that focus on application and process traceability within IoT [33] [34].

Our goal is to research and develop a wearable IoT architecture for healthcare use with the capability of generating trace routes while preserving privacy and reliability. With traceability facilitated, the healthcare facilities can transparently audit the streamed medical data for possible compromises, and eventually automate the mon-