Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 94 (2016) 144 – 151

Procedia Computer Science

The 13th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2016)

Using Provenance and CoAP to track Requests/Responses in IoT

Emmanuel Kaku[a*], Richard .K. Lomotey[b], Ralph Deters[a],

[a]*University of Saskatchewan, Saskatoon, Canada*
[b]*Pennsylvania State University, USA*

Abstract

Until recently, not much attention has been drawn to the need to provide documentary evidence for ensuring reliability, transparency and, most importantly, tracing the source of requests/responses in the Internet of Things. The knowledge of provenance is considered as a key component in establishing the above-mentioned issues. Most research, to a large extent, focus on requesting data, which is based on user inference and decision making, by utilising provenance information. However, little or nothing has been done regarding requests and responses and, most importantly, from the machine perspective. Consequently, this paper proposes a light-weight prototype system for tracing the source of requests/responses using provenance information over CoAP in the Internet of Things. We also provide performance evaluation of the prototypic system using metrics such as response time (ms) and throughput (KB/s). Finally, findings from our experiment are presented and discussed.

Peer-review under responsibility of the Conference Program Chairs

Keywords: IoT; Provenance; REST; URI; Meta-data; CoAP.

1. Introduction

The use of the Internet has now been extended to encompass billions of internet-connected objects. These internet-connected objects were initially everyday things that were not considered part of the Internet. They range from cars,

* Corresponding author. Tel.: +1-639-317-7021.
E-mail address:emk508@mail.usask.ca

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.08.023

buildings, animals, chairs, shirts, TV's, bicycles to mention but a few. They can be tangible or intangible things with limited resources in terms of battery, bandwidth and computational power. Apart from devices such as phones, laptops, switches, routers etc., which are already computerized, these things have identities and are equipped with embedded chips, sensors, actuators and some elements of communication technologies such as Wifi, Bluetooth, etc.). Having the above technologies has made them intelligent, enabling them to sense, self-configure, self-maintain, and interact with one another. As a result, they are able to generate huge amount of data[1,23]. These data are pushed to the cloud for massive analysis which ultimately translates to useful information that has the potential of transforming human lives in so many ways, change business strategies and models and, most importantly, generate economic revenue for the society. This paradigm shift in computing is the Internet of Things (IoT). Some key driving elements of this shift comprise identification, sensing, communication, humans, cloud-computing and actuating technologies[23]. IoT is presently all around us: in our homes, cars, and even on our physical bodies. It is currently connecting citizens to their cities, linking patients to health services and bringing clients closer to companies. With this shift pervading all spheres of human life, Gartner Inc. and Cisco[20, 21] predicted that the total number of devices connected to the Internet would hit 20 to 50 billion by 2020. IDC, a top-notch research institution, also predicted that 30 billion connected devices will generate revenue of 1.7 trillion dollars for the IoT ecosystem by 2020[22]. Such astounding numbers from these predictions indicate the significant impact that IoT will make in our lives in the near future.

Additionally, new exciting possibilities have surfaced in both research and business domains including manufacturing, transportation, smart cities, green energy, e-health, retail and personalized user applications [2,3,4]. The application of this fast-growing technology is undoubtedly beneficial. However, one major problem that seems ignored is the issue of being able to track requests/responses in the midst of the interaction among these devices, which are able to request and provide services as well as data to each other. Again, many have envisioned some issues such as transparency, reliability and confidentiality of data and privacy[5,6,8,1]. Moreover, most research application of provenance in IoT, to a large extent, have focused on requesting data. The provenance data decision making have also been from user perspective rather than intelligent machines. Some researchers have proposed integration of provenance in the Internet of Things in order to solve the above-mentioned issues[6]. Provenance, as defined by W3C "*is information about entities, activities, and people involved in producing a piece of data or thing, which can be used to form assessments about its quality, reliability or trustworthiness*"[11]. This implies that having documentary evidence about the history of requests/responses, together with its origins and its processes, enable good data access, transparency and decision making with regards to tracing the source of requests/responses. This paper, however, seeks to deviate from the traditional norm by exploring how machines can infer about requests/responses in the Internet of Things. For instance, if a request (GET/PUT/POST/DELETE) is made by a mobile device to change the state of a thing within IoT, an intelligent machine, such as raspberry pie, might want to trace the lifecycle of such request, its timestamp, its traversal path, to its current state associated with its response. To achieve this, this paper proposes a provenance-based light-weight prototype, which utilizes CoAP, a machine to machine communication protocol meant for small, resource-constraint devices. Furthermore, we provide performance evaluation of this prototype against metrics such as response time (ms) and throughput (KB/s).

The rest sections of this paper are structured as follows. Section 2 discusses related works. Section 3 describes the details of the system and design and the performance analysis conducted. Section 4 discusses the limitations. Finally, Section 5 focuses on our findings and future works.

2. Related Work

This section provides related works regarding provenance in IoT. Provenance, to a large extent, has been studied and applied in many different domains such as databases[12], cloud computing[13], scientific workflows[14], grid and distributed computing[15]. Most research conducted focus on tracing the origin of data with the aim of establishing the authenticity, trust and the quality of data. Moreover, provenance still continues to be one of the major issues emanating from the concept of the Internet of Things. Indeed, some amount of research has been done in the realm of the Internet of Things[16,17]. Data Provenance in the framework of the Internet of Things requires an extension to include who, timestamp and time periods of processes on data in addition to why, where and when. Bauer et al, 2013[6], proposed a conceptual architectural model by providing IoT connection points to data provenance which comprised of an Information Model from the IoT infrastructure model serving as an infrastructural interface