Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 130 (2018) 318–325

Procedia Computer Science

www.elsevier.com/locate/procedia

9th International Conference on Ambient Systems, Networks and Technologies, ANT-2018 and the 8th International Conference on Sustainable Energy Information Technology, SEIT 2018, 8-11 May, 2018, Porto, Portugal

A physical access control system on the cloud

Filippos Antonolpoulos[a], Euripides G.M. Petrakis[a]*, Stelios Sotiriadis[b], Nik Bessis[c]

[a]*School of Electrical and Computer Enginnering, Technical University of Crete, Chania, Greece*
[b]*Department of Computer Science and Information Systems, Birkbeck, University of London, London, UK*
[c]*Department of Computer Science, Edge Hill University, UK*

Abstract

We present an automated Physical Access Control System (PACS) as a cloud service for controlling users' activity, navigation and access in large residential infrastructures (e.g. apartment buildings, shopping malls). The main idea is to install on buildings beacon Bluetooth radio transmitters that broadcast an identifier to nearby devices (e.g. users' mobile phones) and from there, together with users' information, to transmit this information safely to a private cloud. The service monitors peoples' movements and overall traffic in buildings and public facilities and offers prompt response on cases of critical events (i.e. overcrowding, health incidents, attacks etc.). PACS provides a variety of services aiming to inform the infrastructure manager for possible increase of users' activities or access requests that require permission based on subscriptions or authorization criteria. These services are deployed over secure private clouds capable of dealing safely with sensitive information while ensuring users' privacy. Collectively, anonymous history (log) data are sent to a public cloud for analysis.

Keywords: Cloud computing; Fog computing; Internet of Things; Bluetooth Beacon sensors; Physical access control system, PACS;

1. Introduction

The idea of the Internet of Things (IoT) combined with cloud computing, opens new horizons in the field of real time data collection and analysis. The use of wearable sensors and mobile devices and their capability for Internet connectivity provides significant benefits in applications areas that require fast and continuous monitoring of user data from anywhere (e.g. activity monitoring in health care, smart cities etc.). In real-life applications, huge amounts

* Corresponding author. Tel.: +302821037229; fax: +302821037542.
E-mail address: petrakis@intelligence.tuc.gr

10.1016/j.procs.2018.04.045

of data are collected and analyzed (e.g. for scientific or business purposes). The solutions have to be scalable (to deal with the ever-increasing number of users and size of data), cost-effective, respond within reasonable time (e.g. taking into account the time constraints of the application) and, address concerns related to users' privacy and data safety. Cloud is the ideal environment for IoT applications design and implementation due to reasons related to its affordability (no up-front investment, low operation costs), ease of deployment (taking advantage of IaaS and PaaS solutions already available in the market by many cloud vendors), low maintenance costs (easy software updates and enhancements), scalability (compute resources can be added on demand) and accessibility (IoT services can be accessed anytime from anywhere over the Web).

Cloud computing has some inherent disadvantages and limitations. Even though a cloud may offer virtually unlimited compute resources, internet bandwidth may impede application performance or, business or regulatory requirements of the application mandate for hosting resources in a specific place. This is typically the case with user data where severe restrictions in regards to data transfer and storage to public locations may apply (e.g. military, medical, people activity monitoring applications). Another limitation is with regards to security; although many attempts towards increasing the security on the cloud have emerged lately, users are not always willing to send their data to the cloud due to the unknown storage location and also, due to the perceived "distance" between them and their data. In general, the user or application owner has limited control on cloud infrastructures that are managed only by the service providers. This "distance" is also the main reason for the long delays that are experienced sometimes between the client devices and the services locations[1]. Examples for delay intolerant applications are physical access control systems, health monitoring and factory automation. To address these limitations, the paradigm of fog computing has lately emerged, starting from Cisco[3]. Fog computing can be assumed as an extension of cloud computing, bringing virtualized services closer to the edge of the network (i.e. close to the user on gateways or on user devices[4]). Fog brings the benefits of low latency (due to the close proximity), location awareness and increased security, privacy and availability. Efforts to standardize architectures and platforms for extending the cloud to support functional edge nodes are currently underway[†]. However, since the paradigm of fog computing has emerged only lately, architectures and platforms for extending the cloud to support functional edge nodes have not been fully designed yet.

In this work, we focus on the problem physical access control and activity monitoring of people using (i.e. living in or visiting) large public facilities (e.g. shopping malls, sport arenas or smaller areas such as cinemas, restaurants etc.) and residential infrastructures (e.g. apartment blocks). Access to public areas is granted, controlled or monitored by administrative personnel in order prevent emergency events (e.g. due to overcrowded areas, attacks, fire, health-related incidents etc.). Possible solution to dealing with situations such as the above, would be to warn or prevent users from accessing these sites or, to provide temporary access to user groups on demand or, based on authorization criteria and for specific time periods. Such procedures are often time-consuming and costly since they require the involvement of well trained personnel. For example, administrators of large buildings, may benefit by using computerized services capable of monitoring users' activities and informing them on events taking place in specific areas. In addition to dealing with critical events and ensuring users safety, installing and applying services facilitating access to areas where large numbers of people are concentrated, may also improve users experience (e.g. to avoid overcrowding or queuing, customers are advised to visit a place or use a facility in a later time). Furthermore, the analysis of information collected from large numbers of users (eventually this information becomes big) can lead to important conclusions in relation to users' behavior or the cause of critical events. Also, the analysis of this information may provide the means to real estate owners and tenants to improve their plan for more efficient, safer and profitable management of their facility.

The physical access application requires that services capable of dealing with information acquired from users (e.g. their mobile phones) and sensors run on a fog device (e.g. a local installation providing virtualized resources for data processing and storage). Alongside, to mitigate concerns of user data protection and users' privacy, we opt for

[†] https://www.openfogconsortium.org/wp-content/uploads/OpenFog-Architecture-Overview-WP-2-2016.pdf