Chapter 10
Microsense:
Sensor Framework for IoT System-on-Chip

Srinivasa K.G.
CBP Government Engineering College, India

Ganesh Hegde
M S Ramaiah Institute of Technology, India

Kushagra Mishra
M S Ramaiah Institute of Technology, India

Mohammad Nabeel Siddiqui
M S Ramaiah Institute of Technology, India

Abhishek Kumar
M S Ramaiah Institute of Technology, India

Pradeep Kumar D.
M S Ramaiah Institute of Technology, India

ABSTRACT

With the advancement of portable devices and sensors, there has been a need to build a universal framework, which can serve as a nodal point to aggregate data from different kinds of devices and sensors. We propose a unified framework that will provide a robust set of guidelines for sensors with varied degree of complexities connected to common set of System-on-Chip (SoC). These will help to monitor, control and visualize real time data coming from different type of sensors connected to these SoCs. We have defined a set of APIs, which will help the sensors to register with the server. These APIs will be the standard to which the sensors will comply while streaming data when connected to the client platforms.

DOI: 10.4018/978-1-5225-9866-4.ch010

INTRODUCTION

The Internet of Things (IoT) garnered major attention in the late 20th century. The phrase was coined in the year 1999 and is described as "The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/ network and any service" (Guillemin & Friess, 2009). The IoT field of computational sciences is rapidly expanding with the upcoming powerful embedded platforms such as Intel Galileo, Raspberry Pi, Odroid XU3 and Google Glass. The need of the hour is to ensure there is a unified framework that supports data extraction, data visualization and minimal platform control along with social sharing of the data. One of the daunting tasks is the deployment of the large-scale senor networks in the real world scenario.

IoT is going to comprise of uncountable devices which can sense data, compute and communicate information and potentially actuate. The data generated by these IoT devices have the potentially pave roads for novel, innovative and impactful applications and hence are very valuable. The immense data generated from these devices will challenge the currently existing approaches to data management and contribute to the emerging domain of big data. One of the key challenging tasks is to discover and the configure the sensors and the associated data before collecting and processing data from these devices (e.g. sensors) (Ashton, 2009).

RELATED WORK

In the current scenario, mobile phones not only serve as communication means, but also as a source of data from sensors that the distributed human centric sensing applications can collect and exploit. Among them, environmental monitoring systems and emergency response systems will specifically benefit from human-based sensing. Owing to the restriction on resources of mobile devices, data sensed is normally uploaded to the cloud. Nonetheless, modern solutions lack an integrated approach to support varied applications suitably, whilst lowering the power consumed on the mobile device.

In this context, Fakoor, Raj, Nazi, Di Francesco and Das (2012) put forward an integrated framework to store; process and deliver sensed data to human-centric applications installed in the cloud. The integrated platform forms the backbone of a novel delivery model, namely, Mobile Application as a Service (MAaaS) that permits the development of human-centric applications covering many disciplines, along with mobile social networks and participatory sensing. It particularly addresses a case study of an emergency response system for raising alarm in the event of fire. The framework showed reduction in the energy consumed on the mobile devices by the way of a prototype test bed implementation, while satisfying the requirements of the application.

Additionally, Sharma and Ghose (2009) presented an integrated comprehensive security framework that provides security services for all services of sensor network. Additional components i.e. Intelligent Security Agent (ISA) to evaluate degree of security and cross layer interactions in many components like Intrusion Detection System, Trust Framework, Key Management scheme and Link layer communication protocol.

Sensors attached to the smart phones and smart buildings makes possible mobile sensing and users' behavior modeling that opens the door for cutting-edge applications such as customized intelligent computing, activity prediction, behavior intervention and health monitoring. Privacy is a major hurdle in mobile sensing and behavioral modeling. The end users invariable have less trust in the processing