MedCrave
Step into the World of Research
International Journal of Biosensors & Bioelectronics

Editorial

Open Access
CrossMark

Editorial on sensors for IoT applications

Volume 3 Issue 3 - 2017

Vincenzo Conti
University of Enna Kore, Italy

Correspondence: Vincenzo Conti, Faculty of Engineering and Architecture, University of Enna Kore, Viale delle Olimpiadi, 94100 Enna, Italy, Email vincenzo.conti@unikore.it

Received: October 23, 2017 | **Published:** October 30, 2017

Editorial

The e-infrastructures are becoming more widespread and pervasive and, by enabling effective sharing of information and coordination of activities between diverse, dispersed groups, they are expected to transform knowledge-based tasks. E-infrastructures must support the development of heterogeneous applications for workstation network, for mobile and portable devices, which are not necessarily inter-operable and inter-cooperative for effective data portability, service and resource sharing, discovery, scheduling and integration. Specifically, the rapid developments in networking and resource integration domains have resulted in various distributed and collaborative computational technologies including Web 2.0, social networking, SOA, P2P, sensors, Grids, Clouds and Crowds. In this context and relating to all collaborative and pervasive computer technology, Internet of Things (IoT) and the underlying sensor platforms play a very important role. IoT is still a challenging vision as it aims to connect everyday 'things' and to enable them to inter-operate in an M2M in order to support human users in everyday interactions with the physical world. IoT technologies guarantee extended reach and reduced costs, improving typical scenarios where a tight human-computer interaction is required, like home automation, biomedical and environmental monitoring, wireless sensor networks, surveillance and access control, systems. Only by bringing innovation to all layers of the IoT system (business applications, services and sensors) by changing fruition modes and enabling new collaboration modes among "things" and humans on both local and global scales, this vision will be realized. For this purpose, heterogeneities in hardware, communication stacks, operational modes and support from e-infrastructures, will require the achievement of interoperability from multiple perspectives. One of the most important problems to approach in this context is related to security, privacy and trust: the discovery, communication and interaction between heterogeneous "things" that pertain to different operational contexts should be secured. The support from security infrastructure to "things" based on intelligent sensors represents a fundamental step in the whole process. Due to their low security capabilities, it is also important to understand and evaluate at design time the risks to the wider system associated to the integration of IoT "things" in that system. Implicit and plain threats to the privacy of human users must also be taken into account: while the sensitive data has to be restrained, also the traceability of the user inside the platform must be limited. Specific rules and standards are currently missing, and efforts in this field seem to be reduced if compared to the scientific and technological ones.

Acknowledgements

None.

Conflict of interest

The author declares no conflict of interest.