Editorial

Sebastian Steinhorst*

Internet of Things

https://doi.org/10.1515/itit-2020-0047

Internet of Things (IoT), together with adjacent terms digitalization and Industry 4.0, is currently dominating discussions as much in industry as in academic research. IoT describes a system architecture where all components are communicating using Internet technology and provide an unprecedented level of connectedness across all architecture layers. This enables a multitude of novel applications in previously non-digitalized domains.

A conventional IoT system is organized in a hierarchical fashion and composed of end devices, which are combining computation, communication, sensing and actuation capabilities in resource-constrained embedded platforms. Such IoT devices are then connected to the higher system layers, where IoT edge gateways link to the backend architecture. The backend architecture is currently synonymous with cloud computing where information is aggregated, processed and turned into control actions which are propagated back to the end devices.

From a higher-level perspective, together with cloud platforms as a service, the convergence of enabling technologies in power-efficient embedded computing platforms, wireless short and long range communication and the broad availability of cheap sensing and actuation devices and use cases enabled the wide adoption of IoT. However, there are many ongoing challenges and threats which are slowing down the further application of IoT, especially from a system complexity perspective.

This special issue of "Information Technology" will address such challenges which need to be overcome in order to contribute to a sustainable future for IoT and highlight recent research advancements.

Among these core challenges for IoT is the establishment of a cybersecurity methodology which can cope with the paradox of securing open systems. Traditionally, security protected a system from outside attacks. With modularity and interoperability being strongly promoted in the context of heterogeneous open architectures, security can no longer be considered on system level and instead has to be guaranteed on a component level. This is particularly challenging due to the limitations in security capabilities introduced by constrained IoT end devices. At the same time, security becomes a safety issue in all safety-critical IoT applications where a compromised system from the cybersecurity perspective turns into an unsafe system.

Integration of heterogeneous system components provided by different vendors creates an interoperability problem which calls for standardization of IoT system interaction. In current industrial IoT systems, required integration efforts between different vendors and ecosystems are high and discourage the desired open system architecture.

From the perspective of platform efficiency, many challenges still stem from the trade-off between locally computing with less performance at the edge, but saving communication overhead, and offloading computational tasks to the cloud backend. There is a common trend towards edge computing which, in certain real-time scenarios, is the only way to meet timing requirements and increase system resilience. However, application specific computational methods such as enabled by reconfigurable computing are not yet fully utilized in edge computing paradigms.

From a testing and verification perspective, the possibilities of formal methods to verify component and system architectures have not been systematically exploited and are a major research opportunity in the context of IoT.

Equally important are approaches to make complex architectures predictable and to gain insights into emerging technologies such as machine learning which inherently pose black-box challenges. Architecture decentralization by creating collaborating self-aware and self-organizing system components might be a relevant contributor to building resilient, secure and safe systems in a compositional way and opens up many research opportunities.

The collection of papers in this special issue of "Information Technology" addresses the discussed aspects from different angles and contributes to a better understanding of emerging scientific solutions and remaining open challenges.

***Corresponding author: Sebastian Steinhorst,** Technical University of Munich, Department of Electrical and Computer Engineering, Embedded Systems and Internet of Things, Arcisstr. 21, 80333, Munich, Germany, e-mail: sebastian.steinhorst@tum.de

Bionotes

Sebastian Steinhorst
Technical University of Munich, Department of Electrical and Computer Engineering, Embedded Systems and Internet of Things, Arcisstr. 21, 80333, Munich, Germany
sebastian.steinhorst@tum.de

Prof. Dr. Sebastian Steinhorst is an Associate Professor at Technical University of Munich in Germany. He leads the Embedded Systems and Internet of Things group in the Department of Electrical and Computer Engineering. He is also a Co-Program PI in the Electrification Suite and Test Lab of the research center TUMCREATE in Singapore. The research of Prof. Steinhorst centers around design methodology and the hardware/software co-design of distributed embedded systems for use in IoT, smart energy and automotive applications.