Chapter 4
Smart-M3 Techniques

ABSTRACT

The previous chapters elaborated the design principles that guide the development of smart spaces-based applications using the Smart-M3 platform. The principles aim at such properties for applications as (i) interoperability for a multitude of participated heterogeneous devices, services, and users localized in the physical surrounding and (ii) context-aware, situational, and personalized service construction and delivery. In this chapter, we present selected ontology-oriented modeling techniques for applying the principles. The aspect of shared semantic information management becomes essential for service construction. We describe techniques how implement this management in a smart space. A question of what is a smart service compared with regular service is still debatable. We describe techniques how implement various intelligence attributes in services constructed and delivered in M3 spaces.

INTRODUCTION

As we showed in Chapters 2 and 3, the M3 architecture and its open source implementation in the Smart-M3 platform employ such ontology-aware technologies of the Semantic Web as RDF and OWL (Gutierrez, Hurtado, Mendelzon, & Perez, 2011). This chapter elaborates some selected ontology-oriented modeling techniques to management of shared information within a smart space-based application (Korzun, 2016). The techniques show concrete possible directions for applying the proposed design principles, enhancing the principles to an application development methodology.

DOI: 10.4018/978-1-5225-2653-7.ch004

Context awareness is crucial for making services smart (Vasilev, Paramonov, Balandin, Dashkova, & Koucheryavy, 2012; Korzun, Nikolaevskiy, & Gurtov, 2015). In a Smart-M3 based application the context is shared, i.e., accessible and interpretable by required participants (Smirnov, Kashevnik, Shilov, Boldyrev, Balandin, & Oliver, 2009). To achieve the interoperability, the ontology-oriented technique is used (Kiljander et al., 2014). Moreover, the smart space supports virtualization for effective knowledge sharing (Korzun & Balandin, 2014). That is, we consider the smart space as consisting of information objects and semantic relations among them, resulting in knowledge corpus representation in the form of a semantic network. Its basic structure is defined by problem domain and activity ontologies (classes, relations, restrictions). Factual objects in I are represented as instances (OWL individuals) of ontology classes and their object properties represent semantic relations between objects.

Access to the shared information in the smart space is based on requests (or operations). In addition to instant read and write operations, advanced search queries and persistent queries are possible (D'Elia, Honkola, Manzaroli, & Cinotti, 2011; Galov & Korzun, 2014a). In this case, micro virtualization mechanisms can be used (Smirnov, Kashevnik, Shilov, & Teslya, 2013). Virtual private micro smart spaces are built on the combination of the role-based and attribute-based access control models. Roles are assigned dynamically based on the smart space participant's trust level. The role separation allows simplifying policies and makes them human-readable and easy to configure. The trust level calculation is based on the participant's context, which includes identification attributes; location; current date; device type, etc. Access control rules can be used to calculate the trust level, to assign roles based on the trust level, and to grant permissions to the smart space resources.

Smart space deployment becomes a non-trivial problem due to the essential variety of IoT devices (Korzun, Balandin, & Gurtov, 2013). The traditional case, when a data storage is located on a powerful machine, now is not the best solution. Smart space is considered as a very ad-hoc system, when SIB can run on embedded or mobile devices (Korzun, Galov, & Lomov, 2016; Korzun & Balandin, 2016). Furthermore, the SIB functionality is composite, and some modules can be added or removed in customization of the smart space for given IoT environment and the application problem needs (Galov, Lomov, & Korzun, 2015). The same composite property can be implemented

Related Content