

Web for Information and Knowledge Exploration, Sharing and Security

Topical Issue for Springer Nature - Computer Science

Objectives

This Special Issue of Springer Nature will explore new trends and research in advanced software technologies, including three main themes related to: (1) adaptive and reconfigurable service-oriented and component-based applications and architectures; (2) semantic technologies for smart information sharing and Web collaboration; (3) security, safety, and trust management. These technologies are explored using theoretical approaches as well as using practical experience. They are present in both well established and emerging interdisciplinary applications and domains, including, for instance, Industry 4.0, Big Data, Social Networks, Internet of Things, eHealth, Smart Cities and Communities, Entertainment, eLearning, eGov, Digital Agriculture, Cybercrime, and Internet Security.

The topics related to the **first theme** address one or more of the different challenges of this new context. The adaptive and reconfigurable software systems, and the associated architectures, are of most interest for a wide family of distributed activities with different application domains. An adaptive and reconfigurable software system, in order to successfully complete its own mission, can repair itself when execution or communication problems occur, while fulfilling functional and Non-Functional agreements. In the design of an adaptive and reconfigurable software system, several aspects have to be considered based on the knowledge models, which includes the dynamics of parameters, and the reasoning over their evolution. For instance, the system should be able to predict or to detect service degradations and failures as soon as possible, and to enact suitable recovery actions. For this purpose, different R&D directions are being investigated to address system description, monitoring, analysis, and repair models and solutions. Different techniques are being considered for the context of virtualization and softwarization of networking and processing technologies.

The **second theme** tackles knowledge and data sharing based on software engineering, artificial intelligence, and methods for Knowledge Organization Systems (KOS) (e.g. ontologies, taxonomies, etc.). Improvements obtained through enhanced organization and management of knowledge calls for new techniques of knowledge exploration, analysis, sharing, and security in order to support enhanced collaboration on the Web. New advances in web-based systems drive changes in cooperative activities, where humans are increasingly supported via the internet and the Web. Web practitioners, users, and applications explore, in rapidly varying ways, the richness of the Web to support the user's activities. Based on these considerations, the focus of this theme is on information creation, maintenance, disambiguation, and interlinking. Reasoning and deep learning techniques are also considered, since these lead to better decisions or awareness of events. The theme considers the concept of "working together" by exploring decision support assistance, collective intelligence, semantic search, smart environments, intention-based analysis, and other collaborative-based ways for problem solving.

The **third theme** focuses on security and privacy research areas. Information and Knowledge security has become the main challenge in this continuously evolving technological era, as well as in the threats landscape. These threats pose critical issues that might disrupt the seamless provision of services, which requires the overall infrastructure of an organization consisting of Humans and data retention, and communication channels. The other critical issue of such continuously emerging cyber threats is the poisoning of the learning data used in decision support systems by any organization, resulting in inconsistent or malicious results for the knowledgebase. This theme shall emphasize contributions from the research

community that address these grave challenges of information and knowledge security.

Keywords

Theme 1.

IoT; Smart Cities; Intelligent Automated System Management; Dynamic Reconfiguration; Context-aware Management

Theme 2.

Ontologies; Knowledge Graphs; Knowledge Engineering; Semantic Technology; Semantic Web

Theme 3.

Security; Safety; Trust; Privacy; Dependability; Cybersecurity; Mission Assurance

Topics Covered

Overall, this Special Issue addresses Intelligent (web-Based) Solutions for Software, Information, and Knowledge Exploration, Sharing, and Security, and is concerned with improvements obtained through enhanced organization, and management of information and knowledge. Examples of topics are models and tools for intelligent system management. Other examples are dynamic changes in shared information, smart (context-aware) Web applications, and experiences in new domains of application of semantic techniques, integrating social networks, big data, Internet of Things, enhanced connectivity, and mobile technologies. Examples of security, safety, and trust include models and tools for critical infrastructure, security in cloud, cyberwar, cybercrime analysis, and security software development.

We structure this topical issue into three main themes:

Theme 1. Information and Knowledge Exploration

- ☐ Advances in IoT/M2M solutions and cognitive models for Smart Cities
- ☐ Intelligent and automated service and function description, discovery and selection
- ☐ Dynamic reconfiguration of cloud and edge environments
- ☐ Context-aware and semantic-enabled system management

Theme 2. Information and Knowledge Sharing

- ☐ Ontologies and Knowledge Graphs
- ☐ Semantic sharing, and collaborative knowledge management
- ☐ Collaborative semantic web techniques and applications
- ☐ Experiences analyzing publicly available datasets

Theme 3. Information and Knowledge Security

- ☐ Data Security and Privacy
- ☐ Critical Infrastructure Security
- ☐ Legal Aspects of Information Security
- ☐ Malware Detection and Analysis
- ☐ Dependable Security
- ☐ Security in Cloud Computing
- ☐ Organizational Information Assurance Mechanisms
- ☐ Secure Software Development

- ☐ Cyber-Crimes

Important Dates

- ☐ Submission deadline: November 30, 2019
- ☐ 1st round of reviews: February 15, 2020
- ☐ Final round of reviews: March 15, 2020
- ☐ Publication date: April 30, 2020

Guest Editors

- ☐ Haider ABBAS, Nat. Univ. of Sciences & Technology, Pakistan
- ☐ Hammad AFZAL, Nat. Univ. of Sciences & Technology, Pakistan
- ☐ Rodrigo BONACIN, CTI, Brazil
- ☐ Ismail BOUASSIDA, University of Sfax, ReDCAD lab, Tunisia
- ☐ Khalil DRIRA, LAAS-CNRS and Univ Toulouse, France
- ☐ Mariagrazia FUGINI, Politecnico di Milano, Italy
- ☐ Riccardo MARTOGLIA, UniMoRe, Italy
- ☐ Olga NABUCO, CTI, Brazil
- ☐ Fatiha SAÏS, LRI, Paris Sud University, France

Paper Submission

Papers submitted to this topical issue must be written in English, formatted according to the formatting instructions available on the submission website ("Instructions For Authors" link), and submitted in PDF format. Papers must contain: (i) original contributions not published or submitted elsewhere or (ii) already published works with a minimal 30% addition of new contributions (invited extended paper). When submitting the article, in the 'Additional Information' tab, authors must select the "Web for Information and Knowledge Exploration, Sharing and Security" topical issue, and specify the Theme they are submitting to. Papers have to be submitted through the Springer Nature Submission system <https://www.editorialmanager.com/snscs/>.