



# Service-enabled systems and applications: current and future trends

Karim Benouaret<sup>1</sup> · Patrick C. K. Hung<sup>2</sup> · Ladjel Bellatreche<sup>3</sup>

Received: 27 May 2021 / Revised: 30 May 2021 / Accepted: 2 June 2021 / Published online: 23 June 2021  
© The Author(s), under exclusive licence to Springer-Verlag London Ltd., part of Springer Nature 2021

## 1 Introduction

Since its establishment as a software design style, Service-Oriented Architecture (SOA) has taken the Information and Communications Technology (ICT) world by storm. The keyword for this success is adaptivity: SOAs are implemented through a wide range of technologies and tools leading to numerous combinations that meet the application requirements in the desired way.

With the emergence of Industry 4.0, the development of SOAs has to deal with a specific combination of application characteristics and requirements, e.g., data-intensive tasks coupled with temporal requirements. Big Data and the Internet of Things (IoT) applications are simply two general application categories that come with exactly those characteristics. The challenges are justified because SOA was not originally designed for these kinds of applications.

## 2 Challenges and current solutions

In this section, we discuss some of the most important challenges in building service-enabled systems and applications and some popular solutions.

### 2.1 Service composition

Service composition, including orchestration, choreography and transaction concepts, is still among the challenges characterizing our paradigm [4]. The literature on service

composition is rich; we refer the reader to the related research works in [9,11] for a systematic treatment of this research area.

These challenges arise not only in the standard problem of Web service composition but also in more recent fields, particularly in IoT service composition. IoT services are different from traditional Web services due to the dynamic environment in which they arise. The authors [2] presented a systematic literature review on several service composition approaches that are applied in the IoT environment between 2012 and 2017. The authors presented a technical taxonomy that classifies the studies into functional and non-functional aspects. The former aims to verify the behavior of the service composition, while the latter considers the Quality of Service (QoS) factors of the service composition. The approaches are compared, and their pros and cons are discussed. The authors [5] developed an agile IoT service communication and orchestration platform using event-driven SOA paradigm, which allows the IoT service communication and orchestration respond quickly to the dynamic changes in the physical world in a timely manner. The authors [1] proposed an ontology-based model for the integration of the IoT and Cloud Enterprise Resource Planning (ERP) systems by using Semantic Web services and Artificial Intelligence (AI) planning technique to semi-automatically compose IoT and Cloud ERP services.

### 2.2 Security and privacy

Security and privacy are among the most significant challenges, particularly when services manipulate sensitive data. For example, patients who have access to a cloud-based healthcare system. Such a system is subjected to various security concerns due to the number of hosts were connecting to the Cloud storage service. The authors [14] analyzed privacy and security concerns on 1,550 users of COVID-19 tracking applications. The authors identified a set of measures and guidelines that can be exploited by the developers of mobile tracking applications to address the identified concerns. The authors [12] addressed the problem of securing data transmis-

✉ Karim Benouaret  
karim.benouaret@univ-lyon1.fr

Patrick C. K. Hung  
patrick.hung@ontariotechu.ca

Ladjel Bellatreche  
bellatreche@ensma.fr

<sup>1</sup> Université Claude Bernard Lyon 1, Villeurbanne, France

<sup>2</sup> Ontario Tech University, Ontario, Canada

<sup>3</sup> ISAE-ENSMA, Chasseneuil-du-Poitou, France

sion between IoT objects and applications in gateway-based IoT architectures. The authors proposed a secure and end-to-end data encryption scheme, which allows an untrusted IoT platform to distribute the data transmitted by IoT objects to several applications based on their data access rights without decrypting the data. The authors [3] presented a method for preserving the privacy and improving the utility of sensitive documents hosted in public cloud environment. Even though the privacy and utility are inversely proportional, both of them are balanced using effective metrics.

### 3 Future trends

In this section, we present some possible research perspectives in the area worth exploring in the future.

#### 3.1 Uncertain urban data management

With the proliferation of online social media and the use of sensors, and location technologies, the data available in modern cities have experienced explosive growth. Offering new applications for analyzing and exploiting the data collected in modern cities will be a booming research direction. Especially since the data handled by the services are suggested to the uncertainty and imprecision. For example, people leave behind them geographical traces, in the form of explicit Global Positioning System (GPS) traces (e.g., running and hiking routes) or implicit (e.g., tweets and purchases), often uncertain and accompanied by secondary information (e.g., text and images). Designing techniques that deal with the imprecision and uncertainty of urban data will certainly be popular.

#### 3.2 Fairness-aware service recommendation

Service Recommendation aims at suggesting interesting services to users based on their preferences and context [10]. Most service recommendation techniques ([13,17]) usually recommend popular services to users due to their reputation and trust and become a barrier for the unpopular services to startup even if they are likely to meet user preferences. Hence, these services often leave the platforms. Taking into consideration the notion of fairness during the recommendation process would be of great use. This may be done, for example, by considering the notion of novelty when recommending services.

#### 3.3 Machine learning for cybersecurity in social robots

Machine learning employs software tools from advanced analytics disciplines such as data mining, predictive ana-

lytics, and text-based on a set of algorithms that attempt to model high-level abstractions in data by using multiple processing layers with complex structures or nonlinear transformations. In this context, different machine learning techniques can be applied, although some of them naturally have a greater predisposition to be useful, such as artificial neural networks and decision trees, as they have already shown good results in other areas of application besides SOA [7]. Cybersecurity is defined as a set of processes, human behavior, and related systems that help safeguard and protect resources against potential cyberthreats. Cyberthreats vary from simple sniffing and eavesdropping to full-fledged attacks such as Denial of Service (DoS), Man-in-The-Middle (MiTM), Structured Query Language (SQL) injection, cross-site scripting, hacking, and malware attacks. Machine learning can be applied for solving cyber-security problems, e.g., intrusion (cyberattack) detection model. A social robot consists of a physical robot component to interact with humans that connect through a network infrastructure to a computing system with Cloud services that enhance traditional robot functionality like an IoT device such as ASUS Zenbo and Softbank Robotics Pepper. Machine learning can be applied for solving cybersecurity problems in IoT devices such as social robots, e.g., intrusion (cyberattack) detection model [6,8].

#### 3.4 Resilience-driven web service design

We cannot conclude this editorial without addressing one of the important issues highlighted by the COVID-19 pandemic related to resilience. In March 2020, an interesting paper was published in the Communications of the ACM by Prof. Moshe Y. Vardi entitled Efficiency vs. Resilience: What COVID-19 Teaches Computing [15]. This article points the crucial responsibility of computer scientists and professionals for developing services/systems that recognize the trade-off between efficiency and resilience. More precisely, during this pandemic, suddenly we realize that our daily lives depend on may be efficient and non-resilient services. This contributes to having degraded public health services caused by the shortage of masks, ventilators and personal protective acquirement. In education and remote work, we found ourselves face to security and privacy issues of the Zoom platform. The finding identified by Moshe's paper applies to Service Web. This is because efficiency was one of the nonfunctional requirements considered when designing Service Web [16]. This manner of designing offers a kind of short-time optimization, but ignores the long-term optimization. As scientists, we have to provide guidelines for young researchers to consider resilience requirement in designing and deploying Web services. This resilience has to include fault tolerance, security, and energy. The integration of resilience in Web Services requires researchers

to provide strong survey Quality of Service (QoS) adaptation, interface/protocol adaptation, cross-layer adaptation, autonomous adaptation, and adaptive substitution of services. This resilience has to be accompanied by formal methods to verify this adaptation. Another issue concerns the development of cost-benefit analysis for the resilience implementations.

**Acknowledgements** We hope our readers will find the content of this special issue, interesting to the point of motivating young scientists to develop solutions for service-enabled systems and applications. The guest editors of this special issue wish to express their sincere gratitude to all contributing authors. We are also grateful to the Reviewing Committee for their hard work and constructive feedback provided to the authors. As guest editors of this special issue, we also wish to express a special acknowledgment to the Editor-in-Chief Prof. Kuo-Ming Chao for the opportunity to edit this special issue. Last but not least, we also thank the Journal's staff for their editorial assistance. We acknowledge the following *Reviewing Committee members*: Idir Ait Sadoune (France), Mahmoud Barhamgi (France), Amel Benna (Algeria), Benjamin Bogdanovic (United Kingdom), Christopher Chan (Canada), François Charoy (France), Marco Comuzzi (South Korea), Sayda Elmi (Singapore), Ernesto Exposito (France), Catarina Ferreira da Silva (Portugal), Emna Hachicha Belghith (Belgium), Slim Kallel (Tunisia), Sylvain Lefebvre (Japan), Michael Mrissa (Slovenia), Samir Ouchani (France), Gwen Salaun (France), Salma Sassi (Tunisia), Akila Siriweera (Japan).

## References

1. Androcec D, Picsek R, Mijac M (2018) The ontologically based model for the integration of the iot and cloud ERP services. In: Proceedings of the 8th International Conference on Cloud Computing and Services Science (CLOSER), pp 481–488
2. Asghari P, Rahmani AM, Javadi HHS (2018) Service composition approaches in iot: A systematic review. *J Netwo Comput Appl* 120:61–77
3. Benifa JVB, Mini GV (2020) Privacy based data publishing model for cloud computing environment. *Wireless Pers Commun* 113(4):2215–2241
4. Bouguettaya A, Singh MP, Huhns MN, Sheng QZ, Dong H, Yu Q, Neiat AG, Mistry S, Benatallah B, Medjahed B, Ouzzani M, Casati F, Liu X, Wang H, Georgakopoulos D, Chen L, Nepal S, Malik Z, Erradi A, Wang Y, Blake MB, Dustdar S, Leymann F, Papazoglou MP (2017) A service computing manifesto: the next 10 years. *Commun ACM* 60(4):64–72
5. Cheng B, Zhao S, Niu M, Chen J (2018) Agile iot service communication and orchestration platform using event driven SOA paradigm. In: *IEEE INFOCOM*, pp 1–2
6. Fantinato M, Hung PCK (2021) Machine learning and secure service-oriented architecture (soa). In: *Encyclopedia of Machine Learning and Data Science*, Springer Nature
7. Hung PCK, Blake MB (2018) Reflecting on two decades of services computing. *IEEE Internet Comput* 22(5):3–7
8. Hung PCK, Iqbal F (2021) Machine learning for cybersecurity in smart toys. In: *Encyclopedia of Machine Learning and Data Science*
9. Lemos AL, Daniel F, Benatallah B (2016) Web service composition: A survey of techniques and tools. *ACM Computing Surveys* 48(3):33:1–33:41
10. Mezni H, Benslimane D, Bellatreche L (2021) Context-aware service recommendation based on knowledge graph embedding. *IEEE TKDE*
11. Paik H, Lemos AL, Barukh MC, Benatallah B, Natarajan A (2017) *Web Ser Implement Compos Tech*. Springer, Berlin
12. Peng C, Chen J, Vijayakumar P, Kumar N, He D (2021) Efficient distributed decryption scheme for iot gateway-based applications. *ACM Tran Internet Technol* 21(1):1–23
13. Samanta P, Liu X (2017) Recommending services for new mashups through service factors and top-k neighbors. In: Altintas I, Chen S (eds) 2017 IEEE International Conference on Web Services (ICWS), IEEE, pp 381–388
14. Sharma T, Dyer HA, Bashir M (2021) Enabling user-centered privacy controls for mobile applications: Covid-19 perspective. *ACM Trans Internet Technol* 21(1):1–24
15. Vardi MY (2020) Efficiency vs. resilience: what COVID-19 teaches computing. *Communications of the ACM* 63(5):9
16. Xu B, Luo S, Yan Y, Sun K (2012) Towards efficiency of qos-driven semantic web service composition for large-scale service-oriented systems. *Ser Orient Comput Appl* 6(1):1–13
17. Zhang Y, Lei T, Wang Y (2016) A service recommendation algorithm based on modeling of implicit demands. In: *IEEE International Conference on Web Services (ICWS)*, pp 17–24

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.