Journal of King Saud University – Computer and Information Sciences (2016) **28**, 470–480

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Journal of
King Saud University –
Computer and
Information Sciences

Trust-based Service-Oriented Architecture

Zainab M. Aljazzaf [a,*], **Miriam A.M. Capretz** [b], **Mark Perry** [c]

[a] *Department of Information Science, Kuwait University, Kuwait*
[b] *Department of Electrical and Computer Engineering, Western University, Canada*
[c] *School of Law, The University of New England, Armidale, NSW, Australia*

Received 17 May 2015; revised 28 October 2015; accepted 22 December 2015
Available online 22 April 2016

KEYWORDS

Trust;
Service-Oriented Architecture;
Service providers

Abstract Service-Oriented Architecture (SOA) is an architectural style in building Web applications based on services. In SOA, the lack of trust between different parties affects the adoption of such architecture. Because trust is an important factor in successful online interactions, it is a major criterion for service selection. In the context of online services and SOA, the literature shows that the field of trust is not mature. The definitions of trust and its essential aspects do not reflect the true nature of trust online. This paper proposes a comprehensive trust-based SOA solution based on an identified trust definition and its principles for selecting services based on their trustworthiness. In particular, SOA is extended and a new component, the trust framework, which is responsible for the trust process, is added to the architecture. Consequently, its components are identified and built. The trust-based SOA is implemented through experiments and scenarios.

1. Introduction

The development of distributed software requires the interaction of services from different Web service providers. Service-Oriented Computing (SOC) is "a computing paradigm that utilizes services as fundamental elements to support rapid, low-cost development of distributed application in heterogeneous environments" (Papazoglou and Georgakopoulos, 2008). A service is "a discrete unit of business functionality that is made available through a service contract" (Rosen et al., 2008). Specifically, a distributed application may be composed of global services with different properties provided by different organizations. In this environment, the development of trust is challenging.

To realize the potential of SOC, Service-Oriented Architecture (SOA) should be developed. SOA is "a framework for integrating business processes and supporting IT infrastructure as secure, standardized components – services – that can be reused and combined to address changing business priorities" (Bieberstein et al., 2005).

SOA has a significant impact on the way software systems are built. Although there have recently been reports that SOA adoption rates are dropping and that "SOA is dead", Forrester Group reported that SOA adoption is increasing across all of its vertical-industry groups (Lewis, 2013). Gartner Group reports that 50 percent of new vital operational applications and business processes were designed around SOA in 2007

[*] Corresponding author.
E-mail addresses: dr.zainab@ku.edu.kw (Z.M. Aljazzaf), mcapretz@uwo.ca (M.A.M. Capretz), mperry21@une.edu.au (M. Perry).

Peer review under responsibility of King Saud University.

ELSEVIER **Production and hosting by Elsevier**

http://dx.doi.org/10.1016/j.jksuci.2015.12.003
1319-1578 © 2016 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

and that adoption will increase to more than 80 percent by 2010.

Fig. 1 illustrates the relationship between SOA roles and operations. There are three interaction roles in SOA: the *service provider*, which owns, implements, and controls access to the services; a *service requestor*, which is an application, service, or client who is searching and invoking a service; and a *service broker* that groups all of the services together and maintains a registry of available services (Papazoglou and Georgakopoulos, 2008). A service registry is a directory in which the services are published by the providers and searched by the requestors (Papazoglou, 2012).

Moreover, there are three operations within SOA (Papazoglou, 2012). In the *publish operation*, service providers publish their services into the registry. In the *find operation*, requestors search and find services from the service registry. Finally, in the *bind operation*, requestors invoke services at run time using the technical information provided in the WSDL file to bind to the services.

To build a service-oriented application, requestors can select services from different providers on the Internet. Because there are many services with similar functionalities, requestors need to differentiate between them. The only differentiating factor between similar services may be their non-functional properties, which can be considered criteria for service selection. As a non-functional property, trust has been used as a criterion for service selection (Dragoni, 2009; Huhns and Singh, 2005; Kalepu et al., 2003; Azarmi et al., 2012; Kim and Doh, 2013).

Trust is *''the willingness of the trustor to rely on a trustee to do what is promised in a given context, irrespective of the ability to monitor or control the trustee, and even though negative consequences may occur*'' (Aljazzaf et al., 2010). A service requestor, or *trustor*, may select a service from a service provider, *trustee*, based on their trustworthiness. Thus, trust can help requestors in their service selection. In addition, some service providers provide poor services or intentionally offer services that are not consistent with their promises (Jin-Dian et al., 2005). Thus, it is necessary to determine the trustworthiness of services and to select a trustworthy service. Moreover, trust is a less expensive approach for service selection than monitoring or Service Level Agreements (SLA) (Wang and Vassileva, 2007).

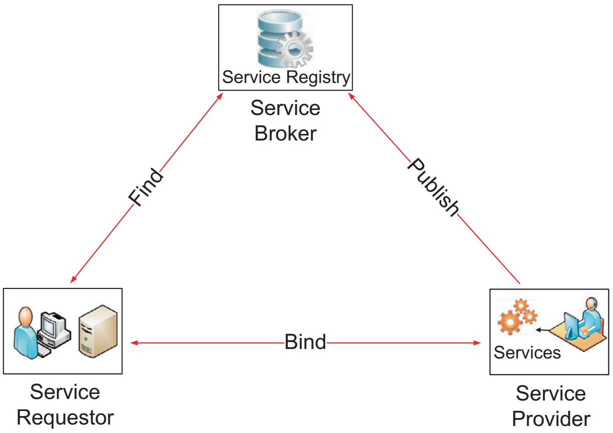

Fig. 1 Service Oriented Architecture (SOA) (Papazoglou, 2012).

There are different principles that reflect the core nature of trust. These principles consider trust aspects and identify requirements for establishing a comprehensive and concrete solution for trust (Aljazzaf et al., 2010; Daignault et al., 2002). Some principles include the following: trust and risk are related, the trust development phases should be considered, trust is dynamic, trust depends on identity, trust is based on information.

Although SOA continues to be broadly adopted, there has been surprisingly little interest in building complete solutions that facilitate trust-based service selection. Such a complete solution is required and should be described in detail. Accordingly, there is a need to extend SOA to support trust, and such extension includes building a unified framework and model of trust considering trust definition and trust principles that incorporate many trust aspects, can be easily extendible, and resolve different trust challenges.

The rest of the paper is presented as follows. Section 2 presented the related work. The proposed trust-based SOA is introduced in Section 3. Section 4 covers the proposed trust framework and discusses its components. The experiment is presented in Section 5, and its evaluation is discussed in Section 6. Finally, Section 7 presents the conclusion and future work.

2. Related work

Research on trust has attracted a great deal of attention in SOC. However, the literature about trust on SOA is still immature. Existing solutions for trust in SOA, including trust frameworks and models, are not built based on a standard definition of trust and do not follow principles that reflect the core nature of trust.

Existing OASIS WS-Trust and WS-Security standards ensure hard security mechanisms of SOA applications. However, trust is not covered as an essential service that reflects the nature of trust as we have defined it.

Moreover, Azarmi et al. (2012) provide a solution for end-to-end security auditing in SOA and maintaining a dynamic trust among services. The trust broker specifies the various levels of trust (Certified, Trusted, or Untrusted) and uses a reputation-based system to preserve the trust levels based on several criteria, including the history of previous interactions. Kim and Doh (2013) build a framework and add a trust mediator as a QoS broker for governing the trust process. The authors propose a trust management model that supports service discovery and selection based on QoS, specifically utilizing security, trust, and reputation. However, the authors define trust as a QoS, and their mechanism uses consumers' feedback, which is highly human dependent and therefore error-prone. Liu et al. (2014) introduce a Web Service evaluation model by leveraging trust as an approach. They incorporate a trust management module into the standard SOA and then transform a Web Service network to a small-world network. However, their framework is built upon only a trust management module and is based on small-world networks. Many researchers have studied security certification, which is aimed at increasing the confidence of the clients by satisfying their security requirements (Anisetti et al., 2012; Anisetti et al., 2013; Katopodis et al., 2014; Kaluvuri et al., 2013; Cimato et al., 2013).