Future Generation Computer Systems 49 (2015) 142–148

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure service composition with information flow control in service clouds

Ning Xi [a,b,*], Cong Sun [a], Jianfeng Ma [a], Yulong Shen [a]

[a] School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China
[b] School of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, China

HIGHLIGHTS

- For the dynamic dependences in service chain, we propose a Secure Information Flow Model for service composition in service clouds.
- We specify the security constraints for each service participant based on the dependences and lattice model.
- We propose a distributed compositional information verification algorithm for the secure service composition in service clouds.
- Our approach simplifies the complexity of model checking and decreases the cost of the verification work effectively.

ARTICLE INFO

Article history:
Received 28 February 2014
Received in revised form
12 December 2014
Accepted 28 December 2014
Available online 28 January 2015

Keywords:
Service cloud
Service composition
Data dependencies
Information flow security

ABSTRACT

Service clouds built on cloud infrastructures and service-oriented architecture provide users with a novel pattern of composing basic services to achieve complicated tasks. However, in multiple clouds environment, outsourcing data and applications pose a great challenge to information flow security for the composite services, since sensitive data may be leaked to unauthorized attackers during service composition. Although model checking has been considered as a promising approach to enforce information flow security precisely, its high complexity on modeling and the heavy cost on verification cause great burdens to the process of service composition. In this paper, we propose a distributed approach to composing services securely with information flow control. In our approach, each service component is first verified through model checking, and then a compositional verification procedure is executed to ensure the information flow security along with the composition of these services. The experimental results indicate that our approach can reduce the cost of verification compared with the global verification approach.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

With the advancement of sharing the utility resources in a virtualization way, cloud platforms provide a new and promising paradigm for delivering IT services more effectively and conveniently [1,2]. In service-oriented clouds, people can access various types of services integrated by cloud platform anytime and anywhere. Meanwhile the composition and cooperation of different services have become a new trend for the service delivery in clouds. By composing services together, customers can access more powerful applications, e.g. travel planning composed by tickets booking and room reservation services [3]. For each service, there are different candidate services located in multiple clouds. From a variety of the candidate services, users can select appropriate services to compose the desired applications dynamically according to different criteria and requirements, e.g. QoS, trustworthiness, security and so on [4,5].

However, outsourcing data and applications in clouds pose a great challenge to data security for the service composition in clouds. Due to the multi-domain characteristic of the service clouds, data located in different clouds may have different security levels. For instance, the personal medical records in e-health cloud are with high security level while the position of the ambulance in e-transportation cloud are with lower security level. When these services are composed together for the patient's emergency, data with different security levels are transmitted among these services respectively. If these services are composed in an insecure way, an operation in a service may transmit confidential data to a public channel and cause the information leakage. Access control has

* Corresponding author at: School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China.
E-mail addresses: xining@stu.xidian.edu.cn (N. Xi), suncong@xidian.edu.cn (C. Sun), jfma@mail.xidian.edu.cn (J. Ma), ylshen@mail.xidian.edu.cn (Y. Shen).

http://dx.doi.org/10.1016/j.future.2014.12.009
0167-739X/© 2014 Elsevier B.V. All rights reserved.

been widely used for protecting sensitive information of individual service from being released to unauthorized attackers [6–8]. However, for a composite service, data may be processed by several service components from multiple clouds. Access control cannot detect the information leakage caused by the subsequent operations in other service components. Therefore, information flow security is one of the major concerns about the service composition in service clouds.

Due to the dynamic dependencies among objects storing data in different service participants, it is critical to analyze information flow in these composite services precisely. There are various approaches for the information flow enforcements, e.g. type system, program analysis and model checking. Dieter et al. [9] specify the secure composition rules based on type system. These rules are used to ensure the security of dynamically derived data and their proliferation to other web services. Xi et al. [10] obtain the dynamic intra and inter dependencies among the objects in composite service based on program slicing. Nakajima [11] verifies the information flow of composite services in BPEL (Business Process Execution Language) based on model checking. Rossi et al. [12] expand Nakajima's model [11] to support more flexible and dynamic security policies rather than security labels based on a simple lattice-based model. The contributions using type system and program analysis mainly focus on the information flow enforcement on programming languages, while model checking can be used to validate both programs and models in abstract forms.

Besides, service-oriented clouds compose a distributed system with multiple domains. It is necessary to design a secure and efficient service composition algorithm in a distributed environment. She et al. [13] proposes a policy-driven service composition approach with information flow control in multiple service domains. In She's approach, the security levels of the output in a component is computed according to the transformation factor, then the insecure composite service is filtered. However, it is hard to define the transformation factor precisely. She et al. also develops a run-time information flow control model for service composition in clouds to analyze the dependencies between the inputs and outputs dynamically in [14]. But it requires that the initial user inputs for the service execution be static. So when user's initial inputs change, the verification process needs to be rebuilt, which brings extra cost for the secure service composition. Although model checking [11,12,15] can be used to analyze secure information flow precisely, the traditional model checking approaches must perform a global verification on the composite service. It is impractical to employ a centralized entity in multiple clouds to verify the information flow security in a global way. Moreover, the cost of verification can increase rapidly when the application involves more components and the number of the candidate services increases. First, the same service component has to be reverified in different composite services. Second, the state explosion problem arises if each service component is complicated.

In order to ensure the information flow security and improve the efficiency of the service composition process, we present a distributed secure service composition approach with information flow control in service clouds. In our approach, each service component is verified through model checking, which can reduce the complexity of modeling compared to the global verification approach. Then compositional information flow verification algorithm is proposed for the secure service composition in service clouds, which works in a distributed way.

The rest of the paper is structured as follows. Section 2 presents the secure information flow model for service composition in service clouds. In Section 3, we propose the secure service composition approach based on the secure information flow model. Section 4 evaluates the proposed approach. Section 5 concludes the paper.

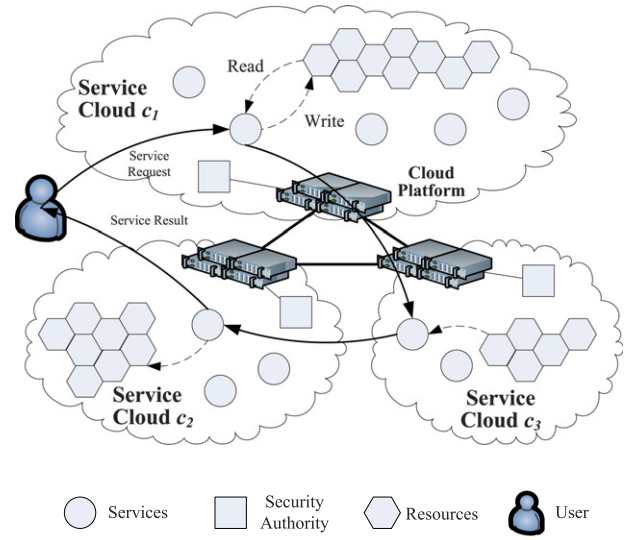

Fig. 1. Service-oriented clouds system.

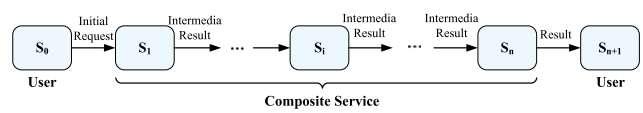

Fig. 2. Service chain.

2. Secure information flow model for service composition in service clouds

2.1. Service-oriented clouds system model

Fig. 1 shows a typical architecture of the Service-Oriented Clouds System (SoCS) consisting of multiple service clouds. In each service cloud c, there are various services s_i and resources R_c, and a security authority SA_c, where SA_c is responsible for the security management of cloud resources and services, e.g., data security level, security certificate, and so on.

The individual services s_i located in different service clouds can be composed to generate a more powerful service. In this paper, we investigate a typical scenario of service composition, i.e., the service chain s_{ch} [10], as shown in Fig. 2. Compared to the complex composite service with conditional and loop structures, service chain is easy to control and deploy, which is widely used in service composition. In a service chain s_{ch}, each service s_i has a single predecessor s_{i-1} and a single successor s_{i+1}. The initial service s_0 denotes the user who sends the initial request. Service s_{n+1} denotes the user who receives the result from the composite service.

2.2. Multi-level security model

In SoCS, data are with different sensitivities, e.g. environment data are public while personal position and medical data are private. The multi-level security model can be defined on a lattice as Definition 2.1.

Definition 2.1. Multi-Level Security Model is defined as a lattice $(SL, \leq)$, where SL is a finite set of security levels that is totally ordered by $\leq$.

For simplicity, we mainly consider the binary security model, i.e., $SL = \{L, H\}$, where $L \leq H$.

Download English Version:

https://daneshyari.com/en/article/424595

Download Persian Version:

https://daneshyari.com/article/424595

Daneshyari.com