Computer Standards & Interfaces 44 (2016) 220–233

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Security-aware Business Process as a Service by hiding provenance

Mehdi Bentounsi [a,*], Salima Benbernou [a], Mikhail J. Atallah [b]

[a] Université Paris Descartes, Sorbonne Paris Cité, France
[b] Purdue University, Department of Computer Science, 305 N. University Street, West Lafayette, IN 47907-2107, USA

ARTICLE INFO

Article history:
Received 20 January 2015
Received in revised form 8 July 2015
Accepted 20 August 2015
Available online 28 August 2015

Keywords:
BPaaS
Cloud computing
Process composition
Process reuse
Security by design

ABSTRACT

We adress in this paper the security issues that arise when outsourcing business processes in the BPaaS (Business Process as a Service). In particular when sharing and reusing process fragments coming from different organizations for faster and easier development of process-based applications (PBA). The goal is twofold, to preserve the process fragment provenance, i.e., the companies's business activities which provide the reused fragments in order to avoid the competition, and to guarantee the end-to-end availability of PBA to fragment's consumers. We formally define the problem, and offer an efficient anonymization-based protocol. Experiments have been conducted to show the effectiveness of the proposed solution.

1. Introduction

Cloud services have been extensively studied in recent years and two categories were proposed: application services and utility computing services [1]. Application services, i.e., Software as a Service (SaaS), offer complete and pre-designed services, where end-users access with authentication protocols and use services maintained by cloud providers. Utility computing services, i.e., Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), provide fundamental computing resources that are used to develop, test, deploy and monitor process-based application (PBA). Therefore, *hosting* business processes in specialized cloud providers may lead to lower costs, by sharing hardware and software resources, as well as administrative staff, and enables pay-as-you-go pricing model [2].

The cloud model also gives the opportunity for organizations to compose and re-use cloud services from a variety of cloud providers to create what's known as cloud syndication [3–5]. Cloud syndications at the SaaS level are termed Business Process as a Service (BPaaS), which, according to business analysts, is the next step forward in the evolution of cloud computing [6]. The BPaaS model considers a *multi-party* cloud system, which consists of multiple cloud platforms and cloud's users. Thus, we define each cloud platform as being a *process curator* that hosts a set of business processes and maintains them long-term such that they are available for execution.

Currently, organizations outsource more and more business processes to process curators in order to take benefits from the cloud business model, and also to share data and services [7]. Each *complex* business process deployed can be broken down into smaller (and more manageable) process fragments suitable for re-use to accelerate future process modeling [8–13]. Indeed, a process fragment represents a self-contained and functionally complete artifact for process design and execution. These organizations are therefore defined as *process providers*.

As a result, process curators built over time and maintain large repositories of process fragments [14]. Such repositories may contain hundreds or even thousands of process fragments (e.g., Amazon.com, schema.org, etc.). These process fragments can be extracted, published and shared through libraries, allowing the design of new PBAs by selection [15–18]. The development of new PBAs supports to reduce not only the cost of designing new business processes but also to enhance homogeneity between them. In this paper, we use the term *process consumer* to refer to such third organization that re-uses process fragments provided by process curators in the cloud.

The main problem that cloud computing paradigm implicitly contains is that secure outsourcing of sensitive as well as business-critical data and processes [19]. In fact, there are several security risk issues when reusing process fragments in the BPaaS delivery model. The first issue is *how to ensure the end-to-end availability of PBAs?* Existing secure process composition mechanisms assume a fully trusted process provider, which is not always true, and focus on announced Service-Level Agreement (SLA) availability rates of process fragments.

However, in reality, a process provider may suspend the outsourcing of a given service including process fragment. Consequently, all PBAs that re-use this cloud service will be impacted and abnormalities on

* Corresponding author at: Université Paris Descartes, 45 rue des saints pères, 75270 Paris Cedex 06, France. Tel.: (+33) 1 83 94 57 41.
E-mail addresses: mehdi.bentounsi@parisdescartes.fr (M. Bentounsi), salima.benbernou@parisdescartes.fr (S. Benbernou), mja@cs.purdue.edu (M.J. Atallah).

http://dx.doi.org/10.1016/j.csi.2015.08.011
0920-5489/

their executions will occur. One possible solution consists in keeping a copy of each process fragment by the process curator as long as it is needed. However, this solution requires that the process provider should let available its own process fragments after unsubscribing. In some cases that may well be true, but very often that is not the case.

A second key problem in outsourcing is that the hosting, the execution and the re-use of process fragments are considered as sensitive that may contain business secrets or provide personal information (e.g., SSN). Consequently, fragment's compositions may expose process providers' business activities, as well as process consumers and their end-users to confidentiality issues. Thereby, an adversary may be able to:

1. Reveal sensitive information about the process provider activities, such as details of how certain process fragments are composed or the list of process fragments provided by an organization;
2. Infer connections between end-users and a process provider by analyzing intermediate data, like input/output values produced by a process fragment, thus obtain and/or modify confidential and sensitive information by using SQL injection attacks [20].

Both are considered to be unacceptable breaches of confidentiality.

Existing solutions characterize security as a set of attributes, where process providers and process consumers define their security constraints in terms of these attributes (e.g., Goettelmann et al. [21]). Thus, PBA's security is ensured if the security constraints of each fragment reused satisfy security constraints of the process consumer. But as the first issue, these mechanisms assume a fully trusted process provider and consumer, and are used to prevent only external attacks. In the case where an attacker is one of parts of cloud system, these mechanisms are not efficient.

In our previous works [22,23], we proposed a privacy agreement model that spells out a set of requirements related to consumer's privacy rights in terms of how Web Service provider must handle privacy information as a bilateral SLA. Moreover, we provided a private data usage flow model to monitor at run time the compliance of requirements defined in the privacy agreement [24,25]. However, such approaches are not handling privacy preservation and do not deal with the availability of Web Services involved in a fragment of a business process and in a setting of the Cloud. There have been some works on security-aware compositions [26–28]. Unfortunately, these works do not consider service provenance and focus on access control, data integration and provenance.

This paper is an extension of our earlier works [29,30] in which we formalized the reuse of process fragments in the cloud, and introduced the notion of anonymous process fragments for privacy-preserving business activities of organizations. In this paper, we investigate how much we can secure PBAs while multi-organizations share a BPaaS in a multi-party cloud system and we provide a positive answer to the above questions. For that purpose, we propose an anonymization-based approach providing anonymous views on BPaaS to preserve the confidentiality of multi-tenant fragments, and to reduce the cost associated with the approach. At the same time, we enrich the approach with a notion of diverse view to guarantee the end-to-end availability of PBAs, and to reduce the cost associated with the approach. We make the following contributions:

1. Anonymous and diverse views: In order to hide the activity of a process provider sharing some of its process fragments with other organizations, we define a new notion of *views on BPaaS* handling the instances of shared and reused process fragments. Moreover, to ensure the availability of process fragments for building new PBAs, we also introduce the notion of diverse views handling the diversity of process fragment provenances.
2. Confidentiality and availability costs: To quantify the proposed framework's security, we use two types of cost: one for confidentiality, and another for the availability of process fragments in the BPaaS.
3. Secure Business Process as a Service: To take into account the aforementioned goals, the proposed secure framework is based on a multi-objective optimization approach.
4. Evaluation on real datasets: To validate the effectiveness and evaluate the performance of the proposed protocol, we have applied it to the QWS datasets [31,32], then studied the impact on the quality of the BPaaS views. Experiments permitted us to set parameter values of the protocol.

The remainder of the paper is structured as follows: Section 2 describes the problem statement through motivating examples. Section 3 gives some preliminaries on BPaaS and process fragment provenance for faster and easier design of process-based applications. After defining the security model for the BPaaS in Section 4, Section 5 presents the details of our protocol, including the anonymous and diverse views on BPaaS model for securing process fragment reuse. Experiment results of the proposed protocol and an optimization are presented in Section 6. Section 7 discusses related works and Section 8 concludes the paper.

2. Motivating examples

We start by setting out examples that motivate the research presented in the paper. We present scenarios for reusing process fragments, that cannot resist several possible attacks. We assume the existence of two kinds of adversaries: *curious* and *malicious*. Curious adversaries attempt to learn or make use of information from the system but do not affect system resources (i.e., make passive attack). However, malicious adversaries attempt to alter system resources or affect their operations (i.e., make active attack). These scenarios infer availability and confidentiality issues.

2.1. Availability issue

In the first scenario, we allow for the possibility of an adversary using the BPaaS to outsource new business processes as process provider. Accordingly, an adversary may enrich the repository with new process fragments that can be reused by other organizations. We also allow for the possibility of an adversary to remove its own process fragments previously deployed on the BPaaS. Thereby, the availability of the adversary's process fragments will not be assured. The following example illustrates the availability issue.

Example 1. Let us consider an Employer Business Process EBP used by a Human Resources Department (HRD) to manage employee accidents at work. EBP is a simple sequential pattern, it means an activity is enabled after the completion of another one. So, EBP can be represented as a business graph with a set of activities as depicted in Fig. 1. Activities are listed in the following:

1. Check insurance number (CIN).
2. Create new accident declaration (CNA).
3. Check personal information (CPI).
4. Validate employee declaration (VED).
5. Make insurance declaration (MID).
6. Make appointment with insurance (MAI).

Note that compositions in the application level (SaaS) are similar to the Web service compositions in SOC (Service-Oriented Computing). Thus, CIN, MID and MAI are considered as cross-organization activities and require service invocations and data exchanges with insurance company through application programming interface (API).

The main problem in this scenario is, an adversary may provide a set of process fragments in the BPaaS as a process provider. Suppose MAI is one of these process fragments. As depicted in Fig. 2, MAI is split up into two roles: the sender (entity A) and the receiver (entity B). Sometime later, Bob, the process designer of HRD, uses the BPaaS