
Amina Ahmed Nacer, LIMED Laboratory, Faculty of Exact Sciences, University of Bejaia, Bejaia, Algeria & LORIA Laboratory, University of Lorraine, Nancy, France
Elio Goettelmann, LIST Luxembourg Institute of Technology and Loria, Luxembourg, Luxembourg
Samir Youcef, LORIA Laboratory, University of Lorraine, Nancy, France
Abdelkamel Tari, LIMED Laboratory, Faculty of Exact Sciences, University of Bejaia, Bejaia, Algeria
Claude Godart, LORIA Laboratory, University of Lorraine Nancy, France

ABSTRACT

To enjoy the benefits of cloud computing, organizations managing complex business processes want to outsource their processes. However, as such processes express their know-how and because of the nature of the cloud, they are still reluctant to do so. To prevent such a know-how exposure, this article proposes a design-time approach for obfuscating a BP model by splitting its model into a collaboration of BP fragments semantically equivalent to the initial BP. This breaking down renders the discovery by cloud providers of-the-deep content of a critical fragment, and more of the whole process, much harder when these fragments are deployed in a multi-cloud context. While existing contributions on the topic of BP obfuscation remain at the level of principles, the authors propose an algorithm supporting automatically such a BP model transformation. The approach is validated against an obfuscation metric introduced in the article. The obtained results show that the authors’ algorithm generates BP fragment with a high obfuscation level, contributing to protect BP know-how when deployed in a multi-cloud context.

KEYWORDS

1. INTRODUCTION

The huge development of technologies pushes companies to be innovative in order to remain competitive. One way for them is the use of cloud resources which avoids upfront infrastructure costs, and helps organizations to focus on their core business activities instead of their system infrastructure.

DOI: 10.4018/IJWSR.2018100104

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
However, as business processes (BP) of companies express their know-how, and because the cloud introduces new security risks, they are still reluctant (Cloud Security Alliance, 2014; European Network and Information Security Agency, 2009) to use the cloud for deploying their BP.

Therefore, for enjoying cloud advantages, one way for companies to prevent security and especially know-how exposure risks, is to transform their process models at premises so that it is difficult for cloud providers to discover the deep content of a critical fragment, and more of the whole BP.

(Goettelmann, Mayer, & Godart, 2013) has proposed a methodology for transforming and obfuscating a BP (Business Process) model before its deployment in the cloud. But, this obfuscation process is yet at the level of recommendations, and the obfuscation work has to be done mainly by designers’ hands. The objective of the work described in this paper is to go one step further by providing an approach for partly automating this obfuscation process, more precisely the BP model splitting recommended in the methodology.

The research questions addressed in this work are: how to efficiently split a BP model into a collaboration of BP fragments models, each fragment containing as less as possible know-how of the global process? On which language constructs to rely for automating this process? In addition, this work must remain compatible with existing workflow management systems and other dimensions of security and quality of services.

As a result, the contributions of this paper are:

- An algorithm for automating the splitting of a BP into a collaboration of BP fragments. The main idea is to split critical tasks where “decisions” are taken and “synthesis” done into complementary BP fragments assigned to different clouds (section 4);
- A BP obfuscation metric for evaluating the cloud configurations generated by our algorithms with other cloud configurations.

The rest of this paper is organized as follows. The next section establishes the motivation and the context of this work. Then the notion of a critical BP fragment (“decision” or “synthesis”), on which we pay a particular effort for obfuscation is characterized in section 3. Section 4 explains how obfuscation is put into practice in our architecture. Section 5 proposes an obfuscation metric and discusses our model validity. The state of the art is discussed in section 6 and finally, we conclude our paper and introduce some future work in the last section.

2. MOTIVATION AND CONTEXT

2.1. Motivating Example

Figure 1 depicts a loan process in a bank using BPMN (Object Management Group[OMG], 2011) which aims to accept or reject a loan request, depending on the customer history and other parameters (loan amount, etc.).

Figure 1. The loan process
Advances in Privacy Preserving Record Linkage
[www.igi-global.com/chapter/advances-privacy-preserving-record-linkage/53271?camid=4v1a](www.igi-global.com/chapter/advances-privacy-preserving-record-linkage/53271?camid=4v1a)

NAM: A Network Adaptable Middleware to Enhance Response Time of Web Services
[www.igi-global.com/chapter/nam-network-adaptable-middleware-enhance/31209?camid=4v1a](www.igi-global.com/chapter/nam-network-adaptable-middleware-enhance/31209?camid=4v1a)