bpCMon: A Rule-Based Monitoring Framework for Business Processes Compliance

Ping Gong, Department of Computer Science, Fujian Normal University, Fuzhou, China
David Knuplesch, Institute of Databases and Information Systems, Ulm University, Ulm, Germany
Zaiwen Feng, State Key Laboratory of Software Engineering, Wuhan University, Wuhan, China
Jianmin Jiang, Department of Computer Science, Fujian Normal University, Fuzhou, China

ABSTRACT

Business processes compliance monitoring checks whether running business processes comply with involved compliance rules. Business processes in modern enterprise are rarely supported by a single and centralized workflow system, but instead implemented over different applications (e.g., CRM, ERP, WfMS, and legacy systems). The running data (i.e., event) about process executions are scattered across these applications. Under such circumstance, understanding the compliance of running processes entails the compliance monitoring enabling to correlate events from different applications and even different process instances. This paper introduces a framework named as bpCMon for business process compliance monitoring. bpCMon consists of an expressive compliance rule language ECL and a rule system ERS. ECL is a pattern-based formal language for specifying compliance rules of multiple process perspectives, and also allows for describing event-correlation conditions. ERS, generated from compliance rules in ECL, in turn plays as a compliance monitor enabling to correlate events efficiently by means of an indexing structure created from event-correlation conditions. The applicability of bpCMon is demonstrated by experiments on real-world data sets, and the efficiency of bpCMon is illustrated by comparing with related approaches. Overall, bpCMon enables business process compliance monitoring to meet real-world requirements.

KEYWORDS

bpCMon, Business Process Compliance, Compliance Monitoring, Event Correlation

1. INTRODUCTION

Business processes compliance (BPC) requires that business processes are executed in conformance with prescribed and approved sets of compliance rules. The latter may stem, for example, from norms, standards, and laws (Sadiq, et al. 2011). In general, there are compliance checking approaches of various kinds taken on different phases of process life cycle to enforce the BPC, e.g., a-priori checking at design time or a-posteriori checking based on the event logs of completed process instances.

However, a-priori checking is not always sufficient, since process instances may deviate from prescribed process implementations (Schonenberg, et al. 2008). Furthermore, in many enterprise systems, processes are not model-driven, but more or less hard coded in the respective system (de Lenoi, et al. 2016). In turn, a-posteriori checking might be inapplicable for decision making when quick reaction is needed for compliance violations. These thus emphasize the need for run-time compliance checking, i.e., compliance monitoring.
1.1. Problem Statement

Business processes in modern enterprise are rarely supported by only one centralized workflow system. Instead, business processes may refer to activities whose executions are supported by various applications (e.g., CRM, ERP, WfMS, or legacy systems) (Reza Montahari-Nezhad, et al. 2011). The information about processes executions, i.e., events, are generated from and recorded in different applications. Furthermore, for a wide variety of enterprise information systems, there does not always have any in-built mechanisms, which could correlate those scattered events from applications to the same process instances. These systems are classified as non-process-aware information systems for differentiating from process-aware information systems (PAIS) (Perez-Castillo, et al. 2014). Although those scattered events could be collected through proper message oriented middleware (MOM, e.g., ActiveMQ or Kafka) as Figure 1, understanding the compliance of the executions of processes is still challenging under such circumstance.

First, unlike existing works in BPC, which in general implicitly assume that input events for compliance monitors are already correlated correctly to the same process instance by build-in mechanisms of PAIS (Ly, et al. 2015), the compliance monitoring for non-process-aware information systems entails compliance monitors enabling to correlate events to the involved compliance rules. Those correlated events, as inputs to monitors, might not always belong to the same process instances, but might sometimes from different process instances. These facts unfortunately invalid most of existing

Example 1.

Following compliance rules address the prevention of frauds in banking domain (Basin, et al. 2013, 2015):

B1. Every bank transfer of a customer, who was involved in a suspicious bank transfer (e.g., with an amount greater than €10,000) within the last 30 days, must be reported afterward within 2 days.

B2. The sum of withdraws from account within 30 days, must not exceed the limit of €10,000.

B3. For each user, the number of withdrawing peaks over the last 30 days does not exceed a threshold of 5, where a peak is a value at least twice the average over some time window (30 days).
Efficiently Compositing and Optimizing the Quality of Heterogeneous Services
[www.igi-global.com/article/efficiently-compositing-and-optimizing-the-quality-of-heterogeneous-services/122816?camid=4v1a](www.igi-global.com/article/efficiently-compositing-and-optimizing-the-quality-of-heterogeneous-services/122816?camid=4v1a)

Cloud State Surveillance: Dark Octopus Tentacle Clouds From the Atlantic
[www.igi-global.com/chapter/cloud-state-surveillance/217922?camid=4v1a](www.igi-global.com/chapter/cloud-state-surveillance/217922?camid=4v1a)