Future Generation Computer Systems 28 (2012) 1177–1193

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

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

Modeling and analyzing the impact of authorization on workflow executions☆

Ligang He [a,*], Chenlin Huang [b], Kewei Duan [c], Kenli Li [d], Hao Chen [d], Jianhua Sun [d], Stephen A. Jarvis [a]

[a] *Department of Computer Science, University of Warwick, Coventry, UK*
[b] *Institute of Software, School of Computer Science, National University of Defense Technology, Changsha, China*
[c] *Department of Computer Science, University of Bath, Bath, UK*
[d] *School of Computer and Communication, Hunan University, Changsha, China*

ARTICLE INFO

Article history:
Received 28 September 2011
Received in revised form
15 February 2012
Accepted 1 March 2012
Available online 5 March 2012

Keywords:
Modeling
Authorization
Workflow
RBAC

ABSTRACT

It has been a subject of a significant amount of research to automate the execution of workflows (or business processes) on computer resources. However, many workflow scenarios still require human involvement, which introduces additional security and authorization concerns. This paper presents a novel mechanism for modeling the execution of workflows with human involvement under Role-based Authorization Control. Our modeling approach applies Colored Timed Petri-Nets to allow various authorization constraints to be modeled, including role, temporal, cardinality, BoD (Binding of Duty), SoD (Separation of Duty), role hierarchy constraints etc. We also model the execution of tasks with different levels of human involvement and as such allow the interactions between workflow authorization and workflow execution to be captured. The modeling mechanism is developed in such a way that the construction of the authorization model for a workflow can be automated. This feature is very helpful for modeling large collections of authorization policies and/or complex workflows. A Petri-net toolkit, the CPN Tools, is utilized in the development of the modeling mechanism and to simulate the constructed models. This paper also presents the methods to analyze and calculate the authorization overhead as well as the performance data in terms of various metrics through the model simulations. Based on the simulation results, this paper further proposes the approaches to improving performance given the deployed authorization policies. This work can be used for investigating the impact of authorization, for capacity planning, for the design of workload management strategies, and also to estimate execution performance, when human resources and authorization policies are employed in tandem.

1. Introduction

Business processes or *workflows* are often used to model enterprise or scientific applications [1–4]. A workflow consists of multiple tasks with ordered execution, i.e., a task can only start execution after another task in the workflow has completed (the former task is called the latter's child). It has received considerable research interest to automate workflow executions on computer resources, which has led in part to BPEL being proposed as a standard for specifying and executing workflows [4]. However, many workflow scenarios still involve human activities and will be comprised of a mixture of human tasks and computing tasks (which we term a *hybrid workflow* in this paper) [5–9]. For example, in IT-based video production workflows [9], human interactions are still required for decision making and artistic choices (e.g., video editing decisions). In mortgage business processes in banks [10], various human tasks (e.g., a manual approval step is required if the mortgage value exceeds some amount) could be involved in order to make the final decisions. Indeed, in many application domains, the completion of a task in a workflow replies on the subjective judgment of human. It would be very difficult, if not possible, to use computers to completely replace humans in such scenarios.

In traditional workflow management systems, human interactions in a workflow are not well supported, and therefore a workflow with human involvement can be regarded as a semi-automated workflow [11]. Motivated by the requirements of integrating human interactions into business processes, research exists to support human tasks in workflow contexts. WS-HumanTask and BPEL4People, which have been proposed to overcome the lack of support for human activities in BPEL [11,10], are the exemplar products of these research efforts. WS-HumanTask and BPEL4People enable the integration of human tasks into business processes, and therefore the executions of the workflows containing human tasks can also be automated [11,10].

Human involvement introduces authorization concerns, requiring restrictions on who is allowed to perform which tasks at what

☆ The preliminary version of this paper was presented in the 8th IEEE Intl. Conf. on Services Computing (SCC'11), 2011.

* Corresponding author. Tel.: +44 24 76573802; fax: +44 24 76573024.
E-mail address: liganghe@dcs.warwick.ac.uk (L. He).

0167-739X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2012.03.003

time. Research has been conducted to attach authorization information (such as roles and permissions) to activities, and to impose authorization constraints (such as separation of duty) on workflow executions [12–18]. For example, in BPEL4People, authorization concepts such as roles and permissions are defined, and various authorization constraints are supported, including cardinality constraints, separation of duty, binding of duty, etc. The authorization specified in BPEL4People can be categorized as Role-based Authorization Control (RBAC), under which users are assigned to certain roles, while the roles themselves are associated with prescribed permissions.

When we assess resource capacities, or evaluate the performance of workflow executions on supporting platforms, it is often assumed that when a task is allocated to a resource, the resource will accept the task and start the execution once a processor becomes available. However, when human activities and authorization constraints are taken into account, the issue can become complex. The following example illustrates such a situation.

A bank will need both human activities and computing-based activities to support its business. A workflow will typically contain both *Human Tasks* (HT) and *Computing Tasks* (CT): A human task may consist of a person (or a *user* in the RBAC terminology) with an official position (or a *role* in RBAC, e.g., a branch manager) signing a document; a computing task may involve running an application on a computing resource to assess risk for an investment. Further, the computing applications may be hosted in a central resource pool (e.g. a cluster), and the invocation of an application may be automated without human intervention, which we term an *Automated Computing Task* (ACT), or for security reasons, can only be initiated by a user with a certain role and be executed under that role/user, which we term a *Human-aided Computing Task* (HCT). The following authorization constraints are often encountered in such scenarios [17]: (1) Role constraints: A human task may only be performed by a particular role; a computing application may only be invoked by assuming a particular role; (2) Temporal constraints: A role or a user is only activated during certain time intervals (e.g., a staff member only works in morning hours); (3) Cardinality constraints: The maximum number of tasks (computing or other) running simultaneously under a role is N; (4) Separation of Duty constraints: If Task A (HT or CT) is run by a role (or a user), then Task B must not be run by the same role (or user); (5) Binding of Duty constraints: If Task A is run by a role (or user), then Task B must be run by the same role (or user); (6) role hierarchy constraints: if multiple roles are eligible and available to run a task, the task must only assume the role with the least privilege.

In real-world applications, a more complex task may contain both human and computing activities. For example, a task may first require a person to handle the task, and then require a computing application being invoked to compute additional data. Such a complex task can be regarded as the combination of an HT and an ACT/HCT. Therefore, in this paper, we assume that the time spent by a user handling an HCT is negligible.

It is common to find such authorization constraints and interaction between human and automated activities; our domains of interests include healthcare systems [19], the video management domain [9] and the manufacturing community [6,20]. Human intervention and associated authorization clearly affects the processing of tasks and impacts on both application-oriented performance (e.g. mean response time of workflows) and system-oriented performance (e.g. utilization of the computing resource pool). Obtaining these performance data will be critical in capacity planning, designing authorization policies and developing workflow management strategies.

To date, little attention has been paid to investigating performance when running hybrid workflows under deployed authorization policies. The purpose of this paper is to model execution and authorization of hybrid workflows that are supported by cluster-based resource pools. Various types of authorization constraints are modeled in this paper, including role constraints, temporal constraints, cardinality constraints, Binding of Duty (BoD), Separation of Duty (SoD) constraints, and role hierarchy constraints. Workflow executions, as well as the interactions between workflow execution and authorization controls are also modeled in this paper. In this paper, the Timed Color Petri-Net (TCPN) formalism is applied to model workflow authorization and execution. Moreover, the modeling mechanism is developed in such a way that the model construction can be automated. This feature is very helpful in modeling a large collection of authorization policies or complex workflows.

The constructed models are then simulated and analyzed to obtain various performance metrics, including authorization overhead, system-oriented performance (e.g., utilization and throughput) and application-oriented performance (e.g., response time of workflows).

A high level Petri-net tool, called the CPN Tools [21,22], is utilized to implement and simulate the model. Based on the model simulations, the methods are proposed to analyze the authorization overhead and the performance bottlenecks in the system. Further, we propose the approaches to enhancing performance under the specified authorization constraints.

The work presented in this paper can be used for capacity planning, designing workload management strategies, or for estimating application performance in the presence of authorization policies. Since we can calculate from the models the overhead caused by the authorization constraints, this work also provides insight into how to tune performance by adjusting authorization policies so as to achieve a good balance between performance and security overheads.

Note that this paper investigates the executions of hybrid workflows (containing both computing tasks and human tasks) at an abstract level. Whether the execution of a hybrid workflow is semi-automated or automated is an implementation issue (depending on whether the workflow execution is programmed using BPEL4People or traditional workflow management methods), which does not affect the results obtained in this paper.

The remainder of this paper is organized as follows: Section 2 discusses related work; Section 3 introduces the Timed Color Petri-Net formalism applied in this paper; workflow authorization and execution are modeled in Section 4; model simulations and overhead analysis are discussed in Section 5. Section 5 also presents the approaches to reducing authorization overheads and improving performance. Section 6 presents the simulation results and, Section 7 concludes the paper.

2. Related work

Workflow management has been extensively studied and as a result is well documented in related literature [23,1,24,3]. Much of this research is aimed at automating the execution, and enhancing the performance, of workflows in parallel and distributed systems [1],43. Some of this research has also utilized Petri-nets to model workflow execution. However we note that their work does not formally investigate the performance of workflow execution under authorization constraints.

Research has also been conducted on the topic of security and authorization constraints in the workflow context [25,14,26–28,16]. Some of this research also uses Petri-nets to model authorization constraints. The work presented in this paper differs from this research in the following respects: First, the work found in the literature [26] does not differentiate human tasks and computing tasks, and does not model the interactions between workflow authorization and workflow execution. The work presented in this