面向活动的BPEL4WS动态访问授权模型及实现研究

上超望[1,2] 刘清堂[1] 赵 刚[1] 童名文[1]
(华中师范大学教育信息技术学院 武汉 430079)[1]
(华中师范大学青少年网络心理与行为教育部重点实验室 武汉 430079)[2]

摘 要 业务流程访问控制机制是Web服务组合应用中的难点。针对现有BPEL4WS安全访问控制研究的不足,提出面向活动的BPEL4WS动态访问授权模型(ADABM)。通过解除组织模型和业务流程模型间的耦合关系,ADABM将BPEL4WS访问权限约束细化到活动一级,用户只在流程执行会话期的活动符合安全需求的情况下才拥有Web服务的访问授权,授权随着业务流程上下文动态授予和收回,授权流与业务流同步执行。文中最后还给出ADABM模型在Web服务安全组合应用中的实施框架。

关键词 Web服务组合,活动,BPEL4WS,访问授权,实现
中图法分类号 TP316 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.020

Study on Activity-oriented Dynamic Access Authorization Model for BPEL4WS

SHANG Chao-wang[1,2] LIU Qing-tang[1] ZHAO Gang[1] TONG Ming-wen[1]
(Department of Information Technology, Central China Normal University, Wuhan 430079, China)[1]
(Key Laboratory of Adolescent Cyberpsychology and Behavior of Ministry of Education, Central China Normal University, Wuhan 430079, China)[2]

Abstract Business process access control mechanism is a difficult problem in Web services composition application. According to the current deficiency of research in BPEL4WS secure access control, an Activity-Oriented Dynamic Access Authorization Model for BPEL4WS(ADABM) was proposed. By dissolving the coupling relationship between the organization model and business process model, ADABM refines the BPEL4WS access permission to activity level. The users can obtain the Web services access authorizations only when the corresponding activity meets the security requirements in BPEL4WS execution session. The grants and revokes of the activity access authorization can be implemented along with the process context. At last, the paper also described the implementation architecture of ADABM in Web services secure composition.

Keywords Web services composition, Activity, BPEL4WS, Access authorization, Implementation

1 引言

组合Web服务能够将已存在的Web服务按照一定规则组装成为一个增值的、更大粒度的服务或系统,以满足用户复杂的业务需求[1]。BPEL4WS(Business Process Expression Language for Web Services,Web服务业务流程语言)是专为Web服务合成应用而制定的规范,目前已经成为Web服务组合领域事实上的标准[2]。然而,BPEL4WS规范对流程系统地访问控制、动态授权管理目前仍然没有可以参考的标准[3]。企业无法利用BPEL4WS所提供的机制保护关键资源,这一问题严重制约了组合Web服务跨平台安全集成优势的发挥[4,5]。合理有效的访问授权机制一直是BPEL4WS安全应用的难点问题[6]。

本文提出了一种面向活动的BPEL4WS动态访问授权模型(Activity-Oriented Dynamic Access Authorization Model for BPEL4WS)ADABM,以解决开放协同环境下BPEL4WS流程的访问控制授权问题。介绍了相关研究工作和进展,讨论了ADABM模型的需求,详细论述了ADABM模型及其访问授权实现,并给出了模型在Web服务可信组合实施环境中的原型系统。

2 相关研究和进展

目前,BPEL4WS访问授权研究已取得了一些成果,其各有不同的特点。代表性的如:文献[7]基于BPEL4WS流程活动的UML模型来扩展权限控制功能,提出业务流程安全形式化元模型[7]。该模型对于业务流程任何变化都需要重新规划安全策略,不能适应BPEL4WS动态变化这一特点,也不支持活动的并行执行操作。文献[8]从任务的角度来构建安全的访问控制框架,提出基于任务的业务流程动态访问控制RTBAC[8]。RTBAC只简单地引入受托人集来表示任务的执

到稿日期:2013-03-27 返修日期:2013-04-18 本文受华中师范大学中央高校基本科研业务费项目(CCNU13A05053),教育部人文社科项目(11YJA880163),湖北省教育规划课题(2011B039),武汉市科技计划项目(2014060101010030),国家"十二五"科技支撑计划课题(2012BAD35B02)资助。

上超望(1980—),男,博士,副教授,硕士生导师,主要研究方向为数字版权、服务计算等,E-mail:scw@mail.ccnu.edu.cn;刘清堂(1969—),男,博士,教授,博士生导师,主要研究方向为智能服务、数字版权等;赵 刚(1982—),男,博士,教授,主要研究方向为知识服务、分布式计算等。

行者，缺少细粒度的权限指派与管理，不能反映 BPEL4WS 多域执行环境下 Web 服务的安全协同特点。文献[9]对业务流程执行结构进行安全扩展，提出工具支持的业务流程安全运行框架[9]，其局限是仍然只停留在项目层次的角色定义上，无法针对业务流程的各部分进行灵活的访问控制。文献[10]提出基于 RBAC 扩展的业务流程访问授权模型 BPEL4RBAC[10]，BPEL4RBAC 没有考虑各种服务之间的业务约束关系，也不支持动态变化的业务流程。此外，文献[11]将业务流程整体作为 RBAC 数据元素集，将服务定义为流程任务的抽象执行和实施访问控制的基本单元，提出了基于 RBAC 扩展的业务流程访问控制模型 RBAC-WS-BPEL[11]，不足是没有考虑各种服务之间依赖性和交互性的业务约束关系，也不适应上下文规约下动态变化的业务流程安全执行。

已有研究成果只是在访问授权模型和流程模型之间建立粗粒度关联，忽略了组合 Web 服务计算环境下 BPEL4WS 流程活动执行的分工性、依赖性和时序性特点[12]，不能很好地满足 Web 服务组合中业务流程的安全访问需求。研究设计一种柔性、灵活和细粒度的 BPEL4WS 流程动态访问授权机制很有必要。

3 BPEL4WS 流程动态访问授权模型 ADABM

3.1 ADABM 模型基本思想

ADABM 模型针对 BPEL4WS 在 Web 服务安全组合应用中的实际特点，通过解除组织模型和业务流程模型间的耦合关系，将业务流程访问权限约束细化到活动一级，通过角色层次简化用户到服务访问授权的指派，引入活动状态迁移概念和授权依赖关系，实现 BPEL4WS 活动访问授权的动态激活及动态调整。活动授权在会话期依据主客体属性和业务流程执行环境，动态授予和收回用户对自治 Web 服务的访问权限，授权流与业务流同步执行。

3.2 ADABM 模型定义

ADABM 模型主要组成部件如图 1 所示。

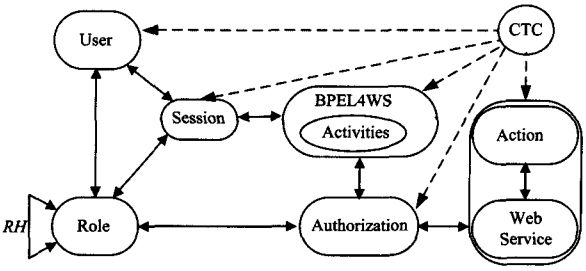

图 1 面向活动的 BPEL4WS 动态访问授权模型(ADABM)

定义 1 ADABM 模型 $ADABM=\{U,R,RH,S,BP,BA,Au,CTC,Ac,WS\}$

$U,R,RH,S,BP,BA,Au,CTC,Ac,WS$ 分别代表用户，角色，角色层级，会话，BPEL4WS 业务流程，BPEL4WS 活动，授权，上下文，行为，自治 Web 服务。

定义 2(用户，User) Web 服务安全组合环境中被赋予一定角色具有相应权限，通过 BPEL4WS 活动访问或调用流程所绑定自治 Web 服务的人员，用户集记为 U。

定义 3(角色，Role) 是一个组织中的工作或位置，代表了一种资格、身份或权限标识，角色集记为 R。

定义 4(角色层级，Role Hierarchies) 表示角色集中的偏序关系，若有 $(r_1,r_2)\in R$ 且 $r_1\succ r_2$，则称 r_1 为父角，r_2 为子角色，r_1 拥有 r_2 的所有权限；角色层级集合记为 RH。

定义 5(会话，Session) 会话表示 BPEL4WS 流程安全执行期用户与其激活的角色之间建立的一个映射。

业务流程活动在上下文驱动下依序实例化并绑定 Web 服务资源，用户只有通过会话与执行期的业务流程建立关联，并在活动实例生命周期内激活角色，才可获得活动授权的访问许可。会话随着活动实例化执行而创建，随着活动实例终止而销毁。由多个会话组成的会话集记为 S。

定义 6(Web 服务业务流程，BPEL4WS) BPEL4WS 包括一组活动以及它们之间的执行顺序关系、过程及活动的启动/终止条件等定义。一个业务流程描述实际应用中一组 Web 服务具体的协同增值过程，完成一个实际业务目标，记为 BP。

定义 7(业务流程活动，Business Activity) 业务流程活动表示组合服务运行过程中一个步骤或任务，各活动之间通过业务依赖关系联结在一起，业务流程活动集记为 BA。流程活动的一次具体完成过程表征为活动实例，同一活动可以有不同的实例。

定义 8(授权，Authorization) 授权表示 BPEL4WS 活动执行的约束，它将服务资源访问许可和角色进行封装，返回请求者对 BPEL4WS 活动及其绑定 Web 服务资源操作能力“是”或“否”的许可判决，授权集记为 Au。

用户开始执行具体活动的那一刻标志着授权事务的开始。对于某一项授权 au，可用四元组 $\langle r,ba,perm,[\tau_s,\tau_e]\rangle$ 表示，说明角色 r 的执行用户在时间点 τ_s 被授予活动 ba 服务资源的访问权限 $perm$，在时间点 τ_e，授权将被收回，$\tau_e-\tau_s=\Delta\tau$ 为 au 的生命期。

定义 9(上下文约束，Context Constraint) 上下文约束描述了实现业务流程活动能够被执行所加的环境或系统等外部约束条件。业务流程活动在上下文驱动下经历实例状态迁移并绑定自治 Web 服务，授权依据活动实例状态动态授予和回收用户对服务资源的访问许可。上下文约束的集合记为 CTC，$CTC=\bigcap_{i=1}^{w}CN_i$，其中 w 为上下文条件总数，CN_i 为上下文条件，表示与活动访问授权有关的环境属性布尔断言。

$CN_i=\langle$Attribute$\rangle\langle$Operator$\rangle\langle$Value$\rangle$，Attribute 是上下文属性，可以是与活动资源访问授权相关的环境因素(如访问主体信息、活动状态、消息驱动及访问授权决策信息等)，也可以是抽象的概念，比如信任管理中的信任级别等；Operator 可以是逻辑操作符$\{=,>,<,\geqslant,\leqslant,\neq\}$，也可以是用户自己定义的操作符；Value 是管理员为 Attribute 设定的值。CN_i 比较 Attribute 的当前值和设定的 Attribute 值，返回一个布尔型的值，满足条件返回真，否则为假。

定义 10(行为，Action) 行为是业务流程活动所绑定 Web 服务的访问操作方法，行为主要通过 BPEL4WS 活动的 Operation 属性对 Web 服务进行操作，行为集记为 Ac。

定义 11(Web 服务，Web Service) Web 服务是被 BPEL4WS 活动绑定的分布式资源单元和组件，也是授权行为操作实施的对象，由多个服务组成的服务集记为 WS。通过流程活动的 portType 属性与 Web 服务 portType 属性绑定，BPEL4WS 将 Web 服务对应到行为操作的客体，合理地安排服务运行顺序，实现服务资源的绑定和分布式协同增值应用。

定义 12 ADABM 中的关系：

①$UR\subseteq U\times R$，多对多的用户到角色的映射关系；

②$AAu \subseteq A \times Au$，多对一的 BPEL4WS 活动到授权的支配关系，每个活动只有一个授权与其对应，而一个授权可以控制多个活动的执行和权限；

③$RAu \subseteq R \times Au$，角色到授权多对多的分配关系；

④$PAu \subseteq Perm \times Au$，多对多的权限到授权的分配关系；

⑤$AD \subseteq 2^A$，业务流程活动集中的偏序依赖关系，记为 $\prec_{AD}$。若 $a_j \prec_{AD} a_i$，称 a_i 是 a_j 依赖前驱，a_j 是 a_i 依赖后继。

3.3 访问授权实现机制

活动角色映射函数：$role: A \rightarrow 2^R$，将每个业务流程活动映射到一个角色集，返回流程活动所指定的角色。

活动实例映射函数 $act: AI \rightarrow A$：将每个业务流程活动实例映射到相应的业务流程活动，返回业务流程活动实例所对应的活动。

活动实例角色映射函数：$roleI: AI \rightarrow 2^R$，将每个业务流程活动实例映射到一个角色集，返回业务流程活动实例指定的执行角色。

用户映射函数 $user: R \rightarrow U$，角色集到用户集的映射，返回角色所对应的用户。

执行者映射函数：$executor: I_a \rightarrow U$，将每个活动实例映射到一个用户集，返回流程活动实例所对应的执行用户。

上下文功能函数：$FCTC(a)$，判断流程活动 a 的 CTC 中所有 CN 断言值是否合取为真，若为是，表示活动 a 实例化执行所需的上下文条件已具备，否则说明 a 实例化执行的上下文条件还不具备。

ADABM 模型根据组合 Web 服务应用特点对 BPEL4WS 实施基于活动的动态访问授权，是一个随着时间、执行上下文环境变化而变化的模型。授权规则在 ADABM 中实体和实体间安全依赖关系的基础上，描述了 ADABM 访问授权实现机制。

授权规则 1

$\forall 1 \leqslant i \leqslant n, r_i \in R, u \in U, au \in Au, r_i \in role(a_i) \wedge u \in user(r_i) \wedge u = executor(a_i) \wedge FCTC(a_i) \wedge Exe\text{-}active(a_i) = \text{true} \Rightarrow Authorize\text{-}au(u, r_i, au_i, a_i) = \text{true} \wedge Revoke\text{-}au(u, r_i, au_i, a_i) = \text{false}$

$\forall 1 \leqslant i \leqslant n, r_i \in R, u \in U, au_i \in Au, r_i \in role(a_i) \wedge u \in user(r_i) \wedge u = executor(a_i) \wedge FCTC(a_i) \wedge Exe\text{-}active(a_i) = \text{false} \Rightarrow Authorize\text{-}au(u, r_i, au_i, a_i) = \text{false} \wedge Revoke\text{-}au(u, r_i, au_i, a_i) = \text{true}$

授权规则 1 是授权动态执行规则，表示 ADABM 动态感知流程上下文环境，只有当某个活动 a_i 被激活，授权 au_i 才被授予相应的用户 u，若 a_i 没有被激活，用户 u 所具有的授权许可将发生改变，所有的授权被收回，授权流伴随着流程执行流的推进而进行。其中，$Authorize\text{-}au(u, r_i, au_i, a_i)$ 是授权许可布尔谓词，$Exe\text{-}active()$ 是实例执行激活的布尔谓词，$Revoke\text{-}au(u, r_i, au_i, a_i)$ 是授权撤销谓词。

授权规则 2

$\forall i_{a,i}, i_{a,j} \in I_a, r_x, r_y \in R, i \neq j, x \neq y, u \in U, a_i = act(i_{a,i}) \wedge a_j = act(i_{a,j}) \wedge r_x \in roleI(i_{a,i}) \wedge r_x \in roleI(i_{a,j}) \wedge u_x \in user(r_x) \wedge u_y \in user(r_y) \wedge u_x = executor(i_{a,i}) \wedge u_y = executor(i_{a,j}) \wedge actconf(a_i, a_j) \Rightarrow ux \neq uy$

授权规则 2 是互斥约束规则，表示若业务流程活动 a_i 和 a_j 是职责互斥活动，a_i 指派角色 r_x 执行，a_j 指派角色 r_y 执行，用户 u 分派给 r_x 和 r_y，a_i 的活动实例 $i_{a,i}$ 和 a_j 的活动实例 $i_{a,j}$ 同属于业务流程活动实例集，并且 u 已经执行了 $i_{a,i}$，则 u 不能被指派执行 $i_{a,j}$，其中 $actconf(a_i, a_j)$ 为互斥活动判断谓词，表示 a_i 和 a_j 不能由同一用户执行。

授权规则 3

$\forall i_{a,i} \in I_a, r_x \in R, u \in U, au_i \in Au, a_i = act(i_{a,i}) \wedge r_x \in roleI(i_{a,i}) \wedge u \in user(r_x) \wedge u = executor(i_{a,i}) \wedge (\tau < exeTime(i_{a,i}) < \tau + l) \Rightarrow Authorize\text{-}au(u, r_i, au_i, a_i) = \text{true}, \tau < auTime(au_i) < \tau + l$

授权规则 3 是权限范围约束规则，表示当某个活动 a_i 在 τ 时间点被激活生成流程活动实例 $i_{a,i}$，在 $i_{a,i}$ 的生命期 l 内，授予主体 u 用于访问 a_i 绑定服务所需的权限许可仅在规定的 $i_{a,i}$ 生命期时间段内有效，不能超过主体 u 完成其职责所需的最小权限[13]。用户对未在生命期内的活动没有访问许可。$exeTime()$ 函数是当前实例执行时间点获取谓词，$Authorize\text{-}au()$ 是权限授予布尔谓词，$auTime()$ 函数是授权执行时间点获取谓词。

3.4 模型特点和安全性分析

(1) ADABM 中流程活动授权的具体实施柔性依赖于活动上下文环境，权限的授予和收回由事件驱动，支持 BPEL4WS 动态访问控制原则。

(2) 活动和活动实例概念可以刻画协同环境下的业务流程状态定义和授权管理，实现与活动执行同步的权限生命期管理，活动执行时只给用户分配所需的最小权限，细化了授权粒度。

(3) 通过授权来关联活动、角色和权限，把业务流程访问权限与用户隔离，便于流程访问控制的快速变更和扩展，使授权许可管理更加灵活。

(4) 通过角色继承关系细化企业组织内部的安全管理粒度；具有互斥角色的不同用户不能执行同一活动，通过敏感活动授权分权依赖实现职责分离，防止权力滥用。

4 ADABM 模型在 Web 服务安全组合系统中的应用

4.1 访问授权系统组成

ADABM 模型已在论文支撑课题中成功实施，模型原型系统的实现框架如图 2 所示。系统由以下几个核心部分组成：身份认证服务器 IAS(Identity Authentication Server)、业务流程访问授权执行点 AEP(Authorization Enforcement Point)、业务流程访问授权决策点 ADP(Authorization Decision Point)、BPEL4WS 引擎(BPEL4WS Engine)及流程活动状态信息库 AI(Activity InformationBase)等。

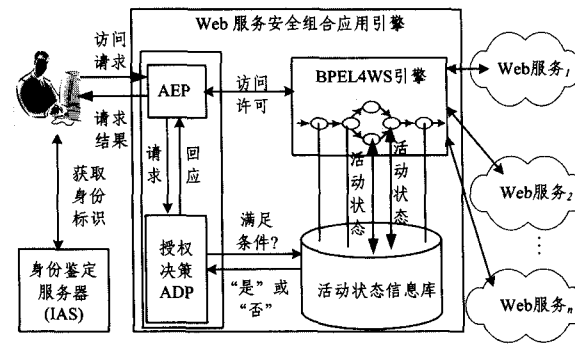

图 2 ADABM 在 Web 服务可信组合实施环境中的原型系统

(下转第 109 页)

与发展,1996,33(5):321-328
[8] 熊曾刚,杨扬,曾明. 基于 Petri 网的两阶段网格任务调度模型与分析[J]. 通信学报,2009,30(8):69-77
[9] 胡志刚,谌任,陈华全. 一种改进的网格资源调度算法及其有色 Petri 网建模和分析[J]. 小型微型计算机系统,2007,28(2):229-232
[10] 韩耀军. 基于 QoS 的信息网格资源调度的建模与分析[J]. 情报杂志,2010(4):146-150
[11] Zhang Jin-quan, Ni Li-na, Jiang Chang-jun. An Algorithm to Construct Concurrent Reachability Graph of Petri Nets[J]. Journal of Donghua University: Eng. Ed., 2004, 21(3): 180-184
[12] Zuberek W M. Timed Petri nets: definitions, properties and applications[J]. Microelectronics and Reliability, 1991, 31(4): 627-644

(上接第 104 页)

4.2 系统运行流程

(1)用户在访问 Web 服务安全组合资源前,首先向身份认证服务器 IAS 证实自己的身份,获取身份认证信息,得到身份认证信息后,向 Web 服务安全组合应用引擎发送组合服务资源访问请求。

(2)业务流程访问授权执行点 AEP 接收用户请求并将请求信息传递给访问授权决策点 ADP,由 ADP 向 ASI 发出活动状态查询的布尔请求。

ASI 查询活动在流程会话期的状态信息并返回"是"或"否"的可执行状态决策。ADP 依据 ADABM 授权约束规则和授权激活条件,结合 ASI 返回信息,进行 BPEL4WS 活动访问授权判决,若判决结果为"是",则激活用户访问授权并授予 AEP 执行当前活动所需的最小权限,同时收回用户拥有的其他活动访问许可;若为"否",则将拒绝访问决策传递给 AEP,由 AEP 将拒绝访问的结果返回给用户。

(3)BPEL4WS 中的每个活动在上下文驱动下经历状态变迁,依照设定逻辑顺序自动执行。依据授权约束规则和授权激活条件,ASI 记录并实时更新执行会话期业务流程活动的启动、激活、完成和夭折等状态信息。

当轮到某个活动执行时,由系统自动标识,然后等待访问主体激活。活动被激活,活动状态信息就自动记入活动信息库。一旦活动处于终止态或夭折态,系统即在活动信息库中标识该任务已经终止,根据上下文启动后续活动准备执行。

(4)在流程活动实例的生命期内,BPEL4WS 引擎启动活动与该活动所绑定自治 Web 服务资源的运行时会话,同时密切监控 ASI 中的活动状态信息。若活动状态被标识变为终止,则回收资源访问授权,授权的激活与回收在上下文驱动下与 BPEL4WS 流程业务执行动态同步进行。

结束语 组合 Web 服务构建于开放的分布式网络环境中[14],合理有效的访问控制机制是 BPEL4WS 安全应用的难点[15]。本文提出了一种面向活动的 BPEL4WS 动态访问授权模型(ADABM)。与已有的 BPEL4WS 安全访问模型相比,ADABM 模型具有上下文感知、动态访问决策、细粒度授权管理等特性,特别适合于 Web 服务基于 BPEL4WS 流程活动分工性、依赖性和交互性的资源安全组合环境。本文对组合 Web 服务业务流程访问控制的研究还需要不断完善。建立一套合理有效的授权验证机制,维护访问控制授权约束的一致性,将是下一步主要研究的内容。

参 考 文 献

[1] 宋巍,唐金辉,张功萱,等. WS-BPEL 服务可替换性分析[J]. 中国科学:信息科学,2012,42(3):264-279
[2] Ahmed A. A compliance management framework for Business Process models[D]. Potsdam: University of Potsdam, 2010
[3] Kristof G. Adaptive workflow composition in service-based systems[D]. Leuven: Katholieke University, 2012
[4] Manuel M, vNicola D. Implementing workflow reconfiguration in WS-BPEL[J]. Journal of Internet Services and Information Security, 2012, 2(2): 73-92
[5] Roman K. Provision of service level agreements in human-enhanced service-oriented computing environments[D]. Vienna: Vienna University of Technology, 2012
[6] Zahra D, Behrouz T L. A model for specification, composition and verification of access control policies and its application to web services[J]. Journal of Information Security, 2012, 3(2): 103-120
[7] Mark S, Jan M. Modeling process-related RBAC models with extended UML activity models[J]. Information and Software Technology, 2011, 53(2): 456-483
[8] Yu Ding-guo. Role and task-based access control model for web service integration[J]. Journal of Computational Information Systems, 2012, 8(7): 2681-2689
[9] Ganna M, Achim D, et al. Security and Safety of Assets in Business Processes[C]//Proceedings of the 27th Symposium on Applied Computing. 2011: 05-12
[10] Wang Xin. A framework to manage message level authorization in service oriented collaborative business processes[D]. Melbourne: Victoria University, 2010
[11] Bertino E, Martino D L, et al. Security for Web services and service-oriented architectures[M]. Berlin: Springer, 2010: 170-175
[12] 上超望,刘清堂,等. 组合 Web 服务访问控制技术研究综述[J]. 计算机科学,2011,42(3):264-279
[13] Allison D S, Miriam A M, Capretz H F, et al. Privacy Protection Framework with Defined Policies for Service-Oriented Architecture[J]. Journal of Software Engineering and Applications, 2012, 9(5): 200-215
[14] Thuemmler C, Fan L, et al. E-Health: Chances and Challenges of Distributed, Service oriented Architectures[J]. Journal of Cyber Security and Mobility, 2012, 1(1): 37-52
[15] Mohsen R. Security analysis for web services compositions [J]. International Journal of Scientific & Engineering Research, 2012, 3(5): 1-8