doi:10.3772/j.issn.1002-0470.2021.09.001

基于合约的 Web 服务个性化访问控制方法①

胡 斌②*** 赵晓芳* 宋永浩* 于 雷* 段东圣*** 张 程*

(*中国科学院计算技术研究所 北京 100190)

(**中国科学院大学 北京 100049)

(***国家计算机网络应急技术处理协调中心 北京 100029)

摘 要 在无中心 Web 服务环境中,用户访问服务的历史行为数据由多个服务提供方分散管理,难以形成全局的用户信任度视图,难以根据用户信任度和使用需求实施个性化的访问控制。本文提出一种基于智能合约的个性化访问控制方法(SC-PAC)。通过结合前期的研究成果为 SC-PAC 提供高质量的用户历史行为数据,实现有可靠数据保障的可信计算服务,通过智能合约中的策略配置及可信度计算模型参数调整,实现服务提供商(SP)对不同用户的个性化的访问控制。在实验环节为 SC-PAC 设计了一个新的信任模型,并对该信任模型及基于 SC-PAC 方法的访问控制进行了实验设计。对结果的分析表明,本文提出的 SC-PAC 方法能够允许 SP 通过智能合约中的计算信任模型、参数及访问控制策略选择,实现对用户的个性化访问控制,并且依据准确的用户历史行为数据提供更可靠的可信度判断,可以有效保护服务。

关键词 Web 服务; 信任评估; 个性化; 动态访问控制; 智能合约

0 引 言

基于信任的动态访问控制(trust based access control, TBAC)[1-2]是解决 Web 服务与用户之间脆弱的信任关系[3]的一种重要方法。它基于用户的历史行为表现,结合服务提供商(service provider, SP)自定义的数据分析模型动态给出一个标量值作为调整访问控制权限的依据。

然而,无中心网络环境下,用户历史行为数据的准确收集是一项困难的工作。一方面,不存在中心化的机构或者服务来收集用户的历史行为数据。用户与服务之间交互所产生的行为数据,往往分散在许多不同的服务之中。因此,指定用户的行为数据收集是一项困难的工作[4-5]。另一方面,准确和全面的数据收集又与网络用户的隐私保护诉求冲突[3]。此外,围绕个性化访问控制研究,普遍停留在以角色或行为组为单位的层面。陆悠等人[6]及钱继安等人[7]在研究中通过建立策略、规范与角色之间的映射关键,实现以角色为粒度的粗放型个性化访问控制。Zerkouk 等人[8]虽然提出了基于用户行为的细粒度个性化访问控制,监控信息却违背了用户对隐私保护的诉求。如何调和数据收集及分享和隐私保护之间的冲突是制约动态访问控制技术发展的难点。

本文经过问题分析和基于前期研究[9]基础,提出一种基于合约的个性化动态访问控制方法(smart contract based personalized access control, SC-PAC)。该方法中,SP 与用户建立智能合约,并通过合约内的权益及规则定义,建立个性化访问控制关系。用

① 国家自然科学基金(U1836111, U1736106)和国家重点研发计划(2018YFB0904503)资助项目。

② 男,1985 年生,博士生;研究方向:信息安全,区块链;联系人,E-mail: hubin@ncic.ac.cn

(收稿日期:2020-09-07)

户访问 Web 服务前,通过合约在用户本地自动运行 SP 提供的计算模型,分析用户的历史行为数据,将计算结果反馈给 SP 作为动态访问控制的依据。这种方式在满足 SP 对用户行为数据准确性要求的同时,也满足了用户对自身行为数据的隐私保护诉求。此外,基于 SC-PAC 的访问控制方法通过允许 SP 配置和调整智能合约内的策略、模型和参数,可以有效提升 SP 对用户的个性化访问控制,极大提升服务的安全防护程度。

本文组织如下,第 1 节是相关研究工作,第 2 节描述 SC-PAC 设计,第 3 节进行案例与实验设计以及结果分析,最后在第 4 节总结全文。

1 相关研究

1.1 TBAC

信任是社会关系中的重要方面,在安全领域、数据访问领域、推荐系统等方面都有着重要的影响力。TBAC 就是这种社会关系在数据访问领域融合的表现。区别于传统的访问控制技术,TBAC 在社会关系的动态性认识上向前迈出了一步。相较于其他的动态访问控制技术,TBAC 则通过对用户在社会关系中的可信度评估来分析和判断应该分配怎样的权限以及是否需要调整现有权限。

基于 TBAC 的应用研究众多,Sajjad 等人[10]提出一种基于邻居节点可信度计算的方法来执行入侵检测并在信任计算与安全等级之间建立了标量连接。Adams 等人[11]则将 TBAC 运用到了 Ad-hoc 网络的协作,它综合节点的历史交互数据以及其他反馈信息评估节点可信度,动态建立协作。Toumi 等人[12]运用 TBAC 管理多组织环境中的用户和组织机构,引入两种动态信任向量并基于知识、声誉以及经验分别进行计算和评估。Yan 等人[13]将 TBAC 运用到云计算领域,通过研究云服务提供商之间的信任关系来提升安全资源保护。Tran 等人[14]在研究中提出通过直接信任、间接信任、直接贡献以及间接贡献等指标来评估访问权限的方法。Yu 等人[15]则指出,推荐、看法等不确定性信息会影响模型的计算结果可靠性。更重要的是,用户行为数据收集与用户的隐私保护诉求有冲突。Bedekar 等人[3]在研究中指出了用户信息在隐私保护方面面临的一些挑战,例如个人隐私数据的售卖。为解决前述问题,Hu 等人[9]在研究中提出新的方法为计算模型提供可靠的用户历史行为数据和隐私保护的数据分享方法。

1.2 智能合约

合约是提供服务的一种重要方式。Ruohomaa 和 Kutvonen[16]指出,通过明确表达隐含期望的合约可以鼓励更多的信任进而减少不确定性。然而,合约通常与商业服务内容密切相关。例如,Schnjakin 等人[17]以合约形式呈现服务和业务,给用户一个清晰的服务内容。由于技术难度和业务衔接问题,合约的适用具有挑战性。智能合约概念最早由 Szabo 于 1997 年提出,它主要是指依靠一段可执行的计算机代码来完成一段确定的业务逻辑。智能合约通过以太坊[18]区块链平台被大家广为熟知,并被许多知名区块链平台(如 Hyperledger Fabric[19])广泛采纳和用于交易。区块链提供了一个可靠的分散环境,其智能合约具有可以强制执行、交易可跟踪的特点。

许多研究都利用区块链和智能合约技术来解决当前的安全问题。例如,Chen 等人部署了基于区块链技术的高性价比的支付收付监管系统[20]。随着智能合约的使用及与食品行业标准的结合,Tao 等人[21]实现了整个产业链的不合格食品的自动检测和预警。Yong 等人[22]通过区块链和智能合约技术解决疫苗过期和疫苗记录欺诈问题。Hu 等人[9]将分布式数据收集问题转换为基于智能合约的数据管理,为信任计算提供了高质量的用户历史行为数据。

本文在前期工作[9]基础上,即以基于智能合约的数据管理方法为基础,为信任计算提供关于用户的高质量历史行为数据。本文更进一步地提出基于智能合约的个性化动态访问控制方法(SC-PAC),将前述可靠的用户历史行为数据应用于服务安全控制,实现动态的访问权限和安全策略的分配。同时,通过智能合约自动执行安全策略,对用户的交互行为进行监控和更新。本文提出的 SC-PAC 为基于 TBAC 的方法提供了更准确的用户行为数据,也为 SP 提供了个性化和动态的访问控制机制。

2　SC-PAC 设计

2.1　SC-PAC 框架

本文提出的基于智能合约的个性化动态访问控制方法(SC-PAC)中合约服务是基础,它包含对用户历史行为数据的管理,将 SP 的访问控制协议转换为智能代码并自动监管用户行为,对发现的违规行为上报以及评估用户可信度。

本文在前期研究工作[9]基础上,给出了 SC-PAC 架构图,如图 1 所示。它包括服务于用户端的基于智能合约的数据服务(smart contract based data sharing, SCDS)模块和用户端本地存储用户交互行为数据的用户信任证书(trust certificate, TC),以及服务于 SP 的服务相关智能合约(service related smart contract, SRSC)管理模块,还包括抵抗信息欺诈的区块链基础设施以及抗欺诈账本模块。TC 以及抗欺诈账本设计参考文献[9]。本文的 SCDS 包含与文献[9]一致的交互行为管理、数据分享设计。不同之处在于,前者统一通过一个智能合约管理、分享用户数据,而 SCDS 将许多服务以用户的智能合约的方式进行独立发布,即 SCDS 包含了许多特定功能的智能合约,它是用户端智能合约集合。例如:信任计算合约、哈希计算合约、TC 读取合约等。这样的设计,一方面减小了合约因智能代码过多而可能包含的逻辑错误量,另一方面允许灵活的合约服务选择与组合服务。SRSC 是服务端发布的服务交互监管协议,代表了依照 SP 意志对用户行为监控的服务过程,也是动态访问控制的核心所在。它以 SCDS 计算得到的用户可信度作为输入,匹配 SP 的安全等级,动态分配访问权限和安全策略并基于安全策略对交互行为进行监控。

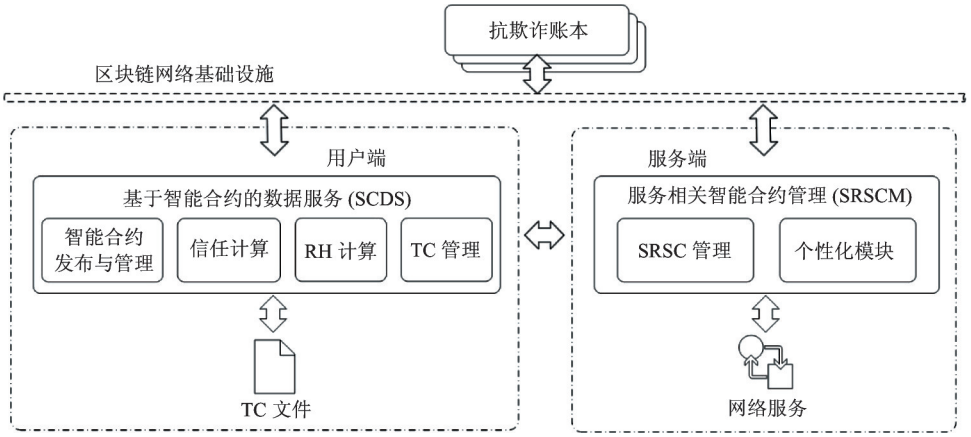

图 1　SC-PAC 框架

个性化模块则包含了 SP 的安全策略、可信度计算模型及参数配置等内容,代表了 SP 对服务安全的个性化需要。

2.2　SC-PAC 服务流程

如图 2 所示,基于智能合约的网络服务访问控制方法包括如下步骤。

(1)初始状态下,用户发布其 SCDS 智能合约集,包括验证 TC 有效性以及可信度计算等。服务端则发布自己的安全策略以及信任模型等。

(2)用户发起访问网络服务端的访问请求。

(3)服务端调取用户发布的 TC 有效性验证服务,验证签名并计算出一个哈希值(root hash, RH)。服务端收到此 RH 值,并通过用户的 TC 编号(ID)从账本中读取用户的根哈希(RH)。通过二者比对区分是否存在数据欺诈。

(4)调用用户的信任计算服务,并将其信任模型作为输入和启动信任计算。

(5)获得用户反馈的可信度结果。

(6)服务端依据可信度结果与安全等级的匹配,动态分配服务安全策略。

(7)服务端启动 SRSC 合约服务,并将前述安全策略作为交互的监控依据。

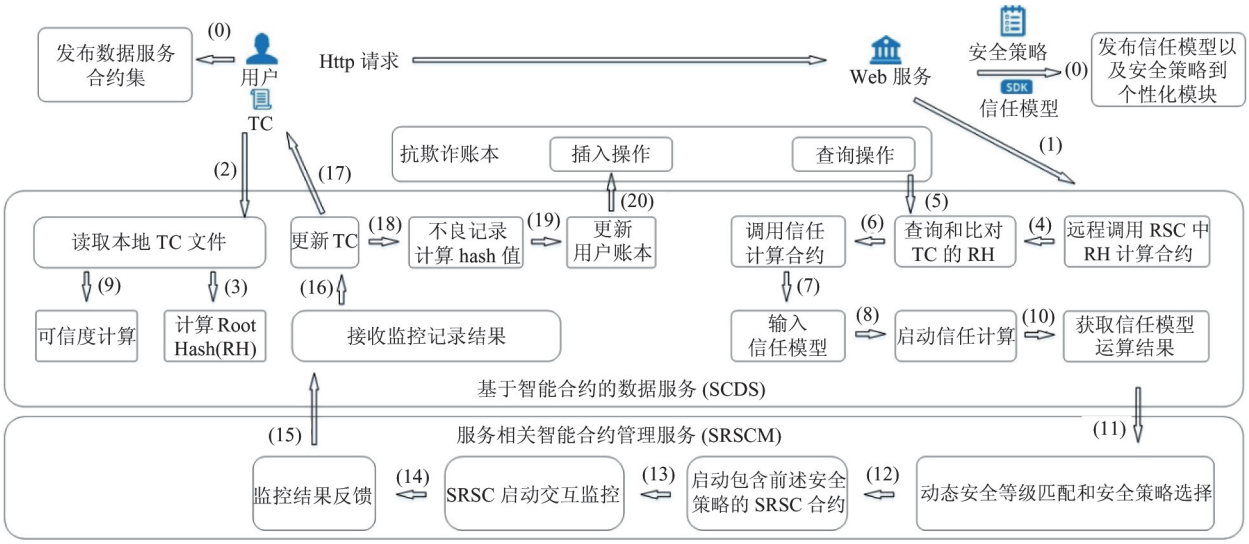

图 2　SC-PAC 流程

(8)服务端 SRSC 将监控结果上报至 SCDS。

(9)SCDS 据此结果更新用户端 TC 文件(包括 TC 文件中的 RH 更新)。

(10)如果结果存在不良记录,则 SCDS 将运算得到此不良记录的哈希结果值。

(11)将哈希结果插入用户的账本,更新其账本中的 RH 值。

3　案例研究

为了评估 SC-PAC,分别从信任模型、参数、访问策略 3 个维度综合分析合约的个性化效果。首先,参照 FIRE[23]、PET[24] 及 SPORAS[25] 等出色的计算信任模型,设计了一个基于累积声誉与风险的 TBAC 模型,其次设计了实验,最后对实验结果进行分析。

3.1　信任模型设计

从 Trustwave 近 3 年的全球安全报告总结发现,数据泄露已经成为威胁网络安全的一个重要因素并且以聚集的趋势集中出现在某几个服务行业。例如 2019 年遭受影响的行业中有 18% 在零售业,11% 在金融业。那么,显然同行业的近况对于其他服务 SP 来说显得非常重要。传统信任模型的数据收集方法受限于其他不同服务在信息收集上的角度以及信息分享的意愿程度,评估者收集的关于特定用户的行为数据一般是零碎、模糊的,难以形成有序、准确的用户行为画像。而指定行为发生的上下文环境对于分析和预测用户下一次的行为表现又有极为重要的作用。例如,FIRE[23]、PET[24]、Dossier[25] 等在信任模型建模中以时间函数作为评定行为影响力的重要方法。显然,目前的模糊、不准确的行为数据对于进行下一步行为预测无法起到预期作用。本文在实验设计中引入了服务关联性参数来丰富计算信任模型。

考虑如下场景,用户 u 通过交互 I 访问服务 p 提供的服务。用户 u 出示 TC 作为信任证书,此证书包含了此用户的网络服务交互总量 N_{all} 和不良记录的总量 N_{bad},并且通过服务 p 提供的信任计算模型可以计算得到一个可信度 T。用户 u 的交互历史标记为 $I = \{I_i \mid i \in N_{all}\}$,其不良交互历史标记 $I^{bad} = \{I_i^j \mid i \in N_{all}, j \in N_{bad}\}$。每次交互的评估结果被赋予 0 或 1 的值,其中 $I_i = 1$ 代表了良好的交互,而 $I_i = 0$ 代表了一次违规交互。

用户 u 的不良交互历史可能包含了许多的不同服务。那么,从不良交互历史就能轻易得知 u 过去是否对特定 p 有过违规的记录(称之为相关度)以及在哪一次交互产生了违规行为。标记 u 与服务 p 之间的不良行为总量为 $N_{related}$($N_{related} \leqslant N_{bad}$),并且这些与服务 p 相关的交互记录构建起了一个相关性序列,标记为 $I^{related} = \{I_i^j \mid i \in N_{all}, j \in N_{related}\}$。

用户 u 在接下来访问服务 p 交互行为中执行违规行为的概率(称之为风险)记为 $R(u, p)$。式(1)展示了 u 访问服务 p 的风险方程。

$$R(u, p) = (1-\gamma)\cdot P_{bad}(u) + \gamma \cdot P_{related\ in\ bad}(u \mid p) \tag{1}$$

式(1)中包含了两类风险:第一,用户 u 接下来执行违规行为的概率,记为 $P_{bad}(u)$;第二,用户 u 接下来对服务 p 执行违规行为的概率,记为 $P_{related\ in\ bad}(u \mid p)$。参数 γ 是介于[0,1]区间内的服务相关性系数,其值越大意味着风险考虑中越关心用户 u 可能对服务 p 执行违规行为的概率,越小则意味着更关心用户 u 最近的交互行为对接下来的行为的影响程度。式(2)和(3)分别展示了式(1)中的两种风险概率模型,并且都考虑了时间因素的影响,即随着时间的推移,过去的行为对未来行为的影响力越来越小。式(4)使用了一个权重模型来模拟前述时间因素的影响,其系数 θ 定义了权重函数的衰减速率。

$$P_{bad}(u) = \frac{\sum_{j=1}^{N_{bad}} W(I_i^j)}{\sum_{i=1}^{N_{all}} W(I_i)} \tag{2}$$

$$P_{related\ in\ bad}(u \mid p) = \frac{\sum_{j=1}^{N_{related}} W(I_i^j)}{\sum_{j=1}^{N_{bad}} W(I_i^j)} \tag{3}$$

$$W(B_i) = e^{-\frac{N-i}{\theta}} \tag{4}$$

$$R(u, p) = (1-\gamma)\cdot \frac{\sum_{j=1}^{N_{bad}} W(I_i^j)}{\sum_{i=1}^{N_{all}} W(I_i)} + \gamma \cdot \frac{\sum_{j=1}^{N_{related}} W(I_i^j)}{\sum_{j=1}^{N_{bad}} W(I_i^j)} \tag{5}$$

基于风险模型 R, SP 就可以通过计算得知用户 u 接下来在服务中的表现,并做出以何种访问权限来提供服务的决定。这就为 SP 提供了更积极和可靠的决策依据。一旦用户 u 对服务 p 的服务请求得到通过,则意味着 u 通过了服务 p 的风险评估。同时服务 p 会为其动态分配一个合适的访问权限。本文通过为服务 p 分配一个介于[0,D]之间的可信度标量(本文设置 D = 100),并将此标量与服务安全等级建立映射,实现自动化的动态权限分配机制。

定义信任(记为 T)为用户历史行为的一种累积表现。从社会学的角度来看,需要引入惩罚或者奖励机制来抑制或者鼓励对应的网络行为。因此,在第 i 次交互中,有可信度 T_{i-1} 的用户 u 会因其行为受到奖励,记为 $R_e(i)$。式(6)展示了可信度 T 的计算过程。

$$T_i(u) = \begin{cases} T_{i-1}(u) + \dfrac{1}{\mu}\cdot \Phi(T_{i-1})\cdot R_e(i), \\ \qquad I_i = 1 \quad 则\ \mu > 1 \\ T_{i-1}(u) + \Phi(T_{i-1})\cdot R_e(i), \\ \qquad I_i = 0 \quad 则\ \mu = 1 \end{cases} \tag{6}$$

$$\Phi(T_{i-1}) = 1 - \frac{1}{1 + e^{-\frac{T_{i-1}-100}{\sigma}}} \tag{7}$$

$$R_e(u) = \begin{cases} 0.01 & I_i = 1 \ 且\ T_{i-1} = 0 \\ T_{i-1}\cdot\left(I_i - \dfrac{T_{i-1}}{100}\right) & 其他 \end{cases} \tag{8}$$

这种递归式的信任计算过程模拟了累计信任的过程。参数 σ 是阻尼函数 Φ 中加速因子,它控制了可信度 T 的变化速率。从文献[26]的研究中可以知道,参数 σ 应该被设置为 $\sigma \leqslant 0.11D$, 并且 $T_i(u)$ 已经被证实是大于 0 且小于 100 的值。系数 $1/\mu$ 是学习因子,它控制了奖励效果。$1/\mu$ 越小,则可信度 T 会越稳定。

3.2　实验设计

SC-PAC 的个性化通过合约的可配置实现,即合约的个性化。它包括 SP 可指定信任模型及其运行时参数,可以指定运行安全策略。

为分析 SC-PAC 方法的个性化特点,本节设计了两大类实验:首先,设计实验对 3.1 节的信任模型在不同参数(学习因子、服务相关系数)控制下的表现,一方面验证本文设计的信任模型的有效性,即作为一个有效的信任模型,在信任度学习速率表现、异常响应等方面有正确的表现。另一个方面,验证参数调整对于个性化访问控制的作用。它具体包括下文所述的实验 1 和 2;其次,模拟了基于合约的访问控制场景,分析基于合约的方法所能带来的动态和个性化访问控制效果。它具体包括下文所述的实验 3。

实验 1　本实验主要测试 3.1 节中信任模型的

信任获取速率以及对异常行为的反应。实验中随机生成了包含 2000 次访问行为的序列 S,它包含了 3 次异常交互行为且索引位置分别为 977、997 和 1117。本次实验中的服务相关系数 γ 设置为 0.6,衰减速率参数 $\theta = 11$。阻尼函数 Φ 中的加速因子设置为 $\sigma = 11$。

实验 2　该实验的评估指标是不良行为容忍度(misbehaving tolerance)。本文将不良行为容忍度定义为模型在停止包含不良行为的请求之前所遇到的不良行为数量。假设所有这些模型都面对同一个用户,初始状态是包含 1500 次已结束的交互记录,其中包含 30 次不良行为记录,并且假定所有这些不良行为都与 SP 无关。接下来,该用户将故意违规访问 SP N 次。

实验 3　本实验以 hyperledger fabric 为区块链实验环境,基于 GoAhead 搭建了 2 个简易网络服务。用户与 2 个服务之间分别签订智能合约,合约包括 3.1 节的信任模型,并设定两个 SP 使用了相同的风险阈值 0.6 和相同的相关度 0.4,也包括相同的 4 级访问控制策略设置。初始状态下,用户连续访问一个 SP,当信任值大于 75 时,它随机执行不良行为。本文有意设置这个用户执行几个不良行为来触发风险阈值,然后这个用户因为风险太高而被拒绝服务。该用户必须访问第 2 个 SP,并始终保持良好的表现以赚取更多的累积信任,进而可以再次访问第 1 个 SP。这个模拟实验试图说明基于合约的方法对用户的访问痕迹和权限、风险变化的动态性和个性化控制效果。

3.3　结果分析

合约可靠性分析　智能合约作为可自动执行的、可验证的代码,能够提供可靠的控制机制。此外,区块链账本可追溯的特性,也允许对合约执行历史进行验证。最重要的是,基于前期研究成果,合约方法能够对平衡数据共享和隐私保护之间的冲突起到重要的作用。具体地,通过合约方法在用户端管理和存储历史行为数据。SP 需要使用用户数据时,通过在用户端执行合约内的信任模型,计算得到可信度结果并反馈给 SP,即在隐私保护前提下,为 SP 提供关于用户的丰富历史行为数据。

合约个性化分析　智能合约是 SP 与用户之间建立的一对一的服务关系。SP 可以在合约中设置个性化的信任计算模型,研究者因对信任理解差异、选择的数学方法不同等,会设计出不同的信任模型,例如 FIRE[23]、PET[24]、Dossier[25]等研究中的信任模型。合约的机制允许 SP 对指定用户的分析采用不同的信任计算模型,极大丰富了 SP 对用户的分析方法。SP 也可以对相同的模型设置不同的参数。例如,采用 3.1 节设计的信任模型,配置不同的学习因子、服务相关性系数等参数。图 3 所示为实验 1 的结果,表示 3.1 节的信任模型在不同的学习因子下信任获取速率会有不同。学习因子越大则信任累积速率越快。一般,有较高安全需求的 SP 可以设定较为缓慢的学习速率,即较小的学习因子值。这让潜在的攻击者通过积累足够的可信度发起攻击更为困难。即便发起了攻击行为,信任模型也能够通过迅速降低信任值做出响应。图 4 展示的是实验 2 的结果,即在同样的信任模型下,不同的风险阈值参数可以对异常行为有不同的反应速率。可以从图 4 看到,设定 $\gamma = 0.6$ 时,第一次异常交互的出现就触发了风险阈值进而阻断了后续的异常流量。当降低 γ 值至 0.2 时,SP 需要 7 次连续的异常交互才会阻断后续的异常流量。允许 SP 配置不同的服务相关系数 γ,可以实现灵活控制服务。这种机制给了 SP 更多的个性化选择空间,那些有较高安全需求的 SP,可以设置一个较高的 γ(通常等于或者接近风险阈值)。更重要的是,基于合约的方法能够可靠地为SP提供关于用户的历史行为数据做分析,即

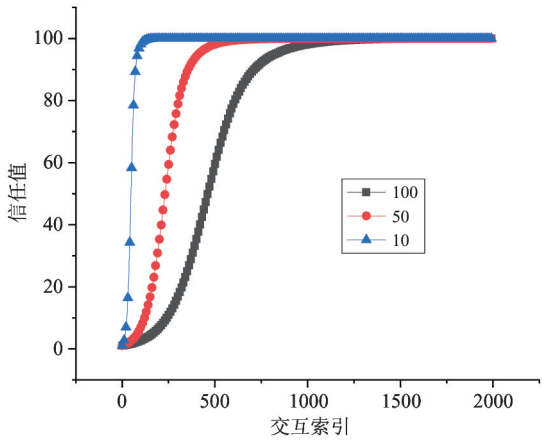

图 3　3 种不同学习因子下累积信任值变化速率

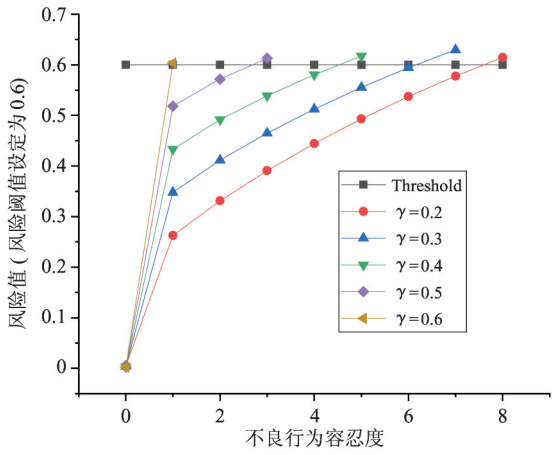

图 4　不同风险阈值参数下的异常拦截表现

具备准确刻画用户画像的条件。这也有利于信任模型的设计,例如本文引入的服务相关性参数。基于丰富的历史行为数据,研究者可以从各种不同的角度设计出丰富的信任模型,这也意味着有更多个性化的信任模型支撑下的访问控制。

合约的动态性访问控制分析　实验 3 在可信度与访问控制权限间建立了 4 级映射关系,拥有响应的可信度值才能拥有相应的访问权限。图 5 显示了模拟实验 3 的运行结果,从图中可以看到,在第 705 次交互中,用户触发风险阈值并被拒绝服务。然后用户转向访问其他 SP 并以正常的访问方式以图降低其风险并获得更多的信任值。如图 5 所示,间隙区域(gap)是此用户在其他 SP 上的访问踪迹。在其他 SP 与原 SP 之间没有服务相关性的情况下,用户基于原有的历史交互行为访问其他 SP 也不会触发风险阈值,进而可以通过良好的行为表现重新获取较高的累积信任值。例如,原 SP 是金融业服务,用户基于合约方法执行了某些违反规定的操作,并被记录到区块链账本。当此用户继续访问此 SP 时,因前述操作被拒之门外。此时,如果此用户转而访问其他类似的金融业服务时,仍有可能被其过往历史拒之门外,这就动态地保护了类似的其他相关服务。此用户可选的策略是访问与金融业服务不相关的其他服务,例如食品服务,并以良好的表现来提升其综合可信度。在图 5 中,约 200 次交互之后,此用户能够再次访问初始 SP 服务。如果此用户在后续交互中再次执行异常行为并再次触发风险阈值,SP 可以通过其合约中的个性化模块动态调整参数,提高对此用户服务的风险阈值,做到对用户的个性化安全服务和动态的访问控制。

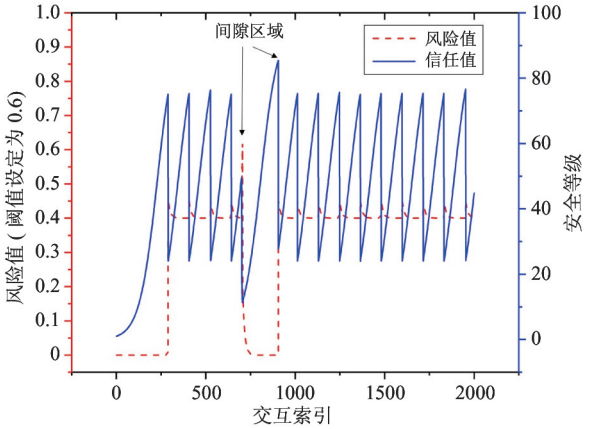

图 5　基于合约自动响应的动态访问控制表现

4　结　论

对用户画像的准确刻画是制约访问控制可靠性的一个重要因素,尤其是在 Web 服务环境中,用户的行为数据往往分布在许多不同的服务中,Web 服务难以准确地掌握用户的行为信息。许多研究在基于信任计算的访问控制研究中,通过引入服务评价、推荐等信息,以期丰富对用户的认识,提升可信度值的可靠性。然而,研究离准确描述用户信息仍有距离,对用户信息量的缺失也约束了信任计算模型的设计。此外,许多个性化访问控制的研究集中在以角色为单位的粗粒度访问控制,无法做到针对用户的细粒度个性化访问控制。在一些有限范围的应用场景下,虽然实现了行为级别的细粒度控制,但又缺乏有效的隐私信息保护。本文在前期工作基础上,提出了基于智能合约的个性化访问控制方法,可以为 Web 服务提供关于指定用户的高质量的行为数据信息,也充分考虑了用户隐私保护。这种方法一方面可以提升现有信任模型的可信度结果可靠性,另一方面也允许 Web 服务通过智能合约的策略、模型以及参数控制实现对用户的个性化访问控制。

参考文献

[1] Yan Z, Li X, Kantola R. Controlling cloud data access based on reputation[J]. *Mobile Networks and Applica-*

tions, 2015, 20(6): 828-839

[2] Singh A, Chatterjee K. Trust based access control model for securing electronic healthcare system[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2019, 10: 4547-4565

[3] Bedekar M, Zahoor S, Atote B S, et al. Personalization in user profiling: privacy and security issues[C]//2016 International Conference on Internet of Things and Applications (IOTA), Pune, India, 2016: 415-417

[4] Aberer K, Despotovic Z. Managing trust in a peer-2-peer information system[C]//Proceedings of the 10th International Conference on Information and Knowledge Management, New York, USA, 2001: 310-317

[5] Alexopoulos N, Vasilomanolakis E, Ivánkó N R, et al. Towards blockchain-based collaborative intrusion detection systems[C]//International Conference on Critical Information Infrastructures Security, Lucca, Italy, 2017: 107-118

[6] 陆悠, 张妮, 吴宏杰. Web 服务协同环境下个性化访问控制框架的实现[J]. 计算机工程与应用, 2007, 43(18):157-160

[7] 钱继安, 蒋兴浩, 孙锬锋. 基于隐私本体的个性化访问控制模型[J]. 信息安全与通信保密, 2011(2):67-70

[8] Zerkouk M, Cavalcante P, Mhamed A, et al. Behavior and capability based access control model for personalized TeleHealthCare assistance[J]. *Mobile Networks and Applications*, 2014, 19(3):392-403

[9] Hu B, Zhao X F, Zhang C, et al. A contract based user-centric computational trust towards e-governance[C]//International Conference on Web Services, Honolulu, USA, 2020: 133-149

[10] Sajjad S M, Bouk S H, Yousaf M. Neighbor node trust based intrusion detection system for WSN[J]. *Procedia Computer Science*, 2015, 63: 183-188

[11] Adams W J, Davis N J. Toward a decentralized trust-based access control system for dynamic collaboration[C]//Proceedings of the 6th Annual IEEE SMC Information Assurance Workshop, New York, USA, 2005: 317-324

[12] Toumi K, Andrés C, Cavalli A. Trust-orbac: a trust access control model in multi-organization environments[C]//International Conference on Information Systems Security, Berlin, Germany, 2012: 89-103

[13] Yan Z, Li X, Wang M, et al. Flexible data access control based on trust and reputation in cloud computing[J]. *IEEE Transactions on Cloud Computing*, 2015, 5(3): 485-498

[14] Tran H, Hitchens M, Varadharajan V, et al. A trust based access control framework for P2P file-sharing systems[C]//Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, USA, 2005: 1-10

[15] Jin Y, Wang F, Zhao H W, et al. Survey on trust mechanisms in the environment of cloud computing[J]. *Journal of Chinese Computer Systems*, 2016, 37(1): 1-11

[16] Ruohomaa S, Kutvonen L. Trust management survey[C]//Proceedings of the 3rd International Conference on Trust Management, Paris, France, 2005: 77-92

[17] Schnjakin M, Alnemr R, Meinel C. Contract-based cloud architecture[C]//Proceedings of the 2nd International Workshop on Cloud Data Management, New York, USA, 2010: 33-40

[18] Wood G. Ethereum: a secure decentralised generalised transaction ledger[EB/OL]. https://ethereum.github.io/yellowpaper/paper.pdf:Ethereum, 2020

[19] The linux foundation. Hyperledger fabric[EB/OL]. https://www.hyperledger.org/projects/fabric: hyperledger, 2020

[20] Chen P W, Jiang B S, Wang C H. Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet[C]//2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Rome, Italy, 2017: 139-146

[21] Tao Q, Cui X, Huang X F, et al. Food safety supervision system based on hierarchical multi-domain blockchain network[J]. *IEEE Access*, 2019(7): 51817-51826

[22] Yong B B, Shen J, Liu X, et al. An intelligent blockchain-based system for safe vaccine supply and supervision[J]. *International Journal of Information Management*, 2020, 52: 1-12

[23] Huynh T D, Jennings N R, Shadbolt N R. An integrated trust and reputation model for open multi-agent systems[J]. *Autonomous Agents and Multi-Agent Systems*, 2006, 13(2):119-154

[24] Liang Z, Shi W. PET: A personalized trust model with

reputation and risk evaluation for p2p resource sharing [C]// Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, USA, 2005: 1-10

[25] Botelho V, Kredens K V, Martins J V, et al. Dossier: decentralized trust model towards a decentralized demand [C]//2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design, Nanjing, China, 2018: 371-376

[26] Zacharia G, Maes P. Trust management through reputation mechanisms [J]. *Applied Artificial Intelligence*, 2000, 14(9):881-907

A smart contract based personalized access control method towards Web service

Hu Bin[*,**], Zhao Xiaofang[*], Song Yonghao[*], Yu Lei[*], Duan Dongsheng[***], Zhang Cheng[*]

([*] Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

([**] University of Chinese Academy of Sciences, Beijing 100049)

([***] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029)

Abstract

Trust based dynamic access control (TBAC) is one major technique on protecting service providers' (SPs) resources. The personalized access control and the reliability of trust are the central problems of TBAC. To solve it, this paper proposes a smart contract based personalized access control method (SC-PAC). It introduces a smart contract-based access control procedure, which allows SPs to flexibly set the trust model, parameters, and the access control policies, to provide a customer-level personalized access control. Combined with the previous work, reliable behavior data of users are provided to ensure a reliable trust evaluation. A new trust model is designed in case study and experiments are designed to test this trust model and the SC-PAC method. The results of experiments show that the SC-PAC can provide a customer-level personalized access control compared with the traditional work and a more reliable trust evaluation through the accurate behavior data of users.

Key words: Web service, trust evaluation, personalization, dynamic access control, smart contract