Journal of Computer Applications
计算机应用, 2020, 40(6): 1674 - 1679
ISSN 1001-9081
CODEN JYIIDU
2020-06-10
http://www.joca.cn

文章编号:1001-9081(2020)06-1674-06
DOI:10.11772/j.issn.1001-9081.2019101780

基于区块链和用户信用度的访问控制模型

王海勇[1],潘启青[2*],郭凯璇[2]
(1. 南京邮电大学 计算机学院,南京 210003; 2. 南京邮电大学 物联网学院, 南京 210003)
(*通信作者电子邮箱 why@njupt.edu.cn)

摘　要:针对当前访问控制中用户权限不能随着时间动态变化和访问控制合约中存在的安全性问题,提出了一种以基于角色的访问控制(RBAC)模型为基础,同时基于区块链和用户信用度的访问控制模型。首先,角色发布组织分发角色给相关用户,并把访问控制策略通过智能合约的方式存储在区块链中,该合约设定了访问信用度阈值,合约信息对系统内任何服务提供组织都是可验证、可追溯且不可篡改的。其次,该模型根据用户的当前信用度、历史信用度和推荐信用度评估出最终信用度,并根据最终信用度获得对应角色的访问权限。最后,当用户信用度达到合约设定的信用度阈值时,用户就可以访问相应的服务组织。实验结果表明,该模型在安全访问控制上具有一定的细粒度、动态性和安全性。

关键词:区块链;智能合约;基于角色的访问控制模型;访问控制;用户信用度
中图分类号:TP309.2　　**文献标志码**:A

Access control model based on blockchain and user credit

WANG Haiyong[1], PAN Qiqing[2*], GUO Kaixuan[2]
(1. *School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu* 210003, *China*;
2. *School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu* 210003, *China*)

Abstract: Focusing on the problem that user privileges cannot dynamically change with time in the current access control and the security problems in the access control contract, an access control model based on Role-Based Access Control (RBAC) model, blockchain and user credit was proposed. Firstly, the roles were distributed to relevant users by the role publishing organization, and the access control strategy was stored in the blockchain through smart contract method. In the contract, the access credit threshold was set, and the contract information was verifiable, traceable and tamper-proof to any service provider organization in the system. Secondly, the final credit was evaluated by the model according to current credit, historical credit and recommended credit of the user, and the access privileges of the corresponding role was obtained based on the final credit. Finally, when the user credit reached the credit threshold set in the contract, the user can access the corresponding service organization. Experimental results show that the proposed model has certain fine granularity, dynamicity and security in the security access control.

Key words: blockchain; smart contract; Role-Based Access Control (RBAC) model; access control; user credit

0　引言

随着信息时代的快速发展,组织之间的信息共享已经在生活中得到了非常广泛的应用,数据共享所带来的社会变革也已深入到我们生活的方方面面。跨组织访问控制主要是让不同组织的用户可以访问到其他组织的信息资源,让独有的信息资源得到更大化的利用。例如,医生想要理解一些疑难杂症,就需要对大量病人的临床医疗数据[1]进行分析,这有利于更好地了解病情,并作出精确的诊断治疗、提高对流行疾病的预警能力和采取有效的基础措施预防突然爆发的流行病。但是不同医院的病人资料都是独享的,医生想要更准确地分析出病症的状况,就需要访问到其他医院的相关病人资料。现有的很多方法是把不同组织的数据集中在一起[2],再进行访问,这种集中式的处理方法可能会造成信息的大量泄漏。由此可见,访问控制之中的数据如何管理,角色之间如何分配和相关安全性问题具有一定的研究价值。

传统的访问控制模型主要有自主访问控制(Discretionary Access Control, DAC)、强制访问控制(Mandatory Access Control, MAC)、基于属性的访问控制(Attribute Based Access Control, ABAC)[3-4]和基于角色的访问控制(Role-Based Access Control, RBAC)[5]。这四种访问控制模型都具有对不同主体访问对应客体的授权和控制能力。例如,在DAC系统中,主体可以决定将自身拥有的权力授予给其他主体,但是其开销过大、效率不高,不适合大型复杂的系统,只能应用于简

收稿日期:2019-10-20;**修回日期**:2019-12-02;**录用日期**:2019-12-11。　**基金项目**:江苏省教育信息化研究资助重点课题(20172105);江苏省现代教育技术研究2017年度智慧校园专项课题(2017-R-59518);南京邮电大学教学改革重点项目(JG06717JX66);南京邮电大学校园信息化创新项目(NYXX217002,NYXX217004);赛尔网络下一代互联网技术创新项目(NGII20180620)。

作者简介:王海勇(1979—),男,江苏南京人,副研究员,博士,CCF会员,主要研究方向:计算机网络与安全、信息网络; 潘启青(1994—),女,江苏南京人,硕士研究生,主要研究方向:区块链、智能合约、访问控制; 郭凯璇(1991—),女,山东枣庄人,硕士研究生,主要研究方向:区块链、共识算法、物联网。

单系统。MAC是根据系统管理员制定的访问控制策略,用来进行多层级别的访问控制,但制定的规则缺乏灵活性、应用率不高。ABAC在用户和权限之间引入了属性判断条件,所有的权限通过用户不同的属性进行授予而非直接分配给用户,所以具有支持大规模复杂系统和高灵活性的优势,但是过程比较复杂、难以管理。RBAC是把角色分配给用户,让用户根据不同的角色来访问不同的权限,而非直接把权限分给用户,所以易于管理、具有灵活性,因此RBAC较为适合用于一般不同组织之间资源交互的访问控制。Salim等[6]提出了基于预算感知的角色访问控制,该模型明确定义了资源的价值,将使用预算和成本加入了RBAC中,并为用户分配了有限的预算,通过这些预算支付所需权限的成本,就可以访问相应的资源。这种方法使用户访问受到分配预算的限制,能够防止用户滥用权限能力,但其访问控制合约的安全性还存在一定的问题。Jason等[7]提出了一种使用智能合约的角色访问控制模型,这是一个利用以太坊智能合约技术实现跨组织访问的平台,使得应用程序可以自主、分散地运行,并实现了用户对角色所有权的质询-响应身份验证协议,提高了访问控制安全性和灵活性,但其细粒度划分不够,动态性有待改善。余波等[8]提出了基于属性和信用的访问控制模型,将密文属性加密思想和用户信用评估的方法相结合,不仅把角色加入了信用阈值的访问结构,还为每个用户分配了一个包含信用值属性的属性集合,只有用户属性集合和角色相匹配时,才能行使相关权限。这种方法增强了访问结构的动态性和权限的细粒度,但是访问控制策略的交互和安全问题还有待考察。黄美蓉等[9]提出了一种基于特征提取的访问控制方法,该方法通过将RBAC模型和BLP(Bell-LaPadula)模型结合在一起,从而解决了用户在不同时间、不同安全级别和不同空间的多级授权管理问题,并对历史访问记录进行数据分析,判断访问请求是否合理。这种方法对用户的访问请求有较高的正确评判率,但没有对其细粒度和安全方面进行分析。

综上所述,对于现有技术中存在的问题,本文将区块链技术、用户信用度分析和RBAC模型相结合,提出了基于区块链和用户信用度的访问控制(RBAC based on Blockchain and user Credit, BC-RBAC)模型,该模型将用户信用度评估加入到RBAC策略中,并将用户信用度和访问控制策略发布到区块链中。区块链作为一种分布式处理机制,具有去中心化、开放性、不可篡改的特点[10]。两种方式的结合,使得该模型具有更好的细粒度、动态性和安全性。

1　相关知识

1.1　RBAC模型

RBAC是一种传统的访问控制模型,主要为了实现角色分配和访问控制之间的关系[8]。在RBAC之中,包含用户users、角色roles、目标objects、操作operations、许可权PERM(PERMissions)五个基本数据元素。图1显示了用户、角色、访问权限和会话之间的关系。

1)用户(users):指的是系统上的任何个人,可以与系统中的组织进行交互。

2)角色(roles):指的是角色发布组织给角色分配的权限位置,用户可以根据拥有的权限进行相应的访问操作,角色是用户和组织之间沟通的桥梁,具有至关重要的位置。

3)许可权(PERM):权限描述的是操作和目标对象之间的关系,在权限范围内,权限持有者可以在系统中执行相应能力,是一种行为操作。

4)会话(sessions):表示用户和角色之间被激活的映射关系。一个用户可能会拥有多个角色,会话可以把所拥有的角色联系起来,用户可以激活所有角色的并集。

5)用户角色分配(User Assignment, UA)和角色许可分配(Permission Assignment, PA):单个用户可以拥有多个角色,一个角色也可以拥有不同的用户,都是多对多的对应关系。同理,每个角色都可以对应多个权限,一样的权限也可以分配给不同的角色。角色作为用户和权限之间的连接者,能够提供更好的管理方式。

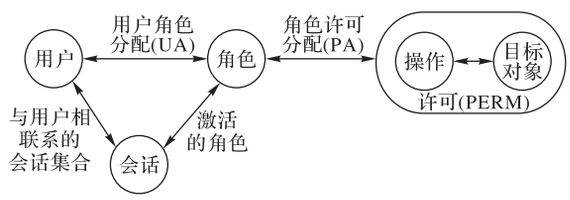

图1　RBAC模型

Fig. 1　RBAC model

1.2　区块链技术基本原理

区块链是一种在分布式网络环境下基于透明度和共识算法规则的数据结构,根据时间戳顺序将存入区块的数据以链条连接的方式组合起来,并以hash算法、数字签名、零知识证明的方式保证其数据不可伪造、不可篡改、可溯源,保障用户的隐私。基于区块链分布式的特点,不仅数据可以存储在区块链上,数据也可以记录在区块链上,即所有节点达成共识,共同参与和维护整条链,这样可以避免单个节点造成破坏而影响整个系统;并且区块链的应用能很好地避免由于组织间信息共享和访问控制存在的安全性问题。

区块链涉及多方面技术创新知识:点对点的存储结构和密码学技术[11]为区块链提供了去中心化、隐私保护和防篡改的功能;链式结构的连接方式保障了数据的可溯源、真实性和完整性;智能合约为系统提供了分布式、自动化执行的方式;共识机制实现了分布式节点的公开验证一致性。这些技术结合到一起,形成了一种新的数据存储、记录方法,增强了数据记录的安全性。

1.3　智能合约

智能合约[12-13]是存储在区块链上能够在分布式网络节点上进行自动运行的脚本,由Nick Szabo在1994年首次提出相关概念,定义它为一种通过代码程序来自动执行的交易协议。只要交易双方满足合约条款,则不需要第三方管理者的监督就可自动执行交易。虽然智能合约的想法在很早之前就被提出,但一直都无法落地实现,由于缺乏可支撑合约自动执行的平台和相关技术,直到区块链技术的出现,才为智能合约提供了可支撑的平台。由于区块链具有的安全、去中心化、不可篡改的特点,确保了智能合约运行环境的安全性。智能合约的用户可以在可信的环境下,按照合约顺序自动执行操作条件,同时利用区块链的公开性和可追溯性,时时追踪合约的动态变化。随着区块链的不断发展,第二大区块链平台以太坊[14]设计了一种基于去中心化的以太虚拟机(Ethereum Virtual Machine, EVM)来处理点对点的合约策略,任何开发者都可以基于这款区块链公共平台来进行开发操作,扩大了区块链的运用领域,加快了区块链的发展。

2 基于区块链和用户信用度的访问控制模型

2.1 BC-RBAC框架及工作流程

本文提出的基于区块链和用户信用度的访问控制(BC-RBAC)模型,主要为了研究如何能安全有效地实现组织之间的访问控制。BC-RBAC是一种基于区块链和智能合约的访问认证机制,图2给出的是所提出系统的框架结构,主要由角色发布方、用户、服务提供方、合约层和合约信用层组成。角色发布方A既可以发布角色,也可以提供服务。同理,服务提供方B既提供服务,也可以发布角色。A、B之间可以相互访问。为了方便叙述,此架构主要以A为角色发布方、B为服务提供方进行描述。

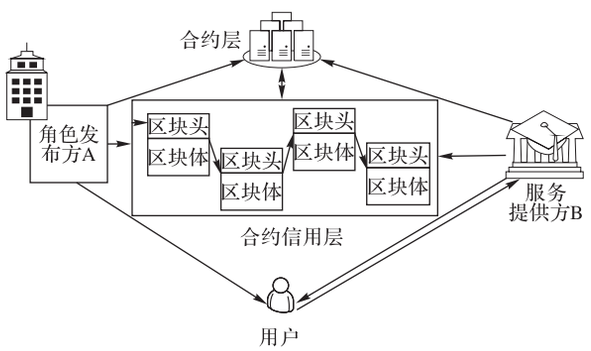

图2 BC-RBAC框架

Fig. 2 Framework of BC-RBAC

BC-RBAC框架中访问控制工作流是对RBAC模型工作流的扩展。访问控制之间的工作步骤为:

1)角色发布方A给用户分配角色,并制定角色许可权限,把相应的访问策略(包含制定用户信用度阈值)通过智能合约的形式发布在区块链上,也将用户信用度评估值发布在区块链上,作为其他组织的推荐信用度。

2)用户从角色发布组织A获得角色信息,向服务提供方B资源访问请求。当用户初次进入访问系统时,没有对应的信用度。

3)服务提供方B接收到用户的访问请求,先查看智能合约上的访问策略,审核用户是否拥有相关角色,如果审核通过,对应智能合约就被激活。激活的智能合约根据合约设定和用户的信用度,允许或禁止用户的访问。

4)当用户信用值达到合约条件或用户未拥有用户信用度时,服务提供方B确认用户请求,并对用户的访问过程进行信誉评估。会根据从区块链上其他组织提供的推荐信用度、用户之前访问的历史信用度和当前信用度值,得出用户最终信用度,并写入区块链中,方便其他组织参考。

5)当评估的信用度低于智能合约中设定的信用值时,相应的智能合约就会自动暂停,用户将无法访问到服务提供方B。

2.2 面向BC-RBAC的智能合约

合约层放置着系统内所有的智能合约(Smart Contract,SC),SC用于创建用户的角色分配和设置信用值的阈值,然后在区块链上发布。SC为创建用户角色分配提供了安全、便捷的方式。SC也是一种高效安全的可编程资产,其运行与编程完全相同。SC具有以下特征:

1)允许角色发布组织向用户发布角色(和其他相关信息);

2)允许角色发布组织以透明的方式管理和修改信息;

3)允许角色发布组织在需要时撤销向用户发布的角色;

4)允许合约根据信用度状态和设置的访问信用值,自动运行或停止相关合约。

智能合约(SC)功能设计如下:

Adduser(*u.role*, *u.notes*):这个功能只能由SC的所有者或创建者执行,主要在SC中添加用户并发出相应的角色和相关信息执行函数。它将要发给*u*的角色(*u.role*)和注释(*u.notes*)作为输入,其中包含一些其他相关信息,如到期日期和个性化设置。该功能输出SC更新状态和执行命令时的时间戳。

Removeuser:此功能只能由SC所有者或创建者执行,以从SC中删除用户并撤消其角色,该功能输入删除数据,输出SC更新状态和时间戳。

Changestatus:此功能只能由SC所有者或创建者执行以停用SC。一旦部署了SC,SC就将永久保留在区块链上,因此,判断SC是否处于活动状态是很重要的,输入停用操作,输出SC状态和时间戳。

Setstatus:此功能只能由SC所有者或创建者根据信用度存在状态,来设置相应判断结果,输入用户信用度有或无,输出结果和时间戳。

Setvalue:此功能是根据SC所有者或创建者设定的信用度阈值和用户的实际信用值来自动执行,输入信用度阈值和用户信用度,输出执行或暂停,还有时间戳。

2.3 用户信用度计算方法

用户信用度是由当前信用度、历史信用度和推荐信用度组成的。*Current_T*(*u*)、*History_T*(*u*)、*Recommend_T*(*u*)分别表示当前信用度、历史信用度和推荐信用度。

2.3.1 当前信用度

对于用户当前信用度的评估,主要采用的是模糊层次分析法(Fuzzy Analytic Hierarchy Process, FAHP)[15]。这个方法是先将用户行为分为*n*个特性,再把每个特性分为多个证据类型,从而把模糊的、不确定的用户行为信用评估问题细化成简单的、明确的信用证据加权求和问题,如图3所示。

功能特性*P*	可靠特性*R*	安全特性*S*
*p*1 平均CPU利用率		
*p*2 平均吞吐量		
*p*3 平均IP包传输延迟	*r*1 平均用户误码率	*s*1 平均用户非法连接次数
*p*4 平均用户所占线程数	*r*2 平均IP丢包率	*s*2 平均扫描重要端口次数
*p*5 平均IP包延迟抖动时间	*r*3 平均连接建立成功率	*s*3 平均尝试越权次数
*p*6 平均IP包网络带宽占有率	*r*4 用户平均故障服务次数	*s*4 平均用户感染实体病毒数
*p*7 平均用户IP响应时间		
*p*8 平均用户占有存储资源率		

图3 用户行为证据分类

Fig. 3 User behavior evidence classification

这些初始证据数据可以根据软硬件检测获得,表示为$\boldsymbol{A}=(a_{ij})_{mn}$,其中$m$表示特性中最大项数,不够的项用零补齐。为了便于数值计算和用户行为评估,需要把证据全部规范化为在区间[0,1]沿正向递增的无量纲值,表示为矩阵$\boldsymbol{E}=(e_{ij})_{mn}$。

为了获得初始判断矩阵$\boldsymbol{EQ}=(eq_{ij})_{m\times m}$,有$m$个矩阵$\boldsymbol{E}=(e_1,e_2,\cdots,e_m)$,将矩阵集中在$e_i$和$e_j$重要性作二元对比:

$$eq_{ij}=\begin{cases}0, & e_i<e_j\\ 0.5, & e_i=e_j\\ 1, & e_i>e_j\end{cases} \tag{1}$$

将初始判断矩阵转换成模糊一致的矩阵$\boldsymbol{Q}=(q_{ij})_{m\times m}$,其中:

$$q_{ij}=\frac{q_i-q_j}{2m}+0.5;\ q_i=\sum_{k=1}^{m}eq_{ik} \tag{2}$$

计算某个特性的m个证据的权重向量$\boldsymbol{W}=(w,{}_1w_2,\cdots,w_m)^{\mathrm{T}}$,其中:

$$w_i=\frac{\sum_{k=1}^{m}q_{ik}-0.5}{m(m-1)/2} \tag{3}$$

接着计算用户行为特性的评估值矩阵,由证据矩阵$\boldsymbol{E}=(e_{ij})_{m\times n}$、权重矩阵$\boldsymbol{W}=(w_{ij})_{m\times n}$,根据$\boldsymbol{E}\times\boldsymbol{W}^{\mathrm{T}}$得到的矩阵的对角线上的值就是特性评估值矩阵$\boldsymbol{F}=(f_1,f_2,\cdots,f_n)$。最后用户的行为信用度为:

$$Current\_T(u)=1-\boldsymbol{F}\times\boldsymbol{W}_f^{\mathrm{T}}=1-\sum_{i=1}^{n}f_iw_i \tag{4}$$

其中:$Current_T(u)$代表用户的当前信用度;$\boldsymbol{W}_f=(w_{f1},w_{f2},\cdots,w_{fn})$是用户行为特性的权重。

2.3.2　历史信用度

当用户第一次登录进行访问控制后,系统会根据用户的软硬件操作产生首个历史信用度:$History\_T_1(u)=Current\_T_1(u)$。随着访问的次数逐渐增多,用户的历史的信用度就需要根据时间的推移而逐渐改变:

$$History\_T(u)=\begin{cases}0, & n=0\\ \sum_{i=1}^{n}(Final\_T_i(u)\times t_i)\Big/\sum_{i=1}^{n}t_i, & n>0\end{cases} \tag{5}$$

其中:$Final_T_i(u)$对应着用户每次访问结束的最终信用度;t_i记录的是访问时间,该参数计算用户从登录访问到结束退出系统的总时间。当$n=0$时,则表示用户是初次登录系统,没有相应的历史信用值。

2.3.3　推荐信用度

当用户初次进行访问时,不存在历史信用度,推荐信用度就会具有一定的参考价值,用户的推荐信用值是根据用户与其他服务组织之间的信用值计算所得。假设存在n个可信的访问组织$S=(s_1,s_2,\cdots,s_n)$,T和N分别代表服务组织s_i与用户u_i的历史信用值和成功访问的次数,则推荐信用度的表达式为:

$$Recommend\_T(u)=\begin{cases}0, & n=0\\ \sum_{j=1}^{n}(N_j\times T_{u_i}^{s_i})\Big/\sum_{j=1}^{n}N_j, & n>0\end{cases} \tag{6}$$

2.3.4　最终信用度的计算

综合当前信用度、历史信用度和推荐信用度,得出最终信用度:$Final\_T(u)=a\times Current\_T(u)+b\times History\_T(u)+c\times Recommend\_T(u)$,其中$a+b+c=1$,$a>b>c$。在计算中,三者关系所占的比重为:$Current\_T(u)>History\_T(u)>Recommend\_T(u)$。当用户首次进入访问系统时,则用户的历史信用度为0,即$History_T(u)=0$;如没有在其他组织进行访问,则参考信誉度$Recommend_T(u)=0$。对于a、b、c的概率分配,其中a的比重最大,a的大小还依据用户当前操作的危险级别来进行调整,危险级别分为高危级别和低危级别,分别对应a_1和a_2,$a_1>a_2$。当用户当前操作的危险级别为高危级别时,a_1无限趋于1,b和c的比重就趋于0。设置等级的目的是为了防止用户恶意刷取信用度,把信用度刷到最高级别,然后进行高危操作。

3　实验仿真和结果分析

实验主要从两方面进行分析:用户信用度和区块链安全性。在配置为I5-8265U处理器、8 GB内存、512 GHz固态硬盘(Solid State Drive, SSD)的Windows 10系统下,通过Matlab 2017a进行仿真实验。

3.1　用户信用度分析

根据用户当前信用度、历史信用度和推荐信用度进行仿真实验。通过测量得出用户的行为证据值,再规范处理后,求出平均的证据值P、R、S。之后,根据当前的网络测试经验得出不同特性证据的重要性程度划分为:功能特性是$p1=p4=p6=p7>p2=p8>p3=p5$,可靠特性是$r3=r4>r1=r2$,安全特性是$s2=s3>s1>s4$。最后计算出用户信用度,实验结果如图4所示。

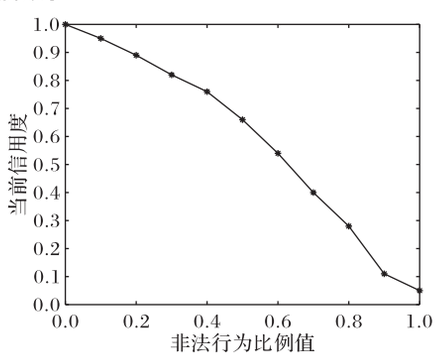

图4　当前信用度变化趋势

Fig. 4　Current credit trend

用户在访问组织资源时,不断进行非法行为的操作,用户的当前信用度就会随着非法行为的比例值增加而大幅度降低,符合实际情况,有利于及时更新用户的访问权限。当用户的访问次数不断增加时,用户的当前信用度y_d、历史信用度y_s和推荐信用度y_t也会随之不断变化。如图5所示,用户在前9次访问时,信用度值变化不大,第10次访问时突然进行高危操作,当前信用度急剧下降,但用户的历史信用值和推荐信用值还比较高,根据计算得出的最终信任值就会处于一个中等状态,不能很好反映用户信用的实际情况。因此本文加入了高危操作和低危操作的区分,如图6所示。

当用户发生高危操作,a的比值无限趋于1,最终用户信用度差不多就等于当前用户信用度,能够更好地反映用户的真实状态,保护系统的安全性。

3.2　区块链安全性分析

智能合约分布在区块链上,所以两者的安全性是紧密相连的。如今区块链所面临的危险,主要来自于攻击者对区块

链中共识机制的攻击，以下主要对两种共识机制进行安全性分析。

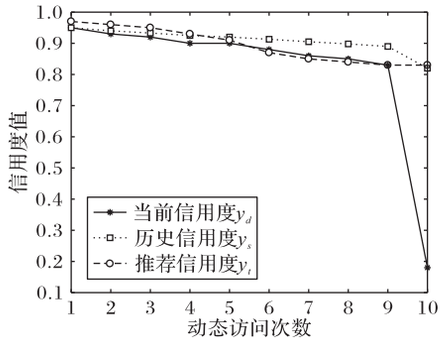

图5 三种信用度变化趋势

Fig. 5 Trends for three kinds of credit

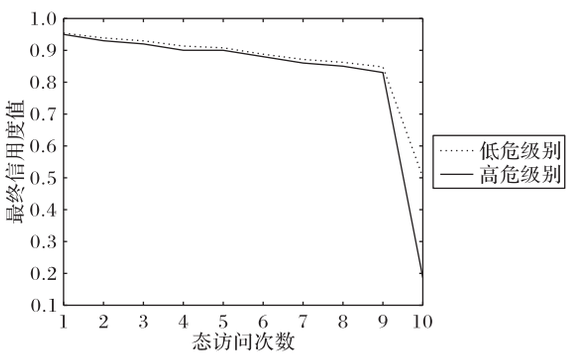

图6 低危、高危信用度变化区别

Fig. 6 Low-risk, high-risk credit change difference

3.2.1 工作量证明机制

工作量证明(Proof of Work, PoW)是共识机制的一种，在PoW中谁的算力多，谁最先解决问题的概率也就最大，当攻击者掌握超过全网的一半算力时，就能控制住网络中链的走向。实验以PoW为例，分析区块链的自身抗攻击能力，运用文献[16]提出的攻击模型进行详细分析。诚实节点产生的链条与攻击者产生的链条之间存在竞赛的关系，可以用二叉树随机漫步(Binomial Random Walk)的过程来进行描述。当诚实节点领先时，诚实者的链条延长一个区块；反之，则攻击者的链条延长一个区块。攻击者成功填补z个区块落后的差距，类似于赌徒破产问题(Gambler's Ruin problem)，那么攻击者填补上亏空，赶上诚实链条的概率为：

$$q_z=\begin{cases}1, & p\leqslant q\\ (q/p)^z, & p>q\end{cases} \tag{7}$$

其中：p表示诚实节点获得下个一节点所有权的概率；q表示攻击者获得下个一节点所有权的概率，q_z表示攻击者填补上z个区块落后的差距。当$p>q$时，攻击者攻击成功的概率就随着区块的增长而呈现下降趋势。假设诚实区块以平均预期的耗费时间产生一个区块，那么攻击者的潜在进展就符合泊松分布计算，期望值为：

$$\lambda=zq/p \tag{8}$$

为了计算攻击者产生节点追上诚实节点的概率P_z，将攻击者获得潜在进展区块数量的泊松分布与该数量下攻击者仍然可以追赶上诚实节点的概率相乘，得出式(9)：

$$P_z=\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(q/p)^{(z-k)}, & k\leqslant z\\ 1, & k>z\end{cases} \tag{9}$$

为了避免对无限数列求和，化简后为：

$$P_z=1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left(1-(q/p)^{(z-k)}\right)=$$
$$1-\sum_{k=0}^{z}\frac{(zq/p)^k e^{-zq/p}}{k!}\cdot\left(1-(q/p)^{(z-k)}\right) \tag{10}$$

攻击者成功篡改区块的概率和区块差距的关系变化如图7所示。

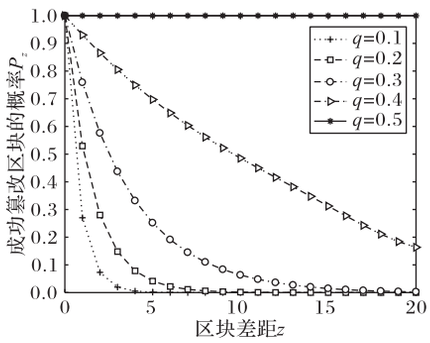

图7 攻击者成功概率

Fig. 7 Attacker success probability

当攻击者获得下一个节点所有权的概率小于0.5时，攻击者成功篡改的概率随着区块差距的增加而逐渐减小；反之，当攻击者获得下一个节点所有权的概率大于等于0.5时，攻击者就可成功篡改下一个区块。也就是说，只有当攻击者取得区块链上50%以上的算力时，才能够掌控整个区块链数据走向。由于区块链中节点较多，攻击者想要拥有全网50%的算力要付出巨大的成本，因此很难攻破，所以运用区块链在组织访问中能够达到非常好的抗攻击效果。

3.2.2 拜占庭容错算法

实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)算法能够在网络中存在恶意节点的情况下保证最终决策的一致性和正确性，为智能合约的安全部署奠定基础。该算法节点分为主节点和备份节点，主节点主要负责将客户端的请求排序，备份节点按照主节点提供的顺序执行请求。PBFT一般包含三种基本协议：一致性协议、检查点协议和视图更换协议。

一致性协议的目的是让来自客户端的请求能够按照确定的顺序在每个服务器上执行，客户端将收集到的信息转化为证明文件，再发送给服务器。当拜占庭系统中包含$3f+1$台服务器时，至少需要收集到$2f+1$台服务器发送的正确信息，才能确保达到一致性。由于在拜占庭系统中，可能存在系统资源被大量日志占用和服务器状态不一致的情况。因此，检查点协议会周期性地执行，用来处理日志、节约资源，同时纠正节点状态。视图更换协议的作用就是当主节点发生错误时，用备份节点替换掉主节点，并且保证已经被正常节点执行完毕的请求不会被篡改。通过三种协议的共同合作，保障了PBFT的容错性和安全稳定性。

3.3 模型特点分析

与其他访问控制模型(文献[7,8,15]模型)相比，BC-RBAC具有突出的优势，比较结果如表1所示。BC-RBAC能

够根据用户的信用度动态修改用户的访问控制权限,相较文献[7]模型的授权过程更加灵活;同时,BC-RBAC还对危险操作等级和用户的任用度进行划分,加入了历史信用度和推荐信用度,使所求最终结果准确度更高,相较文献[8,15]模型中用户信用度更具有参考性;BC-RBAC还将访问控制策略以智能合约的形式发布在区块链中,相较文献[8,15]中的模型更加安全可靠。

表1　BC-RBAC与其他模型对比

Tab. 1　Comparison between BC-RBAC and other models

模型	权限动态调控	操作等级细粒度划分	访问过程安全性
BC-RBAC	✓	✓	✓
文献[7]模型	×	×	✓
文献[8]模型	✓	×	×
文献[15]模型	✓	×	×

4　结语

本文针对组织间信息访问存在的特点和安全性问题,提出了一种基于区块链和用户信用度的访问控制模型。首先,将访问控制策略写入智能合约,通过分析用户行为,引入FAHP完成用户当前信用度的计算,并根据多方面的评价结合和划分危险操作级别,得出用户最终信用度;再将区块链技术与RBAC模型相结合,借助区块链所具有的不可篡改、可追溯、透明性的特点,将用户信用度值和智能合约发布在区块链上。实验结果表明,该模型可以有效地对用户行为进行分析评估,动态更新和细粒度划分用户访问的权限。同时,区块链的运用有利于防止不法分子对于合约的攻击和篡改,增强了访问控制的安全性。BC-RBAC模型实现了安全、可靠、透明的新型访问控制模型,能够有效促进组织间信息共享并提供安全保障。

参考文献(References)

[1] DIMITROV D V. Medical internet of things and big data in healthcare [J]. Healthcare Informatics Research, 2016, 22(3): 156-163.

[2] ALANSARI S, PACI F, SASSONE V. A distributed access control system for cloud federations [C]// Proceedings of the IEEE 37th International Conference on Distributed Computing Systems. Piscataway: IEEE, 2017: 2131-2136.

[3] YUAN E, TONG J. Attributed Based Access Control (ABAC) for Web services [C]// Proceedings of the 2005 IEEE International Conference on Web Services. Piscataway: IEEE, 2005: 561-569.

[4] 房梁,殷丽华,郭云,等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报,2017,40(7):1680-1698. (FANG L, YIN L H, GUO Y, et al. A survey of key technologies in attribute-based access control scheme [J]. Chinese Journal of Computers, 2017, 40(7): 1680-1698.)

[5] FERRAIOLO D F, SANDHU R, GAVRILA S, et al. Proposed NIST standard for role-based access control [J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[6] SALIM F, REID J, DULLECK U, et al. Budget-aware role based access control [J]. Computers and Security, 2013, 35: 37-50.

[7] JASON P, YUICHI K, NAOTA Y. RBAC-SC: role-based access control using smart contract [J]. IEEE Access, 2018, 6: 12240-12251

[8] 余波,台宪青,马治杰. 云计算环境下基于属性和信任的RBAC模型研究[J]. 计算机工程与应用,2020,56(9):84-92. (YU B, TAI X Q, MA Z J. Study on attribute and trust-based RBAC model in cloud computing [J]. Computer Engineering and Applications, 2020, 56(9): 84-92.)

[9] 黄美蓉,欧博,何思源. 一种基于特征提取的访问控制方法[J]. 计算机科学,2019,46(2):109-114. (HUANG M R, OU B, HE S Y. Access control method based on feature extraction [J]. Computer Science, 2019, 46(2): 109-114.)

[10] 刘敖迪,杜学绘,王娜,等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报,2018,29(7):2092-2115. (LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security [J]. Journal of Software, 2018, 29(7): 2092-2115.)

[11] 刘敖迪,杜学绘,王娜,等. 基于区块链的大数据访问控制机制[J]. 软件学报,2019,30(9):2636-2654. (LIU A D, DU X H, WANG N, et al. Blockchain-based access control mechanism for big data [J]. Journal of Software, 2019, 30(9): 2636-2654.)

[12] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of things [J]. IEEE Access, 2016, 4: 2292-2303.

[13] TAPSCOTT D, TAPSCOTT A. 区块链革命:比特币底层技术如何改变货币、商业和世界[M]. 凯尔,孙铭,周沁园,译. 北京:中信出版社,2016: 7-14. (TAPSCOTT D, TAPSCOTT A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World [M]. KAI E, SUN M, ZHOU Q Y, translated. Beijing: China CITIC Press, 2016: 7-14.)

[14] BUTERIN V. Ethereum white paper [EB/OL]. [2019-06-20]. https://github.com/ethereum/wiki/wiki/White-Paper.

[15] 张凯,潘晓中. 云计算下基于用户行为信任的访问控制模型[J]. 计算机应用,2014,34(4):1051-1054. (ZHANG K, PAN X Z. Access control model based on trust of users' behavior in cloud computing [J]. Journal of Computer Applications, 2014, 34(4): 1051-1054.)

[16] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2019-08-18]. https://www.audible.com/pd/Bitcoin-A-Peer-Electronic-Cash-System-Audiobook/B077T5SCP2.

This work is partially supported by the Jiangsu Provincial Education Informationization Research Funded Key Topic (20172105), the Modern Education Technology Research 2017 Smart Campus Special Topic of Jiangsu Province (2017-R-59518), the Teaching Reform Key Project of Nanjing University of Posts and Telecommunications (JG06717JX66), the Campus Informationization Innovation Project of Nanjing University of Posts and Telecommunications (NYXX217002, NYXX217004), the CERNET Innovation Project (NGII20180620).

WANG Haiyong, born in 1979, Ph. D., associate research follow. His research interests include computer network and security, information network.

PAN Qiqing, born in 1994, M. S. candidate. Her research interests include blockchain, intelligent contract, access control.

GUO Kaixuan, born in 1991, M. S. candidate. Her research interests include blockchain, consensus algorithm, Internet of things.