计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190700157

大数据风险访问控制研究进展

王静宇　刘思睿
内蒙古科技大学信息工程学院　内蒙古 包头 014010
(13734728816@126.com)

摘　要　大数据访问控制是确保大数据数据安全与信息共享的重要技术之一,但由于传统的访问控制策略无法满足动态环境下访问信息的实时性与动态性,因此在访问控制中引入风险评估方法,以协调访问控制策略,提高访问控制在动态环境中的应用。鉴于此,文中对国内外风险访问控制研究的主要工作进行系统的回顾与总结,分析近年来最新研究成果。首先,分析总结了扩展到传统的访问控制模型和基于XACML框架的访问控制模型的风险访问控制,及其在不同环境中的应用;其次,对风险访问控制的技术与方法进行总结与分析,并且对风险自适应访问控制(Risk-Adaptable Access Control,RAdAC)进行分析与研究;最后,对未来大数据环境下风险访问控制的研究进行了展望,提出一些具有研究价值的问题。文中认为,在未来大数据访问控制研究技术中,基于风险的访问控制仍然是大数据访问控制的重要研究内容。

关键词:访问控制;风险量化;风险因素;风险阈值;风险自适应
中图法分类号　TP391

Research Progress on Risk Access Control

WANG Jing-yu and LIU Si-rui
School of Information Engineering,Inner Mongolia University of Science and Technology,Baotou,Inner Mongolia 014010,China

Abstract　Big data access control is one of the important technologies to ensure the security and information sharing of big data. However,because the traditional access control strategy can not meet the real-time and dynamic access information in the dynamic environment,the risk assessment method is introduced in the access control to coordinate access control policies,improve the application of access control in dynamic environments. In view of this,this paper systematically reviews and summarizes the main work of risk access control research at home and abroad,and analyzes the latest research results in recent years. Firstly,the risk access control extended to the traditional access control model and its XACML framework-based access control model is analyzed and summarized,and the application in different environments is summarized. Secondly,the techniques and methods of risk access control are summarized and analyzed,the risk is self-contained,and Risk-Adaptive Access Control (RAdAC) is analyzed and researched. Finally,the future research on risk access control in big data environment is prospected,and some problems with research value are proposed. This paper argues that risk-based access control is still an important research content of access control in future big data access control research technology.

Keywords　Access control,Risk quantification,Risk factor,Risk threshold,Risk-adaptation

1　引言

访问控制是保障信息安全的一种手段,是大多数系统(包含计算机系统和非计算机系统)都需要用到的一种技术。自主访问控制[1](Discretinoary Access Control,DAC)、强制访问控制[2](Mandatory Access Control,MAC)、基于角色的访问控制[3](Role Based Access Control,RBAC)等传统的访问控制是基于明确区分允许访问和拒绝访问的预定义策略做出的授权,具有静态、严格按照策略规则进行授权访问的特点,无法适应目前动态、分布式的网路环境。然而,随着物联网、云计算以及大数据等技术的高速发展与应用,大数据应用环境下的云计算平台的访问控制方案必须具有高度的可扩展性、灵活性和高效性。并且,由于基于大数据环境的访问控制的动态性和实时交互访问等特点,导致特殊的实时访问请求在匹配传统预定义访问策略时无法满足动态匹配的问题,因此将风险引入访问控制是解决该问题的一种方法。

2　基于风险的访问控制

风险是指未来事件结果的不确定性,其深层含义强调的是风险产生的结果表现为损失的不确定性[4]。基于风险的访

到稿日期:2019-07-22　返修日期:2019-10-02　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金资助项目(61662056);内蒙古自然科学基金资助项目(2016MS0609,2016MS0608)
This work was supported by the National Natural Science Foundation of China(61662056) and Natural Science Foundation of Inner Mongolia Autonomous Region,China(2016MS0609,2016MS0608).
通讯作者:刘思睿(liusirui11@163.com)

问控制从本质上来说是一种有根据的猜想,系统试图通过访问控制来平衡未来出现的风险与需求,但是并非所有的风险和需求都能被策略制定者预见,所以要求评估风险,权衡收益,使系统在风险评估之后能够采取缓解和降低风险的措施。风险评估由以下几个重要部分组成:

(1)风险评估因素的确定。在访问控制中的风险评估是对当时环境中的访问请求进行评估,即通过对环境与访问请求各属性的评估量化出风险,如式(1)所示:

$$riskValue=\sum_{i=1}^{n} weigh_i * riskIssue \tag{1}$$

访问请求的目的和评估方法的不同,使得在不同情境下,风险评估因素根据不同的访问请求目的有不同的选择。

(2)权重的计算。构建权重是风险评估中的重要一环。权重决定着风险评估最后的结果,不同比例的权重设定意味着不同的风险评估因素在访问请求过程造成的风险的可能性不同。权重的确定方法通常分为主观定权法和客观定权法。常用的确定权重的方法如表 1 所列。

权重的估计需要与访问控制中的历史访问记录关联。权重估计的结果应当满足在访问过程中对风险评估因素的不确定性的解释。在权重估计的过程中,应当尽量避免受试者和实验者的主观性,用客观的方法进行估计,可以尽可能地采用多种对比方法进行权重估计。

表 1 权重确定方法

Table 1 Weight determination methods

方法分类	具体方法
主观定权法方法	专家评分法[5] Satty 权重法[6]
客观定权法	熵权法[7] 主成分分析法[8]

(3)评估方法的选择。评估方法是基于评估者对于风险因素量化方式的不同来选择的。量化方式可分为 3 种:定性评估、定量评估、基于定性与定量相结合的总和评估方法。3 种方法的比较如表 2 所列。通常情况下,风险评估方法得出的结论是对各个风险因素的判断,通过判断结果优劣对各对象进行排序或分类。但是,通常风险访问控制是通过对访问控制过程中的各风险因素进行量化,分析估计各风险因素的权重,将量化后的值累加加权后得出风险值。所以应将风险评估方法借鉴到基于风险的访问控制中,而不是仅将风险评估方法直接应用于访问控制。

表 2 风险评估方法的比较

Table 2 Comparison of risk assessment methods

	优点	缺点	评估方法
定性评估方法	能够直观反映评估对象蕴含的深层含义,使评估结果更加全面,更深刻	主观性很强,对评估者本身的要求很高	推导演绎理论分析、逻辑分析法、德尔菲法、因素分析法、历史比较法、风险综合评价法
定量评估方法	用直观的数据表示结果,使研究结果更加严密、科学、深刻	使本来复杂的事务简单化、模糊化,但可能因为量化而曲解风险因素	熵权系数法、风险图法、决策树法、因子分析法、时序模型、回归模型、聚类分析法、模糊综合评价法、效用函数
综合评估方法	通过定性与定量评估相结合的方式,计算得出评估结果,适用范围广	具有一定的局限性	层次分析法、障碍树法、风险矩阵分析法、数据包络分析

3 研究现状分析

拥有二元访问控制策略的访问控制系统无法实时满足组织的要求,这种系统的不灵活性成为处理关键组织中的实时信息共享的重要阻碍。因此需要对实时的情况(即主体在缺少适当权限的情况下)以及可能的风险进行评估,来授予主体访问权限。JASON 项目组最早提出基于风险访问控制系统(Risk-based Access Control system,RAC)以解决问题[9]。其提出在新系统中关注风险,并概述了有关风险评估的 3 个基本原则。

(1)量化风险,当风险因素无法直接测量时,通常可以合理地估计,然后使用随后的专家经验或学习的知识经验来获得更好的估算。

(2)建立一个可接受的风险等级,在访问控制中,可以忍受秘密 X 信息和绝密 Y 信息的泄露。如果可以将 X,Y 的资源等级全部设置为零,则所有的操作将会停止,因为操作的不规范或者恶意操作会带来风险。故访问资源时,资源可接受的风险访问是什么?这将是一个急需解决的问题。

(3)确保将信息一直分发到可接受的风险等级。系统管理者在访问时一直试图将风险降至最低。但是实际上,在大数据信息共享的环境中,我们希望确保将可接受风险等级增加到可容忍的最大值,而不是将风险降至最低。

在传统访问控制的风险评估中,风险判断的依据通常很单一,例如在模糊 MLS 模型[10]中,风险判断的依据是对主体和对象成员资格进行评估。但随着互联网及分布式系统的发展以及大数据、云计算等技术的出现,传统的访问控制模型并不能应对复杂多元的访问请求,因此出现更细粒度和更加灵活的访问控制模型,例如基于属性的访问控制[11-12](Attribute-Based Access Control,ABAC)。因此,面对不同的访问控制应用场景时,风险评估的方式和评估因素各有不同。

3.1 传统访问控制中的风险评估

风险评估是决策过程中行之有效的方法。虽然风险本质上是一种结果的可能性,是不确定的,但模糊逻辑方法允许使用真实度来计算结果。学者通过引入模糊逻辑方法来处理风险评估的不确定性和不精确性,从而在访问控制中作出决策。模糊方法的基本思想是运用模糊集合理论解决实际问题,而模糊集合是用隶属度表达的,其隶属度在连续实区间[0,1]中,而不是在集合{0,1}中[13]。Lelliott 首次尝试建立基于模

糊逻辑的计算机风险分析模型——模糊 MLS 模型(Fuzzy Multi-Level Security model)[14]。模糊 MLS 模型是在 BLP[15]模型上发展的风险自适应访问控制模型。Bell 等首次在模型中建立一个可行的风险等级如图 1 所示。该模型将风险定义为未经授权的披露而导致的预期损失价值的可能性,价值被定义为由于未经授权的方式披露此信息而造成的损害。确定未经授权披露的可能性需要预测未来用户的行为,导致在进行风险量化时,不可能进行精确的确定。因此,主体在访问一个类别中的对象时,对于类别,主体在隶属区间[0,1]中被赋予模糊成员资格,表示主体需要该类别中的信息;对象也被赋予模糊成员资格,表示该对象与类别的相关性,并且使用基于主体安全标签和对象安全标签之间的差异的 Sigmoid 函数来量化访问请求的风险。将模糊逻辑应用在此模型中可以明确地表达标签分配中的不确定性。

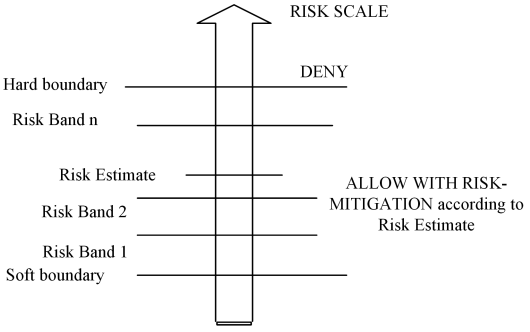


图 1 QRRAC 的风险等级

Fig. 1 QRAAC on a risk scale

Ni 等[16]进一步将模糊推理应用到风险评估中。由于风险评估通常依赖于相关风险因素的不完整和不精确的信息与知识,因此专家根据一些高水平经验或历史知识提出有效的规则。这些有效的规则会自然地转化为模糊推理系统中的规则库。而出现在主观知识中的一些模糊概念可以通过模糊推理系统中主观定义的隶属函数自然地描述。该评估过程通过代数运算聚合不同风险因子的隶属度,以生成先行词的隶属度,这种隶属度被作为风险因子的成员的置信度,以及规则的隶属程度。这些操作通常足以描述最佳实践的规则和建议。

Lazzerini 等[17]认为确定风险因素与风险之间的关系是风险分析和管理(Risk Analysis and Management)面临的挑战之一。但是,大多数使用模糊逻辑的风险评估方法都不具有足够的代表性,Lazzerini 因此提出扩展模糊认知图(Extended Fuzzy Cognitive Maps)法来描述风险因素与低性能、时间延迟、低质量和高成本风险之间的关系。E-FCMs 有两种类型的元素:概念和因果关系。其中,用模糊集合表示语言的概念,因果关系是概念之间的关系,因此关系可以是正面的(用"+"表示),也可以是负面的(用"-"表示)。

Li 等[18]提出一种基于模糊建模的方法,应用于医疗保健的访问控制中。该方法定义 3 个输入(数据敏感性、动作严重性和风险历史),使用模糊集进行建模,并用于计算与云环境中医疗信息访问相关的风险级别。基于公共健康领域的模糊系统如图 2 所示。其中,圆内表示系统的输入(概念),两个概念之间的线表示因果关系,而因果关系用模糊逻辑术语表达。

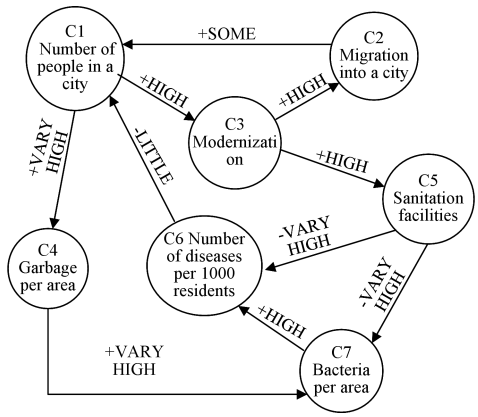


图 2 公共健康领域的 EFCM

Fig. 2 EFCM of public health domain

在 21 世纪初,随着计算技术的普遍应用和移动服务的部署,应用程序需要更加灵活的访问控制机制。由于这些应用程序的访问控制决策取决于用户所需凭据与系统上下文和状态的组合,因此扩展的传统访问控制模型是基于上下文的访问控制,是一种自适应解决方法,相比传统访问控制管理更加灵活。其灵活性在于两个方面:

(1)当用户的上下文发生变化时,用户的权限发生变化;

(2)当系统的资源信息(例如网络宽带、CPU 使用率、内存使用量)发生变化时,其访问权限会发生变化。

Moyer 等[19]最早提出将对象与环境两个新的概念引入基于角色的访问控制(Generalized Role-Based Access Control),这种访问控制模型是以上下文信息作为访问控制决策的因素,捕获系统中所有与安全相关的状态。Zhang 等[20]则是在基于动态角色的访问控制模型中使用了上下文参数。该模型根据上下文信息动态调整角色分配和权限分配。虽然基于上下文的访问控制是一种新兴的自适应解决方法,但是没有考虑制定决策过程中的安全方面以及安全问题对系统的影响,因此在基于上下文访问控制中将风险引入访问控制中建立一个普适环境风险评估模型,以解决普适环境中安全问题。Diep 等[21]提出一种基于风险评估和上下文的访问控制管理方法。当访问请求被提交给访问控制管理器时,访问请求管理器查找由此操作而可能发生的相关结果,并在发送必要的参数后查询风险评估模块以计算风险值。风险评估模块再根据原则、环境和资源的背景计算可用性、机密性和完整性方面的成果,评估行动后的价值。最后根据风险评估模块的风险值,在访问控制管理器中将风险值与风险阈值相比较得出结果,由访问控制管理器返回决策。该访问框架如图 3 所示。

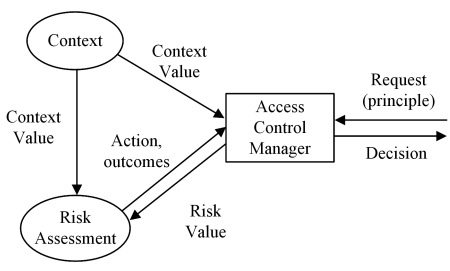


图 3 访问控制框架

Fig. 3 Access control framework

由于动态环境中共享信息日益增加，因此将风险感知扩展到基于角色的访问控制已成为新的方向。开发风险感知访问控制的核心目标是提供一种机制，可以在无法访问资源且能产生深远后果的情况下，将管理访问允许作为授权访问风险与拒绝访问成本之间的控制点。当用户请求访问某些资源时，风险感知访问控制机制将通过估计授予权限的预期成本和收益来评估：如果风险超过某个系统定义的阈值，则可能拒绝要求；如果超过预期收益，则拒绝该请求。

Chen 等[22] 较早地开发了风险感知 RBAC 模型(R2BAC)。R2BAC 使用有向图 G 计算访问控制中的风险，通过两种方式确定 au(用户-角色)路径的风险将不同的风险组合成适当的风险值：1)定义与路径相关的风险，路径的风险由集合中的最小值确定，路径中的风险由用户(u)的可信度、u 执行 r 的能力以及权限(p)适当性决定；2)计算存在且与路径的每部分相关联的风险并累加存在的风险值。其过程如图 4 所示。

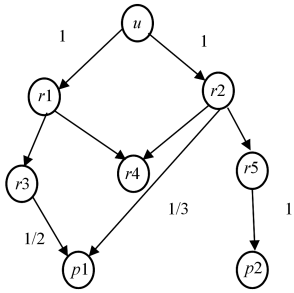


图 4 R2BAC 的风险计算

Fig. 4 R2BAC risk calculation

存在从 u 到 $p1$ 的两个 au 路径，即 $u\rightarrow r1\rightarrow r3\rightarrow p1$ 和 $u\rightarrow r2\rightarrow p1$。如果使用第一种方法来计算这两个 au 路径的风险，则风险(u，$r1$，$r3$，$p1$)=1−1/2=1/2，风险(u，$r2$，$p1$)=1−1/3=2/3。因此，授予执行 $p1$ 的风险由与 au-path：$u\rightarrow r1\rightarrow r3\rightarrow p1$ 相关的风险决定，即风险(u，$p1$)=1/2。如果使用第二种方法计算两个 au-path 的风险，那么风险(u，$r1$，$r3$，$p1$)=1，风险(u，$r2$，$p1$)=2/3。因此，授予(u，$p1$)的风险为 2/3，这由与 au-path：$u\rightarrow r2\rightarrow p1$ 相关的风险决定。

3.2 基于 XACML 框架的风险访问控制

随着云计算、物联网等新型计算环境的出现，新型计算环境具有的特点给访问控制计算的应用带来了巨大的挑战。在云中应用访问控制的主要问题是在动态和异构环境中支持大量用户和资源的必要灵活性和可扩展性，以及协作和信息共享的要求。传统访问控制模型无法安全地管理云资源：云服务器无权访问外包数据内容以保护数据的机密性，数据资源本身不再受到所有者的完全控制。传统访问控制并未考虑不确定性和风险，使得 RBAC 很难适应云环境的动态特性。因此，将风险评估扩展到基于 XACML 标准的访问控制模型中，是解决云中动态性的有效方法。

Santos 等[23] 提出一种扩展 XACML 的访问控制模型，将风险引擎、风险量化 WEB 服务和风险策略扩展到模型中，如图 5 所示。

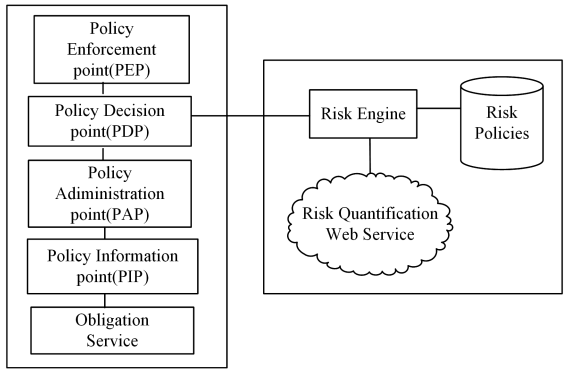


图 5 访问控制组件概述

Fig. 5 Overview of access control components

系统使用风险策略中定义的风险度量和聚合来管理用户对云资源的访问，其中风险策略由资源所有者创建。随着云规模的扩大，云联盟成为关注的重点。为实现云联盟中分组的多个云之间的资源共享，就必须实现云之间的信任，必须使得云之间的用户身份是相互关联的。但是文献[23]中应用的是基于风险的访问控制模型，可以在没有身份联合时允许使用云联盟。因此，将风险扩展到云中访问控制模型中，使风险分析与 XACML 决策相结合能够更快速地匹配访问控制中的访问控制策略。但是其仅指出通过风险决策描述风险度量，并未细化量化风险的过程。

文献[24]描述了云中联合身份管理的挑战，特别是信任协议，这种风险评估方法可实现动态身份联合，但这项工作缺乏参考指标。而在 Santosl 等[25] 提出的方案中，将本体作为度量因子，通过调整每个度量标准的权重来解决访问授权，使用本体和推力器的推理能力，尝试以动态的方式在可用数据中推断并导出丢失的上下文信息(以度量中使用的属性形式)。在云中通过促进对专业社交网络[26](Professional Social Networking)的部署和采用，以促进社交网络中不同组织之间信息、资源和任务的交换。Bouchami 等[27] 将用户级定义的细粒度与组织级的全局风险策略结合，将应用风险度量和访问控制结合，能够帮助企业在外部访问主体不够信任时拒绝访问尝试，将每条风险访问评估的风险级别与给定的阈值相比，以排除风险太大的请求。

因虚拟技术引起的动态环境安全问题在访问控制很少被关注，但是却能够使敌手入侵网络应用程序。所以 Chen 等[28] 提出了一种新型动态访问控制，落脚于虚拟安全，并强调风险度量是一个附加的指标。该模型将环境状态与访问历史操作风险结合，得到一个高效、低消耗的访问控制方法。但是，该模型并不关心如何从虚拟主机得到环境状态，也不关心如何从实体中获得属性。在云平台风险访问控制中，Yang 等[29] 提出一种新型风险访问控制模型(Dynamic Risk Access Control Model for Cloud Platform)，通过事件推演构造动态规则匹配模块，通过优化带约束的线性回归算法动态分配权重，构造风险评估模块，使其对访问请求有较高的灵敏度。而 Kamoun-Abid 等[30] 提出一种分布式与协作的基于风险访问控制决策的防火墙技术，该决策提高了连接用户与公共云平台之间的安全性。

虽然新型系统拥有新的安全问题，例如分布、动态等，但未授权的泄露、拒绝服务和数据篡改仍然是云中至关重要的问题。利用风险量化滥用授权以及滥用授权访问所造成的损害，并利用风险-收益分析得到授权后访问的最大化权益是实现基于属性的访问控制策略的一种可行性方法。为实现特殊授权，Xu 等[31]提出一种模糊扩展 ABAC（fuzzy-extended ABAC）技术，通过模糊机制评估不符合策略的请求和辅助信贷机制，提高紧急授权和特殊授权的灵活性和效率。Krautsevich 等[32]提出在授予或拒绝访问对象时定义属性的值，利用风险收益来分析定义策略接受的属性值。将用户授予的权限与用户可能滥用获得的权限的风险相关联，使得授予或拒绝访问的收益超过可能的风险。但是，文中仅使用风险指定的属性域且该属性域可分为两个子域的策略，并未动态地使用风险来做出访问控制决策。此模型中使用风险的目的是建立属性值和访问决策之间的映射。Metoui 等[33]提出一种基于风险的隐私感知访问控制框架，通过比较隐私风险和请求的可信度来评估每个访问请求。当风险与信任级别相比过大时，该框架可以应用自适应调整策略来降低风险。

当前信息系统中，大量的异构元素通过非线性交互连接形成不同类型的网络系统。这些系统也会受到外部和内部的漏洞攻击，造成云上的信息遭到破坏，因此基于图的风险评估适应于随时间变化的云环境。文献[32]的方法通常通过基于图的模型构成在目标系统中识别的基本漏洞及其关系。

文献[35-36]将攻击图用于评估与系统漏洞相关的风险。但 Yassine[34]将风险评估图作为风险分析模型，引入支持风险，将节点风险和全局风险作为风险评估的判断依据，将图中路径的不良状态通过风险累积量化。但是，这种图的应用在云上有两个主要的限制：1）大量的异构元素之间的不同交互关系使攻击图的构建难度增大；2）攻击图中无法动态地定义在拓扑结构中随时间而演变的漏洞。

基于风险的访问控制模型的主要优点之一是能够处理异常访问请求，当用户被动授予执行关键操作的权限时，即使是以前从未被授权这样做，均可以这样处理。这种访问控制模型解决的另一个问题是访问资源的灵活性，通过量化和聚合资源所有者创建的风险策略中定义的风险度量，来管理用户对云资源的访问。基于风险的模型建立在 XACML 上，并允许使用 RBAC 或 ABAC 以及风险分析，可为用户和云服务提供商提供灵活的访问控制。表 3 比较了相关风险访问控制，包含用于估计每个模型中的风险值的风险评估技术、用于估计风险值的风险因素以及每个模型的限制。

表 3 基于风险的访问控制模型

Table 3 Risk-based access control models

相关文献	风险评估方法	风险因素	限制
文献[15]	Fuzzy MLS Model	主体安全标签、客体安全标签	忽略了用户在风险评估过程中过去的行为，缺乏风险自适应性且时间开销高
文献[17]	Fuzzy Inference	主体安全级别、客体安全级别	模糊推理的时间开销高，缺乏自适应的特征
文献[18]	E-FCMs	概念	只关注风险因素与风险之间的关系，没有考虑风险因素本身
文献[19]	Fuzzy Model	数据敏感性、动作严重性、用户历史风险	没有明确定义的风险边界并缺乏自适应特征
文献[21]	Risk Assessment	行动的结果	风险因素单一，没有使用风险预测技术，缺乏自适应性和用户背景
文献[22]	Risk Assessment	原则、环境和资源背景	缺乏自适应性特征
文献[23]	Methematics Functions	风险策略	风险评估因素单一，缺乏自适应性特征
文献[25]	Methematics Functions	访问请求	忽略用户访问请求的历史风险，缺乏自适应性
文献[27]	Methematics Functions	用户、资源、上下文属性	对于权重的设定过于主观且固定
文献[28]	Methematics Functions	访问控制属性组	未使用风险预测技术以及缺乏自适应
文献[29]	Methematics Functions	环境状态、访问历史	仅提出一种计算方法，并未全面考虑访问控制过程
文献[30]	EC;PR	访问活动、主体属性、漏洞评分	未明确访问活动和主体属性的具体计算方法
文献[34]	Methematics Functions	隐私风险、请求可信度	忽略在访问过程中环境因素的影响

3.3 风险访问控制在环境中的应用

基于风险的访问控制是基于每个动态分析请求的控制，不仅要考虑预定义的策略，还要考虑操作风险、用户需求和风险收益等信息。虽然基于风险的访问控制目前仍然处在初始阶段，主要应用于学术或实验环境中，但已有越来越多的基于风险的访问控制应用于现实环境中，例如：医疗卫生系统、物联网系统、门禁系统和入侵防御系统等。

在医疗访问系统中，未授权医生获取其患者的医疗信息有可能导致严重后果。通过实时的风险管理访问控制系统管理医疗系统能够保护患者的隐私。Wang 等通过定义敌手模型，为诚信用户与恶意用户的行为建模，以统计方法进行记录，用信息论中的熵有效地计算不同访问请求的风险分数，并

为用户设置适当的容忍阈值，控制对患者的隐私保护[35]。在敌手模型中医生是对访问医疗记录相关风险的控制。基于敌手模型定义两类医生：诚实医生打算完成访问任务所需的医疗信息；恶意医生会做诚实医生所做的事情，除非故意访问与任务无关的患者的医疗信息。用户记录越多，聚合的风险越大，请求信息越敏感，在活动中包含的风险就越高。因为恶意医生的医疗记录的标签比所有医生的一般访问模式的标签更加多样化，所以使用熵计算恶意医生访问与给定目的无关记录的概率。但是由于粗粒度的风险量化与建模，造成评估结果与现实有差异，因此，Zhen 等[36]更加细化敌手模型中医生的行为模型，使其更符合现实医生的行为，其采用 EM 算法区分诚实医生与恶意医生在信息访问上的行为的差异，将得出的访问行为的先验分布作为风险量化的基准。随着网络技术的发展，近年来电子卫生服务系统利用云计算技术发展壮大，其形成的云叫做 E-Health Cloud。E-Health Cloud 可以紧密联系各个医疗部门，并在业务中的医疗机构之间进行协调。Sharma 等[37]提出实现云辅助电子卫生保健系统的原型，为确保基于机密性、完整性和可用性要求的访问授权，使用风险的动态访问控制，基于 HL7 的消息传输协议以实现不同的医疗保健系统和应用程序之间的互操作性。该模型由于使用预定义的动作图来确定访问，遵循静态方法，因此可以在基于 XACML 的架构上实现电子健康云系统。同样，在医疗保健领域，保护电子健康记录对于保护患者的隐私尤为重要。Aqeeli 等[38]提出一种隐私保护缓解方法，开发新的风险测量公式，根据信任水平以及此类数据暴露所带来的风险，利用开发的度量公式得到的风险，缓解数据披露算法，控制可能暴露隐私的数据。

现今网络空间活动比以往都要频繁，主要依赖于各种网络与不断变化的合作服务提供商进行动态交互和信息共享。以前旨在保护基础设施的方法改变了威胁对象，以至于针对网络攻击的行为变成网络运维中最大的威胁。Cleveland 等通过使用统计机器学习，使得基于行为的访问控制模型(Behavior-Based Access Control)能够分析追踪目标攻击内部人员的行为以及评估信息的可信度，但并不适应于 XACML 框架[39]。Ben 等提出基于 XACML 决策的风险和角色动态访问控制[40]，其使用风险策略中引入的风险因素的量化来管理用户对云服务的访问。此方案通过 RBAC 模型与 XACML 结构创建，通过计算和更新风险度量以丢弃非授权用户，达到防止针对云网络的入侵。而 P2P 作为一种分布式体系结构模型，对等系统的分散控制和自组织等特性给系统带来一系列的安全风险。文献[41]根据信息系统的任务交互中出现的风险，通过模糊评价确定在交互任务中的主体的脆弱性和目标节点的威胁性，从而确定任务交互中的风险。

协作信息系统(Collaborative Information System)部署在各种环境中。现在越来越多的领域应用这种信息系统来管理敏感信息，使得在环境中的信息成为恶意攻击的目标。对于一个异常检测系统(Anomaly Detection System)，虽然有检测系统内部威胁的安全机制，但是这些机制既没有建模，也不是用于监视用户所在的协作环境。所以 Chen 等[42]介绍了一种无监督的学习框架，根据协作环境的访问日志中记录的信息来检测内部威胁，通过使用正式的统计模型来衡量用户与推断的通信之间的偏差，以预测异常的用户，并使用真实的电子健康记录系统的访问日志信息验证了此模型较先前的模型[43-44]的性能有明显的提高。同样地，由不同通信技术连接在一起提供服务的物联网也存在许多安全挑战，例如物联网系统的动态与异构特性。为增加信息共享和可用性，Atlam 等[45]提出应用于物联网的基于自适应风险的访问控制模型(Adaptive Risk-based Access Control)，通过采用风险因素估计与访问请求相关联的风险值进行访问决策，并且使用专家评审讨论并验证。

4 自适应风险访问控制

早在 2004 年，研究人员就信息共享带来的安全挑战提出基于传统的访问控制的下一代访问控制——风险自适应访问控制(Risk Adaptive Access Control)，其访问过程如图 6 所示。

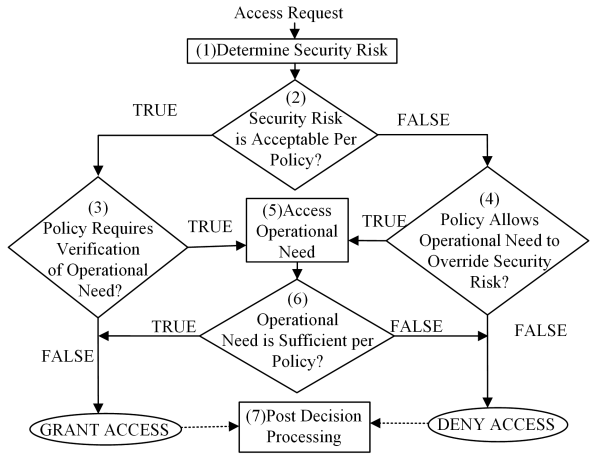


图 6 RAdAC 抽象过程

Fig. 6 RAdAC abstraction process

与传统的访问控制不同，风险自适应访问控制具有灵活性和自适应性，灵活性在于适应实时的访问控制决策[46]。因此，RAdAC 决策基于以下访问因素。

(1)操作需要(Operational Need)：在模型的决策访问中，操作需要在特殊的情况下比安全风险还重要。

(2)安全风险(Security Risk)：安全风险是由用户的可信任度、保护能力、信息技术组件的鲁棒性、环境的威胁等级、访问对象信息值以及访问历史信息相结合的信息值组成，在进行分析时，对以上所有方面均需要加以考虑。

(3)环境因素(Situational Factors)：正在进行访问决策的环境应被考虑进过程中。

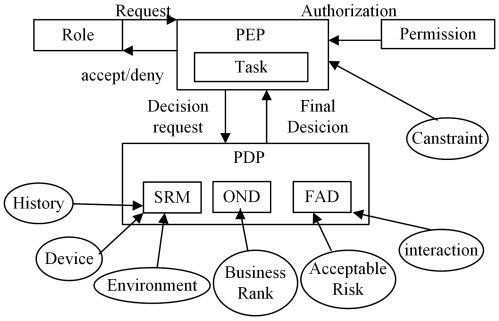
(4)访问控制策略(Access Control Policy)：策略将定义与安全风险因素相关的权重，并能够定义 RAdAC 决策的每一步策略。

(5)启发式(Heuristics)：启发式应该被考虑进每个访问决策中，使策略为其定义级别。而这仅是一种概念性的过程，

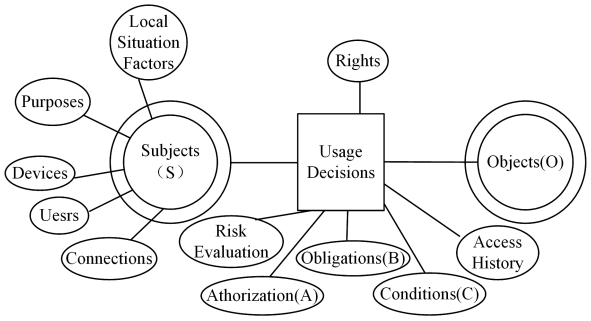
文献[47]通过三角分布使用用户指定的最小值、最大值和最可能值来计算风险量，然后使用蒙特卡洛模拟来增加风险因素测量的不确定性。

传统访问控制受到其策略特点的约束，无法适应于云环境，近年来，传统访问控制与 RAdAC 相结合，提高了访问控制的灵活性与适应性。Huang 等[48]提出一种基于角色的风险自适用访问控制(Role-Based Risk Adaptive Access Control)模型，将传统的 RBAC 与 RAdAC 结合，利用业务流对不同层次进行划分，不同的业务有不同的权值，反映了不同级别的业务流程的不同侧重点，其模型如图 7(a)所示。

另一方面，静态传统授权机制在云中的使用，导致研究者对其是否满足云安全的需求能力产生质疑。就授权机制问题，Fall 等[49]提出一种风险自适应授权机制(Risk Adaptive Authorization Mechanism)，用于简单的云部署、云计算协作和云计算联合，并使用模糊推理系统来证明 RAdAM 的实用性。Kandala 等[50]提出一种基于属性的访问控制来捕获 RAdAC 的特征的新方法，同时将该 RAdAC 模型扩展到 UCON 模型中，其模型如图 7(b)所示。



(a)基于角色的风险自适应访问控制



(b)UCON 模型中的 RAdAC 组件

图 7 RAdAC 在不同模型中的扩展

Fig. 7 Extension of RAdAC in different models

Kandala 提出的新的 RAdAC 范例基于以下概念：授权决策必须包括评估访问风险级别、访问操作需求和访问控制策略，如图 8 所示。RAdAC 引擎使用以下模块的输入来解决授权决策：风险等级模块、操作需求模块和访问控制策略模块。DíazLópez 等[51]在 RAdAC 框架的基础上采用随时间变化的动态策略，以应对每种资源风险等级的变化。为定义适应于特定情况的相对措施，其定义一种基于遗传算法的方法，该方法允许在满足不同要求条件的合理时间范围内找到解决方案。

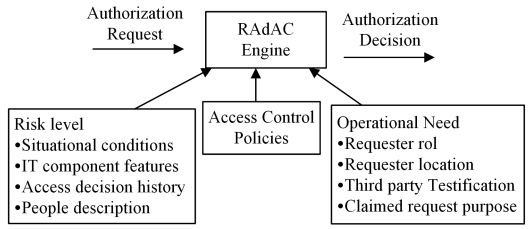


图 8 RAdAC 流程模型

Fig. 8 RAdAC process model

由于动态环境的访问特性，RAdAC 越来越受到关注。将 RAdAC 应用到一些技术与环境中，成为研究者们关注的新焦点。其中，射频识别是一种应用广泛的数据通信技术。以 RFID 访问控制系统的隐私和安全性的研究为基础，AL-Zewairi 等[52]提出了一种用于风险自适应 RFID 门禁系统的混合设计，使访问控制在两种模式之间相互交替(在线(基于服务器)和离线(无服务器))，并根据基于规则的风险情景和当前的风险值来适应风险级别。而在通过各种移动终端连接的生活环境中，访问控制模型需要根据请求时聚合的多个因素确定可适应的访问决策，而不仅是执行预定义的属性之间的比较。由此，文献[53]提出一种新的访问控制模型：社会技术风险适应性访问控制模型(Socio-technical Risk-adaptable Access Control Model)。该模型评估风险与请求的操作需求相平衡，从而提供最准确和安全的访问决策。其通过对医疗保健行业中不同应用场景的模拟，验证了所提模型的可用性。

5 研究展望

综上所述，在云环境的访问控制中，虽然已经出现一些应用于云环境的具有风险访问控制特性的访问控制方法，但是风险访问控制在云环境中的应用仍然具有许多挑战性研究工作。

5.1 风险自适应性

风险自适应访问控制改变了传统的访问控制方式，而未来大数据环境下的风险访问控制的重点在于如何通过处理访问控制过程中的影响因素达到自动识别特殊访问请求与未经授权访问请求。

其一方面要求 RAdAC 包含实时监控，因为风险自适应访问控制中的安全风险可能产生在访问控制决策时，而不是仅像在传统的访问控制过程中对基于主体与客体属性的严格匹配。更多样化地将不同因素结合形成风险评估向量更有利于实时监控访问过程中的风险态势。而设计具有良好表达能力的风险评估策略是今后风险自适应访问控制的研究重点。例如，如何结合各个风险评估因素实时评估访问控制过程中的风险，并且如何将该评估应用到访问控制策略中更具有研究价值。

另一方面，自适应控制的对象具有一定程度的不确定性，使得在访问控制过程中，系统通过在线评估，根据对象的输入与输出数据，不断地学习，使模型在越来越多的学习中获得准确且接近实际的评估结果。在风险访问控制中，启发式算法通常被认为是对访问控制策略和规则的应用，以改进访问控

制策略。应用启发式算法进行访问决策时,通常会考虑算法的输入和输出数据,以及学习过程中参数的调整。在访问请求过程中,要想在学习中得到历史数据的策略模式,就需要将访问请求及其涉及的过程转化成可以输入的数据。对属性集的处理是启发式算法所必须考虑的因素,而属性集中属性值通常会作为算法的输入数据。应用的属性不同,通过不同的方法量化属性,将会得到不一样的风险评估模式。因此,在众多的访问控制属性中,过滤出能够作为风险因素的属性,并且将属性进行量化,使得到的属性值能够作为算法的输入数据是将启发式算法应用到风险访问控制中的首要解决问题。

5.2 模糊风险分析

对于风险的不确定性处理,模糊风险分析也是一种解决方式。早在1965年,Zadeh[54]提出模糊集在处理和转换不确定信息方面起着重要作用,并成功应用于模式识别[55]、图像处理[56]、决策制定和支持[57]等许多领域。虽然,一些研究者将模糊集之间的相似性度量[58-59]应用于风险评估,并且得出一些结论,但针对应用于风险评估的模糊集理论存在以下两方面不足。

(1)在已经提出的模糊风险评估中,通常将失败概率和损失严重程度作为风险度量的因子,使用模糊加权平均法和语言值梯形模糊数的算数计算对每个子分组分量积分,得到总风险。若使用模糊风险评估中上述两种因子,会导致基于云环境的风险访问评估的结果与预期有重大的误差。因此,如何将云中动态、实时的风险评估因素作为模糊集中的评估项,怎样对评估项进行语言值的划分与计算是今后模糊风险研究的方向。

(2)模糊集之间的相似性度量依旧是模糊集理论中的一个重要研究课题,它表明了两个模糊集之间的相似程度。广义梯形模糊数是一个重要的模糊数,可以全面灵活地描述信息。用单一的参数来研究梯形模糊数会造成模糊数之间产生偏差,为有效地处理不精确的信息,需要根据模糊数的形状、位置、面积等参数来研究广义梯形模糊的相似性度量。今后的研究将着眼于对多种参数相结合的广义梯形模糊数的相似程度计算。

5.3 风险阈值与权重的设定

量化风险中研究最多的是对风险值的量化,但是在大多数的风险评估中对风险因素的权重分配通常是固定且主观的,并且风险阈值在计算之后不会再调整。由于大数据环境下访问请求的多样性,使得访问控制模型需要在特定条件下实现访问,允许操作需要在确定访问时超过安全风险。因此,动态调整计算风险阈值与权重成为量化风险值要解决的问题。

结束语 大数据环境的成熟和基础移动设备的普及,使得大数据应用系统的规模与复杂度日益增大,且风险访问控制在大数据环境中仍然面临挑战,因此,相关风险研究将是未来大数据应用场景下访问控制的重要研究方向。文中通过系统地研究国内外风险访问控制的主要工作,分析了近年来的研究成果,提出了一些风险访问控制的研究挑战。

为应对这些挑战,下一步需要系统地研究实现风险评估与访问控制决策融合的新方法和新技术,并完善在大数据下的风险访问控制模型,以满足风险访问控制在大数据中的需求。

参 考 文 献

[1] BIRYUKOV A, CHRISTOPHE D C, WINKLER W E, et al. Discretionary Access Control[M]// Encyclopedia of Cryptography and Security. Springer US, 2011.

[2] SAMARATI P, VIMERCATI S C D. Access Control: Policies, Models, and Mechanisms[C]// International School on Foundations of Security Analysis and Design. Berlin: Springer, 2000: 137-196.

[3] ALTURI V, FERRAIOLO D. Role-Based Access Control [J]. Computer, 1998, 4(3): 554-563.

[4] https://baike.baidu.com/item/%E9%A3%8E%E9%99%A9/2833020?fr=aladdin.

[5] CHEN Y. Application of Fuzzy Analytic Hierarchy Process in Information Security Evaluation of M System[J]. Communication and Information Technology, 2017(3): 45-48.

[6] XU S, TANG Z Q, WANG X. Information Security Risk Assessment Based on D-AHP and Grey Theory[J]. Computer Course, 2019, 45(7): 194-202.

[7] TANG Z Q, HUANG Y J, LIANG J, et al. The grading of information systems based on grey fuzzy comprehensive theory[J]. Journal of Beijing PolytechnicUniversity, 2018, 44(8): 1145-1151.

[8] WANG X R, MA H Z, FENG A R, et al. Network Intrusion Detection Method Based on Information Gain and Principal Component Analysis[J]. Computer Engineering, 2019, 45(6): 175-180.

[9] M. C. Jason Prograrm Office. HORIZONTAL INTEGRATION: Broader Access Models for Realizing Information Dominance [OL]. https://xueshu.baidu.com/usercenter/paper/show? paperid = 39c44011ef24a98c761ce4698c1ff68b&site = xueshu_se.

[10] CHENG P C, ROHATGI P, KESER C, et al. Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control[C]// IEEE Symposium on Security & Privacy. 2007: 222-230.

[11] WANG L, WIJESEKERA D, JAJODIA S. A logic-based framework for attribute based access control[C]// Acm Workshop on Formal Methods in Security Engineering. ACM, 2004: 45-55.

[12] VAANCHIG N, CHEN W, QIN Z. Ciphertext-Policy Attribute-Based Access Control with Effective User Revocation for Cloud Data Sharing System[C]// International Conference on Advanced Cloud & Big Data. IEEE, 2017: 186-193.

[13] JIANG Z J. Fuzzy Mathematics Theory and Method [M]. Beijing: Publishing House of Electronics Industry, 2015: 1-223.

[14] LELLIOTT R. Fuzzy sets, natural language computations, and risk analysis[J]. Fuzzy Sets & Systems, 1988, 27(3): 395-396.

[15] BELL D E, LAPADULA L J. Computer Security Model: Unified

Exposition and Multics Interpretation[OL]. https://www.researchgate.net/publication/238672205_Secure_Computer_Systems_Unified_Exposition_and_Multics_Interpretation

[16] NI Q, BERTINO E, LOBO J. Risk-based access control systems built on fuzzy inferences[C]// Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. 2010.

[17] LAZZERINI B, MKRTCHYAN L. Analyzing Risk Impact Factors Using Extended Fuzzy Cognitive Maps[J]. IEEE Systems Journal, 2011, 5(2): 288-297.

[18] LI J, BAI Y, ZAMAN N. A Fuzzy Modeling Approach for Risk-Based Access Control in eHealth Cloud[C]// IEEE International Conference on Trust. IEEE, 2013: 17-23.

[19] MOYER M J C, AHAMAD M. Generalized role-based access control for securing future applications[C]// In 23rd National Information Systems Security Conference (NISSC 2000). Baltimore, Md, USA, October 2000.

[20] ZHANG G, PARASHAR M. Context-Aware Dynamic Access Control for Pervasive Applications[C]// In Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004). Western Multi Conference (WMC), San Diego, CA, USA, January 2004.

[21] DIEP N N, HUNG L X, ZHUNG Y, et al. Enforcing Access Control Using Risk Assessment[C]// European Conference on Universal Multiservice Networks. IEEE, 2007: 419-424.

[22] CHEN L, CRAMPTON J. Risk-aware role-based access control [C]// International Conference on Security & Trust Management. Springer-Verlag, 2011: 140-156.

[23] SANTOS D R D, WESTPHALL C M, WESTPHALL C B. A dynamic risk-based access control architecture for cloud computing[C]// Network Operations & Management Symposium. IEEE, 2014: 1-9.

[24] ARIAS-CABARCOSP, ALMENAAREZ-MENDOZAF, MARON-LOPEZ A, et al. A Metric-Based Approach to Assess Risk for On Cloud Federated Identity Management[J] J. of Net. And Sys. Man., 20(2012)513-533.

[25] SANTOS D R D, MARINHO R, SCHMITT G R, et al. A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud[J]. Journal of Network and Computer Applications, 2016, 74: 86-97.

[26] ROWLEY, ROBERT D. Professional Social Networking[J]. Current Psychiatry Reports, 2014, 16(12): 522.

[27] BOUCHAMI A, GOETTELMANN E, PERRIN O, et al. Enhancing Access-Control with Risk-Metrics for Collaboration on Social Cloud-Platforms[C]// IEEE Trustcom/bigdatase/ispa. IEEE, 2015: 864-871.

[28] CHEN A, XING H, SHE K, et al. A Dynamic Risk-Based Access Control Model for Cloud Computing[C]// 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom). IEEE, 2016: 579-584.

[29] YANG H Y, NING Y G. A Dynamic Risk Access Control Model for Cloud Platform[J]. Journal of Xidian University, 2018, 45(5): 80-88.

[30] KAMOUN-ABID, FERDAOUS, MEDDEB-MAKHLOUF, et al. Risk-based Decision for a Distributed and Cooperative network policy in Cloud Computing[C]// 14th International Wireless Communications & Mobile Computing Conference (IWCMC). 2018: 1161-1166.

[31] XU Y, GAO W, ZENG Q, et al. A Feasible Fuzzy-Extended Attribute-Based Access Control Technique[J]. Security and Communication Networks, 2018, 2018: 1-11.

[32] KRAUTSEVICH L, LAZOUSKI A, MARTINELLI F, et al. Towards Attribute-Based Access Control Policy Engineering Using Risk[M]// Risk Assessment and Risk-Driven Testing. Springer International Publishing, 2016: 80-90.

[33] METOUI N, BEZZI M, ARMANDO A. Risk-Based Privacy-Aware Access Control for Threat Detection Systems[J]. Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI. 2017: 1-30.

[34] YASSINE N M, PERROT N, KHEIR N, et al. A New Risk Assessment Framework Using Graph Theory for Complex ICT Systems[C]// ACM CCS International Workshop on Managing Insider Security Threats. ACM, 2016: 97-100.

[35] WANG Q, JIN H. Quantified risk-adaptive access control for patient privacy protection in health information systems[C]// Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, 2011: 406-410.

[36] ZHEN H, HAO L I, MIN Z, et al. Risk-adaptive access control model for big data in healthcare[J]. Journal on Communications, 2015, 36(12): 190-199.

[37] SHARMA M, BAI Y, CHUNG S, et al. Using Risk in Access Control for Cloud-Assisted eHealth[C]// IEEE International Conference on High Performance Computing & Communication & IEEE International Conference on Embedded Software & Systems. IEEE, 2012: 1047-1052.

[38] AQEELI S S A, ALRODHAAN M A, TIAN Y, et al. Privacy Preserving Risk Mitigation Approach for Healthcare Domain [J]. E-Health Telecommunication Systems and Networks, 2018, 7(1): 1-42.

[39] CLEVELAND J, MAYHEW M J, ADLER A, et al. Scalable Machine Learning Framework for Behavior-Based Access Control[C]// International Symposium on Resilient Control Systems. IEEE, 2013.

[40] BEN DAOUD W, MEDDEB-MAKHLOUF A, ZARAI F. A Model of Role-Risk Based Intrusion Prevention for Cloud Environment[C]// IEEE International Wireless Communications and Mobile Computing Conference. IEEE, 2018: 530-535.

[41] LIU H, ZHANG L M, CHEN Z G. Task access control model based on fuzzy theory in P2P networks[J]. Transactions of Communications, 2017, 38(2): 44-52.

[42] CHEN Y, MALIN B. Detection of anomalous insiders in collaborative environments via relational analysis of access logs[C]//

Acm Conference on Data & Application Security & Privacy. CODASPY,2011.

[43] LIAO Y,VEMURI V R. Use of K-Nearest Neighbor classifier for intrusion detection[J]. Computers & Security,2002,21(5):439-448.

[44] SHYU M,CHEN S,SARINNAPAKORN K,et al. A novel anomaly detection scheme based on principal component classifier[C]// IEEE Foundations and New Directions of Data Mining Workshop. 2003:172-179.

[45] ATLAM H F,ALENEZI A,HUSSEIN R K,et al. Validation of an Adaptive Risk-based Access Control Model for the Internet of Things[J]. International Journal of Computer Network & Information Security,2018,1(1):26-35.

[46] MCGRAW R. Risk-Adaptable Access Control (radac) [C] // Privilege (Access) Management Workshop. NIST,National Institute of Standards and Technology,Information Technology Laboratory. 2009.

[47] BRITTON D W,BROWN I A. A Security Risk Measurement for the RAdAC Model[D]. Monterey California Naval Postgraduate School,2007:89.

[48] HUANG D H,YANG Y Q. Role-Based Risk Adaptive Access Control Model[J]. Applied Mechanics and Materials,2013,416-417:1516-1521.

[49] FALL D,OKUDA T,KADOBAYASHI Y,et al. Risk Adaptive Authorization Mechanism (RAdAM) for Cloud Computing[J]. Journal of Information Processing,2016,24(2):371-380.

[50] KANDALA S,SANDHU R,BHAMIDIPATI V. An attribute based framework for risk-adaptive access control models[C]// Sixth International Conference on Availability. IEEE Computer Society,2011:236-241.

[51] DÍAZLÓPEZ D,DÓLERATORMO G,GÓMEZMÁRMOL F,et al. Dynamic counter-measures for risk-based access control systems:An evolutive approach[J]. Future Generation Computer Systems,2016,55(C):321-335.

[52] AL-ZEWAIRI M,ALQATAWNA J,ATOUM J. Risk adaptive hybrid RFID access control system[J]. Security and Communication Networks,2015,8(18):3826-3835.

[53] MOURA P,FAZENDEIRO P,MARQUES P,et al. SoTRAACE-Socio-technical risk-adaptable access control model[C]// International Carnahan Conference on Security Technology. IEEE,2017.

[54] ZADEH L. Fuzzy sets[J]. Information and Control,1965,8(3):338-353.

[55] NARANJO R,SANTOS M. A fuzzy decision system for money investment in stock markets based on fuzzy candlesticks pattern-recognition[J]. Expert Systems with Applications,2019,133:34-48.

[56] DHIVYA R,PRAKASH R. Edge Detection of Images Using Improved Fuzzy C-Means and Artificial Neural Network Technique[J]. Journal of Medical Imaging and Health Informatics,2019,9(6):1284-1293.

[57] MENDES W R,ARAUJO F M U,DUTTA R,et al. Fuzzy control system for variable rate irrigation using remote sensing[J]. Expert Systems with Applications,2019,124:13-24.

[58] KANGARI R,RIGGS L. Construction risk assessment by linguistics[J]. IEEE Transactions on Engineering Management,1989,36(2):126-131.

[59] XU Z Y,SHANG S C,QIAN W B,et al. A method for fuzzy risk analysis based on the new similarity of trape zoidal fuzzy numbers[J]. Expert Systems with Applications,2010,37(3):1920-1927.

WANG Jing-yu, born in 1976, Ph. D, professor, is a member of China Computer Federation. His main research interests include cloud computing and information security.

LIU Si-rui, born in 1993, postgraduate. Her main research interests include information security and big data access control.