基于演化博弈的隐私风险自适应访问控制模型

丁红发[1,2]，彭长根[1,3,4]，田有亮[1,3,4]，向淑文[1]

(1. 贵州大学 数学与统计学院公共大数据国家重点实验室，贵阳 550025；2. 贵州财经大学 信息学院，贵阳 550025；3. 贵州大学 计算机科学与技术学院，贵阳 550025；4. 贵州大学 密码学与数据安全研究所，贵阳 550025)

摘 要：社交网络、医疗信息系统等以数据为中心的大规模用户(访问者)开放信息系统，亟需能够保护隐私的细粒度自适应访问控制模型。现有基于理性的访问控制模型难以满足适应性保护隐私的需求，且博弈参与者的完全理性假设太强，不符合实际场景。提出一种面向隐私保护的多参与者理性风险自适应访问控制模型，包含了新的隐私风险量化模块和演化博弈决策模块。首先，基于信息量对访问请求的数据集隐私信息量进行量化，构造了访问请求隐私风险函数和用户隐私风险函数；其次，基于演化博弈在有限理性假设下构建多参与者的访问控制演化博弈模型，利用复制动态方程分析了访问控制参与者的动态策略选择和演化稳定状态形成机理，提出了隐私风险访问控制博弈演化稳定策略的选取方法。仿真实验和对比表明，所提出的访问控制模型能够有效动态自适应地保护敏感信息资源系统中的隐私信息，具有更好的隐私风险适应性，有限理性参与者的动态演化访问策略选取更加符合实际场景。

关键词：风险自适应访问控制；隐私保护；演化博弈；隐私风险量化；信息量

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2006)01-0001-06

A privacy risk adaptive access control model via evolutionary game

DING Hong-fa[1,2], PENG Chang-gen[1,3,4], TIAN You-liang[1,3,4], XIANG Shu-wen[1]

(1. College of Mathematics and Statistics, State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China;

2. College of Information, Guizhou University of Finance and Economics, Guiyang 550025, China;

3. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China;

4. Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China)

Abstract: In the private sensitive date centralized and opening information systems, such as social network and

收稿日期：2005-10-10；**修回日期**：2005-11-10

基金项目：国家自然科学基金项目（U1836205, 61662009, 61772008, 11761020）；贵州省科技计划资助项目（黔科合重大专项字[2018]3001, 黔科合重大专项字[2018]3007, 黔科合重大专项字[2017]3002, 黔科合支撑[2019]2004, 黔科合支撑[2018]2162, 黔科合支撑[2018]215, 黔科合基础[2019]1049）；“十三五”国家密码发展基金(MMJJ20170129)；贵州大学研究生创新基金(研理工 2017068)

Foundation Items: National Natural Science Foundation of China (U1836205, 61662009, 61772008, 11761020); Science and Technology Program Foundation of Guizhou Province(Guizhou-Science-Contract-Major-Program [2018]3001, Guizhou-Science-Contract-Major-Program [2018]3007, Guizhou-Science-Contract-Major-Program [2017]3002, Guizhou-Science-Contract-Support [2019]2004, Guizhou-Science-Contract-Support [2018]2162, Guizhou-Science-Contract-Support [2018]2159, and Guizhou-Science-Contract-Foundation [2019]1049); The 13th Five-Year National Cryptography Development Foundation (MMJJ20170129); The Graduate Innovation Foundation of Guizhou University(Graduate-Science-Engineering 2017068)

*通信作者：彭长根（Email：peng_stud@163.com）

health-care information system, large-scale users access such system, and a fine-grained and self-adaptive access control model for privacy preserving is desperately needed. Existed risk based, rational access control models cannot meet the requirement of adaptable privacy preserving, the participants of are entirely rational, which is too strong to match the real scenarios. To this end, a rational multi-player risk-adaptive based access control model for privacy preserving is proposed. In this model, novel modules of privacy risk estimation and evolutionary game modeling are suggested; firstly, the privacy risk values of access request and requester are formulized by the private information quantity of the requested dataset, and by using Shannon information; secondly, a risk-adaptive based access control evolutionary game model is constructed by using evolutionary game under the supposing of bounded rational players, furthermore, dynamic strategies of participants and formation mechanism of evolutionarily stable states are analyzed by using replicator dynamics equation, and the method of choosing evolutionary stable strategy is proposed. Simulation and comparison results show that, the proposed access control model is effective to dynamically and adaptively preserve privacy in private information system, is more privacy risk adaptive, and dynamic evolutionary access strategies of the bounded rational participants are more suitable for practical scenarios.

Key words: risk-adaptive based access control; privacy preserving; evolutionary game; privacy risk estimation; quantity of information

1 引言

访问控制是信息系统保障数据安全和系统安全的重要和基础性工具[1]。云计算、大数据及物联网的兴起和发展，使得网络和系统更加复杂、开放，数据安全和隐私需求更加多样化，用户和系统的角色、属性更加难以发掘，需要更加动态化、自适应、细粒度的访问控制模型以满足新环境下的安全和隐私需求[2]。

强制访问控制[3]、自主访问控制[4]、基于角色访问控制[5]等访问控制模型的访问策略是静态的、访问控制粒度粗放，且面对大规模用户的开放系统，难以预先指定用户身份，故这些模型难以适用云计算、大数据和物联网中新型的应用场景。基于属性访问控制[6]因其访问控制粒度较细、不需要指定用户身份或角色而受到的广泛的关注，在云计算场景、物联网等得到了广泛的应用，但其需要预先定义访问策略，属性挖掘与属性撤销的计算和实施都比较困难，不能适应动态访问控制需求[7]。为了解决基于属性访问控制等传统访问控制模型存在的诸多问题，风险和信任被先后引入到访问控制中，提出了基于角色或属性的风险访问控制模型[8-10]，一定程度上解决了用户访问的动态控制，并进一步发展为基于风险访问控制[11, 12]，更加适用于大数据环境的访问控制需求。同时，医疗、社交网络、位置信息服务等系统的大量多样性数据集访问有了开放性、动态性和隐私敏感需求，隐私侵犯来自内部和外部访问[13]，迫切需要能对用户隐私信息在访问过程中进行隐私保护。

访问控制模型中存在授权不足或过度授权的现象，引发数据和系统安全、隐私泄露的风险，亟需能够平衡安全隐私与授权度间的解决方案。访问控制可看做访问主体（用户）与访问客体（服务提供者或系统）间的冲突与合作。博弈论[14]作为一种解决参与者对抗与合作，并使得参与者获取最大化利益的数学工具，被自然引入到访问控制以平衡安全和访问效用[15-17]，但现有研究多集中于二人访问控制博弈，要求参与者是完全理性的，难以客观描述访问控制模型中多个用户与系统间的博弈。

本文针对现有访问控制模型难以满足适应性保护隐私的需求，且其访问控制博弈模型难以刻画多用户与系统间的非完全理性对抗与合作问题，基于用户访问隐私风险量化和多人演化博弈，面向开放环境的数据存储隐私保护，提出一种基于演化博弈的多参与者的理性风险访问控制模型，并分析其演化稳定状态和演化稳定策略求解。该访问控制模型在保持风险访问控制优势的同时，并通过用户访问隐私风险约束，限制用户高隐私风险的恶意、好奇访问请求，实现隐私保护，同时仅假设参与者有限理性，用多人非合作博弈对多用户对系统资源访问的策略、收益进行分析，通过演化达到博弈演化稳定状态实现了用户和系统间的均衡及稳定，有效平衡隐私保护和访问效用，更加符合现实场景中用户与系统间的策略动态变化选取特征。具体而言，

本文的贡献如下：

1）面向开放环境的数据存储隐私保护，在有限理性假设下，通过分析多用户场景的敏感数据隐私保护访问控制问题及需求，提出了一种包含隐私风险量化和演化博弈模块的多人隐私风险自适应访问控制模型。减弱了现有理性访问控制模型的参与者完全理性假设，将二人博弈扩展为多人的群体博弈，且能够适应以数据问中心的系统敏感数据隐私保护需求。

2）在“Need-to-Know”的原则下，根据用户访问请求敏感资源的特征，定义了基于信息量化的访问请求隐私风险和用户隐私风险，并给出了自适应的动态隐私风险计算方法。

3）对所提出的多用户隐私保护访问控制模型构建了演化博弈模型，提出了基于隐私风险自适应的效用函数，并利用动态复制方程分析并求解了所提出的访问控制模型的博弈演化均衡策略。

4）利用动力学理论对所提出的该访问控制模型的演化博弈过程进行了仿真，结果表明所提出的多用户隐私风险自适应访问控制模型可在有限理性的演化博弈过程中达到演化稳定状态，能够实现自适应风险的敏感数据隐私保护。

5）与相关基于风险访问控制模型和理性访问控制模型相比，分析表明所提出的访问控制模型在以数据为中心的信息系统隐私保护方面具有更好的优势，风险自适应程度好、访问控制参与者假设更符合实际、能达到较好的隐私保护效果。

本文的结构如下：第 2 节，介绍并分析相关工作；第 3 节，给出风险访问控制及演化博弈的相关概念；第 4 节分析本文所要解决的问题，并构建面向隐私保护的理性风险访问控制模型；第 5 节定义访问请求隐私风险和用户访问隐私风险，并给出计算方法；第 6 节，构建理性风险访问控制的演化博弈模型，并分析其均衡和稳定策略状态；第 7 节，利用动力学原理对所提出的模型有效性进行仿真实验；第 8 节，将所提出的模型与已有工作进行对比，讨论其不同与优势；第 9 节给出结论。

2 相关工作

在风险访问控制[18]的概念提出后，Cheng 等[11]用多层安全的思路量化了风险，将风险划分为不同等级，实现了该模型的一个实例，但该量化方法缺乏数学理论支持；随后，Ni 等[12]用模糊推测理论在 Cheng 等的基础上重新量化风险，使得风险量化满足合取、析取及取反操作需求，用以处置访问访问控制中的紧急访问需求。但文献[11, 12]中风险量化是静态的，因无法应对访问需求多样、无法预先定义安全等级而缺乏适用性，同时不能满足系统的隐私保护需求，也不能对访问主体的高风险访问进行激励约束。

针对文献[11, 12]的风险量化静态、不适应高敏感环境问题，Shaikh 等[19]利用历史访问行为进行风险和信任动态量化，其风险通过威胁概率和数据泄露影响量化，利用指数移动加权平均算法提出了动态风险的访问控制，以保护系统安全。Armando 等[20]参照基于策略访问控制，将访问风险和用户信任进行对比，通过增强用户信任、削减访问安全风险以平衡二者，保护系统资源安全。Diaz-Lopez 等[21]将访问风险量化多层分类，并定义对应的风险控制策略，利用遗传算法为动态访问的访问行为提供安全应对措施，以保护高敏感环境的数据安全。但这些方法在风险量化过程中所依赖的信息过多，在实际环境中不能全部获取，易使风险量化不精确而导致访问控制失败。为此，dos Santos 等[22]提出基于权重的多因子聚合风险量化，并提出一种面向云安全的风险访问控制框架。Ding 等[23]利用马尔科夫模型对主体访问行为的风险进行量化，并提出了基于信用卡额度约束的风险访问控制模型，在云环境数据安全保护中激励低风险访问行为，约束高风险访问行为。但文献[19-23]所提出的方法因风险量化是面向安全的，不适用于隐私保护需求。

为了隐私保护需求，Wang 等[24]针对医疗信息系统，利用信息熵按照“需要知道”的原则，通过对恶意医生和诚实医生间访问信息的不同，对医生访问病患信息的风险进行量化，提出了一种灵活的风险访问控制模型，但该模型预先假定了诚实医生的行为，风险量化缺乏适应性以对应访问需求变化。在文献[24]的基础上，惠榛等[25]利用 EM 二分算法对基于信息熵的医生访问行为进行区分，监测和控制隐私侵犯的高风险访问性。Zhang 等[26]定义了隐蔽非诚实医生行为，基于时间盒和迭代实现了以主题建模为核心的风险自适应访问控制模型。文献[24-26]所提出的方法仅适用于医疗信息系统隐私保护，且并未考虑访问主体与客体间的合作与对抗。针对用户匿名保护需求，Armando 等[27]将风险访问控制与匿名访问结合，同时考量匿名与数据效

用，在匿名系统中抑制高风险访问。

与传统访问控制模型中的参与者博弈[16, 28, 29]类似，基于风险访问控制中的访问主体与客体间也存在二人或多人冲突与合作关系。Helil 等[15]基于二人非合作博弈模型，利用用户信任和访问风险刻画效用函数，分析了风险访问控制模型中的子博弈完美 Nash 均衡，有效的保证了访问控制决策的科学性，其并未考虑多访问主体访问客体间的冲突与合作。

本文针对开放、动态的大规模多样性数据访问隐私保护需求及多用户与系统间的冲突与合作关系，提出一种多参与者的理性隐私风险自适应访问控制模型。相比于已有工作，该模型仅要求参与者有限理性，通过对访问控制过程中的多参与者的行为、策略和隐私效用的博弈要素进行多参与者演化博弈建模，解决了现有文献对风险访问控制参与者行为刻画不足的问题；通过对历史访问行为和资源建模，利用信息论对访问请求和用户的隐私侵犯风险量进行评估，仅用少量先验信息资源，减少了对系统历史访问信息的要求；仅利用隐私风险量化，不再依赖信任机制，简化了模型的设计复杂度；通过多人演化博弈的演化稳定策略状态求解，不但有效约束了高隐私风险的访问请求，激励用户进行低隐私侵犯访问，且实现了动态风险访问控制的优化访问决策，可有效保护系统隐私数据。

3　基础知识

本节介绍风险访问控制模型，信息论与博弈论相关基础知识，为提出面向隐私保护的基于演化博弈风险自适应访问控制模型提供基础。

3.1　基于风险访问控制模型

基于风险访问控制往往包含访问控制管理、风险量化评估和上下文检索三个核心模块[18, 23, 26]，如图 1 所示，其中风险量化评估模块是其关键模块，其负责对访问请求的安全或隐私风险进行量化，以支持访问控制管理模块做出允许访问或者拒绝访问决策。风险的量化取决于当前访问请求及其关联的上下文资源，如历史访问行为，拟访问的信息资源等，通过上下文检索模块实现对上下文资源的关联应用。访问控制管理模块通过对风险值和上下文的处理，做出访问决策。

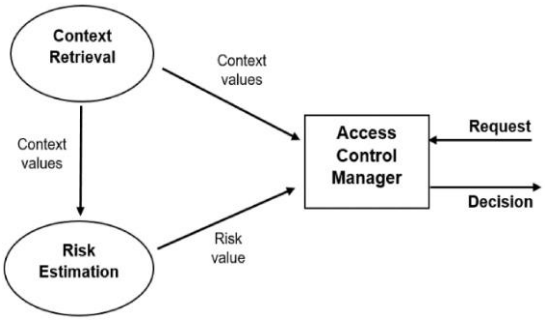

图 1　基于风险访问控制模型示意图

根据风险值计算的对象不同，基于风险访问控制模型可分为面向安全需求[12]和面向隐私保护需求[26]。根据风险的计算方法不同，可分为基于模糊逻辑[12]、基于历史决策的分类训练[22]、基于用户历史行为[24]等。

3.2　自信息与信息熵

信息论[30]是一种量化信息量和不确定度的有效工具，在访问控制中有广泛的应用[23-25]。一般地，有随机变量 $X=(x_1,x_2,\cdots,x_n)$ 及其概率分布 $P(X)=(p(x_1),p(x_2),\cdots,p(x_n))$，则事件 x_i 的香农信息或自信息为

$$I(x_i)=-\log p(x_i) \tag{1}$$

自信息表示了事件所蕴含的信息量，自信息越大，该事件携带的信息量越多，反之越少。香农信息熵是香农信息的平均值，可表示为

$$H(X)=-\sum_{i=1}^{n}p(x_i)\log p(x_i) \tag{2}$$

信息熵表示随机变量的不确定度，熵越大，不确定度越大，反之越小。香农信息熵也被扩展为极大熵、极小熵、正规熵、Renyi 熵等，以适应不同的场景[31]。

3.3　博弈模型与演化博弈

3.3.1　博弈模型

博弈论[14]研究利益存在冲突的多个理性主体在对抗合作过程中的策略选择。经典博弈论中的理性参与者总是选择对自己最有利的策略，并达到均衡。策略博弈模型 $\Gamma=(P,A,u)$ 中包含参与者 $P=\{P_1,P_2,\cdots,P_n\}$、所有参与者行为集合 $A=\{A_1,A_2,\cdots,A_n\}$ 和效用函数 $u=\{u_1,u_2,\cdots,u_n\}$。称 n 个参与者的行为有序集合 $a=(a_1,a_2,\cdots,a_n)$ 为行为组态，其中 $a_i\in A_i$ 是参与者 P_i 在其行为集合 A_i 中的一个策略选择。行为组态 a 可表示为 $a=(a_i,a_{-i})$，其中 a_{-i} 表示除参与者 P_i 之外参与者的策略组合。$u_i(a_i,a_{-i})$ 表示参与者

P_i 在策略组合 (a_i, a_{-i}) 状态下的效用函数。

定义 1 (Nash 均衡) [14]在策略博弈 Γ 中，对任意参与者 $P_i \in P$，其效用函数有

$$u(a_i, a_{-i}) \geq u(a_i^{'}, a_{-i}) \tag{3}$$

其中 $a_i^{'} \in A_i$，则称策略组合 $a = (a_1, a_2, \cdots, a_n)$ 达到 **Nash 均衡**。

策略博弈是一次性博弈，其可进行多次扩展，称为扩展式博弈。博弈可分为合作博弈与非合作博弈，亦可分为完美信息博弈和非完美信息博弈。

3.3.2 *演化博弈*

演化博弈[32]将经典博弈中参与者的理性假设放宽为有限理性，并引入了群体演化。参与者的策略选择在每一次博弈中不一定是最优的，其可在演化过程中模仿其他参与者的高收益策略，调整其后续博弈策略以提高其收益。演化博弈关注所有参与者策略的动态平衡，其核心在于演化稳定策略。

定义 2 演化博弈中，若一个被所有个体采用的策略可成功抵抗所有其他策略的少量个体入侵，则此策略就被称为**演化稳定策略**。形式化地，若策略 s_e 满足

$$E(s_e, s_e) > E(s_i, s_e), \forall i \neq e \tag{4}$$

或

$$\begin{aligned} &E(s_e, s_e) = E(s_i, s_e), \forall i \neq e \\ &E(s_e, s_i) > E(s_i, s_i), \forall i \neq e \end{aligned} \tag{5}$$

则称策略 s_e 为**演化稳定策略**[32]，其中 $E(s_e, s_i)$ 表示当策略 s_e 遇到 s_i 时 s_e 的收益。

4 问题描述与建模

本节首先分析本文所构建的多参与者博弈的风险访问控制模型所要解决的问题，其次提出多参与者隐私风险访问控制模型。

4.1 多参与者隐私风险访问控制问题描述

在医疗信息系统、情报信息系统、外包计算数据池等环境中存在大量包含个人隐私信息数据，访问的用户量大，且用户不断动态更新访问需求，用户的角色、属性、访问策略等信息难以预先定义，用户为完成其职责不断动态变化访问请求，这些信息难以随用户的访问而动态更新。为了保护隐私信息，需对访问请求的数据所包含的隐私量进行量化，现有的风险访问控制模型难以对隐私进行有效描述和精确动态的量化。访问控制模型中，参与者间是长期的多次访问控制交互，在访问过程中往往无法对所有背景知识和他人的信息全部了解，也无法在每次访问时理性地做出最佳的策略选择，但参与者可模仿其他参与者的高收益策略，调整其后续行为策略，但对非完全理性的多参与者间的冲突与合作博弈行为进行描述极为困难，如何设计激励相容的机制使得参与者诚实合作，尽可能不侵犯隐私，且取得高收益，并使参与者短期利益和长期利益一致。非理性参与者的多人扩展式动态博弈是一个复杂的博弈模型，均衡的存在性证明和求解都极为困难，通过多次交互式博弈和参与者自发策略调整可使博弈逐步处于一种相对稳定状态，即用户稳定地请求低隐私风险访问，即使偶有高隐私风险访问，也会后续调整至为低隐私风险访问策略，系统稳定地授权用户低隐私风险访问，即使偶有拒绝授权此类访问，也会后续调整授权策略。

在所提出面向隐私保护的多参与者理性风险访问控制模型中，试图通过以下措施解决上述问题。

（1）定义并量化访问请求的隐私风险。依据“Need to Know”的原则，用户为完整工作职责而访问到信息资源中的敏感信息不应当是隐私侵犯，除此之外的访问应当认为是隐私侵犯。在经认证的用户群体中，用户会优先完成自己的职责，其大多数访问请求都是为了完成自己的职责，则该用户单次访问请求与其历史访问请求产生偏移距离，偏离的越远，其违背“Need to Know”原则越严重，访问的隐私信息资源的隐私量越大，隐私风险越高。

（2）定义并量化用户的隐私风险。将具有相似访问请求行为模式的用户群看作具有相同职责的用户，在历史访问过程中，某一用户的访问偏离该用户群的距离越远，其违背“Need to Know”原则越严重，其用户隐私风险越高；此外，其用户隐私风险直接受其历史访问行为影响，单次的高隐私风险访问将使用户隐私风险提高很过，而单次的低风险访问对用户隐私风险的降低影响较小

（3）构建演化博弈以刻画多用户和系统的非理性多次博弈。不再对参与者进行绝对理性的假设，而将所有用户和系统视为有限理性的参与者。将访问控制系统的所有参与者看作用户群体和信息资源系统群体，两个群体之间进行多次动态的博弈。博弈过程中，群体中的低收益者会模仿高收益

参与者的博弈选择策略，不断进行演化，最终达到稳定的状态，该状态下的参与者策略选择即为演化稳定策略，是参与者的最优策略。

（4）对（3）中博弈模型设计激励相容的机制。在博弈模型中，对用户的激励主要是通过效用函数的设计来实现。本文对用户的效用函数设计，通过隐私风险量化来计算访问请求的隐私风险和用户隐私风险，分别兼顾短期利益和长期利益。效用函数受到这两个变量的影响，使得对用户而言，长期诚实地访问能使其获得更高的收益，短期的恶意访问虽然能有额外的获得，但却远低于长期收益。同时通过惩罚机制，对短期恶意访问的隐私侵犯行为进行惩罚。促使用户能长期诚实地访问系统。同时，在尽可能吸引更多用户访问系统，亦可阻止恶意的隐私侵犯访问请求的利益促使下，使薪资资源系统能够更加精确、动态地做出有效的策略选择，授权诚实的正常访问，拒绝侵犯隐私的恶意访问。

（5）对（3）中的博弈模型求解。利用动态复制方程在动力学原理下，分析所提出风险自适应访问控制演化博弈模型的参与者收益函数和信念函数，进一步分析其演化稳定状态及其机理，提出演化稳定策略的求解公式。在不同的初始状态下，通过博弈的不断演化，访问控制博弈总能达到某个演化稳定状态，该状态下的博弈策略选择即为参与者的最优策略。

4.2　多参与者隐私风险访问控制模型构建

面向隐私保护需求，多用户和信息资源系统间的有限理性参与者隐私风险访问控制模型如图 2 所示，包含访问请求决策管理模块、演化博弈建模模块、隐私风险评估模块、上下文信息模块和风险策略模块。

图 2 中，访问请求决策管理模块接收用户访问请求，根据博弈结果和风险策略模块提供的信息做出授权或不授权等访问决策，并反馈至上下文信息模块；演化博弈建模模块对参与访问控制的用户和系统进行博弈演化，博弈过程中通过隐私风险信息和上下文信息进行动态策略选择，并给出演化策略结果，并将结果反馈给上下文信息模块和访问请求决策管理模块；隐私风险量化模块对访问请求隐私风险和用户隐私风险进行动态量化，支撑演化博弈建模和风险策略更新，并将结果反馈存储至上下文信息模块中；上下文信息模块动态记录并存储用户、信息资源、访问历史、历史隐私风险值、历史博弈策略及收益函数等信息；风险策略池动态更新各用户的隐私风险访问控制策略。

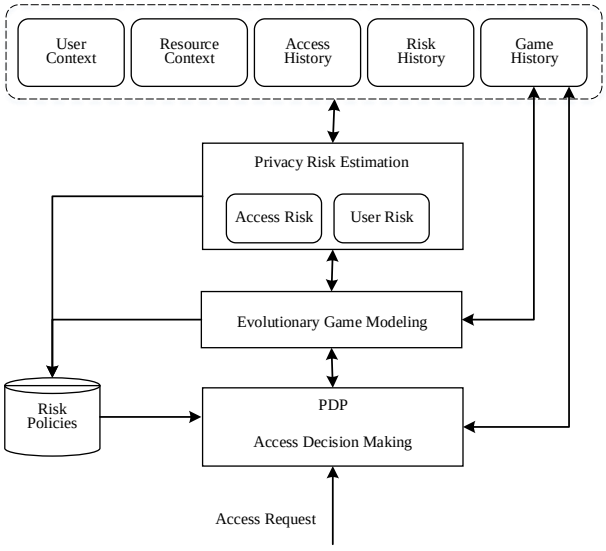

图 2　基于演化博弈的隐私风险访问控制模型

5　隐私风险定义及自适应计算方法

本节针对第 4.1 节所述隐私风险量化问题，分别定义访问请求隐私风险和用户隐私风险，并给出自适应风险计算方法。

5.1　访问请求隐私风险

访问控制系统中，信息资源可以通过自然语言处理或机器学习的方式进行标注化，使得所有信息资源记录或原子集合都包含和系统资源使用功能、目的相关的标签信息，如医疗系统中所有的医疗数据可以根据 ICD-10 标准进行标签化处理，情报系统中所有的情报信息可按照情报属性和功能进行标签化标注。将访问控制过程按照时间划分为不同的时间段 ${{T}_{0}},{{T}_{1}},{{T}_{2}},\cdots$，每个时间段是一小时、一天或一周等。用户 U 在前一个时间段 T 内和当前时间段截止目前向系统发出了 n 次访问请求 $q_{1}^{U},q_{2}^{U},\cdots ,q_{n}^{U}$，对应的访问信息资源集合（实际应用中利用信息资源集合对应的标签集合进行风险计算）为 $R_{1}^{U},R_{2}^{U},$ $\cdots ,R_{n}^{U}$，则 U 访问的信息资源集合为 $R_{{}}^{U}\text{=}\bigcup\nolimits_{i=1}^{n}{R_{i}^{U}}$。当前用户 U 的访问请求为 q_{0}^{U}，该请求对应的系统信息资源集合为

R_{0}^{U}。根据各用户的历史访问信息资源集合的相似性和聚类，可将具有相似访问行为的用户划分为一组，在某一组中，所有的用户具有相同的系统职责，在访问行为上仅有较小的差异。设用户 U 属于用户分类组 g，用户分类组 g 在前一个时间段 T 内和当前时间段截止目前，访问的信息资源集合为$R_{{}}^{g}$。则用户 U 的当前访问请求q_{0}^{U}隐私风险为

$$r(q_0^U)=\begin{cases}1, & \text{if } R_0^U / R^g \neq \varnothing \\ \alpha \dfrac{-\left|R_0^U / R^U\right| \max\limits_{x \in R_0^U / R^U}\{\log p(x)\}}{-\sum\limits_{x \in R^U} \log p(x)}+\beta \dfrac{-\sum\limits_{x \in R_0^U \cap R^U} \log p(x)}{-\sum\limits_{x \in R^U} \log p(x)}, & \text{if } R_0^U / R^g=\varnothing\end{cases} \tag{6}$$

其中$p(x)$表示 x 在$R_{{}}^{g}$中的概率，$1>\alpha >\beta >0$，且$\alpha \text{+}\beta \text{=}1$。

根据用户组 g 中用户的访问请求风险值的历史及分布可利用分位数设置阈值${{t}_{g}}$，若$r(q_{0}^{U})>{{t}_{g}}$，则定义q_{0}^{U}为隐私侵犯访问请求，否则其为非隐私侵犯访问请求。特别注意的是，前述定义是从系统的角度看待某一访问请求，用户 U 会主动选择正常访问或隐私侵犯访问，但系统仅根据访问请求本身来判定，可能将用户的正常访问识别为隐私侵犯访问，亦有可能将用户的隐私侵犯访问识别为非隐私侵犯访问。当将某一访问请求为识别为隐私侵犯访问时，用户可通过风险消除措施降低隐私风险，文献[21]讨论了相关措施。

5.2 用户隐私风险

用户 U 的隐私风险是根据其访问行为特征而发生变化，当用户访问请求隐私风险值高，则用户的隐私风险提高，用户访问请求隐私风险值低，则用户隐私风险降低，且用户隐私风险提高的速率高而降低的速率低。这样的假设与银行对客户的信用风险评估一致，若客户发生一次信用违约，其信用风险提高很快，而需要很多次的信用守约才能将其信用风险降低至原来的值。用户隐私风险仅与其前一隐私风险值和前一次访问请求隐私风险值相关。设用户 U 的初始隐私风险值为r_{0}^{U}，其在当前访问请求q_{0}^{U}之前的隐私风险值为r_{n}^{U}，则当前访问请求q_{0}^{U}发出之后，系统根据其隐私风险值r_{n}^{U}和访问请求q_{0}^{U}的隐私风险值$r(q_{0}^{U})$计算用户 U 的更新隐私风险值

$$r_{n+1}^{U}=\begin{cases}r_n^U+r(q_0^U) & \text{if } q_0^U \text{ is a privacy voilation access;} \\ r_n^U\ 0r(q_0^U) & \text{otherwise.}\end{cases} \tag{7}$$

由于当q_{0}^{U}是隐私侵犯访问请求时，其隐私风险值要大于当q_{0}^{U}是非隐私侵犯访问请求时的隐私风险值，故公式(7)中用户 U 的隐私风险值r_{n+1}^{U}符合增长快，下降慢的特征。

6 所提出访问控制模型的演化博弈模型及均衡分析

本节将访问敏感信息的用户和信息资源系统看作两个有限理性的群体，两个群体中的参与者进行动态演化博弈，通过不断演化达到演化稳定状态，所有博弈参与者都选取到最优博弈策略。定义隐私风险访问控制的演化博弈模型，包含参与者、博弈策略、信念和收益函数，并给出演化稳定策略均衡求解计算方法，进一步分析演化稳定状态及演化稳定策略的特征和机理。

6.1 隐私风险访问控制的演化博弈模型

在有限理性参与者假设下，基于演化博弈可构建面向隐私保护的风险自适应访问控制演化博弈模型。

定义 3 风险自适应访问控制演化博弈模型（Risk-adaptive based access control evolutionary game model），可表示为 4 元组\[RaBACEGM=(P,A,\]\[\Pr ,u)\]。

（1）$P=\{U,S\}$是演化博弈的参与者空间，其中U是用户，S是信息资源系统。

（2）$A=\{{{A}_{U}},{{A}_{S}}\}$是博弈策略空间，其中${{A}_{U}}=$ $\{Normal,Malicious\}$是用户的可选策略集合，包含正常访问和恶意访问两种，${{A}_{S}}=\{Grant,Deny\}$是信息资源系统的可选策略集合，包含授权和拒绝两种。

（3）$\Pr =\{p,q\}$是博弈信念集合，其中\[p=\]$\{{{p}_{Normal}},{{p}_{Malicious}}\}$表示用户分别采取正常访问和恶意访问的概率，且${{p}_{Normal}}\text{+}{{p}_{Malicious}}=1$；$q=\{{{q}_{Grant}},$ ${{q}_{Deny}}\}$表示信息资源系统分别采取授权和拒绝的概率，且${{q}_{Grant}}+{{q}_{Deny}}=1$。

（4）$u=\{{{u}_{U}},{{u}_{S}}\}$是博弈参与者的收益函数集合，其中${{u}_{U}}\text{= }\!\!\{\!\!\text{ }u_{U}^{N,G}\text{,}u_{U}^{N,D},u_{U}^{M,G},u_{U}^{M,D}\text{ }\!\!\}\!\!\text{ }$是用户的收益函数，${{u}_{S}}\text{= }\!\!\{\!\!\text{ }u_{S}^{N,G}\text{,}u_{S}^{N,D},u_{S}^{M,G},u_{S}^{M,D}\text{ }\!\!\}\!\!\text{ }$是信息资源系统的收益函数，二者的值由参与者的访问策略选择所决定。

本文的访问控制系统中，用户 U 和资源信息系统 S 都有两个策略可以选择，在博弈的不同阶段，用户和资源信息系统对策略的选择概率不同，且该概率根据演化博弈的演化学习机制而不断变化，使得访问控制参与者的策略选择形成动态变化的过程。该博弈模型形成的基本博弈树如图 3 所示，表示单次博弈中用户与信息资源系统的博弈策略和收益情况。

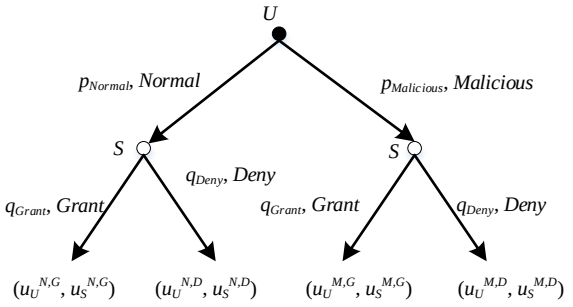

图 3 风险自适应访问控制演化博弈模型的基本博弈树

博弈参与者根据自身和其他参与者的策略选择而获取不同的数值收益，所有参与者的收益矩阵如表 1 所示。

表 1 风险自适应访问控制演化博弈模型的基本收益矩阵

		Information resource system S	
		q_{Grant}, *Grant*	q_{Deny}, *Deny*
User U	p_{Normal}, *Normal*	$u_U^{N,G}$, $u_S^{N,G}$	$u_U^{N,D}$, $u_S^{N,D}$
	$p_{Malicious}$, *Malicious*	$u_U^{M,G}$, $u_S^{M,G}$	$u_U^{M,D}$, $u_S^{M,D}$

表 1 中对演化博弈模型中各参与者的信念、策略和收益进行了形式化描述，特别的，参与者的收益根据访问请求的隐私风险不同而不同。

（1）$u_U^{N,G}>0$ 表示用户采用正常访问策略，被授权访问时的收益。该收益由正常访问获取工作职责完成的信息价值决定，并受到用户的隐私风险影响，用户的隐私风险越低其收益越高，反之越低，可表示为 $u_U^{N,G}=U_{Benefit}^{N,G}(r_{\max}^{U}-r^{U})$，其中 $U_{Benefit}^{N,G}$ 为用户采用正常访问策略被授权访问时的基础性收益，$r_{\max}^{U}$ 为用户的最大隐私风险，r^{U} 为用户的当前隐私风险。

（2）$u_U^{N,D}=0$ 表示用户采用正常访问策略，被拒绝访问时的收益，为 0。

（3）$u_U^{M,G}>0$ 表示用户采用恶意访问策略，进行隐私侵犯访问被授权访问时的收益。该收益由用户正常访问的收益、隐私侵犯访问的额外收益组成，并受用户的隐私风险和当前访问请求的隐私风险影响。收益表示为 $u_U^{M,G}=U_{Benefit}^{N,G}(r_{\max}^{U}-r^{U})+U_{Extra}^{M,G}\cdot(r_{\max}^{U}-r^{U})\cdot r(q^{U})$，其中 $U_{Extra}^{M,G}$ 为用户采用恶意访问策略被授权访问时的基础性额外收益。

（4）$u_U^{M,D}<0$ 表示用户采用恶意访问策略，进行隐私侵犯访问被拒绝访问时的收益。该收益是信

息资源系统对用户的惩罚，并受到用户隐私风险和访问请求隐私风险的影响，风险值越大惩罚越大。该收益表示为 $u_U^{M,D}=U_{Punish}^{M,D}\cdot r^U\cdot r(q^U)$，其中 $U_{Punish}^{M,G}$ 是对用户在采取恶意访问策略时的基础性惩罚。

（5）$u_S^{N,G}>0$ 表示信息资源系统授权用户正常的访问请求时的收益。该收益是用户正常访问时完成工作职责时对系统的正向回馈，并受用户的隐私风险影响，用户隐私风险越低，系统收益越大。该收益可表示为 $u_S^{N,G}=S_{Benefit}^{N,G}(r_{\max}^U-r^U)$，其中 $S_{Benefit}^{N,G}$ 为系统得到的基础性正向回馈。

（6）$u_S^{N,D}<0$ 表示信息资源系统拒绝用户正常的访问请求时的收益。该收益是信息资源系统拒绝用户正常访问，无法完成用户工作职责而对系统造成的损失，用户的隐私风险越低，对系统的损失越大。该收益可表示为 $u_S^{N,D}=S_{Loss}^{N,D}(r_{\max}^U-r^U)$，其中 $S_{Loss}^{N,D}$ 为系统受到的基础性损失。

（7）$u_S^{M,G}<0$ 表示信息资源系统授权用户恶意访问请求时的收益。该收益是被用户恶意访问所损失的隐私信息价值，受用户访问请求的隐私风险和用户隐私风险，风险值越大，信息资源系统的损失越大。该收益可表示为 $u_S^{M,G}=S_{Loss}^{M,G}\cdot r^U\cdot r(q^U)$，其中 $S_{Loss}^{M,G}$ 表示信息资源系统授权用户恶意访问时的基础性损失。

（8）$u_S^{M,D}=0$ 表示信息资源系统拒绝用户的恶意访问时的收益。

基于表 1 可计算用户不同访问策略的期望收益和平均收益为

$$\begin{aligned}
&u_U^{Normal}=q_{Grant}u_U^{N,G}+q_{Deny}u_U^{N,D}\\
&u_U^{Malicious}=q_{Grant}u_U^{M,G}+q_{Deny}u_U^{M,D}\\
&\bar{u}_U=p_{Normal}u_U^{Normal}+p_{Malicious}u_U^{Malicious}
\end{aligned}\tag{8}$$

由于风险访问收益较低者会学习模仿高收益者所选取的策略，针对用户可选策略集合 $A_U=\{Normal,Malicious\}$，选取不同策略的用户比例将随时间而发生变化，用 $p_{Normal}(t)$ 表示选取正常访问策略的用户比例，$p_{Malicious}(t)$ 表示选取正常访问策略的用户比例，满足 $p_{Normal}(t)+p_{Malicious}(t)=1$。对于某一用户访问策略，选取该策略的用户比例是时间的函数，其动态变化速率可用复制动态方程[33]表示。

$$D(p_i)=\frac{dp_i(t)}{dt}=p(u_U^i-\bar{u}_U)\tag{9}$$

其中 $i\in\{Normal,Malicious\}$。

同理，信息资源系统不同策略选择的期望收益和平均收益为

$$\begin{aligned}
&u_S^{Grant}=p_{Normal}u_S^{N,G}+p_{Malicious}u_S^{M,G}\\
&u_S^{Deny}=p_{Normal}u_S^{N,D}+p_{Malicious}u_S^{M,D}\\
&\bar{u}_S=q_{Grant}u_S^{Grant}+q_{Deny}u_S^{Deny}
\end{aligned}\tag{10}$$

对信息资源系统的博弈策略选取亦可建立复制动态方程

$$A(q_j)=\frac{dq_j(t)}{dt}=q(u_S^j-\bar{u}_S)\tag{11}$$

其中 $j\in\{Grant,Deny\}$，且 $q_j(t)$。通过联立式(9)和(11)，令

$$Y=\left[\begin{aligned}&D(p)\\&A(q)\end{aligned}\right]=f(Y,t)=0\tag{12}$$

通过求解(12)，即可得到隐私风险访问模型的演化博弈平衡状态点，从而实现访问控制策略选取的分析和预测。

6.2 隐私风险访问控制博弈演化稳定策略均衡求解

所提出的隐私风险访问控制模型中，用户选取不同的访问行为策略会产生不同的收益，收益低的用户会模仿收益高的用户所选取的访问行为策略。对于相同工作职责的 n 个用户，有两种访问策略{*Normal*, *Malicious*}可选，选取这两种访问策略的用户比例随着时间发生变化，分别为 $p_{Normal}(t)$和 $1\text{-}p_{Normal}(t)$。对于访问策略 *Normal*，选取该策略的

用户人数比例是时间的函数，其动态变化速率可表示为动态复制函数

$$D(p_{Normal})=\frac{dp_{Normal}(t)}{dt}=p_{Normal}(u_U^{Normal}-\bar{u}_U) \tag{13}$$

令 $D(p_{Normal})=0$，将式(8)代入(13)可求解，得 $p_{Normal}=0$，$p_{Normal}=1$ 和 $q_{Grant}=\frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}\text{-}u_U^{M,G}+u_U^{M,D}}$。

类似地，信息资源系统的两种可选行为策略 {*Grant*, *Deny*} 及其策略选取概率 $q_{Grant}(t)$ 和 1-$q_{Grant}(t)$，对于策略 *Grant* 的选取概率时间变化函数，亦可求解得 $q=0$，$q=1$ 和 $p_{Normal}=\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}\text{-}u_S^{M,G}+u_S^{M,D}}$。

将用户与信息资源系统的策略选取复制动态方程相结合，构建隐私风险访问控制演化博弈方程组，对博弈模型进行稳定性分析。求解方程组得 5 个解 $Y_1=\begin{bmatrix}0\\0\end{bmatrix}$，${{Y}_{2}}=\left[\begin{align} & 0 \\ & 1 \\ \end{align} \right]$，${{Y}_{3}}=\left[\begin{align} & 1 \\ & 0 \\ \end{align} \right]$，${{Y}_{4}}=\left[\begin{align} & 1 \\ & 1 \\ \end{align} \right]$ 和 ${{Y}_{5}}=\left[\begin{align} & \frac{u_{S}^{M,D}-u_{S}^{M,G}}{u_{S}^{N,G}-u_{S}^{N,D}\text{-}u_{S}^{M,G}\text{+}u_{S}^{M,D}} \\ & \frac{u_{U}^{M,D}-u_{U}^{M,G}}{u_{U}^{N,G}-u_{U}^{N,D}\text{-}u_{U}^{M,G}\text{+}u_{U}^{M,D}} \\ \end{align} \right]$。其中，$Y_1=\begin{bmatrix}0\\0\end{bmatrix}$ 表示用户选取纯策略恶意访问请求 *Malicious*，信息资源系统选取纯策略拒绝访问 *Deny*；$Y_2=\begin{bmatrix}0\\1\end{bmatrix}$ 表示用户纯策略选取恶意访问请求 *Malicious*，信息资源系统选取纯策略允许访问 *Grant*；$Y_3=\begin{bmatrix}1\\0\end{bmatrix}$ 表示用户纯策略选取正常访问请求 *Normal*，信息资源系统选取纯策略拒绝访问 *Deny*；$Y_4=\begin{bmatrix}1\\1\end{bmatrix}$ 表示用户纯策略选取正常访问请求 *Normal*，信息资源系统选取纯策略允许访问 *Grant*；$Y_5=\begin{bmatrix}\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}\text{-}u_S^{M,G}+u_S^{M,D}}\\ \frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}\text{-}u_U^{M,G}+u_U^{M,D}}\end{bmatrix}$ 表示用户以混合概率组合 $\left(\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}\text{-}u_S^{M,G}+u_S^{M,D}},\ 1\text{-}\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}\text{-}u_S^{M,G}+u_S^{M,D}}\right)$ 选取策略 {*Normal*, *Malicious*}，信息资源系统以混合概率组合 $\left(\frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}\text{-}u_U^{M,G}+u_U^{M,D}},\ 1\text{-}\frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}\text{-}u_U^{M,G}+u_U^{M,D}}\right)$ 选取策略 {*Grant*, *Deny*}。根据演化稳定策略理论可知 Y_1、Y_2、Y_3、Y_4 为鞍点，Y_5 为中心点，故所提出的风险自适应访问控制演化博弈模型存在演化稳定均衡。

6.3 隐私风险访问控制博弈演化稳定策略分析

演化稳定策略是演化博弈模型中能够抵抗侵犯的策略。在所提出的风险自适应访问控制演化博弈模型中，用户和信息资源系统双方各自存在复制动态，以用户为例，对其演化稳定策略进行分析。通过式(13)可知，用户正常访问请求策略选取的复制动态相位有 3 种，当 $q_{Grant}=\frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}\text{-}u_U^{M,G}+u_U^{M,D}}$ 时，对任意的用户正常访问

请求 *Normal* 策略选取概率 p_{Normal}，有 $\frac{dp_{Normal}(t)}{dt}=0$，但是一旦 q_{Grant} 的取值发生偏移，$\frac{dp_{Normal}(t)}{dt}$ 就会剧烈变化，其所代表的状态不具有稳定性；当 $q_{Grant}>\frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}-u_U^{M,G}+u_U^{M,D}}$ 时，$p_{Normal}=1$ 为用户的演化稳定策略；当 $q_{Grant}<\frac{u_U^{M,D}-u_U^{M,G}}{u_U^{N,G}-u_U^{N,D}-u_U^{M,G}+u_U^{M,D}}$ 时，$p_{Normal}=0$ 为用户的演化稳定策略。

同理，信息资源系统授权策略选取的复制动态相位有 3 种，当 $p_{Normal}=\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}-u_S^{M,G}+u_S^{M,D}}$ 时，对任意的授权访问策略选取概率 $q_{Grant}(t)$，有 $\frac{dq_{Grant}(t)}{dt}=0$，该状态不具有稳定性；当 $p_{Normal}>\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}-u_S^{M,G}+u_S^{M,D}}$ 时，$q_{Grant}(t)=1$ 是信息资源系统的演化稳定策略；当 $p_{Normal}<\frac{u_S^{M,D}-u_S^{M,G}}{u_S^{N,G}-u_S^{N,D}-u_S^{M,G}+u_S^{M,D}}$ 时，$q_{Grant}(t)=0$ 是信息资源系统的演化稳定策略。

7　实验仿真与分析

本节对本文提出的隐私风险自适应访问控制模型的演化博弈过程，利用动力学理论进行仿真，分析隐私风险自适应访问控制演化博弈模型的最优访问策略选取问题。

由 6.2 节可知，该访问控制模型的演化博弈稳定状态为 $Y_1=[0,0]'$，$Y_2=[0,1]'$，$Y_3=[1,0]'$ 和 $Y_4=[1,1]'$，下面针对 p_{Normal} 和 q_{Grant} 的不同初始状态，进行实验仿真。通过仿真可以观察出 p_{Normal} 和 q_{Grant} 的演化趋势，得到最终的演化稳定状态，通过演化分析，实现隐私风险访问控制系统中参与者的策略选择预测，从而选取出最优的访问控制策略。本文的仿真实验中，根据 6.1 节中的分析对用户的效用函数设定为 $u_U^{N,G}>u_U^{M,G}>u_U^{N,D}>u_U^{M,D}$，对信息资源系统的效用函数设定为 $u_S^{N,G}>u_S^{M,D}>u_S^{N,D}>u_S^{M,G}$。

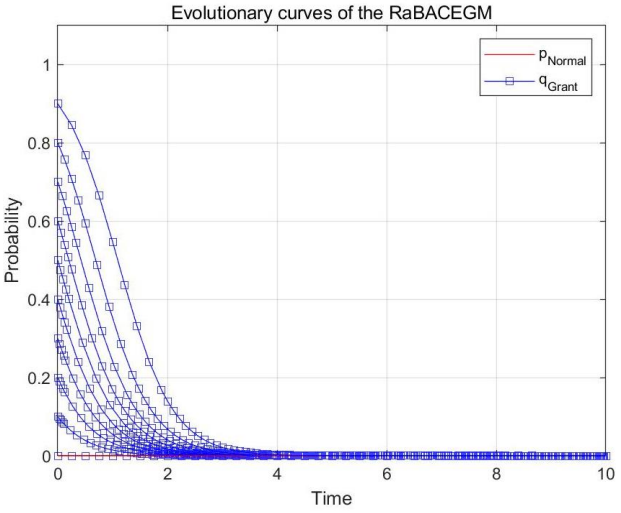

图 4　初始状态为 $p_{Normal}=0$，$q_{Grant}\in[1,0)$时，隐私风险自适应访问控制演化博弈模型的演化曲线，演化稳定状态为 $p_{Normal}=0$，$q_{Grant}=0$

1）当初始状态为 $p_{Normal}=0$，$q_{Grant}\in[0,1)$ 时，用户以概率 1 选取恶意访问 *Normal* 策略，信息资源系统以概率 1 选取拒绝访问 *Deny* 策略或任意其他混合策略选取授权访问 *Grant*、拒绝访问 *Deny* 策略，通过系统仿真，经过演化，用户和信息资源系统双方的策略选取都会演化为 $p_{Normal}=0$，$q_{Grant}=0$ 的概率，即用户以纯策略选取恶意访问 *Malicious*，信息资源系统以纯策略选取拒绝访问 *Deny*。${{p}_{Normal}}$和${{q}_{Grant}}$的具体演化曲线如图 4 所示，在达到演化稳定状态 $Y_1=[0,0]'$ 时，风险自适应访问控制演化博弈模型的博弈参与者两方博弈策略选取最优。

2）当初始状态为 $p_{Normal}=0$，$q_{Grant}=1$ 时，用户以概率 1 选取恶意访问 *Malicious* 策略，信息资源系统以概率 1 选取授权访问 *Grant* 策略，通过演化，该演化博弈模型的博弈双方的策略选取不变，p_{Normal} 和 q_{Grant} 的具体演化曲线如图 5 所示。

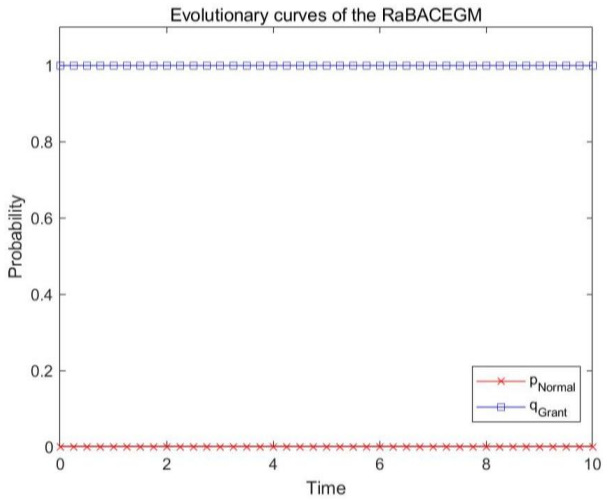

图 5 初始状态为时 p_{Normal}=0，q_{Grant}=1，隐私风险自适应访问控制演化博弈模型的演化曲线，演化稳定状态为 p_{Normal}=0，q_{Grant}=1

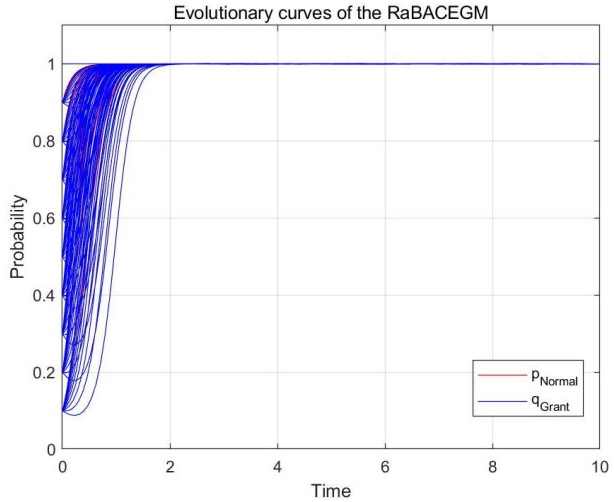

图 6 初始状态为 $p_{Normal}\in(0,1]$，$q_{Grant}\in(0,1]$时，隐私风险自适应访问控制演化博弈模型的演化曲线，演化稳定状态为 p_{Normal}=1，q_{Grant}=1

在图 5 中，尽管该演化过程的最终状态 $Y_2=[0,1]'$ 是所提出的演化博弈模型的演化稳定状态，但在实际应用中，信息资源系统为了遏制恶意访问请求，保护系统中的隐私数据，同时尽可能吸引更多用户访问系统，其不会以纯策略方式选取授权访问 *Grant*，故当用户初始访问策略选取为纯策略恶意访问 *Malicious* 时，会转换为图 4 所示的演化曲线。

3）当初始状态为 $p_{Normal}\in(0,1]$，$q_{Grant}\in(0,1]$ 时，用户以混合策略方式选取正常访问 *Normal*、恶意访问 *Malicious*，或以纯策略方式（概率为 1）选取正常访问 *Normal*，信息资源系统以混合策略方式选取授权访问 *Grant*、拒绝访问 *Deny*，或以纯策略方式（概率为 1）选取拒绝访问 *Deny*，博弈模型通过不断演化，会达到演化稳定状态 $Y_4=[1,1]'$，即用户以纯策略方式选取正常访问 *Normal*，信息资源系统以混合策略方式选取授权访问 *Grant*。该状态下风险自适应访问控制演化博弈模型的博弈策略选择最优，p_{Normal} 和 q_{Grant} 的演化曲线如图 6 所示。

4）当初始状态为 $p_{Normal}\in(0,1]$，q_{Grant}=0 时，用户以混合策略方式选取正常访问 *Normal*、恶意访问 *Malicious*，或以纯策略方式（概率为 1）选取正常访问 *Normal*，信息资源系统以纯策略方式（概率为 1）选取拒绝访问 *Deny*，通过不断演化，会达到演化稳定状态 p_{Normal}=1，q_{Grant}=0，即用户以纯策略方式选取正常访问 *Normal*，信息资源系统以纯策略方式选取拒绝访问 *Deny*。p_{Normal} 和 q_{Grant} 的具体演化曲线如图 7 所示。

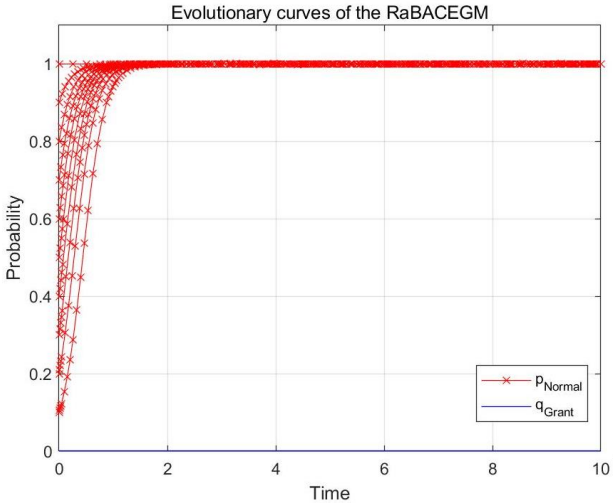

图 7 初始状态为 $p_{Normal}\in(0,1]$，q_{Grant}=0 时，隐私风险自适应访问控制演化博弈模型的演化曲线，演化稳定状态为 p_{Normal}=1，q_{Grant}=0

在图 7 中，最终达到的演化状态是风险自适应访问控制演化博弈模型的演化稳定状态 $Y_3=[1,0]'$。

但在实际应用中，信息资源系统为了吸引更多用户访问系统，其不会以纯策略方式选取拒绝访问*Deny*，会以混合策略的方式选取其博弈策略，其演化过程会转换为图 6 所示的演化曲线。

由以上仿真结果可知，给定不同的策略选取初始状态，经过演化，所提出的风险自适应访问控制模型在演化博弈过程中会达到某个稳定状态。通过观察对比，本演化博弈模型的模拟演化结果与第 6 节中的理论分析保持一致，说明该演化博弈模型与现实系统中的规律相符。因此，本文提出的风险自适应访问控制演化博弈模型具有有效性，可将其应用于面向隐私保护的风险自适应访问控制系统中，为访问控制系统的参与者进行隐私保护访问策略选取提供依据。

8　对比与讨论

在风险访问控制、基于博弈的访问控制和基于演化博弈的信息安全模型方面均有相应的研究，本节针对这些研究工作进行对比，如表 2 所示。

由表 2 可知，相较于文献[12,19,22]，本文所提出的风险访问控制从系统安全保护扩展至数据隐私信息保护，同时在有限理性假设下，应用多人演化博弈对自适应风险访问控制的参与者群体进行了建模和分析；相较于文献[24,26]，本文将隐私保护的应用范围推广至一般以隐私数据为中心的系统中，并利用博弈论对隐私保护的访问策略选择进行了分析；相较于文献[16,29]，本文不关注系统的安全，而关注于系统中的敏感数据隐私保护，通过隐私风险量化对博弈的效用函数进行定义，且放松了对博弈参与者的绝对理性假设，用演化的思想动态分析参与者的访问策略选择；相较于文献[15]，本文的主要目标是隐私保护，将传统访问控制的二人博弈扩展为有限理性下的多人动态博弈，更加适用于访问控制的真实场景，风险量化函数也通过信息量的量化对隐私风险进行描述，并反映到博弈效用函数中；相较于文献[28]，本文不局限于特定场景的隐私保护，其适用于通用的隐私保护场景，并且通过对用户隐私风险和访问请求隐私风险进行动态量化，实现了隐私风险自适应。在多人博弈场景中，对参与者的理性假设放松为有限理性，利用演化的思想对参与者的策略选择进行动态更新，更加符合现实场景中参与者的访问行为变化特征。

表 2　所提出风险自适应访问控制模型的对比

文献	访问控制目的	风险量化	博弈参与者	博弈方法
文献[12]	安全保护	静态安全风险量化	-	-
文献[19]	安全保护	风险和信任动态量化	-	-
文献[22]	云安全保护	多因子聚合风险量化	-	-
文献[24]	医疗信息隐私保护	静态隐私风险量化	-	-
文献[26]	医疗信息隐私保护	动态隐私风险量化		
文献[16]	云安全保护	-	二参与者	重复博弈
文献[29]	蜂窝网络接入安全	-	多参与者	Stackelberg 博弈
文献[15]	数据安全	动态安全风险量化	二参与者	非零和合作博弈
文献[28]	社交网络隐私保护	静态隐私风险量化	多参与者	多方控制博弈
本文	敏感数据隐私保护	隐私风险自适应量化	多参与者	演化博弈

9　结论

隐私保护是以数据为中心的开放系统的核心问题之一，设计有效的细粒度自适应访问控制模型能够保护系统中的隐私数据不被恶意、好奇的访问行为侵犯隐私。本文面向隐私保护，在有限理性假设下，提出了一种基于演化博弈的隐私风险自适应访问控制模型，该模型利用隐私信息量化的方法对访问请求隐私风险和用户隐私风险进行量化，在此基础上构建了两方群体的演化博弈模型，群体中博弈参与者不断学习模仿高收益的参与者博弈策略，最终达到演化稳定状态。通过复制动态方程分析了所提出的风险自适应访问控制演化博弈模型中参与者的策略选择变化过程和演化稳定状态形成机理，提出了演化稳定策略的求解公式。通过仿真实验，对所提出自适应隐私风险访问控制模型的有效

性进行了验证，该模型能有效应用于隐私保护的访问控制；通过与相关文献对比，该模型提出了新的隐私风险自适应量化方法，减少了对系统历史信息的要求，具有更好的隐私风险动态适应性，并将自适应隐私风险量化结果用以设计演化博弈的效用函数；提出了有限理性多参与者的风险访问控制演化博弈模型，该模型中参与者的博弈策略选择动态更新，更加适用于真实场景。

参考文献：

[1] Sandhu R S, Samarati P. Access control: principle and practice[J]. IEEE Communications Magazine, 1994, 32 (9): 40-48.

[2] HAO L, MIN Z, DENG-GUO F, et al. Research on access control of big data[J]. Chinese Journal of Computers, 2017, 40 (1): 72-91.

[3] McCune J M, Jaeger T, Berger S, et al. Shamon: A system for distributed mandatory access control[C]//2006 22nd Annual Computer Security Applications Conference (ACSAC'06). [S.l.: s.n.], 2006: 23-32.

[4] Downs D D, Rub J R, Kung K C, et al. Issues in discretionary access control[C]//1985 IEEE Symposium on Security and Privacy. [S.l.: s.n.], 1985: 208-208.

[5] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29 (2): 38-47.

[6] WANG G, LIU Q, WU J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[C]//Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010. [S.l.: s.n.], 2010: 735-737.

[7] SERVOS D, OSBORN S L. Current research and open problems in attribute-based access control[J]. ACM Computing Surveys (CSUR), 2017, 49 (4): 65:1-65:45.

[8] DIMMOCK N, BELOKOSZTOLSZKI A, EYERS D, et al. Using trust and risk in role-based access control policies[C]//SACMAT '04: Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies. New York, NY, USA: ACM, 2004: 156-162.

[9] KANDALA S, SANDHU R, BHAMIDIPATI V. An attribute based framework for risk-adaptive access control models[C]//2011 Sixth International Conference on Availability, Reliability and Security. [S.l.: s.n.], 2011: 236-241.

[10] KRAUTSEVICH L, LAZOUSKI A, MARTINELLI F, et al. Towards attribute-based access control policy engineering using risk[C]//BAUER T, GROSSMANN J, SEEHUSEN F, et al. Risk Assessment and Risk-Driven Testing. Cham: Springer International Publishing, 2014: 80-90.

[11] CHENG P C, ROHATGI P, KESER C, et al. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control[C]//2007 IEEE Symposium on Security and Privacy (SP '07). [S.l.: s.n.], 2007: 222-230.

[12] NI Q, BERTINO E, LOBO J. Risk-based access control systems built on fuzzy inferences[C]//ASIACCS '10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM, 2010: 250-260.

[13] BOULARES S, ADI K, LOGRIPPO L. Insider threat likelihood assessment for access control systems: Quantitative approach[C]//CUPPENS F, WANG L, CUPPENS-BOULAHIA N, et al. Foundations and Practice of Security. Cham: Springer International Publishing, 2017: 135-142.

[14] OWEN G. Game theory[M]. 3rd edition ed. San Diego: Academic Press, 2001.

[15] HELIL N, HALIK A, RAHMAN K. Non-zero-sum cooperative access control game model with user trust and permission risk[J]. Applied Mathematics and Computation, 2017, 307: 299 - 310.

[16] GAO L, YAN Z, YANG L T. Game theoretical analysis on acceptance of a cloud data access control system based on reputation[J]. IEEE Transactions on Cloud Computing, 2018: 1-1.

[17] WANG Y, TIAN L, CHEN Z. Game analysis of access control based on user behavior trust[J]. Information, 2019, 10 (4).

[18] MCGRAW R. Risk-adaptable access control (RAdAC)[R]. [S.l.]: NIST Privilege (Access) Management Workshop, 2009.

[19] SHAIKH R A, ADI K, LOGRIPPO L. Dynamic risk-based decision methods for access control systems[J]. Computer Security, 2012, 31 (4): 447-464.

[20] ARMANDO A, BEZZI M, CERBO F, et al. Balancing trust and risk in access control[C]//Proceedings of the Confederated International Conferences on On the Move to Meaningful Internet Systems: OTM 2015 Conferences - Volume 9415. Berlin, Heidelberg: Springer-Verlag, 2015: 660-676.

[21] DIAZ-LOPEZ D, DOLERA-TORMO G, GOMEZ-MARMOL F, et al. Dynamic counter-measures for risk-based access control systems[J]. Future Generation Computer Systems, 2016, 55 (C): 321-335.

[22] DOS SANTOS D R, 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 (C): 86-97.

[23] DING H, PENG C, TIAN Y, et al. A risk adaptive access control model based on markov for big data in the cloud[J]. International Journal of High Performance Computing and Networking, 2019, 13 (4): 464-475.

[24] WANG Q, JIN H. Quantified risk-adaptive access control for patient privacy protection in health information systems[C]//ASIACCS '11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM, 2011: 406-410.

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

[26] ZHANG W, LI H, ZHANG M, et al. Privacy-aware risk-adaptive access control in health information systems using topic models[C]//SACMAT '18: Proceedings of the 23Nd ACM on Symposium on Access Control Models and Technologies. New York, NY, USA: ACM, 2018: 61-67.

[27] ARMANDO A, BEZZI M, METOUI N, et al. Risk-based privacy-aware information disclosure[J]. International Journal of Secure Software Engineering, 2015, 6 (2): 70-89.

[28] HU H, AHN G J, ZHAO Z, et al. Game theoretic analysis of multiparty access control in online social networks[C]//SACMAT '14: Proceedings of the 19th ACM Symposium on Access Control Models and Technologies. New York, NY, USA: ACM, 2014: 93-102.

[29] LIU C, XING S, SHEN L. Dynamic hybrid-access control in multi-user and multi-femtocell networks via stackelberg game competition[J]. IET Communications, 2016, 10 (7): 862-872.

[30] SHANNON C E. A mathematical theory of communication[J]. Bell System Technical Journal, 1948, 27: 379-423.

[31] CSISZáR I, SHIELDS P C. Information theory and statistics: A tutorial[J]. Communications and Information Theory, 2004, 1 (4): 417-528.

[32] NEWTON J. Evolutionary game theory: A renaissance[J]. Games, 2018, 9 (2): 31.

[33] 王元卓, 于建业, 邱雯, 等. 网络群体行为的演化博弈模型与分析方法[J]. 计算机学报, 2015, 38 (2): 282-300.

作者简介：

丁红发（1988-），男，河南南阳人，博士生，讲师，主要研究方向为数据安全、隐私保护。

彭长根（通信作者，1963-），男，贵州锦屏人，博士，贵州大学教授、博士生导师，主要研究方向为密码学、数据安全、隐私保护等。

田有亮（1982-），男，贵州盘县人，博士，贵州大学教授、博士生导师，主要研究方向为委托计算、区块链、隐私保护等。

向淑文（1965-），男，湖南溆浦人，博士，贵州大学教授、博士生导师，主要研究方向为博弈论、优化算法等。