论文编号：2015010008

貴州大學

2019届博士学位论文

理性隐私保护模型及应用

学科专业：应用数学

研究方向：密码学与数据安全

中国·贵州·贵阳

2019年 10月

目　录

摘　　要

TBC

关键词： 隐私保护，博弈论，隐私量化，隐私推测，基于风险访问控制

Abstract

TBC

Keywords: Privacy preserving, Game Theory, Privacy quantification, Privacy inference, Risk adaptable based access control

第一章　绪论

1.1　研究背景及意义

互联网、移动互联网和物联网快速发展，以及5G技术的不断推进和商用推广，社交网络、位置服务、医疗健康、生物基因、工业控制等海量数据被主动或被动采集、传输、存储、流转、分析并应用。海量数据的产生和应用推动了云计算、大数据和边缘计算等新兴产业和技术的爆发式增长，并产生了智慧医疗、智慧交通、智慧政府、智慧城市等不同的应用，极大地丰富了人们的物质和精神生活。同样，数据海量化增长、网络跨域泛在、计算云端化、应用多样复杂化等新的变化为安全和隐私带来了巨大挑战，大量的病毒、漏洞、攻击和数据关联分析，致使隐私严重泄漏，引发了人们极大的担忧。表1.1展示了近年来主要的隐私泄露事件，充分表明了隐私泄露已经成为网络空间的重要威胁。在此背景下，深入的理解隐私并保护隐私变得尤为重要。

表 1.1: 近年来主要隐私泄露事件简况

时间	事件	影响	原因
2017年7月	韩国加密货币交易所客户数据泄露	3万个人用户数据被盗并遭受电话诈骗	黑客入侵攻击
2017年10月	全球11个国家41个凯悦酒店数据泄露	数据量不详，涵盖信用卡姓名、卡号、到期日期、验证码等	通过恶意软件进行黑客入侵
2017年10月	马来西亚超过总人口的手机用户信息泄露	4620万人用户地址、身份证号、手机识别卡信息泄露	不详
2017年10月	埃森哲服务器大量敏感信息泄露	19亿敏感的密码和解密密钥泄露	操作失误将数据放到未保护的云服务上
2017年10月	南非史上最大规模数据泄露	3160万人个人资料被公之于众	数据在未保护的服务器上导致黑客窃取
2018年3月	Facebook用户数据泄露	5千万用户数据泄露，影响美国大选	越权采集并分析用户喜好、性格、行为特点、政治倾向
2018年8月	华住集团数据泄露	5亿条、140G华住旗下酒店的用户数据泄露	不详
2018年8月	谷歌采集设备、地图、搜索位置信息	全球超20亿用户数据被越权采集	谷歌公司故意采集

由于90%以上的数据被提供公共服务的政府、社会组织和企业所采集、存储，为了使数据发挥更大的价值，往往需要对包含大量隐私信息的数据进行共享、开放、交

换和分析处理；同时很多信息服务也是基于个人隐私信息与服务质量的交换，如网站注册服务、公共WIFI接入、云存储、智能手机导航、信息搜索与广告推送、在线信用卡支付、RFID应用等。这些场景中由于法律法规要求和个人意愿，需要对隐私信息进行保护，同时服务提供方、数据利用方或恶意第三方希望获取更多的隐私敏感信息，以提供更好的服务、获取更大数据价值，得到更好的数据效用，两个目标同时存在且相互冲突，需要均衡解决。

关于隐私的研究，自2006年 k 匿名模型[1]被提出以后逐步变成系统化的研究，隐私研究发展为基于密码学的方案[2-3]和基于非密码学的方案[1,4-7]两大类，这些方案被大规模应用于以数据为中心的开放、复杂、跨域场景中，如云存储、社交网络、基于位置服务、物联网、边缘计算、数据挖掘、机器学习、医疗健康等。众多应用场景中，隐私保护目标和数据利用目标天然矛盾，如何平衡二者的关系是核心问题之一。在这两类隐私研究中，基于密码学的方案通常利用可证明安全理论定义密码学意义上的隐私保护目标，设计对应的密码学方案，如同态加密、可搜索加密、属性密码方案等实现隐私保护目标[2-3]；基于非密码学的方案主要是定义了匿名性设计达到匿名化效果的算法来实现用户的身份匿名隐私保护[1,4-5]，通过定义邻近数据集的查询结果不可区分性，设计加噪的方法达到这种不可区分性来实现属性值的隐私保护[6]，通过定义数据动态隐私，设计自适应的风险的细粒度访问控制实现隐私数据不被非授权用户访问[7]。其中，基于密码学的方案具有严格的理论方法支撑，能够达到预期的隐私保护目标，但是这些隐私定义是密码学意义上安全性定义，隐私保护方案设计也依赖公钥密码，其计算高度复杂导致效率低下，且难以采用折中的措施实现隐私保护效果和数据效用的平衡；基于非密码学的方案通过概率或信息论定义匿名性和不可区分性意义上的隐私，并设计泛化匿名或加噪的方式实现匿名或属性值隐私保护，效率高且有利于平衡隐私保护效果和数据效用。目前，以数据为中心的开放应用场景多样化，特别是数据开放共享应用中，大规模的个人隐私需要在保证数据可用的前提下得到实用性的隐私保护，研究基于非密码学的方案可以达到这一目标，平衡隐私保护与数据效用，具有重要的现实意义。

隐私领域的研究主要有三方面科学问题。**第一、隐私定义与度量**。如何恰当形式化的定义隐私、并对隐私进行量化。特别是隐私量化，既包括对特定数据集中隐私量的量化，又包括在某种隐私分析攻击模型下，个人隐私潜在泄露量、隐私分析攻击后隐私泄露量评估，还包括某一隐私保护模型对数据集隐私保护能力的量化。**第二、隐私分析与推测**。在某一场景下针对保护后的隐私信息数据集进行隐私分析与推测，如何最大程度的获取更多隐私信息。**第三、隐私保护**。如何对某一场景下的隐私数据集进行有效隐私保护，如何在保护隐私的同时平衡隐私保护效果和数据效用。深入研究科学问题一和科学问题二有助于对隐私的理解和认识，能够对隐私泄露的机理进行深入剖析，能够对设计更好的隐私保护方案提供科学理论依据和评价方法，研究科学问

题三能够实现对数据隐私的预期性保护，如可量化的、动态性的、自适应的隐私保护，能够平衡隐私保护效果与数据效用间的关系。上述三个科学问题对基于非密码学的方案研究有重要的理论意义，能够有助于该领域完善其基础理论支撑，可在保证其实用性基础上提高隐私定义形式化及度量、隐私泄露机理、隐私保护方案的科学性。

面对上述隐私领域的主要科学问题挑战，本文主要针对数据开放共享场景下的基于非密码学隐私研究领域，展开隐私度量、隐私分析、隐私保护及隐私保护与数据效用平衡方面研究，旨在能够深入探究隐私基础理论，提高对隐私泄露及隐私保护机理的理解，以提出能够动态、自适应地对包含大量隐私信息的数据集进行隐私保护，并实现隐私保护与数据效用间的平衡。

1.2　研究现状

本节围绕本文的研究内容，就相关研究领域的现状进行梳理和分析，包括隐私度量、隐私分析、隐私保护，以及隐私保护与数据效用间的平衡四个方面，以更加深入的理解本文研究的背景。

1.2.1　隐私度量

早期对隐私的认知是法理上的“隐私权”，在技术上被定义为匿名性（nonymity），即在一个匿名集中元素不能被唯一标识的状态。在匿名通信系统中，匿名性最初被量化为匿名集阶的自然对数 $A = log_2(N)$[8]，并有信息熵、正规熵、条件熵等方法，详见2009年Edman和Yener的综述[9]，但这些方法并不适用数据共享和应用中的匿名性度量。2002年，Sweeney[1]将数据集中某一记录的匿名性量化为$d = 1/k$，其中 k 是数据集中与该记录不可区分的记录数量；随后，该方法被扩展为 l 多样性匿名[4]和 t 邻近匿名[5]。针对数据集的匿名性定义被扩展到了基于位置服务[10]、社交网络[11]等应用场景，并用以不同形式的数据发布[12-13]。这些方法都是将匿名性量化为与匿名集大小相关的概率值，并不能对敌手去匿名化攻击获取的信息量进行量化，且无法根据敌手的背景知识进行动态量化。Li等[14]在 k 匿名和 l 多样性匿名的基础上，根据数据集中敏感属性的分布，通过EMD(Earth Mover's Distance)计算敏感属性全局概率分布和任意等价类中该属性值概率分布的差异，提高了匿名性度量的灵活性。林欣等[15]发现位置 k 匿名算法匿名集大小无法在连续查询攻击下刻画匿名集中位置的匿名度，提出了匿名集查询结果信息熵的匿名度量化方法 $AD(q) = 2^{H(q)}$；Xu和Cai[16]认为在连续查询的位置 k 匿名中，模糊区域中用户会约束后续查询模糊区域的位置，进而提出了一种基于模糊区域大小和区域内实体数量的熵度量方式；为了使匿名性的度量能根据背景知识更动态更新，王彩梅等[17]针对Slient Cascade轨迹隐私保护将模糊区域前后用户假名间的联系性进行量化 $D(u_i) = H(u_i)/H_{max}(u_i)$。基于匿名集的大小及其数据概率分布对匿名性的度量，不能达到数学上的严谨证明，在2006年Dwork[6]定义了差分隐私的

概念，并通过添加高斯或拉普拉斯噪音的方法保护隐私，应用控制噪音量的隐私预算 ε 来量化隐私；2016年，Cuff与Yu[18]应用互信息给出了差分隐私算法对隐私保障的上界；随后，Wang等[19]从信息论角度对差分隐私、可识别性与互信息间的关系进行了量化。为了提高差分隐私的适用性，(ε,δ) 差分、本地差分[20]和Renyi差分[21]的定义被相继提出，基于匿名和差分结合的新的隐私定义也被提出[22]，并应用Renyi熵等信息论工具对差分隐私能力进行了量化。身份隐私的另外一类是成员关系隐私（Membership Privacy），即某一实体是否属于特定数据集的关系。2013年，Li等[23]定义了积极成员隐私和消极成员隐私，并分析了成员关系隐私与差分隐私间的关系。

云数据共享、位置服务、社交网络等众多场景中，数据集中的个人身份信息是对外公开的，需要对数据某字段值、位置点、个人喜好、政治倾向等属性隐私进行量化和保护，主要还是通过取值范围、集合的阶、正确率、精准率、信息熵、互信息等方面进行量化[24-25]。除了对隐私进行分类定义和量化之外，对隐私保护算法的能力与敌手模型隐私分析攻击能力也需要量化。2011年，Shokri等[26]将轨迹去匿名化、位置攻击、会面泄露攻击等形式化为概率推测，并应用推测得到条件概率来估计隐私分析结果，应用精准度、正确性、确定性三个指标来量化隐私，度量隐私保护算法的性能。2015年，Ma等[27]对时间序列型数据隐私进行量化，除了利用互信息、正规互信息和条件熵，还提出了离线条件熵，即某时间点相邻的数据点协助推测该时间点的条件熵来量化隐私。2018年，Zhao与Wanger[28]应用一致性指标对图结构匿名性、可去匿名化从从成功率、信息泄漏量等方面进行量化。此外，俞艺涵等[29]利用信息熵和BP神经网络实现隐私数据分级分类，对数据集记录的隐私量采用两层信息熵加权的方式进行量化。

可见，隐私量化主要是根据隐私定义和隐私目标进行形式化的，通过不同形式的可量化指标进行度量，对隐私保护机制能力和隐私分析攻击模型能力的量化主要是通过隐私数据集中元素的前后变化量来度量。这两方面的度量还未形成统一的框架，尽管信息论等工具被广泛应用于隐私量化，还需要再基础框架上进行统一，为不同场景下隐私目标的设定、隐私的量化提供理论支持；同时，还需要对多样化的应用场景定义适应性的隐私，以应对隐私的动态性、多样性需求。

1.2.2　隐私分析

由于商业、政治利益，以及为了更好地理解隐私、量化隐私、保护隐私，隐私分析一直是研究热点，主要集中在去匿名化推测分析和属性值推测分析两方面。对基于位置服务中用户的位置信息进行直接 k 匿名保护的情况，林欣等提出了一种连续查询攻击[15]，在不同 k 匿名保护算法下的位置查询中成功区别出位置发送者。2013年，Humbert等[30]应用置信传播算法对亲属间的基因序列隐私进行了重构推测攻击分析，并应用信息熵、正确率来量化敌手获取的隐私量。2017年,Olteanu等[31]利用置信传播算

法对社交网络共现位置的隐私进行了推测攻击分析。2018年，Deznabi等[32]利用亲属关系、基因组高阶关联、基因表现型等更多公开基因组数据，对亲属间的基因序列隐私进行了重构推测攻击分析，并量化了隐私攻击能力。manousakas等[33]利用图结构基于核的相似性构造了一个人类迁徙网络拓扑结构的去匿名化推测模型，成功识别出了手机移动网络中的个体身份。2019年，Cao等[34]针对差分隐私保护的连续发布数据情形，建立了基于马尔科夫关联的条件概率推测模型，从前向数据发布和后项数据发布分析了隐私泄露量的上界。关于成员关系隐私，2017年，Shokri等[35]通过对机器学习训练模型建立多个“shadow”模型，对输入数据进行多个模型训练，根据输出数据的分布差异判断目标数据记录是否属于某个训练集合。2018年，Rahman等[36]针对基于差分隐私的深度学习训练数据集，在不同的差分隐私预算下分析了图片分类学习模型的成员关系隐私。

可见，隐私分析主要是敌手利用获取的先验或后验知识，建立与隐私分析目标相关联的推测模型，通过置信度、置信传播、贝叶斯推断、马尔科夫等方法建立概率推断优化模型，获取目标隐私信息。通过隐私分析，可以帮助人们更加深入的认识隐私，理解隐私泄露的深层原因，通过各种不同的隐私攻击敌手模型为设计更好地设计高效的隐私保护算法提供理论依据。在各类场景中隐私分析的敌手模型多样复杂，需要更加深入的研究数据共享应用领域的隐私分析方法。

1.2.3　隐私保护

针对数据集的隐私保护算法是在隐私定义和量化的基础上提出来的。针对匿名隐私，通过泛化的方法实现 k 匿名[1](即数据集中任意记录都至少有 $k-1$ 条数据与之无法区分)之后，因为不同的匿名性定义不适用所有的场景，不能抵抗链接攻击、动态攻击、背景知识攻击等，驱动了 l 多样性匿名[4]、 t 邻近匿名[5]算法的提出。如同隐私量化，实现这些不同匿名性的算法也被扩展到各个领域，如基于位置服务[10]、社交网络[11]、数据发布[12-13]。类似地，不同的差分隐私算法根据差分隐私定义而迅速发展，(ε,δ) 差分、本地差分[20]、Renyi差分[21]、分布式差分隐私[37]等不同形式的算法被提出，并被应用于对抗生成网络[38]，深度学习模型发布[39],社交网络数据发布[40]等各类场景。

访问控制是一种有效的安全和隐私保护方法，也被广泛应用在各领域[41]。2007年，Ni等[42]就扩展基于角色的访问控制使其适应隐私需求，还有更多面向隐私保护的访问控制模型被提出,如基于属性的隐私访问控制[43]。面向隐私保护的非密码学访问控制主要有基于信任[44]、基于风险[7]、基于激励[45]、基于目的访问控制[46]的方案。基于风险的访问控制具有较好的动态性和适应性，对系统设置依赖较为简单，在动态化细粒度的隐私保护需求方面受到了广泛关注。在Cheng等[47]利用模糊逻辑提出多层安全的风险访问控制模型后，被迅速推广为标准草案[48]。2011年，Wang等[49]应用于保护医疗

信息系统中病人隐私，随后有了更进一步的发展[7,41]。

可见，隐私保护研究的目标之一是设计更加严谨、有效、灵活的方案，包括基于非密码学和基于密码学的方案。鉴于本文主要关注前者，有关基于密码学的隐私保护方案可参阅黄刘生等[3]的综述。由于隐私保护的场景多样复杂，隐私需求动态变化，该领域需要更加丰富的研究，以支持当前以数据为中心的开放、动态应用场景隐私保护需求。

1.2.4　隐私保护与数据效用间的平衡

除了要保护隐私，数据效用是数据发布、数据共享时考虑的重要因素，Li等[50]较早考虑了数据发布的隐私与效用平衡问题，认为隐私泄露与效用获取不能直接对比，提出了一种基于投资组合风险与收益的隐私损失与数据效用对比方法。Sui与Boutilier[51]在机制设计领域的第二价格拍卖协议和设施选址协议中，减少数据效用可以提高隐私保护效果。Guo与Chen[52]通过挖掘Facebook的用户隐私设置和用户偏好，为用户个性化隐私设置和社交效用权衡提供支持。Sanker等[53]提出用条件熵和互信息对数据集共享时，在保证最低限度隐私保护来达到最大的数据效用关系进行权衡。Kalantari等[54]对差分隐私保护从汉明失真的角度讨论了隐私与效用的权衡，并用互信息来量化隐私损失率。He与Li[55]用概率模型基于因子图和DNA中基因型与表现型间的统计关系，提出了可优化隐私与效用的基因数据发布方案。这些方案都指出隐私与效用间存在权衡关系，但并未提出如何平衡该关系，如何达到隐私与效用间的平衡。博弈论作为解决合作与冲突的数学工具，在网络安全各领域都有广泛的应用[56]，天然适用于解决隐私领域的隐私保护与数据效用间的冲突与联系问题。Freudiger等[57]在2009年将 n 方完美信息博弈引入到位置隐私保护，分析了用户最大化其位置隐私的博弈均衡，并提出了基于贝叶斯纳什均衡的理性保护方案；随后Santos等[58]针对位置服务中多代理协作位置共享场景，应用纯策略博弈和流行病模型设计了阈值博弈策略，实现了多代理间的合作与非合作效用最大化。2014年，Wang和Zhang[59]对智能手机上下文隐私感知的动态敌手模型，构建了 2 方零和博弈模型，并设计了动态优化的隐私防护措施。2017年，Shokri等[60]进一步将博弈论应用于优化的轨迹隐私，实现隐私保护与位置数据效用的平衡。2019年Du等[61]将社区结构的演化博弈应用于社交网络中用户社交关系与隐私保护行为建模，激励用户隐私保护行为动态演进。可见，博弈论对隐私保护与数据效用的平衡有重要的作用，访问控制作为隐私保护的重要工具[2,7,49]，也需要能够恰当的解决此问题。2014年，Hu等[62]面向社交网络协同数据共享，提出了一种基于多方访问控制的多方控制博弈模型，以平衡隐私控制者隐私设置与收益间的关系。2016年，Liu等[63]将序贯博弈应用于多播蜂窝网络接入的混合访问控制中。Helil等[64]和Wang等[44]分别将非合作博弈应用于基于信任的访问控制模型中。2018年，Gao等[65]引入信誉和重复公共物品博弈到云存储数据共享

的服务提供者与数据访问者间的信用困境，提高存储率降低非诚实参与者行为。

可见，尽管博弈论对平衡隐私保护与数据效用多方面的进展，但面向隐私保护的访问控制领域的进展还较少，无法有效解决数据共享过程中访问者访问隐私敏感数据时，系统隐私保护需求与用户数据效用需求间的平衡问题；此外，现有基于博弈的访问控制模型都假设参与者是完全理性的，总能采取最优策略，现实场景中参与者由于信息不完全等各类因素不能总是完全理性的，故难以适应真实场景，需要有更好的理性博弈模型，解决有限理性条件下访问隐私保护与数据效用间的平衡问题。

1.3　有待解决的关键问题

本节围绕本文的研究内容，对相关的关键问题进行总结，为后文研究这些问题并提出相应的解决方案奠定基础。

1. **隐私度量**。信息论已经成为隐私度量的重要工具，但其在匿名隐私、成员隐私和差分领域的应用仅利用了信息熵、互信息等概念[25]，某一具体的度量方法往往仅能适用于一种具体的场景，尚未对隐私度量形成体系化的框架[26,33]；其次，对隐私保护机制和隐私分析敌手模型的度量也相对割裂，并未有统一的模型同时适用于两方面的度量；再次，当前的隐私定义和隐私量化都是静态隐私，由于隐私是一个随场景、时间和需求发生变化的感性概念，需要动态适应性的定义并量化隐私。

   此外，现有的信息论度量方法大多基于Shannon信息论，仅有少量工作扩展应用了Renyi熵，由于Shannon信息论不能刻画偏好、结构等信息，对具有时间序列特征数据、复杂结构图数据的隐私量化有天然的不足，需要进一步扩展信息论工具，更加有效的量化复杂结构数据的隐私。

2. **隐私分析**。隐私分析是建立在对隐私恰当定义并量化的基础上，现有的隐私分析针对匿名性的分析，实现去匿名化的研究较多[15,33]，对实体属性的隐私分析还较少。大量数据在云服务等环境中存储、共享或应用，特别是隐私分析推测攻击对象相互关联、隐私属性相互关联，敌手获取的背景知识不明确且包含大量公开背景知识，隐私泄露机理变得难以梳理。现有的隐私分析主要围绕位置数据、社交网络数据等场景，需要以更强的背景知识假设，对新型数据如时间序列数据（如连续社交轨迹数据）、基因序列数据（如医疗基因组数据）等进行进一步分析，更加深入的理解隐私。

3. **隐私保护**。目前基于匿名、差分的隐私保护模型都是静态的、粗粒度的方案，且具体的方案仅适用于某一特定场景，难以适应数据存储、共享及应用过程中动态个性化的隐私保护，难以满足大规模数据及分布式大规模用户动态数据需求的隐

私保护。细粒度的访问控制模型，特别是基于风险的访问控制模型具有更加适用于大规模数据的动态需求特征[41]，但在隐私风险定义和量化方面，在访问控制自适应性方面都需要进一步研究。

4. **隐私保护与数据效用平衡**。数据效用成为隐私保护机制考量重要因素，需要设计能够兼顾隐私保护需求和数据效用需求，且能平衡二者关系的隐私保护机制。在细粒度动态实现隐私保护的风险访问控制模型中，如何真实地刻画隐私保护和数据效用、如何设计恰当的博弈过程及求解其均衡，如何更加符合真实场景地描述隐私保护参与方的非完全理性行为，如何描述隐私保护与数据效用逐步达到均衡点的过程，都需要进一步研究。

1.4　本文研究内容和成果

本文主要聚焦在以信息论通信模型及其扩展工具研究隐私度量的基础性框架模型，能够对隐私定义、隐私分析攻击模型和隐私保护机制进行量化；以概率推断为工具建立序列型隐私数据的属性隐私分析低手模型，并针对真实数据进行分析推断攻击，量化低手隐私分析攻击能力；因风险访问控制模型为基础，定义并量化风险隐私，设计动态自适应访问控制模型；以博弈论为工具，刻画访问控制隐私保护机制参与者的隐私和数据效用需求的理性行为和有限理性行为，设计能动态平衡隐私保护和数据效用关系的理性风险访问控制隐私保护机制。具体取得了如下成果：

1.4.1　基于信息通信模型的隐私度量框架

1.4.2　基于信息通信模型的隐私度量框架

1.4.3　基于信息通信模型的隐私度量框架

1.4.4　基于信息通信模型的隐私度量框架

1.4.5　基于信息通信模型的隐私度量框架

1.5　论文结构

第二章　基础知识

本章介绍本文研究所需的信息论、博弈论及隐私保护的基本概念，包括*Shannon*信息论及其扩展，策略博弈、扩展博弈等博弈论概念，隐私分类及隐私保护基本模型。本章的内容主要为后文展开具体研究奠定基础。

2.1　Shannon信息论及其扩展

2.1.1　信息通信模型

信息论[66-67]是信息科学的基本工具，信息论对于量化信息的不确定性和信息量有重要的作用。信息通信模型最早由Shannon在其《通信的数学原理》论文中提出，如图2.1所示。

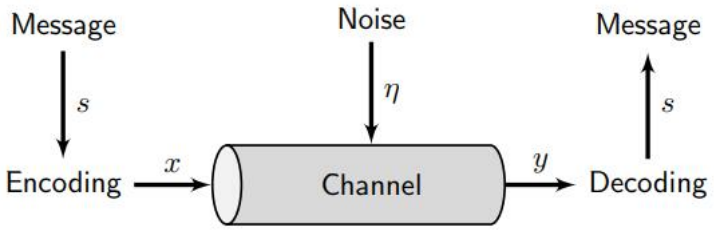

图 2.1: 信息通信模型[67].

信息通信模型[67]由信源消息、编码器、信道、解码器、信宿消息和噪音构成，信源消息（数据）在作为信道输入之前被编码器进行编码；编码后的信源消息在信道中传输，传输过程中会受到噪声影响；解码器从信道中接收到加噪后的信息，解码为信宿消息。

对于事件集中的某一特定事件x，x的概率为$p(x)$，则x的香农信息为$-\log p(x)$。

因此，风险也是关于不确定性的概念，这与香农信息自然相关。在这项工作中，我们打算利用信息来估计访问请求和用户的隐私风险。可以在[?]中找到有关隐私社区中信息论的更多详细信息。

2.1.2　信息熵

2.1.3　互信息

2.1.4　结构信息论

2.2　博弈论

博弈论[??]是一个自我利益实体（即博弈者）之间相互作用的数学模型，它总是用于为这些实体寻找冲突与合作的解决方案。博弈包含实体之间的迭代，并且每个博弈者在每次迭代中都将执行一个操作。最后，博弈达到了解决方案（即平衡），所有博弈者都获得了自己最大的收益。在特定的博弈中，博弈者是理性的，这意味着每个博弈者都会采取行动来响应他人的行动，以获取最大的利益。

有一些术语用来描述博弈、博弈者、行为、回报、策略和均衡[?]。博弈者是参与底层博弈的实体，博弈者可以是人、机构或信息系统；动作是每个博弈者在博弈的每个迭代中所做的动作，每个博弈者都知道每个其他博弈者的所有可选动作；博弈者的回报是对于他在博弈中采取的行动的返回值；博弈者的策略是他/她的行动计划，该计划根据他/她对行动历史的了解来指定要采取的行动。策略可以是纯策略，也可以是混合策略；均衡是一个博弈的解，是所有博弈者各自获得最大利益的策略组合。博弈论在信息安全和隐私保护的许多领域都得到了应用，详见[??]。

2.2.1　博弈模型

2.2.2　策略博弈

2.2.3　扩展博弈

2.2.4　演化博弈

2.3　隐私定义及隐私保护

2.3.1　身份隐私

2.3.2　属性隐私

2.3.3　隐私保护模型

ag

第三章　基于信息通信模型的隐私度量模型

3.1　概述

隐私保护的研究起步较早，但近年来突然受到产业界和学术界的广泛关注是因为大数据的不期而至.坦率地说，大数据的迅速发展让学术界始料未及，大数据的理论研究已经落后于产业需求，尤其是隐私保护成为大数据应用的主要瓶颈，移动网络、社交网络、基于位置服务等新型应用服务的推进，隐私问题更加突出.目前关于隐私保护有两个方向值得关注：一是研究隐私保护算法以更加有效的方式保护隐私;二是通过研究隐私泄露风险分析与评估，解决数据的可用性与隐私保护之间的的平衡.隐私保护算法目前主要集中在匿名方法，包括 k 匿名、 l 多样性匿名和 t 接近匿名及其衍生的方法.隐私度量最早起源于相关匿名算法[1], 在匿名隐私保护算法的研究过程中，不时有学者关注隐私量化问题，尤其是在定位服务领域，位置匿名及轨迹匿名算法上已有不少隐私度量的相关研究[2，3],因此对于隐私保护算法来说，隐私度量仍需进一步深入研究.然而就目前来说，隐私泄露涉及因素众多，设计有效的隐私保护算法仍然是挑战性问题，但政府及企业数据开放共享中迫切的隐私保护需求，促使我们不得不在可用性与隐私泄露之间寻求一种平衡，要解决这个问题，隐私风险分析及评估不失为一种方法.风险分析依然涉及到隐私量化问题，也就是说量化风险评估不失为隐私保护一种可行的解决方案，量化隐私风险必然也涉及隐私度量问题.从这些分析来看，隐私度量的研究具有十分重要的理论意义和应用价值.

信息熵作为信息度量的有效工具，在通信领域已展现出其重要的贡献[4].隐私作为一种信息，自然可以考虑用熵来量化，为此，不少学者或多或少进行了探索，比如事件熵、匿名集合熵、条件熵等[5-7],但其研究还较为零散，更多是针对某一具体领域，如位置隐私保护领域，目前尚未形成统一的模型及体系，其应用范围也受到限制，特别是隐私是具有时空性的，与人的主观感受也有关系，不同的人对同一隐私的认同可能不同. 鉴于以上分析，本文旨在参考Shannon信息论的通信框架[8],提出几种隐私保护信息熵模型，包括隐私保护基本信息熵模型、含敌手攻击的隐私保护信息熵模型、带主观感受的信息熵模型和多隐私信源的隐私保护信息熵模型.在这些模型中，将信息拥有者假设为发送方，隐私谋取者假设为接收方，隐私的泄露渠道假设为通信信道;基于这样的假设，分别引入信息熵、平均互信息量、条件熵及条件互信息等来分别描述隐私保护系统信息源的隐私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量;以此为基础，进一步提出了隐私保护方法的强度和敌手攻击能力的量化测评，力图为隐私泄露的量化风险评估提供一种理论支持.

3.2　相关工作

信息熵理论是Shannon [8]于1948年提出的，解决了信息的量化和通信的理论基础.较早将信息熵考虑到隐私度量的研究是Diaz等[5]和Serjantov等[6],他们提出了用信息熵来度量匿名通信系统的匿名性，在假定攻击者的目的是确定消息的发送者(或接收者)的真实身份的情况下，系统中每个用户都以一定的概率被猜测为消息的真实发送者(或接收者),将攻击者猜测某用户是真实发送者(或接收者)看成一个随机变量X,用信息熵$H(X)=-\sum p(x)\log p(x)$来量化的随机变量的不确定性可表征为系统的隐私水平.随后，有不少学者将信息熵应用于某些具体领域的隐私度量，如位置服务、社交网络和数据挖掘等领域，对于不同的方案[2-3，9-21],其随机变量的概率表现形式和对熵的处理方式不同.在位置服务领域，2007年，Hoh等[9，10]提出了基于信息熵的隐私度量方法度量轨迹跟踪的不确定度，其中随机变量的概率表现为每个位置实例包含在当前跟踪车辆轨迹的概率.2009年，Ma等[11]提出在V2X车联网系统中信息熵的隐私度量方法，其中随机变量的概率表现为每个位置信息关联到某特定用户的概率，该方法还考虑了随机变量的概率随着时间的变化而更新的情况，也即攻击者的累积信息对系统隐私的影响.同年，林欣等[12]针对LBS中的连续查询问题，提出一种连续查询攻击算法，指出匿名集的势不再适合作为查询该算法匿名性的度量，并提出了基于信息熵的度量方法，其中随机变量的概率表现为每个用户u_i是查询q的真正发出者的概率，信息熵计算为$H(q)$,用$AD(q)=2^{H(q)}$度量为系统的隐私水平.2011年，Shokri等[2]将位置隐私的度量准则分为精确性、确定性和正确性，精确性度量为攻击者猜测事件的置信区间，确定性度量为攻击者猜测的不确定性，正确性度量为攻击者出错的概率，其中精确性的度量是基于信息熵的度量方法，随机变量的概率表现为每个观测事件是真实事件的概率.2012年，Chen等[13]针对LBS查询隐私进行度量，随机变量的概率表现为攻击者在无背景知识和有背景知识两种情况下的判断用户u_i是查询q的真实发出者的条件概率，并利用互信息$I(U|q;<rfitfiq>)=H(U|q)-H(U|<rfitfiq>)$度量系统的隐私水平.同年，王彩梅[3]等针对LBS中的轨迹隐私保护方法Silent Cascade提出基于信息熵的隐私度量方法，随机变量的概率表现为某用户的每条可能轨迹的概率，特定用户的熵计算为$H(u_i)$,并用标准熵$D(u_i)=H(u_i)/H_{max}(u_i)$度量为系统的隐私水平.2014年，文献[14，15]均采用了信息熵度量了LBS系统的隐私水平.

在社交网络领域，2010年，Ngoc等[16]针对社交网络隐私泄露的情况，提出了基于信息熵的隐私度量方法，以帮助用户判断所发布信息的隐私水平，其随机变量的概率表现为事件X的取值x的概率.2012年，Yang等[17]总结了社交网络中的风险，并利用信息熵和互信息度量的系统的隐私水平.

此外，信息熵在其它领域的隐私度量中也有所涉及，文献[18，19]研究了信息熵用于数据挖掘领域的隐私度量，文献[20]研究了信息熵用于匿名系统领域的隐私度量，文献[21]研究了信息熵用于增价竞标领域中竞标人的隐私度量，Wagner等[6]对当前存

在的隐私度量方法进行了综述，根据度量系统的输出将隐私度量方法分成八类，其中不确定度的分类中是根据信息熵来度量的.

综上可知，目前存在的基于信息熵进行隐私度量的理论体系较为零散，缺乏统一的模型基础.针对上述问题，本文试图将隐私保护系统看作一个通信模型，力图探讨较为通用的隐私度量信息熵模型，解决隐私度量的一些基本概念和基础体系.

3.3　隐私保护信息熵模型

本文的出发点是：将信息拥有者假设为发送方，隐私谋取者(敌手)假设为接收方，隐私的泄露渠道假设为通信信道.

发送方拥有的一个信息集称为隐私信源，用随机变量X表示,X是由所有的离散基本泄露事件的隐私消息构成的隐私消息空间，即$\{x_1,x_2,...,x_i,...,x_n\}$,其中$x_i(i=1\text{fi}2,...,n)$为基本泄露事件的隐私消息;接收方获取的信息集称为隐私信宿，用随机变量Y表示,Y是由敌手获取的所有基本隐私消息构成，即$\{y_1,y_2,...,y_j,...,y_m\}$,其中$y_j(j=1\text{fi}2,...,m)$为敌手获取的某个隐私消息.相应的，某一种具体的隐私保护算法可以看作是对隐私消息进行转换、编码的方法，它能够对隐私消息进行干扰进而实现对隐私信息的保护，其中隐私保护算法的全体构成隐私保护机制空间，称为隐私保护机制源.敌手在一定背景知识下对隐私信息的挖掘与分析手段称为隐私攻击，所有隐私方法的的全体称为隐私攻击空间.

以此假设为基础，本节将基于Shannon信息论的通信框架[8]提出几种隐私保护信息熵模型，包括：隐私保护基本信息熵模型、含敌手攻击的隐私保护信息熵模型、带主观感受的信息熵模型和多隐私信源的隐私保护信息熵模型.通过引入隐私信息熵、平均互信息量、条件熵及条件互信息等来分别描述隐私保护系统信息源的隐私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量.

3.3.1　隐私保护基本信息熵模型

这里我们首先假设敌手无任何隐私攻击能力，敌手仅通过信道观测到隐私信息，并只考虑离散单隐私信源的情形.模型定义如下：

设单隐私信源X的数学模型可以表示为:

$$\begin{pmatrix} X \\ P(X) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_i & \cdots & x_n \\ p(x_1) & p(x_2) & \cdots & p(x_i) & \cdots & p(x_n) \end{pmatrix} \tag{3.1}$$

其中$0 \leqslant p(x_i) \leqslant 1, \sum_{i=1}^{n} p(x_i) = 1$.同理，隐私信宿$Y$的数学模型可表示为:

$$\begin{pmatrix} Y \\ P(Y) \end{pmatrix} = \begin{pmatrix} y_1 & y_2 & \cdots & y_i & \cdots & y_m \\ p(y_1) & p(y_2) & \cdots & p(y_i) & \cdots & p(y_m) \end{pmatrix} \tag{3.2}$$

针对该模型，定义**隐私信源熵**$H(X)$

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i) \tag{3.3}$$

$H(X)$用于刻画隐私信源的平均隐私信息量，也是隐私信源的隐私不确定程度,$H(X)$越大，隐私泄露就可能越小，从而它亦可以用于衡量隐私的保护程度，在没有外部条件影响时，该值是一个确定的值.

当隐私信宿Y在获取隐私信息条件下，关于隐私信源的不确定程度，可以引入**隐私条件熵**$H(X/Y)$刻画，其定义为:

$$H(X/Y) = -\sum_{j=1}^{m} \sum_{i=1}^{n} p(x_i y_j) \log_2 p(x_i/y_j) \tag{3.4}$$

该条件熵表示隐私信宿在收到Y后，隐私信源X仍然存在的不确定程度，该不确定程度是隐私泄露信道的干扰(隐私保护)造成的，即敌手在长期观测隐私信源过程中，由于隐私保护机制的保护下，敌手对隐私信源仍然存在一定的不确定.

易证上述的隐私信息熵是满足Shannon信源熵的基本性质.即具有非负性、对称性、扩展性、确定性、可加性、极值性、上凸性等，并满足极大离散熵定理，在此不再赘述.

下面我们引入**平均隐私互信息量**$I(X;Y)$来刻画信道上隐私泄露程度，定义为

$$I(X;Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i y_j) \log_2 \frac{p(x_i/y_j)}{p(x_i)} \tag{3.5}$$

$I(X;Y)$表示了隐私信源X和隐私信宿Y之间交互的平均信息量，即在信道上传送的隐私信息量，它正好可以刻画隐私的整体泄露程度，从而可用于度量隐私的泄露.

3.3.2　含敌手攻击的隐私保护信息熵模型

上节提出的隐私保护基本信息熵模型客观上描述了无敌手攻击或敌手无攻击能力情况下的隐私度量问题.在实际系统中往往存在着隐私攻攻击分析分析，敌手可以在一定的背景知识下进行攻击分析，模型定义如下：

在该模型中，表示背景知识空间，其数学模型亦可定义为：

$$\begin{pmatrix} Y \\ P(Y) \end{pmatrix} = \begin{pmatrix} y_1 & y_2 & \cdots & y_i & \cdots & y_m \\ p(y_1) & p(y_2) & \cdots & p(y_i) & \cdots & p(y_m) \end{pmatrix}$$
$$0 \leqslant p(z_k) \leqslant 1, \sum_{k=1}^{l} p(z_k) = 1(k = 1\text{fi}2, ..., l) \tag{3.6}$$

攻击者可以利用背景知识Z加强对隐私进行攻击，对于攻击者来说，可以联合隐私信宿消息Y和背景知识Z进行隐私分析攻击，引入**攻击条件熵**

$$H(X/YZ) = \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i y_j z_k) \log_2 p(x_i/y_j z_k) \tag{3.7}$$

$$I(X;Y/Z)$$

$H(X/YZ)$反映了攻击者在获得隐私信宿消息Y和背景知识Z后，关于X仍然存在的不确定度，它实际了可以作为在具有攻击分析的情况下隐私信息的不确定度，亦可以作为隐私保护强度的度量.进一步定义**隐私攻击平均互信息**$I(X;Y/Z)$

$$I(X;Y/Z) = \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i y_j z_k) \log_2 \frac{p(x_i z_k/y_j)}{p(x_i/z_k)p(y_j/z_k)} \tag{3.8}$$

反映了得到Z的条件下,X和Y之间的平均互信息量，即接收方获得的隐私信息量，即可以刻画具有背景知识攻击下的隐私泄程度.

3.3.3　带主观感受的信息熵模型

信息源发生的隐私事件所泄露的隐私信息是客观存在的，但通常对隐私信息是带有主观感受的，不同的隐私信息的重要程度不同或价值不同.本节将权重引入前两节的信息熵模型中，对含有主观感受的隐私信源的隐私信息进行度量.

(1) 带主观感受的隐私保护信息熵模型

针对图1所述通信模型.隐私信源发出的消息$x_i(i = 1\text{fi}2, ..., n)$,确定一个非负实数作为该消息的重要程度权值，不同的消息，权值越大，重要程度越大.可对该隐私信源建立权值空间:

$$\begin{pmatrix} X \\ W(X) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_i & \cdots & x_n \\ w(x_1) & w(x_2) & \cdots & w(x_i) & \cdots & w(x_n) \end{pmatrix}$$
$$w_i \geqslant 0(i = 1\text{fi}2, ..., 3) \tag{3.9}$$

定义**隐私加权信源熵**$H_w(X)$对隐私信源的隐私信息加权平均隐私信息$w_i(i=1\text{fi}2,..,n)$量进行度量，并刻画了隐私信源对隐私消息的主观感受影响信源的隐私信息量.在相对稳定的时间段内，隐私信源对隐私消息的主观感受或偏好一旦固定，隐私加权信源熵是一个确定的值.

$$H_w(X) = -\sum_{i=1}^{n} w_i p(x_i) \log_2 p(x_i) \tag{3.10}$$

隐私信源加权熵显然有以下性质:

- 非负性.无论一个隐私事件的重要程度如何，隐私信源一旦发生了一个隐私事件，其总能提供一定关于隐私信息的信息量.
- 连续性.隐私信源发生的隐私事件的概率发生微小的变动，形成另一个隐私信源，变化前后的两个隐私信源的加权熵是连续的.该特性对于刻画因时间变化，隐私信源的特性变化是非常有效的.如在某一段时间内，一个人的生活规律是固定的，导致其能够泄露个人隐私的行为模式的概率分布是相对固定的，但随时间的推移，此人的生活规律会连续性的发生微小的变化，进而能够泄露其隐私的行为模式概率分布也发生了微小的变动.但行为发生变化前后关于行为总体的加权熵是连续的.

除此之外，隐私信源加权熵还有对称性，均匀性等不同性质，并在隐私保护系统中有相应的实际意义.

仅考虑隐私信源对隐私消息的主观感受，定义**隐私加权条件熵**$H_w(X/Y)$刻画隐私谋取者对信息拥有者的隐私信息平均不确定程度.

$$H_w(X/Y) = -\sum_{i=1}^{n} w_i \sum_{j=1}^{m} p(x_i y_j) \log_2 p(x_i/y_j) \tag{3.11}$$

同样,仅考虑隐私信源对隐私消息的主观感受，定义**隐私加权平均互信息**$I_w(X;Y)$刻画信息拥有者发生了隐私事件之后，在隐私保护机制的保护下，隐私谋取者观测到的隐私事件后接收到关于信息拥有者的隐私信息量.

$$I_w(X;Y) = -\sum_{i=1}^{n} w_i \sum_{j=1}^{m} p(x_i y_j) \log_2 \frac{p(x_i/y_j)}{p(x_i)} \tag{3.12}$$

这里，隐私加权条件熵和隐私加权平均互信息仅考虑了隐私信源对隐私消息的主观感受和偏好，在实际系统中，不仅仅是信息拥有者对自身的隐私信息有不同的主观感受，隐私谋取者对获取到的隐私信息也有不同的主观感受和偏好.故可以进一步探讨

通信模型中隐私信宿对隐私消息的主观感受并赋予权值，甚至建立刻画隐私信源和隐私信宿双方偏好的权值矩阵，定义更加符合实际的隐私加权条件熵和隐私加权平均互信息.

(2) 带主观感受并含敌手攻击的隐私保护信息熵模型

在本模型中，仍然仅考虑隐私拥有者对其隐私信息的主观感受和偏好.故隐私信源X的**隐私加权信源熵**$H_w(X)$定义如公式.同时定义**加权攻击条件熵**$H_w(X/YZ)$隐私信宿在具备攻击能力后对在主观感受的隐私信源隐私信息的平均不确定程度，可以作为隐私保护在敌手攻击下的保护强度度量.

$$H_w(X/YZ) = -\sum_{i=1}^{n} w_i \sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i y_j z_k)\log_2 p(x_i/y_j z_k) \tag{3.13}$$

在此基础上定义**隐私攻击加权平均互信息**$I(X;Y/Z)$表示在得到Z的条件下，隐私信宿接收到的隐私信息量，具体刻画在具有背景知识条件下隐私泄露的量.

$$I(X;Y/Z) = \sum_{i=1}^{n} w_i \sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i y_j x'_k)\log_2 \frac{p(x_i z_k/y_j)}{p(x_i/z_k)p(y_j/z_k)} \tag{3.14}$$

3.3.4　多隐私信源的隐私保护信息熵模型

客观上，系统中的信息拥有者是多个的，其带有隐私信息的隐私事件通过隐私保护机制进行保护.故可建立多隐私信源的隐私保护通信模型，对相互关联的多个信源的隐私信息的保护和攻击进行度量. 如图3所示的无隐私攻击的多隐私信源隐私保护通信模型和图4所示的带隐私攻击的多隐私信源隐私保护通信模型.

(1) 多隐私信源的隐私保护信息熵模型

在图3所示的通信模型中，隐私信源X_1和隐私信源X_2共同构成隐私信源X,其数学模型为:

$$\begin{gathered}\begin{pmatrix} X_1 \\ P(X_1) \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i_1} & \cdots & x_{1n_1} \\ p(x_{11}) & p(x_{12}) & \cdots & p(x_{1i_1}) & \cdots & p(x_{1n_1}) \end{pmatrix} \\ 0 \leqslant p(x_{i_1}) \leqslant 1, \sum_{i_1=1}^{n_1} p(x_{i_1}) = 1 (i_1 = 1\text{fi}2, ..., n_1)\end{gathered} \tag{3.15}$$

$$\begin{gathered}\begin{pmatrix} X_2 \\ P(X_2) \end{pmatrix} = \begin{pmatrix} x_{21} & x_{22} & \cdots & x_{2i_2} & \cdots & x_{2n_2} \\ p(x_{21}) & p(x_{22}) & \cdots & p(x_{2i_2}) & \cdots & p(x_{2n_2}) \end{pmatrix} \\ 0 \leqslant p(x_{i_2}) \leqslant 1, \sum_{i_2=1}^{n_2} p(x_{i_2}) = 1 (i_2 = 1\text{fi}2, ..., n_2)\end{gathered} \tag{3.16}$$

隐私信宿Y的数学模型如公式(2)所述，定义**多源联合隐私信源熵**$H(X_1X_2)$,该信源熵刻画的多个带关联的隐私拥有者的隐私信息的量.

$$H(X_1X_2) = -\sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2} p(x_{i_1}x_{i_2})\log_2 p(x_{i_1}x_{i_2}) = H(X_1) + H(X_2/X_1) \tag{3.17}$$

已知隐私信宿Y条件下对隐私信源X的**多源联合隐私条件熵**为$H(X/Y) = H(X_1X_2/Y) = H(X_1X_2Y) - H(Y)$.该定义刻画的是多个带关联的信息拥有者发生的隐私事件在隐私保护后，隐私信息获取者对被保护的隐私事件进行观测后其对各信息拥有者的隐私信息的平均不确定程度.

同时，定义**多源联合平均互信息**$I(X_1X_2;Y)$刻画多个带关联的信息拥有者发生的隐私事件在隐私保护后，隐私信息谋取者通过观测被保护隐私事件后获取的各信息拥有者的隐私信息量.

$$I(X_1X_2;Y) = \sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2}\sum_{j=1}^{m} p(x_{i_1}x_{i_2}y_j)\log_2 \frac{p(x_{i_1}x_{i_2}/y_j)}{p(x_{i_1}x_{i_2})} \tag{3.18}$$

(2) 多隐私信源带隐私攻击的隐私保护信息熵模型

在3.3.2节所提带隐私攻击的隐私保护信息熵模型基础上，引入多个带关联的信息拥有者，构成新的关联的多隐私信源，并可进一步构建多隐私信源带隐私攻击的隐私保护信息熵模型，其通信模型如图4所示.

图4所述通信模型的信源数学模型如公式和，隐私信宿Y的数学模型如公式(2)所述.该模型下的**多源联合信源熵**$H(X) = H(X_1X_2)$,**多源联合隐私攻击条件熵**$H(X_1X_2/YZ)$和**多源联合隐私攻击条件平均互信息**$I(X_1X_2;Y/Z)$,其中多源联合隐私攻击条件熵表示的在已知背景知识攻击下接收者对联合隐私信源的隐私信息的不确定度; 多源联合隐私攻击条件平均互信息表示在已知背景知识攻击下接收者收到的联合隐私信源隐私消息所含的隐私信息量.

$$\begin{aligned} H(X_1X_2/YZ) &= H(X_1X_2YZ) - H(YZ) \\ I(X_1X_2;Y/Z) &= H(X_1X_2) - H(X_1X_2Y/Z) \end{aligned} \tag{3.19}$$

3.4　隐私度量及其对隐私保护机制和隐私攻击手段的评价

应用信息熵和平均互信息对隐私信息进行度量，并以此为基础对隐私保护机制的有效性建立评价方法，同时对隐私保护机制对隐私攻击手段的抗攻击能力建立测评方法.

3.4.1　隐私度量方法

针对隐私保护基本信息熵模型，直观地可以用条件熵和互信息在该模型下，对隐私保护机制保护下的隐私进行度量.

针对某一隐私信源，可以应用不同的隐私保护机制对隐私信源发送的隐私消息进行保护，调整能够让隐私信宿接收到的消息的概率分布，改变信宿的熵.以隐私信宿的视角，在接收到被保护后的隐私消息，仍然对隐私信源的隐私信息有一个平均不确定程度，这个程度应用隐私条件熵$H(X/Y)$做量化.记应用某一具体隐私保护机制P_i的对隐私信源X发送的消息件进行保护后的隐私条件熵为$H_{P_i}(X/Y)$,则期望该条件熵尽可能大.

平均互信息刻画的是经过信息传输后，信宿所接收到的平均信息量.隐私平均互信息$I(X;Y)$表示的是隐私信宿X在隐私保护机制的保护下隐私消息被隐私信宿Y所接收到的平均隐私信息量.记应用某一具体隐私保护机制P_i的对隐私信源X发送的消息件进行保护后，隐私信宿Y接收到的隐私信息为$I_{P_i}(X;Y)$,则期望该隐私互信息能尽可能小.

性质1 应用隐私条件熵和隐私互信息进行隐私度量，具有一致性.

证明: 由公式知

$$\begin{aligned} I(X;Y) &= \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i y_j)\log_2 \frac{p(x_i/y_j)}{p(x_i)} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i y_j)\log_2 \frac{1}{p(x_i)} - \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i y_j)\log_2 \frac{1}{p(x_i/y_j)} \\ &= \sum_{i=1}^{n} p(x_i)\log_2 \frac{1}{p(x_i)} - \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i y_j)\log_2 \frac{1}{p(x_i/y_j)} \\ &= H(X) - H(X/Y) \end{aligned} \tag{3.20}$$

故有$I(X;Y) = H(X) - H(X/Y)$,易知隐私信源熵是一个确定的值，隐私条件熵越大，则隐私平均互信息越小.

针对含敌手攻击的隐私保护信息熵模型，隐私度量主要是对隐私信宿本身含有的隐私信息量;敌手在背景知识条件下对发送者的隐私信息进行攻击时，发送者隐私信息的保护强度;以及在敌手攻击下，信息拥有者所泄露的隐私信息量.

隐私信宿本身含有的隐私信息量可用隐私信源熵$H(X)$的大小进行度量，其表示信息拥有者隐私信息的固有量的多少，一旦隐私信宿确定，则此隐私信宿所拥有的隐私信息量就是一个确定的值.

系统隐私度量综合考虑经过隐私保护和隐私攻击后，在一定背景知识条件下，隐私谋取者对信息拥有者的隐私信息的不确定程度$H(X/YZ)$;以及隐私谋取者观测信息拥有者发生的隐私事件所包含的隐私信息量$I(X;Y/Z)$.系统中应用隐私保护机制P_i进行隐私保护和隐私攻击A_r进行隐私攻击，则分别记$H_{P_i,A_r}(X/YZ)$和$I_{P_i,A_r}(X;Y/Z)$作为系统在抵

抗攻击A_y下采用P_i的隐私信息泄露的隐私度量值.$H_w(X)H(X_1X_2)$

3.4.2　隐私保护机制及隐私攻击评价

(1)隐私保护基本信息熵模型下的隐私保护机制评价

应用隐私保护机制对信息拥有者的隐私信息进行保护,$H_w(X/Y)$目标是使隐私信息尽可能少的被隐私谋取者所获得，即期望通过某种隐私保护机制，使得隐私谋取者得到的信息量$I(X;Y)$尽可能小，最好是0.

定义1 若在某种隐私保护机制的保护下，隐私平均互信息$I(X;Y)=0$(隐私信宿从隐私信源接收到的隐私信息量为0),则称该隐私保护机制对此信源是**完全隐私保护**的.

定义2 对同一隐私信源X分别应用隐私保护机制P_i和P_j对隐私消息进行保护，若$H_{P_i}(X/Y)<H_{P_j}(X/Y)$(或$I_{P_i}(X;Y)>I_{P_j}(X;Y)$),则称隐私保护机制$P_j$比隐私保护机制$P_i$**隐私保护有效性好**,简记偏序关系$P_i \prec P_j$.若$H_{P_i}(X/Y)=H_{P_j}(X/Y)$(或$I_{P_i}(X;Y)=I_{P_j}(X;Y)$),则称隐私保护机制$P_i$与隐私保护机制$P_j$**隐私保护有效性相等**,简记等价关系.$P_i \cong P_j$

定理1 设隐私保护机制有效性偏序关系与等价关系如定义2所定义，则偏序关系具有可传递性，等价关系具有自反性，可传递性，对称性.

证明: 若有$P_i \prec P_j, P_j \prec P_k$,则按照定义，对于隐私条件熵有$H_{P_i}(X/Y)<H_{P_j}(X/Y)$和$H_{P_j}(X/Y)<H_{P_k}(X/Y)$,故$H_{protection_i}(X/Y)<H_{protection_k}(X/Y)$,进而有$P_i \prec P_k$;对于隐私互信息有$I_{P_i}(X;Y)>I_{P_j}(X;Y)$和$I_{P_j}(X;Y)>I_{P_k}(X;Y)$,故$I_{P_i}(X;Y)>I_{P_k}(X;Y)$,进而有$P_i \prec P_k$.

证毕偏序关系的可传递性.类似地，易证等价关系的三个特性.

定义3 (隐私保护有效性距离) 在隐私保护基本信息熵模型下, 对同一隐私信源X分别应用隐私保护机制P_i和P_j对隐私消息进行保护，隐私信宿接收到的隐私信息量分别为$I_{P_i}(X;Y)$和$I_{P_j}(X;Y)$,则两种隐私保护机制的有效性距离为$d_I=\left|I_{P_i}(X;Y)-I_{P_j}(X;Y)\right|$.

在隐私保护基本信息熵模型下，隐私保护有效性距离刻画的是保护同一隐私信息的两种不同隐私保护机制有效性差异性大小.显然,d_I越小，两种隐私保护算法的有效性差异越小;d_I越大, 两种隐私保护算法的有效性差异越大.

(2) 含敌手攻击的隐私保护机制及隐私攻击评价

在实际的系统中，应用隐私保护机制对信息拥有者的隐私信息进行保护，目标是即使遭受敌手的各类隐私攻击，仍然使得信息拥有者的隐私信息尽可能少的被隐私谋取者所获得，即期望通过某种隐私保护机制抗敌手在一定背景知识下的隐私攻击，使得隐私谋取者得到的隐私信息量$I(X;Y/Z)$尽可能的小，最好是0.

定义4 对于带敌手攻击的隐私保护系统，若$I(X;Y/Z)=0$,即在敌手在拥有背景知识Z的攻击下，隐私保护机制能够使得信息拥有者的隐私信息泄露量为0，则称隐私系统是**完美隐私保护**的.

定义5 对同一隐私信源X,其与隐私信宿Y进行通信过程中受到敌手应用隐私攻击进行攻击A_r,系统分别应用隐私保护机制P_i和P_j对隐私消息进行保护，若$H_{P_i,A_r}(X/YZ) < H_{P_j,A_r}(X/YZ)(I_{P_i,A_r}(X;Y/Z) < I_{P_j,A_r}(X;Y/Z))$,则称在抗$A_r$攻击下，隐私保护机制$P_j$比隐私保护机制$P_i$**隐私保护有效性好**,简记偏序关系$P_i(A_r) \prec P_j(A_r)$.若$H_{P_i,A_r}(X/YZ) = H_{P_j,A_r}(X/YZ)(I_{P_i,A_r}(X;Y/Z) I_{P_j,A_r}(X;Y/Z))$,则称隐私保护机制$P_i$与隐私保护机制$P_j$**隐私保护有效性**相等，简记等价关系$P_i(A_r) \cong P_j(A_r)$.

定义6 (抗隐私攻击的隐私保护有效性距离)在含敌手攻击的隐私保护信息熵模型中，对同一隐私信源X,针对该信源的隐私消息有隐私攻击A_r,若在该隐私攻击下分别应用隐私保护机制P_i和P_j进行保护，隐私信源Y在该攻击下接收到的隐私信息量分别为$I_{P_i,A_r}(X;Y/Z)$和$I_{P_j,A_r}(X;Y/Z)$,则称两种隐私保护机制在隐私攻击A_r下的有效性距离为$d_I(A_r) = \left|I_{P_i,A_r}(X;Y/Z) - I_{P_j,A_r}(X;Y/Z)\right|$.

在含敌手攻击的隐私保护信息熵模型中, 抗隐私攻击的隐私保护有效性距离刻画的是保护同一隐私信息的两种不同隐私保护机制在同一种隐私攻击下的有效性差异性大小.显然$d_I(A_r)$越小，两种隐私保护算法的有效性差异越小;$d_I(A_r)$越大, 两种隐私保护算法的有效性差异越大.

定义7 对同一隐私信源X,其与隐私信宿Y进行通信过程中应用隐私保护机制P_i进行隐私保护，并分别受到敌手应用隐私攻击A_r和A_α进行攻击，若(),则称在隐私保护机制的保护下, 隐私攻击比隐私攻击的隐私攻击有效性更强，简记偏序关系.若$H_{P_i,A_r}(X/YZ) < H_{P_i,A_q}(X/YZ)(I_{P_i,A_r}(X;Y/Z) < I_{P_i,A_q}(X;Y/Z))$,则称在隐私保护机制$P_i$的保护下, 隐私攻击$A_r$与隐私攻击$A_\alpha$的**隐私攻击有效性相同**,简记等价关系$A_r(P_i) \cong A_q(P_i)$.

定理2 若偏序关系和等价关系如定义5或定义7所定义，则该偏序关系满足传递性，该等价关系满足自反性，对称性，可传递性.

证明: 略.

定义8 (隐私攻击有效性距离)在含敌手攻击的隐私保护信息熵模型中，对同一隐私信源X的隐私消息应用隐私保护机制P_i进行保护，并有隐私攻击A_r和A_α分别进行隐私攻击，隐私信源Y在不同攻击下接收到的隐私信息量分别为$I_{P_i,A_r}(X;Y/Z)$和$I_{P_i,A_q}(X;Y/Z)$, 则称两种隐私攻击针对隐私保护机制P_i的有效性距离为

$$d_I(P_i) = \left|I_{P_i,A_r}(X;Y) - I_{P_j,A_q}(X;Y)\right|$$

在含敌手攻击的隐私保护信息熵模型中, 隐私攻击有效性距离刻画的是针对同一种隐私保护机制的两种攻击方法的有效性及攻击能力差异性大小.$d_I(P_i)$越小，两种隐私攻击的有效性和攻击能力差异越小;$d_I(P_i)$越大, 两种隐私攻击的有效性和攻击能力差异越大.

在隐私保护系统中，敌手在实施攻击时通常具备一定的背景知识，假定背景知识空间为Z,则敌手截获通信系统的消息，背景知识总能提供一定关于隐私信息的信息.

定理3 在带敌手攻击的隐私保护通信模型中，隐私信宿X发送隐私消息，经过隐私保护和隐私攻击，被隐私信宿Y接收，若敌手已知背景知识空间Z,则$I(X;Y) \leqslant I(X;YZ)$.

证明:由平均互信息的计算方程知

$$I(X;Y) = H(X) - H(X/Y) \tag{3.21}$$

$$I(X;YZ) = H(X) - H(X/YZ) \tag{3.22}$$

令公式减去公式，得到

$$I(X;YZ) - I(X;Y) = H(X/Y) - H(X/YZ) \tag{3.23}$$

由于$H(X/Y) \geqslant H(X/YZ)$,故$H(X/Y) - H(X/YZ) \geqslant 0$,有$I(X;YZ) \geqslant I(X;Y)$.

该定理说明敌手在一定背景知识进行隐私攻击与分析, 敌手获得的隐私信息不少于其无背景知识情况下所能获得的隐私信息.同时也为隐私保护提供了一个方向，即尽可能使得敌手截取的隐私消息与其拥有背景知识关联程度尽可能小，从而最大限度的保护隐私信息.

(3) 其他隐私保护信息熵模型下的隐私保护机制及隐私攻击评价

上文讨论了隐私保护基本信息熵模型及其含敌手攻击情况下的隐私保护机制及隐私攻击评价，给出了隐私保护和隐私攻击评价的相关定义、定理和证明。鉴于隐私保护基本信息熵模型和含敌手攻击的隐私保护信息熵模型的基础性，针对这两个模型的评价方法可以通过有效扩展，直接或间接应用于其他隐私保护信息熵模型。

定义1所述完全隐私保护定义蕴含的隐私保护目标是在无敌手环境或敌手无隐私攻击能力情况下，系统对隐私保护机制的期望，可表示隐私保护机制设计的目标。该期望或隐身保护机制设计目标同样适用于其他无敌手隐私保护信息熵模型，故该定义可扩展于无敌手的带主观感受的隐私保护信息熵模型和无敌手的多隐私信源的隐私保护信息熵模型。类似的，定义2、定义3和定理1亦可通过引入隐私敏感偏好、多隐私信源联合，进而应用于这两种模型。

定义4所述完美隐私保护是在敌手进行隐私攻击时隐私保护机制设计的目标，该目标是一般隐私系统的通用性目标，同样适用于其他隐私保护信息熵模型。定义5和定义6是在受到一定隐私攻击条件下，对不同隐私保护机制效果的评价，该评价方法相对信源模型独立，故可进行一定的扩展应用到其他隐私保护信息熵模型中，如引入隐私敏感偏好并应用带权条件信息熵或带权条件互信息的比较，应用于带主观感受并含敌手攻击的隐私保护信息熵模型。

同样，定义7、定义8、定理2和定理3，经过相应的扩展和推广，可以很方便的应用于其他模型中。

3.5　实例分析

文中提出的隐私保护的信息熵模型及其度量方法可适用于多种场景，现基于一个简单的位置隐私保护场景对该模型进行分析.假设某用户u在一个被划分为M块的区域内移动，记$R=\{r_1,r_2,\cdots,r_M\}$为M块不同区域的集合，攻击者的目的是确定该用户所在的真实位置.

3.5.1　位置隐私保护基本模型

对应于含敌手攻击的隐私保护信息熵模型，隐私信源为用户可能所处的位置分布R,随机变量R表示用户u处于一位置区域，该变量的取值表示用户u处于具体区域r_i,用$\{r_1,r_2,\cdots,r_M\}$表示用户所处的位置区域空间，各区域的概率为$p(r_i)$,有$0\leqslant p(r_i)\leqslant 1$,$\sum_{i=1}^{M}p(r_i)=1$,该位置分布$R$的概率模型可以表示为:

$$\begin{pmatrix} R \\ P(R) \end{pmatrix}=\begin{pmatrix} r_1 & r_2 & \cdots & r_i & \cdots & r_M \\ p(r_1) & p(r_2) & \cdots & p(r_i) & \cdots & p(r_M) \end{pmatrix}$$

用户的真实位置分布信息是隐私信息，为防止攻击者直接获取用户所处的真实区域，需要对用户的位置分布R进行保护，经过位置隐私保护机制(包括位置泛化、取假名、隐藏或添加虚拟位置等)对位置分布R进行隐私保护处理后，变成可被攻击者直接观察到的可观察位置分布R',同位置分布R,易知$R'=\{r'_1,r'_2,\cdots,r'_{M'}\}$,其中$r'_i$表示用户$u$的经过隐私保护后可被攻击者观察到的所在区域, 可观察位置分布R'的概率模型为:

$$\begin{pmatrix} R' \\ P(R') \end{pmatrix}=\begin{pmatrix} r'_1 & r'_2 & \cdots & r'_i & \cdots & r'_{M'} \\ p(r'_1) & p(r'_2) & \cdots & p(r'_i) & \cdots & p(r'_{M'}) \end{pmatrix}$$

$$0\leq p(r'_i)\leq 1,\sum_{i=1}^{M'}p(r'_i)=1$$

攻击者获取到可观察位置分布R'后，结合背景知识，对用户u进行位置攻击，即得到攻击者对用户u的推断位置$\hat{R}$,同位置分布R,易知$\hat{R}=\{\hat{r}_1,\hat{r}_2,\cdots,\hat{r}_{\hat{M}}\}$,其中$\hat{r}_i$表示攻击者猜测用户$u$所处区域为真实区域, 其概率模型为:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix}=\begin{pmatrix} \hat{r}_1 & \hat{r}_2 & \cdots & \hat{r}_i & \cdots & \hat{r}_{\hat{M}} \\ p(\hat{r}_1) & p(\hat{r}_2) & \cdots & p(\hat{r}_i) & \cdots & p(\hat{r}_{\hat{M}}) \end{pmatrix}$$

$$0\leq p(\hat{r}_i)\leq 1,\sum_{i=1}^{\hat{M}}p(\hat{r}_i)=1$$

图5表示位置隐私保护场景的通信模型，可以看作含敌手攻击的隐私保护信息熵模型的一个具体实例.

3.5.2　相同背景知识下不同隐私保护机制的效果比较

在初始阶段，用户u处于一个真实区域r_i,则该用户处于区域r_i的概率为1，处于其它区域的概率为0，具体为:

$$\begin{pmatrix} R \\ P(R) \end{pmatrix} = \begin{pmatrix} r_1 & r_2 & \cdots & r_i & \cdots & r_M \\ 0 & 0 & \cdots & 1 & \cdots & 0 \end{pmatrix}$$

此时，隐私信源熵即位置分布R的熵为$H(R) = -\sum_{i=1}^{M} p(r_i)\log p(r_i) = 0.$

(1) 弱隐私保护强度的隐私度量

当系统采用的位置隐私保护机制是位置泛化时，我们取用户u的发布位置从区域r_i泛化到$\{r_{i-1}, r_i, r_{i+1}, r_{i+2}\}$,可得到可观察位置分布的概率模型如下:

$$\begin{pmatrix} R' \\ P(R') \end{pmatrix} = \begin{pmatrix} r'_1 & \cdots & r'_{i-1} & r'_i & r'_{i+1} & r'_{i+2} & \cdots & r'_{M'} \\ 0 & \cdots & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \cdots & 0 \end{pmatrix}$$

我们可以用$H(R') = -\sum_{i=1}^{M'} p(r'_i)\log p(r'_i) = 2$表示可观察位置分布的熵，等同于含敌手攻击的隐私保护信息熵模型下的熵$H(X/Y)$.

攻击者在获取到可观察位置分布后，结合其所拥有的背景知识进行分析，在一定的背景知识下，分析得到对用户u的推断位置分布的概率模型如下:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix} = \begin{pmatrix} \hat{r}_1 & \cdots & \hat{r}_{i-1} & \hat{r}_i & \hat{r}_{i+1} & \hat{r}_{i+2} & \cdots & \hat{r}_{\hat{M}} \\ 0 & \cdots & \frac{1}{4} & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \cdots & 0 \end{pmatrix}$$

此时我们可得$H(\hat{R}) = -\sum_{i=1}^{\hat{M}} p(\hat{r}_i)\log p(\hat{r}_i) = 1.75$表示攻击者在具有背景知识的条件下对用户所在位置的不确定度的度量，等同于敌手攻击的隐私保护信息熵模型下的熵$H(X/YZ)$.

(2) 强隐私保护强度的隐私度量

当我们取泛化位置区域变大时，即隐私保护手段变强后，我们取用户u的发布位置从区域$\{r_{i-1}, r_i, r_{i+1}, r_{i+2}\}$变到$\{r_i, r_{i+1}, \cdots \text{fi} r_{i+7}\}$,可观察位置分布的概率模型为:

$$\begin{pmatrix} R' \\ P(R') \end{pmatrix} = \begin{pmatrix} r'_1 & \cdots & r'_i & \cdots & r'_{i+7} & \cdots & r'_{M'} \\ 0 & \cdots & \frac{1}{8} & \cdots & \frac{1}{8} & \cdots & 0 \end{pmatrix}$$

得到$H(R') = -\sum_{i=1}^{M'} p(r'_i)\log p(r'_i) = 3$表示可观察位置分布的熵，攻击者在相同的背

景知识下，分析得到对用户u的推断位置分布的概率模型如下:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix} = \begin{pmatrix} \hat{r}_1 & \cdots & \hat{r}_i & \hat{r}_{i+1} & \hat{r}_{i+2} & \hat{r}_{i+3} & \hat{r}_{i+4} & \hat{r}_{i+5} & \hat{r}_{i+6} & \hat{r}_{i+7} & \cdots & \hat{r}_{\hat{M}} \\ 0 & \cdots & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{32} & \frac{1}{32} & \cdots & 0 \end{pmatrix}$$

此时我们可得$H(\hat{R}) = -\sum_{i=1}^{\hat{M}} p(\hat{r}_i)\log p(\hat{r}_i) = 2.3125$表示攻击者在具有背景知识的条件下对用户所在位置的不确定度的度量，等同于敌手攻击的隐私保护信息熵模型下的熵$H(X/YZ)$.

由$2.3125 > 1.75$可验证含敌手攻击的隐私保护信息熵模型下$H_{P_i,A_r}(X/YZ) < H_{P_j,A_r}(X/YZ)$成立.

3.5.3　相同隐私保护机制下不同隐私攻击的效果比较

(1) 弱隐私攻击强度的隐私度量

同3.5.2节弱隐私保护强度的隐私度量.

(2) 强隐私攻击强度的隐私度量

隐私保护机制同3.5.2节弱隐私保护强度的隐私度量，攻击者在获取到可观察位置分布后，结合其所拥有的背景知识进行分析，在强隐私攻击强度下，分析得到对用户u的更准确的推断位置分布的概率模型如下:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix} = \begin{pmatrix} \hat{r}_1 & \cdots & \hat{r}_{i-1} & \hat{r}_i & \hat{r}_{i+1} & \hat{r}_{i+2} & \cdots & \hat{r}_{M'} \\ 0 & \cdots & \frac{1}{6} & \frac{2}{3} & \frac{1}{12} & \frac{1}{12} & \cdots & 0 \end{pmatrix}$$

此时我们可得$H(\hat{R}) = -\sum_{i=1}^{\hat{M}} p(\hat{r}_i)\log p(\hat{r}_i) = 1.418$表示攻击者在具有背景知识的条件下对用户所在位置的不确定度的度量，等同于敌手攻击的隐私保护信息熵模型下的熵$H(X/YZ)$.

由$1.418 < 1.75$可验证含敌手攻击的隐私保护信息熵模型下$H_{P_i,A_r}(X/YZ) < H_{P_i,A_q}(X/YZ)$成立.

3.6　小结

本章基于Shannon信息论提出了几种隐私保护信息熵模型，其关键出发点是将隐私保护系统视为一种通信模型，通过定义信源、信宿和信道、引入信息熵、平均互信息量、条件熵及条件互信息等概念，初步给出了不同场合的隐私信息度量、隐私泄露度量、隐私保护强度量化和攻击能力量化等方法，并且初步考虑了含隐私信息主观感受的信息熵模型. 本文的工作虽然只给出了较为基本的信息熵模型，但为解决隐私保护系统的量化问题建立了一个可行的体系基础，相信在信息论相关成果的支撑下，其相关

研究可以不断深入，包括连续隐私信源的研究、更复杂的多隐私信源模型、基于随机过程的信息熵模型、贝叶斯隐私信息熵模型和马尔柯夫隐私信息熵模型等，都具备了深入研究的可行性。同时，由于隐私信息带有时空性、主观性、模糊性，下一步拟考虑采用广义信息论、模糊信息论等研究隐私信息熵模型。

第四章　基于结构信息论的隐私度量模型

第五章　相互独立的序列型数据的隐私属性推断模型及其应用

基因序列数据、连续轨迹位置数据等呈现序列化，此类数据在很多共享应用场景（如疾病诊断、车联网导航）中需要非匿名化，需要对其敏感的属性隐私（特定基因座的基因型，特定行车位置）进行保护。保护这些隐私，需要更加深刻的理解隐私泄露的原因。本章针对基因序列数据的基因座值属性隐私，通过对单条敏感数据记录属性值存在的相互关联关系进行分析，构建目标属性值推断的敌手模型，并以此为基础利用抽样、隐马尔可夫推断、卷积神经网络构建概率推断算法，针对不存在亲属关系的群体型基因序列数据共享场景，分析隐私属性泄露情况，通过量化隐私泄露量和敌手获取隐私量等信息，提高对序列型数据属性隐私的认识和理解。本章的相关成果已发表在《*Information Sciences*》上。

5.1　概述

随着测序技术的进步，人们能够更轻松、更便宜地对其DNA进行测序，人类基因组数据已变得越来越可负担和可用。例如，在1000 Genomes项目[68]中，数千名匿名参与者将其DNA数据捐献给了生物医学和精准医学研究。美国、英国、加拿大、法国和中国政府也出于医学和其他原因启动了基因组数据采集项目。此外，越来越多的人，因为娱乐、找与自己想似的病人、或找自己的亲属等原因，通过23andMe.com、PatientsLikeMe.com和Ancestry.com等网站在线分享他们的基因组数据。同时，通过基因组数据可以唯一确定识别一个人，也可以通过基因组数据识别特定的表现型和疾病。然而，基因组数据可用性的提高带来了更加突出的安全和隐私挑战。一旦这些数据被披露或滥用，一个人就可能会面临就业、保险、教育等多方面的歧视风险[69]。

实际上，许多研究结果和实际案例已经引起人们对基因组数据的机密性和隐私性的担忧。在某些情况下，以匿名方式收集的基因组数据仍可能以各种方式泄露个人的敏感信息。例如，Sweeney等[70]通过将个人基因组计划中不公开的姓名和联系信息链接起来，重新识别个体;Gymrek等[71]通过分析 Y 染色体上的短串联重复序列，重新识别个体。全基因组关联研究（Genome-Wide Association Study, GWAS）的结果可用于识别个体[72]。某些疾病的易感性[73]和基因表现型外观特征[74]也可以从基因组数据中推断出来。个人基因组数据的泄露不仅会对其个人隐私造成威胁，而且还会以家族身份[75]或有关亲属基因型信息的形式对其亲属的隐私造成威胁[30]。最近，已经证实遗传学家可以从基因组数据中恢复特定个体的面孔[76]，共享的基因组数据也有可能被恶意机构滥用[77]。

实际情况可能会更糟，为了保护个人自身的基因组隐私，通常他或她可以选择删除或隐藏其基因型的某些部分[78]，只向第三方(如医院或基因组研究机构)共享部分基因组数据。许多没有亲戚关系的人可以通过这种方式共享他们的基因组数据似乎是安全的。但是，这并不有效。在本章中，我们将揭示敌手可以利用该个体的共享部分基因组数据和其他公开可用的基因组数据，稳健地重构个体的基因组数据。

在本章中，我们将提出两种用于重构单个基因型序列的推断攻击方法：一种基于改进的离散隐马尔可夫模型（Improved Hidden Markov Model, iHMM），另一种基于回归卷积神经网络（Convolutional Neural Network, RCNN）模型。这些推断攻击模型既考虑了观察到的被攻击者基因组数据，也考虑了公开可用的基因组数据。我们还将提出度量指标，以量化被攻击者的基因组隐私以及有关不正确性、不确定性和隐私损失的攻击的严重程度。与Samani等[79]先前的工作相比，我们的贡献如下：

- 提出一个针对基因组隐私推断攻击的统一敌手模型，目的是从被攻击者部分观察到的基因组数据中重建不相关个体的基因型序列。
- 提出一种针对不相关个体的基因组隐私推断攻击策略，该策略利用IMPUTE2[80]中单核苷酸多态性(SNPs)和抽样重组模型方法进行关联分析。
- 提出一种采用RCNN的针对不相关个体的基因组隐私推断攻击方法，并研究在基因组隐私攻击背景下机器学习（例如RCNN）的大规模隐私分析攻击功能。
- 从信息量的角度量化隐私推断攻击能力、量化基因隐私量，其代表了攻击者对隐私信息不确定程度的降低和被攻击者基因隐私损失量的增加。
- 与以往的工作相比，我们的结果具有更高的准确性，对推断的基因组数据的不确定性更低，被攻击者的隐私信息损失更大。

5.2　相关工作

5.2.1　基因序列隐私推断攻击

推断攻击利用可用数据通过数据分析来推断潜在的私人信息[81]，是一种非常有效的隐私和安全攻击策略。推断攻击在位置跟踪[82]、社交网络上的属性隐私[83]、机器学习中的成员和属性隐私[35,84]、高级密码学的脆弱性（例如，加密数据库和可搜索加密）[85] 和基因组隐私（例如，成员基因组隐私[86]、基因型隐私[79,87]和亲属隐私[30]）。如文献[88]所述，推断攻击对社交网络，基因组共享，GWAS研究和临床医学等领域的基因组数据构成了巨大的隐私威胁。

本章中，我们重点关注如何基于被攻击者的共享SNP数据（其中隐藏了敏感的SNP数据）和公开可用的基因组数据在推断攻击中损害基因型隐私。

5.2.2　基因组数据隐私泄露

尽管诸多文献关注统计基因组隐私的泄露问题，但其中大多数都与去匿名化的个体识别隐私有关，并依赖于成对连锁不平衡（Linkage Disequilibrium，LD）。Homer等[89]对GWAS统计数据进行的遗传隐私研究表明，可以从参与人的基因型推断出GWAS其疾病状态，人们开始考虑不再为GWAS研究和医学测试捐赠基因组数据。随后，去身份识别被认为不足以保护遗传隐私和机密性。对于许多公开领域数据库，例如美国国立卫生研究院（NIH）的基因型和表现型数据库（dbGaP）[90-91]，访问规则已更改为根据其基因组数据需求进行控制性访问。Wang等[86]的研究结果表明，GWAS结果可以推断个人身份和疾病。即使公开GWAS目录中的数据经过差分隐私保护的，它仍然包含GWAS参与者的个人特征和身份，可以通过基于背景信息的挖掘来攻击个人的这些隐私[92]。通过使用公开的性状位点和表现型数据集，也可以通过将表现型与基因型联系起来分析获取个体的遗传隐私[93]。

本章的研究重点是基因型的隐私性，而不是基于基因组数据的身份隐私[86,92]或疾病状态隐私[86,89]。尽管我们的工作也是针对公开可用的基因组数据，但我们并不需要像文献[86,92-93]中的中那样的性状位点和表型现型数据。我们仅需通过基因共享网站（例如，PatientsLikeMe.com和23andMe.com）捐赠的可观察SNP序列数据以及来自基因研究项目（例如，HapMap项目和1000基因组项目）的公开基因组数据，即可建立隐私分析攻击模型获取基因型隐私信息。

在文献[94]中，作者提出了一种利用基因表达数据推断特定位点个体基因型的贝叶斯方法。Humbert等[30]利用家族关系和成对LD提出了一种基因型推断攻击方法。Samani等人[79]利用各种高阶单核苷酸变体(Single Nucleotide Variant，SNV)相关模型探索了对不相关个体的基因型推断攻击，提出了一种结合和扩展[30] 和[32]工作来推断家族成员基因型的方法。本章中，我们的目的是进行大规模SNP序列的基因型隐私信息推断，而非像在[30] 和[32]中那样，在特定的位点[94]或亲属基因组进行基因型隐私推断。本章提出的基因型隐私推断攻击是针对[79]中相同场景提出的，即在线发布基因组数据共享、应用过程中的隐私问题。与[79]中所提出的利用部分隐藏信息的已公开遗传序列数据、公开可用的参照基因数据等基因组信息的工作相比，本章所介绍的隐私分析推断攻击模型在性能和方法上都得到了提高。本章所提出的基于iHMM的隐私分析推断攻击模型是对[79]中提出的基于重组模型的推断攻击的改进，将隐藏SNPs的基因型隐私分析推断分为多个步骤，而不是直接对基因型进行推断。在该攻击模型中，我们将马尔可夫链蒙特卡罗抽样策略与隐马尔可夫推断模型相结合，计算条件分布，大大提高了攻击能力。此外，提出的基于RCNN的基因隐私推断攻击模型是一种新的基因型隐私属性重构模型。虽然机器学习在基因组学研究[95]中得到了广泛的应用，但较少涉及基因组隐私问题，本章将RCNNs应用于隐藏SNP序列基因型隐私的大规模推断和基因组隐私的量化，促进机器学习算法在序列型隐私分析的应用。

5.3　相关背景知识

在本节中我们简要介绍有关基因组学、HMMs和RCNNs的一些知识。

5.3.1　基因组

人类基因组的简要概述如图 5.1所示[79]，人类有23对染色体，人类基因组被编码为DNA，包含大约30亿个核苷酸对。每个染色体都具有双螺旋结构，由两个互补的核苷酸（A，T，G和C）聚合物链组成。人类可以通过他们的DNA来唯一标识某一个体。99%的人类DNA在所有个体中共享，只有0.5%基因组在不同个体间互不相同。人类基因组由不同的等位基因（A，T，C和G）编码。一个染色体上的等位基因组称为单倍体基因型，一对染色体上的等位基因对组称为二倍体基因型[96]。

单核苷酸多态性(Single Nucleotide Polymorphism，SNP)是发生在基因组特定位置的单核苷酸的变异。每一种变异在一个种群中都有一定程度的存在。相比之下，单核苷酸变体（SNV）是单个核苷酸的变异，不受频率的限制。一个特定个体的SNP序列与其他个体的SNP序列非常不同。因此，可以通过他或她的SNP序列来识别一个人。SNP序列与某些性状和疾病相关，全基因组关联研究(GWAS)是对不同个体的SNP序列进行观测与关联分析性研究，以确定给定的SNP是否与特定性状或疾病相关。

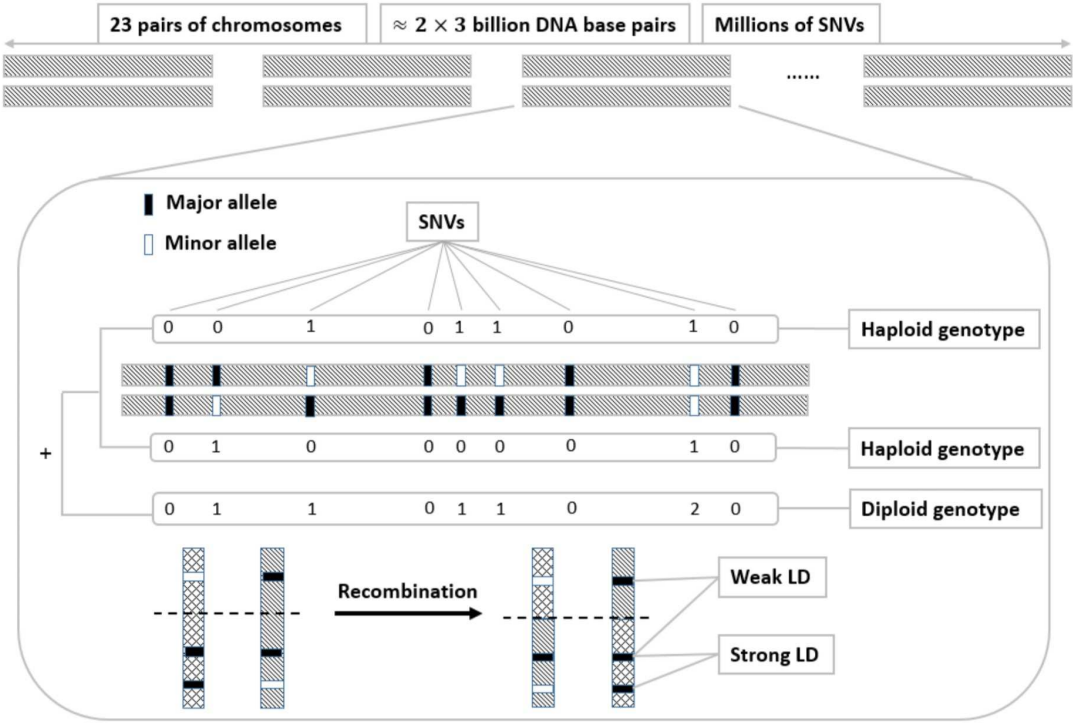

图 5.1: 人类基因组概览[79]

为方便起见，每个SNP位点的三个可能状态（分别为AA，Aa和aa）用0、1和2表示，具体数值取决于每个基因位点上次要等位基因的数量。

连锁不平衡（Linkage disequilibrium，LD）被定义为等位基因在两个或多个位点上的对应关系或非随机关联关系。这种关联关系是遗传机制的结果，即某一个群体有足够的进化时间，基因随机重组的出现将在所有位点产生等位基因的平衡分布。对LD建模的方法有几种，本文中我们主要应用混合建模的LD数据，该建模方法同时考虑了参照基因型数据集和基因重组率的影响。

在遗传过程中，基因重组是一个子过程，在该过程中，一些DNA片段被分离并重新组合，形成新的等位基因组合。基因重组过程产生了所有生物的遗传多样性，基因重组与LD是直接相关的。

5.3.2　隐马尔科夫模型

隐马尔可夫模型（Hidden Markov Model, HMM）[97-98]是一种状态不可观测的统计马尔可夫模型，可以通过简单的动态贝叶斯网络表示。具体来说，本章的研究过程中采用了三个假设：（1）t 时刻的状态是由某个状态为 S_t 隐藏的过程生成的；（2）该过程具有马尔可夫性；（3）隐藏的状态变量是离散的。HMM可用于表征诸如相似性、解码和学习等基本问题。目前，HMM在语音识别[97]、手写识别[99]、基因预测[96]等领域得到了广泛的应用。

本章考虑的问题在某种程度上类似于参数学习问题。由于在给定观测或发射序列的推断过程中，所有隐藏状态变量的后边缘都可以通过计算得到，因此我们考虑采用正向-反向算法。

5.3.3　卷积神经网络

最近，卷积神经网络(Convolutional Neural Networks, CNNs)[77,100]已成为解决图像分类、分割和回归问题的一种流行方法。但是，尚未开发出回归CNN（RCNN）体系结构（其中最后一层是回归层的CNN）来预测基因型序列。与传统的分类分割问题不同，CNN的输出是离散值[77]，而RCNN的输出是连续的。

在章工作中，类似于缺失值预测问题，我们设计了用于单倍型序列预测的RCNN架构。首先，使用公开单倍型数据集来训练和测试所提出的RCNN模型。建立RCNN预测模型后，首先将观测到的二倍体基因序列解析为单倍体，进而推断SNP序列上隐藏SNP基因型，并将其应用于攻击个体的基因型序列隐私信息。

5.4　敌手模型和量化评估指标

5.4.1　敌手模型

本节提出的敌手模型主要针对现实世界中涉及基因组数据共享的场景。在这种情况下，被攻击对象共享其SNP序列用于研究、医学测试或寻找亲属。由于隐私保

护的需求，被攻击者希望隐藏某些可能与遗传病或私人特征有关的敏感SNP。因此，被攻击对象共享其原始SNP序列的变体 $\hat{X}=(\hat{x}_1,\hat{x}_2,...,\hat{x}_n)$，其中 $\hat{x}_i=\{0,1,2\}$，并隐藏其中某些SNP。假设隐藏的SNP用X_H表示，可观测的SNP用 X_O 表示，公开的SNP用 $X=(x_1,x_2,...,x_n)=X_H\cup X_O$，其中 $x_i=\{-1,0,1,2\}$，值 $x_i=-1$ 表示$x_i\in X_H$是隐藏的SNP。假设已观测被攻击者公开SNP X 序列数据的敌手想要重构原始SNP序列 $\hat{X}$。为此，敌手可以通过推断攻击侵入被攻击者的基因组隐私（例如获得其APOE基因状态[101]。要进行这样的推断攻击，敌手将收集一些公开可用的基因组信息[103?]，例如受害人所属人群的次要等位基因频率（MAF）、LD值、遗传重组率和单倍体基因型参照，如图 5.2 所示。

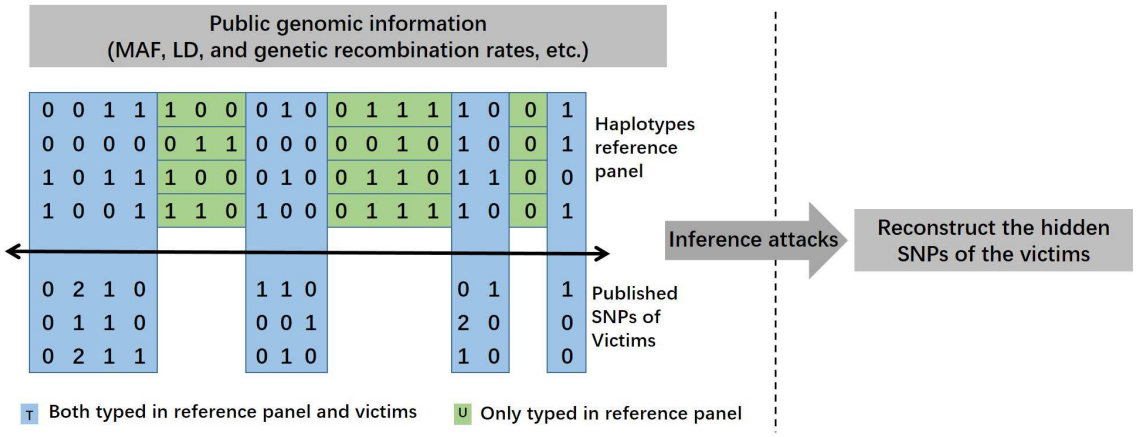

图 5.2: 基因序列数据属性值隐私分析敌手模型概览

假设可访问的公开基因组信息用$INFOR_{Pub}$表示，推断的SNP序列用$\bar{X}=(\bar{x}_1,\bar{x}_2,...,\bar{x}_n)$表示。基于基因型隐私的推断攻击的敌手模型$infer$可以形式化地表示为

$$\begin{aligned}\bar{X}&=infer(X,INFOR_{Pub})\\&=infer(X_H,H_O,INFOR_{Pub}).\end{aligned}\tag{5.1}$$

更具体地说，基因序列数据属性隐私推断攻击可以看作是给定已发布的SNP和公开基因组信息，计算每个隐藏SNP的条件边缘概率分布的过程，即

$$Prob(X=\{0,1,2\})=Prob(X|(X_O,INFOR_{Pub})).\tag{5.2}$$

对于每个隐藏SNP位点的隐私数值，其预测值是条件概率最高的那个值。

5.4.2　量化评估指标

为了量化敌手在基因组隐私推断方面的能力，本章使用Ayday等[104]引入的基因组隐私度量方法，从而评估对手通过推断攻击可以在多大程度上损害被攻击者的基因组

隐私。如同Wagner[105] 所述，有几种不同的基因组隐私度量方法适用于本章的研。在本章中，假设对手的目标是隐藏的推断SNP序列的隐私属性值，且仅考虑个体实际拥有的SNPs。我们应用正规不正确性（即敌手的不正确性），正规熵（即敌手的不确定性）和正规互信息（即被攻击者的隐私损失）来量化推断攻击模型的隐私分析能力。

作为基因组隐私度量，正规不正确性可以表示为

$$E = 1 - \frac{\sum_1^n | \bar{x}_j - \hat{x}_j |}{| X_H |}, \tag{5.3}$$

其中 n 为被攻击者的SNP数量，$\bar{x}_j$ 为推断出的SNP在 j 位点的基因型值，$\hat{x}_j$ 为SNP在 j 位点的原始基因型值，$| X_H |$ 为属于被攻击者隐藏的SNP数量。

尽管不正确性是衡量隐私权的有力指标，但由于被攻击者SNP的原始值不可用，因此它并不适合许多场景。在这些情况下，我们需要其他指标。在本章中，我们采用正规熵来表示敌手的不确定性，该度量可以根据所推导的SNPs的正规熵来评估。特别地，

$$H = \frac{\sum_{j=1}^n \frac{H(X_j)}{log(3)}}{| X_H |}, \tag{5.4}$$

其中$H(X_j) = -\sum_{\bar{x}_j=\in\{0,1,2\}} p(\bar{x}_j) log(p(\bar{x}_j))$ 为推断出的SNP在j位点的熵，$log(3)$为j位点SNP的最大熵，$| X_H |$ 为被攻击者的隐藏SNP数。

该度量标准根据敌手的能力而不是被攻击者的隐私损失来量化对手在其推断攻击中的置信度。如本文第三章所述互信息可以作为这种度量的基础，为此，我们利用不确定性的递减来表示敌手在推断攻击前后对隐藏SNPs的不确定性的变化。因此，本章使用正规互信息来量化敌手对被攻击者的平均隐私损失，由于互信息的估计是一个困难性问题，依赖条件概率的分布，故本章利用熵的变化量来估计互信息，即

$$I = \frac{\sum_{j=1}^n \frac{H_{MAF}(X_j)}{log(3)}}{| X_H |} - H, \tag{5.5}$$

其中$H_{MAF}(X_j) = -\sum_{x_j=\in\{0,1,2\}} p_{MAF}(x_j) log(p_{MAF}(x_j))$ 表示SNP在j位点的自然熵，$p_{MAF}(x_j)$为根据MAF数据集SNP发生的概率。公式 5.5 中定义的度量表示推断攻击引起的熵变化量，从而可以度量推断攻击的能力，它还可以评估被攻击者在推断攻击时的基因组隐私损失。

5.5　所提出的序列型数据隐私分析方法

在这一节中，对于所使用的敌手模型，我们提出了两种推断攻击策略，一个是基

于改进的HMM (iHMM)的隐私推断方法，另一个是基于RCNN模型的隐私推断方法。

5.5.1　基于iHMM的隐私分析推断

为了提高基因组隐私推断的性能，我们选择不像[79]中那样直接推断被攻击者的隐藏的SNP基因型，而是受IMPUTE2[80]基因型插补方法的启发，我们将攻击过程分为三个步骤：(1) 使用马尔可夫链蒙特卡罗抽样策略将观测到的被攻击者的SNPs分阶段转为单倍型；(2) 使用HMM模型分别推断每个被攻击者的隐藏单倍型基因型数值；(3)结合对每个被攻击者推断的单倍型结果，形成推断的基因型序列。

在模型的详细构建中，我们将参照组和被攻击者的SNPs分为 T (同时出现在参照组和被攻击者中的SNPs)和 U (不出现在被攻击者中，但出现在参照组中的的SNPs)。我们假设有 n 个被攻击者， H_R^T 表示 T 中SNPs的参照单倍型集合， H_V^T 表示被攻击者在 T 中观察到的SNPs的单倍型集合， H_V^U 表示与 U 中SNP序列相对应的被攻击者隐藏的单倍型集合， $H_V^T = \{H_{V,1}^T, H_{V,2}^T, ..., H_{V,n}^T\}$ 表示 T 中与SNP序列对应的被攻击者单倍型，其中$H_{V,i}^T$表示第i个被攻击者的单倍型，ρ表示群组基因重组映射率。

更具体地说，基于iHMM的推断攻击可以分三个步骤进行，详细说明如下：

(1) 敌手根据观察到的被攻击者的基因型，随机产生 H_V^T 的单倍型。然后，敌手通过多轮马尔可夫链蒙特卡罗迭代更新 H_V^T 中的单倍型。在每次迭代中，敌手通过从 $P(H_{V,i}^T | G_{V,i}^T, H_{V,-i}^T, H_R^T, \rho)$ 中抽样来更新第 i 个被攻击者的阶段性单倍型对 $H_{V,i}^T$ 。

(2) 敌手通过基因重组模型利用HMM模型推断H_V^U中的单倍型。在每次迭代中，敌手根据条件分布$P(H_{V,i}^U | H_{V,i}^T, H_R^{T \cup U}, \rho)$推断第$i$个被攻击者对应$U$中的SNPs的隐藏单倍型对$H_{V,i}^U$。

(3) 敌手把对每个被攻击者推断出来的单倍型对组合起来，得到被攻击者隐藏的SNPs的推断基因型。

在步骤(1)中每次迭代的分阶段步骤中，抽样条件为k个最接近的单倍型，其结果由其到第i个被攻击者的汉明距离确定。基于基因重组过程，利用HMM模型来推断计算条件分布，采用蒙特卡罗方法重构基因解析空间。因为推断得到的状态空间包含H_R^T中单倍型的所有状态和$H_{V,-i}^T$中当前猜测的单倍型，所以可以获得更多隐私关联信息。

在步骤(2)中，HMM状态空间包含了所有参照单倍型 $H_R^{T \cup U}$ ，此步骤类似于[79]中基于基因重组模型的过程，该模型受[106]的启发。然而，我们推断每个被攻击者的单倍型数值，而不是直接推断基因型数值。

步骤(1)至(3)中描述的攻击策略与文献[79]中描述的攻击策略不同，后者直接推断隐藏SNP的基因型值。在本章中，敌手结合了马尔可夫链蒙特卡洛抽样和HMM推断技术，提高了目标SNP序列的条件分布所获得的隐私分析结果。

5.5.2　基于RCNN的隐私分析推断

基于RCNN的攻击也分为三个步骤，步骤(1)和(3)与基于iHMM的攻击是相同的，只有步骤(2)不同。同样地，敌手观察公开的基因组信息和被攻击者SNP序列，将基因型分为单倍型，分别推断出隐藏的单倍型对，然后将推断出的单倍型对组合成基因型。在这里，我们将基于RCNN攻击的步骤(2)做说明如下。

我们构造基于RCNN的基因序列属性隐私分析目标模型为

$$H_{V,i}^{U} \leftarrow RCNN(H_{V,i}^{T}, H_{R}^{T\cup U}), \tag{5.6}$$

其中，给定一个参照单倍型集和一个基于观察到的SNPs的相位单倍型集，公式5.6的目标是推断这些隐藏部分的值（即，0或1）。由于被攻击者的公开参照单倍型和观察到的SNPs都属于同一群体（如CEU或CHS[107]），因此这些数据具有相同的特征，可以通过神经网络进行分析。

我们对参照数据$H_{R}^{T\cup U}$提出了一个RCNN模型，将这些数据分成两组：一组是训练集$H_{Rtrain}^{T\cup U}$，另一组是测试集$H_{Rtest}^{T\cup U}$。然后我们对最小值$min(\|H_{Rtest}^{U} - \hat{H}_{Rtest}^{U}\|)$的目标选择最佳训练网络，其中$\hat{H}_{Rtest}^{U}$表示测试集的预测值。敌手可以使用这个优化的网络来推断被攻击者单倍型的隐藏值，具体过程如图5.3 所示。

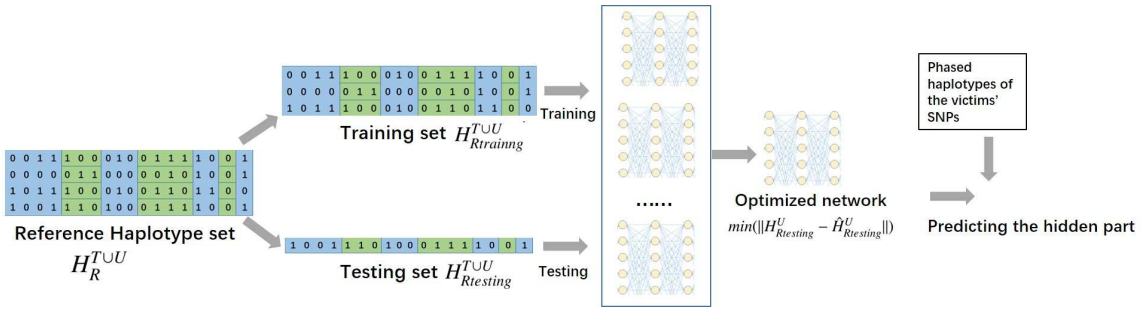

图 5.3: 基于RCNN的隐私分析模型

基于RCNN的基因隐私分析过程如图5.4所示（其中，Conv为卷积层, NA为正规化层, FC为完全联通层），该过程包含8层网络，输入由观察到的SNPs的单倍型组成，最后一层回归层生成隐藏SNP序列的单倍体型值。最后一层是代表隐藏SNPs的单倍型的回归层。在训练阶段，RCNN能够提取基因型的影响因子，检验MES是否收敛。利用RCNN训练得到的分类器，可以对测试数据集中的隐藏SNP序列的单倍型值进行推断。.)

该网络可实现两项主要任务：特征提取和预测。该网络包括八层，两个卷积层（Conv1和Conv2）、两个最大池层（Maxpool1和Maxpool2）、一个整流线性单元层（ReLU）和一个归一化层(Norm)，ReLU层减少了训练所需的时期数，但是因此其错误

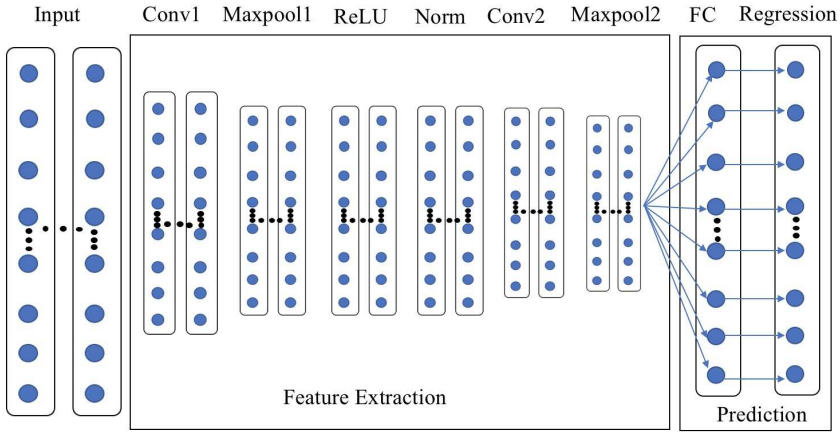

图 5.4: 基于RCNN的基因隐私分析过程

率比传统的双曲正切单位更高。规范层提高了通用性，降低了错误率。值得注意的是，ReLU层和Norm层并不会改变特征映射的大小。池化层汇总了相邻池化单元的输出。预测步骤完全由连接（FC）层和回归层执行。输入层由8×1个影响因子组成(1个月)，Conv1和Conv2各自的过滤器大小（F）为1×1，并且过滤器的数量（N）为25，填充大小（P）为0，Maxpool1和Maxpool2的步长(S)为2×2。因此，在每个max池层之后，特征图的维数除以2。

为训练RCNN模型，我们最小化损失函数，使用均方误差（MSE）作为损失函数，其定义为

$$\text{Loss}=\frac{1}{N}\sum_{i=1}^{N}|d_t^i-d_o^i|^2, \tag{5.7}$$

其中N是数据集中的条目数，下标i表示数据集中的第i个点位。

5.5.2.1　基于RCNN的单倍体型SNP值推断

如图5.4所示，一旦在Maxpool2层中提取了额外的特征，我们就可以将其连接到FC层，并将所有的特征压缩成一个维度。在训练过程中，如果在当前迭代次数未达到期望的MSE，则训练将继续进行，直到达到最大的迭代次数或所期望的MSE。如果达到最大迭代次数，则无论MSE值如何，训练过程都会停止。为了验证该方法的可行性和实用性，将测试数据集输入训练好的RCNN模型中，并利用该模型预测隐藏SNPs的单倍型，从而对总体性能进行评估。

5.6　实验及对比

在本节中，将根据各种指标评估本章提出的攻击方法的性能，并基于一组精心设计的实验所得到的结果，与之前的工作进行比较。

5.6.1　数据集

在这些实验使用了来自HapMap项目[108]第三期的数据集，该数据集在互联网上是公开的。在这个项目中，从世界各地11个不同的人群中收集匿名的基因组数据用于基因研究。在不失一般性的前提下，本章采用了2010年5月发布的北欧和西欧祖先(CEU)人群22号染色体的数据集。该数据集包含了个体的单倍型序列，并且还包括了这些群体的MAFs、成对LD值和基因重组率。我们将这些数据视为公开背景数据。此外，HapMap项目数据集中也包含165个个体的基因型序列。本章将使用这些数据作为选择的无关亲属的基因组数据，同时这个数据集也在文献[79]中使用过。

5.6.2　实验结果

在本节的实验中，随机隐藏被攻击者SNPs的不同百分比(从5%到60%)，使用所提出的攻击模型推断隐藏的SNPs，并根据第 5.4节中所描述的三个指标量化基因组隐私结果。

首先，随机隐藏10%的被攻击者的SNP，并使用不同的攻击模型评估敌手的推断能力。然后，进行20次实验，取每个指标对所有被攻击者的平均值。对基于iHMM和RCNN模型评估攻击，敌手的不正确性、敌手的不确定性和被攻击者的隐私损失结果如表 5.1所示。在此表中，M1-LD，M2和RM分别表示文献[79] 中基于一阶马尔可夫链（利用公开二元LD数据），二阶马尔可夫链和基因重组模型的推断攻击，而iHMM和RCNN分别表示基于iHMM和RCNN模型的推断攻击。在错误率列中比较了不同推断攻击的不正确性，本章提出的两种方法结果都显示出在不正确性指标上总体上明显降低，与RM方法相比，iHMM的性能更好，而RCNN的性能稍差。因为文献[79]中的作者在其论文中没有考虑不确定性和隐私损失的度量，所以本节根据计算这两个度量的需要，对其实验进行了改进。结果表明，这两种度量方法同样适用于基因组隐私的测量，在表 5.1的正规熵列和正规隐私损失列中分别显示了不确定性和隐私损失方面的性能结果。结果表明，利用基于iHMM的推断攻击，敌手可以获得较低的不确定性，并获得更多被攻击者的隐私信息。

为了进一步支撑比较结果，并与文献[79]中提出的实验保持一致，本节进行了另一个含有40%隐藏SNPs的实验。性能结果如表 5.2所示，结果表明与表 5.1中的结论一致，本章所提出的隐私分析方法能够在各种指标对比下获得更好的优势。

接下来，为了观察隐藏SNPs数量对不同推断攻击的影响，本节又进行了一组实验，实验中使用了不同比例(5% - 60%)的隐藏SNPs对LD、2阶马尔可夫链、重组模型、iHMM和RCNN攻击。敌手的不正确性、敌手的不确定性和敌手的基因组隐私损失结果分别如图 5.5、图 5.6和图 5.7所示。

在图 5.5中，根据敌手的不正确性展示了基于不同模型的推断攻击的结果。当被攻击者少量的SNPs被隐藏时，可以观察到这些攻击的推断能力会增加（即，被攻击

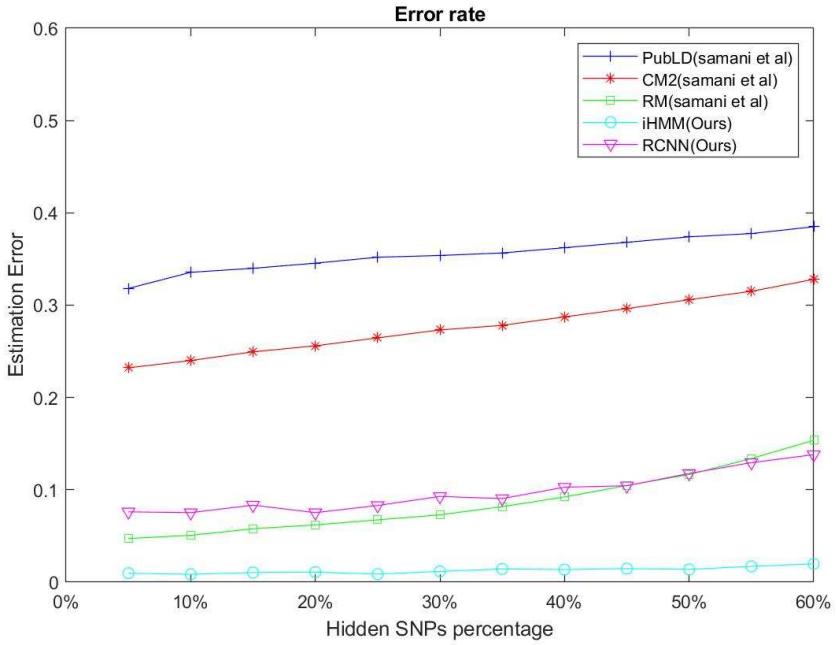

图 5.5: 不同基因隐私分析模型的基因组隐私变化对比（攻击者错误率）

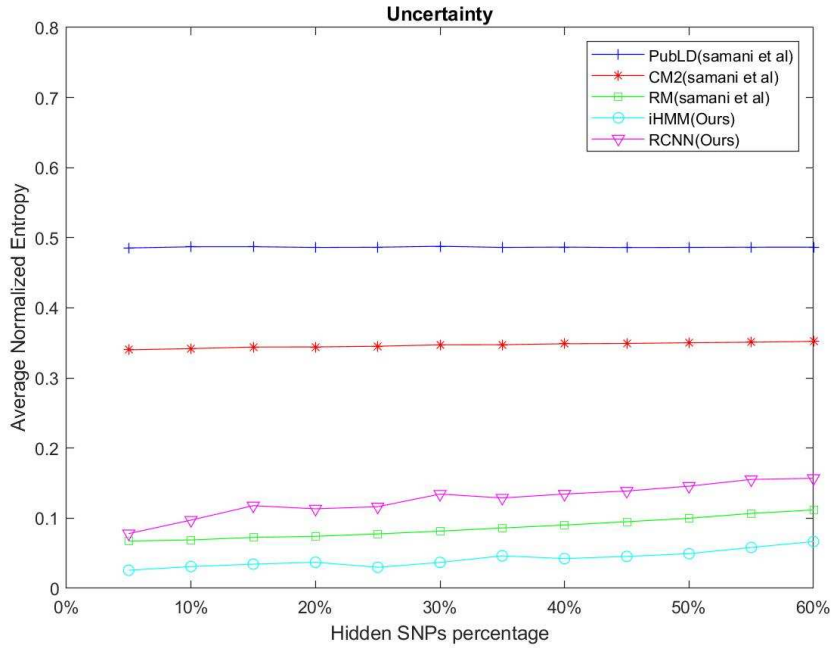

图 5.6: 不同基因隐私分析模型的基因组隐私变化对比（攻击者不确定性）

表 5.1: 当10%SNP序列被隐藏时，不同基因隐私分析攻击效果对比

	Error rate	Normalized entropy	Normalized privacy loss
M1-LD (Samani et al.)	0.3356	0.4872	0.1864
M2 (Samani et al.)	0.2400	0.3419	0.3316
RM (Samani et al.)	0.0578	0.069	0.6046
iHMM (Ours)	0.0085	0.0295	0.6520
RCNN (Ours)	0.0753	0.0973	0.5143

表 5.2: 当40%SNP序列被隐藏时，不同基因隐私分析攻击效果对比

	Error rate	Normalized entropy	Normalized privacy loss
M1-LD (Samani et al.)	0.3623	0.4867	0.1873
M2 (Samani et al.)	0.2873	0.3489	0.3251
RM (Samani et al.)	0.0923	0.0902	0.5838
iHMM (Ours)	0.0136	0.0430	0.6342
RCNN (Ours)	0.1028	0.1345	0.5347

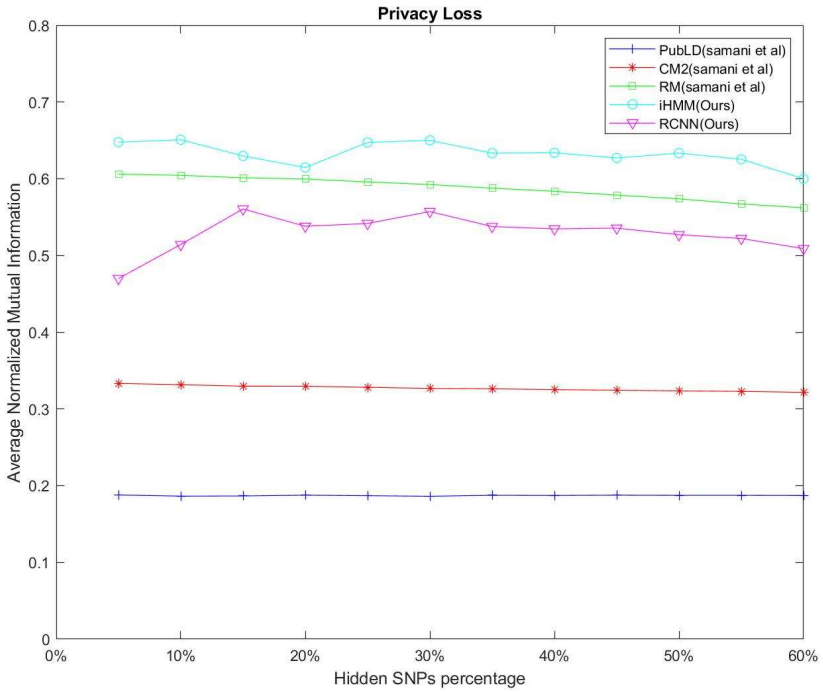

图 5.7: 不同基因隐私分析模型的基因组隐私变化对比（受害人隐私损失角度）

者的SNPs暴露给敌手的越多，不正确性越低）。与之前的工作相比所提出的两种攻击模型在不正确性方面均显示出更好的推断能力。当隐藏更多SNPs(大于50%)时，基于RCNN的攻击性能优于基于重组模型的攻击;当隐藏更少SNPs时(小于45%)时，基于重组模型的攻击性能略差。

在图 5.6中，根据敌手的不确定性显示了基于不同模型的推断攻击的结果。可以看出，当被敌手隐藏的SNPs越少时，这些攻击的推断能力越强(即，被攻击者的SNPs暴露给敌手的越多，不确定性越低)，结果与图 5.5的结果一致。对比表明，基于iHMM的攻击总是比其他攻击效果更好，而基于RCNN的攻击效果并非始终都是好的。

同样的，在图5.7中的结果可以看到被攻击者隐私损失的结果。同样，当被攻击者隐藏的SNP越少，这些攻击的推断能力就越强（即被攻击者的SNPs暴露给敌手的越多，隐私损失越大）。

5.7　小结

本章提出了两种种针对序列型基因数据的隐私分析攻击方法，通过改进的隐马尔可夫模型或回归卷积神经网络模型，利用网络公开基因组信息和个体的部分公开共享SNP序列数据推断个体的隐私基因型信息。研究表明，敌手能够准确、低不确定性和高隐私损失地推断出个体的私有隐藏SNP隐私信息。实验表明，所提出的攻击扩展并显著改进了现有的工作。通过基于公开的基因组数据对个体基因组隐私进行量化，本章的工作可以帮助人们更好地理解当前基因组隐私面临的风险，促进隐私领域更加小心地应用基因组数据，促进研究人员设计更好的隐私保护模型。

在未来，我们将进一步探索机器学习的潜力，将这种方法扩展到对亲属基因组隐私的攻击，并确定抵御基因组隐私攻击的合适方法。

第六章　相互关联的序列型数据的隐私属性推测模型及其应用

第七章　面向隐私保护的风险自适应访问控制模型

本章针对云环境中共享、应用涉及隐私或敏感信息数据的场景研究面型隐私保护的访问控制模型。在此类以数据为中心的开放跨域环境，大量用户以不同形式的应用需求来访问数据，数据拥有者(即数据服务提供者或系统)需要动态化、自适应的提供隐私保护。我们在*XACML*上扩展提出了一种基于风险的自适应访问控制模型，以动态化在访问控制过程中保护数据隐私，约束隐私侵犯行为，激励诚实访问行为。在该模型中，以*Shannon*信息论作为工具，在第三章提出的隐私度量度量模型基础上，提出了基于风险的隐私定义和量化方法；通过风险隐私量化及基于信誉的激励机制，实现访问行为风险阈值的动态调整。对比和分析表明，所提出的模型和方法较现有的工作更加动态化，且实现了隐私保护，易用性更好。本章成果已发表在《*International Journal of High Performance Computing and Networking*》。

7.1　概述

随着云计算的发展和云计算模式的广泛应用，越来越多的敏感数据和隐私信息在云环境中存储、应用，致使云面临着若干安全问题。云计算环境中的隐私、机密性和完整性等身份识别与访问控制相关的安全性需要保证。访问控制模型对云安全极为重要，但云中仍然在大量应用传统的访问控制，而这些方案存在不同层面的安全和隐私问题。传统访问控制模型，例如ACL (访问控制列表)[109], RBAC (基于角色的访问控制)[110], ABAC (基于属性的访问控制)[111]和PBAC (基于策略的访问控制)[112] 是严格和静态的访问控制模型, 需要管理员预定义所有访问策略。在像云环境这样的“按需共享”的大规模信息系统中，用户和资源都是动态的且一直在变化，不可能预先定义访问策略，而传统的访问控制方法无法适应这种情况。

为了解决此问题，基于风险的访问控制[49,113-115]被引入，因为其将风险级别分析作为授权决策过程的主要输入，以实现动态访问控制。基于风险的访问控制通过考虑访问请求的环境和情况以及安全策略来评估风险，并根据阈值确定访问权限。这种决定访问权限的方式可以通过反映情况的本质并防止由于内部人员滥用和滥用数据而导致不必要的隐私信息访问和泄漏，从而实现动态访问控制[116]。因此，风险量化成为基于风险的访问控制中的核心组件。

一般情况下风险定义为潜在的资源价值损失。在信息系统中，访问风险可以被视为因访问数据所可能造成的潜在泄露信息价值。现有以基于风险的访问控制研究进展提供了不同的方法来确保访问对象的安全性和隐私。Chen等[47] 提出了一种模糊多级

风险访问模型，该模型采用模糊理论来评估对象的通行等级和对象敏感度等级对，随后Ni等[113] 将Chen等的思想思想扩展为基于模糊推理的访问控制。Wang和Jin[49] 在健康信息系统的访问控制中提出了一种基于条件熵的风险量化方法，以保护患者的隐私。Shaikh等[114]提出了一种基于动态风险的访问控制系统决策方法的新方法，同时考虑了短期历史访问行为和长期历史访问行为。Khambhammettu等[117] 将威胁资源和低手影响考虑至访问请求风险量化中，并以此提出了一个访问控制模型的风险量化方法。Choi等[115] 对上下文信息进行了分类，通过扩展可扩展的访问控制标记语言(XACML)来应用风险，从而通过基于上下文和处理的权限配置文件和规范来估计和应用风险。但是这些工作都需要使用相同的方法来对访问主体(用户) 和访问客体(资源或信息)进行分类, 且在特定情况下很难找到这种方法。尽管现有工作可以动态地基于风险来决定访问许可，但是其最大可容忍风险值(风险阈值) 是静态的，对于所有用户而言都是相同的容忍度，且缺乏对访问主体的激励机制。

本章目针对上述问题，提出了一种基于马尔可夫和信息论的风险自适应访问控制模型。首先，为基于风险的访问控制模型定义了一个敌手模型，提出了一些自然而有用的假设和定义，仅通过比较访问行为模式即可对访问请求和用户进行分类。然后，提出了一种基于XACML的风险自适应访问控制框架。在此框架中，添加了策略风险评估点(Policy Risk Evaluator Point, PREP), 会话控制和风险缓解服务三个新组件，并增强了策略执行点，策略访问点和策略信息点三个标准组件。针对PREP设计了基于类马尔科夫的公式和方法，以根据访问历史行为来计算访问请求的风险值，基于请求类别识别来允许/拒绝访问请求，并根据访问历史周期性计算用户风险，并设计激励机制通过重新定位风险配额和风险消耗配额。

7.2　相关工作

最近，基于风险访问控制模型吸引了研究人员的注意[49,114-115]。Wang和Jin[49] 考虑了一种实际的访问控制模型，该模型通过考虑医疗保健的实际情况来保护电子医疗系统中的患者隐私。首先，该模型允许医生通过量化与医生的数据访问活动相关的风险来做出访问决策。其次，该模型利用医生的整体统计行为和Shannon条件熵来量化侵犯隐私的风险。Hui等[118]改进, 对此模型进行了改进，但是两个模型都不能在近期历史和旧历史之间取得平衡，也没有采取任何措施来减轻高风险。Shaikh等[114] 提出了一个用于访问控制系统的基于动态风险决策方法。首先，其改进了标准XACML框架，添加了策略风险和信任评估者点。其次，系统根据奖励和惩罚历史计算主体的信任值和客体的风险值。此外，该系统通过使用基于指数加权移动平均值(EWMA) 的方法来考虑近期历史和旧历史的不同影响。最后，分析了允许非法访问和限制合法访问的威胁。该系统可以根据过去的行为自适应并适度增加或减少所有用户对资源的访问权限，但是访问主体和访问客体需要相同的分类方式进行标记。此外，该系统仅根据主体-客体

间奖励或惩罚点做出访问决策，没有针对访问主体历史行为的奖励机制或惩罚机制。Choi 等[115] 提出了一种适用于医疗信息系统的基于风险的访问控制框架，以保护患者的敏感数据和隐私。该方法的主要思想是根据医疗情况和处理的严重性，通过动态访问授权决策来估计和应用风险。在对有关医生的目的，患者的状况和治疗以及医疗数据的上下文信息进行分类之后，可以根据特定患者的状况和治疗的条件下访问请求与目的之间的相关性来评估风险等级。尽管该模型可以在某些严重情况下授予访问权限，但其并未提供缓解高访问风险的措施，使得在后续访问过程造成风险量化混乱。

我们提出的方法与[49,114-115]等文献的方法相比，具有一些新的特性。

1. 该方法中，资源所有者或访问控制系统的管理员只需标记或分类访问对象(例如，资源，存储的数据，数据等) 根据访问对象的属性和要求，通过某些标准方法(例如，用于病历的IDC-10) 或定制方法。不需要为访问主体(例如，经过身份验证的用户) 特定明确的角色或工作职责，也无需为每个访问请求特定目的。

2. 访问主体的工作职责是通过对主体历史访问数据聚类而得到的，且将访问主体划分为不同的非相交组。

3. 基于类马尔可夫模型设计了访问请求风险值计算，用户风险值计算，不同组中用户的迁移等方法。

4. 设计了一种类似于信用卡的激励机制，对主体的所有访问行为进行监督，并通过这种机制约束了风险请求和风险用户。

7.3　基本定义和敌手模型

本节进行若干假设和定义，并此提出基于风险访问控制模型的敌手模型。如第7.1节所述，本章主要聚焦对信息系统中经过身份验证的用户的访问行为控制，以保护敏感数据和隐私。在此类系统中，所有用户，包括敌手，都被授权使用存储的数据，本章的目的是防止用户不履行其在系统中的职责时，访问不该访问的敏感或隐私数据而造成的隐私泄露。

假设7.3.1. *所有通过身份验证的用户都将履行其职责。*

若用户通过了特定信息系统的认证，则他为合法用户，且他有责任履行其工作职责。一旦对员工没有足够的工作职责，系统将不会容忍用户。此外，若用户未履行其工作职责，则不会对敏感或隐私数据造成太大伤害。根据假设 7.3.1，可以将经过身份验证的用户分为几类, 即*诚实用户*和*好奇用户*, 有时将*好奇用户* 认为是*恶意用户*。*诚实用户* 仅访问其职责所需的数据或信息，*好奇用户* 有时会故意或随机访问与其职责无关

的敏感或隐私数据或信息，但与诚实用户相同的访问行为除外。只有当好奇用户故意访问与工作职责无关的敏感或隐私数据或信息时，其才被称为恶意用户。方便起见，在本章的研究中，对这两个概念的不加以区别的对待。

假设7.3.2. 大多数通过身份验证的用户都是诚实用户。相应地，只有一部分经过身份验证的用户是好奇用户或恶意用户。

假设 7.3.2在现实环境中是合理的。现实中的大多数人都是好人，否则我们的社会将会混乱。假定部署在云或本地设备中的任何信息系统都有序运行，且大多数用户都是诚实的。一旦好奇用户 被系统识别，可以通过惩罚或拒绝好奇的用户来确保这一假设。

对于经过身份验证的特定用户，还可以根据访问请求的风险值将其访问行为分为两类。一部分行为具有较高的风险值，而另一部分行为具有较低的风险值。该分类由以下事实决定：没有绝对的分类，即所存储的信息和数据中哪些与该用户的职责有关，哪些与该用户的职责无关。我们的目的是将好奇用户 与诚实用户区分开, 拒绝好奇用户, 并减少诚实用户的偶然高风险行为对诚实用户的访问控制决策的影响。为了实现该目标，需实现以下内容：

1. 根据身份验证用户的工作职责将其分为几组，且每两个组的交集在一段时间内为空；
2. 识别每个用户的职责变更，并将变更后的用户分别分组为适当的组；
3. 评估每个用户的每个访问请求的风险，并识别具有高风险值的请求；
4. 定期评估每个用户的风险，识别好奇的用户并拒绝他们。

以上表明同一组中的所有用户都具有相似的工作职责，因此，若$u \in g$,则不区分用户u 和组g 的职责。在提出的敌手模型中，在特定的用户组中，对于访问行为，若该访问请求的访问数据蕴含隐私信息比历史访问行为多，则访问行为具有高风险。为了对高风险请求和正常请求的风险评估建模，引入两个假设函数，即sr 自我风险函数和gr 组风险函数。其中，$sr(u,q)$ 表示用户u的当前访问请求q 对u自身的历史访问行为的风险值, $gr(u,q)$ 表示风险值u的用户当前访问请求q中u 所属用户组g 的历史访问行为。$sr(u,q)$ 和$gr(u,q)$ 的具体计算公式将在7.4中讨论。

定义 7.1. 令$sr(u,q_0), sr(u,q_1), sr(u,q_2), ..., sr(u,q_{n-1})$ 为过去n 次请求u 的自风险值, 令$sr(u,q)$ 为u 当前(第n次) 请求q 次的风险值。令$\varepsilon_s \in (0,1)$ 为分位数。若$sr(u,q) \geq (1+\varepsilon_s)/n \sum_{i=0}^{n-1} sr(u,q_i))$, 则请求$q$ 是一个**用户自风险请求**。否则，q 是一个**用户自我正常请求**。

定义 7.2. 令$gr(\cdot,q_0),gr(\cdot,q_1),gr(\cdot,q_2),...,gr(\cdot,q_{m-1})$ 是过去m 的组风险值乘以同一用户u 组中的用户请求。并将$gr(u,q)$ 设为用户u 的当前请求q (u 所属组的第m个请求)。令$\varepsilon_g \in (0,1)$ 为分位数。若$gr(u,q) \geq (1+\varepsilon_s)/m\sum_{i=0}^{m-1} sr(\cdot,q_i))$，则$u$ 的请求q 是一个**组风险请求**。否则，u 的q 是一个**组正常请求**。

上述定义7.1和定义7.2 都基于马尔可夫模型，且可以根据访问控制系统的经验自动确定马尔可夫链的长度。此外，两个长度都可以随时间变化。通过这两个定义可以有效识别访问控制系统的高风险访问请求。具体详细计算方法，将在第7.4节中详细讨论。在一个时间段内，特定组的每个用户的请求数据数据的期望服从某些分布，而该组的所有用户请求的数据数据的期望也服从一定的分布。根据假设**??**, 若u 是一个诚实的用户，则用户u 的访问数据的分布D_u 与同一组中所有用户访问的数据的分布D_g 密切相关。相反，若u 是一个好奇的用户，则D_u 与D_g 无关。为了有效描述这种关系，引入相关关系函数 θ 并将在第7.4节中进行讨论。对于用户u 在组g 中通过请求q 访问的数据数据集合r，$\theta_g(r_q,u))$ 返回一个[0,1]的实数，该实数反映r_q 和u 的职责之间的相关程度，$\theta_g(r_q,u))$ 越高, 风险r_q 对于用户u 的职责而言就越高。

定义 7.3. 假定D_g 是特定组g 的所有用户U_g 访问的数据数据集合R_g 的先验概率分布，D_g 使得$Pr(R_i) = \delta \cdot \theta_g(\cdot,u_i))$，其中$u_i$ 是g 中的用户, R_i 是$u_i \in g$ 访问的数据数据集合，而δ 是实数，因此$\Sigma_{u_i \in g} Pr(R_i) = 1$。

- **诚实用户**: 设R_i 为$u_i \in g$ (即诚实用户) 在过去一段时间内访问的数据集, 对于每个数据$r_k \in R_i$, 概率为$(1-\varepsilon_1)$ 时, r_k 的选择遵循D_g 分布; 概率为ε_1 时, r_k 的选择遵循R_g 所有可用数据的均匀分布, 其中$\varepsilon_1 \in [0,1]$.

- **好奇用户**: 设R'_i 是$u'_i \in g$ (即好奇用户) 在过去一段时间内访问的数据集, 对于每个数据$r'_k \in R'_i$, 概率为$(1-\varepsilon_1)(1-\varepsilon_2)$ 时, r'_k 的选择遵循D_g 分布; 概率为$\varepsilon_1(1-\varepsilon_2)+\varepsilon_2$, r'_k 的选择遵循R_g 所有可用数据的均匀分布, 其中$\varepsilon_1,\varepsilon_2 \in [0,1]$.

如定义7.3 所述, 诚实用户的数据访问始终遵守其职责(即，用户总是遵循分配D_g), 例外情况的发生概率小于ε_1. 相反，好奇用户的行为与诚实用户的行为以概率$1-\varepsilon_2$ 相同, 他履行了自己的职责；好奇用户以概率ε_2 过度访问敏感数据。在真实场景中，ε_1 和ε_2 的值都较小。

7.4　所提出的风险访问控制模型

本节根据可扩展访问控制标记语言(XACML)[119] 改进提出一个风险自适应访问控制模型，然后提出如何初始化访问控制系统，如何定义并量化访问请求风险，如何为请求做出访问决策，访问控制过程详细过程、如何动态识别好奇用户，以及如何设计激励机制等具体方法。

7.4.1　风险访问控制模型框架

在标准XACML框架中，一旦策略决策点(PDP) 收到了来自访问主体(即访问控制系统的用户) 的访问请求, 其首先会从策略访问点(PAP) 和策略信息点(PIP) 然后决定接受还是拒绝该请求。此外，策略执行点(PEP) 难以处理与请求者的交互，策略访问点(PAP) 是静态的，且职责服务和策略信息点(PIP) 都缺乏风险管理。在我们提出的框架中，除了对PEP，PIP和PAP进行了增强，还新增了三个组件，即策略风险评估点(PREP)，会话控制和风险缓解服务(嵌入在职责服务的组件中)。在该框架中，一旦PDP收到来自经过身份验证的用户的访问请求，且在做出决定之前，它会请求与特定访问主体(即正在请求访问的用户) 和其历史访问数据相关的风险值。此外，在做出访问控制决策后，一些反馈信息将提供给职责服务。所提出的风险自适应访问控制模型的流程如图 7.1所示。该框架是基于标准可扩展访问控制标记语言(XACML) 提出的，与[114]的框架有所不同，所提出框架的所有新组件均以虚线标记，所有增强的组件均浅灰色标记。

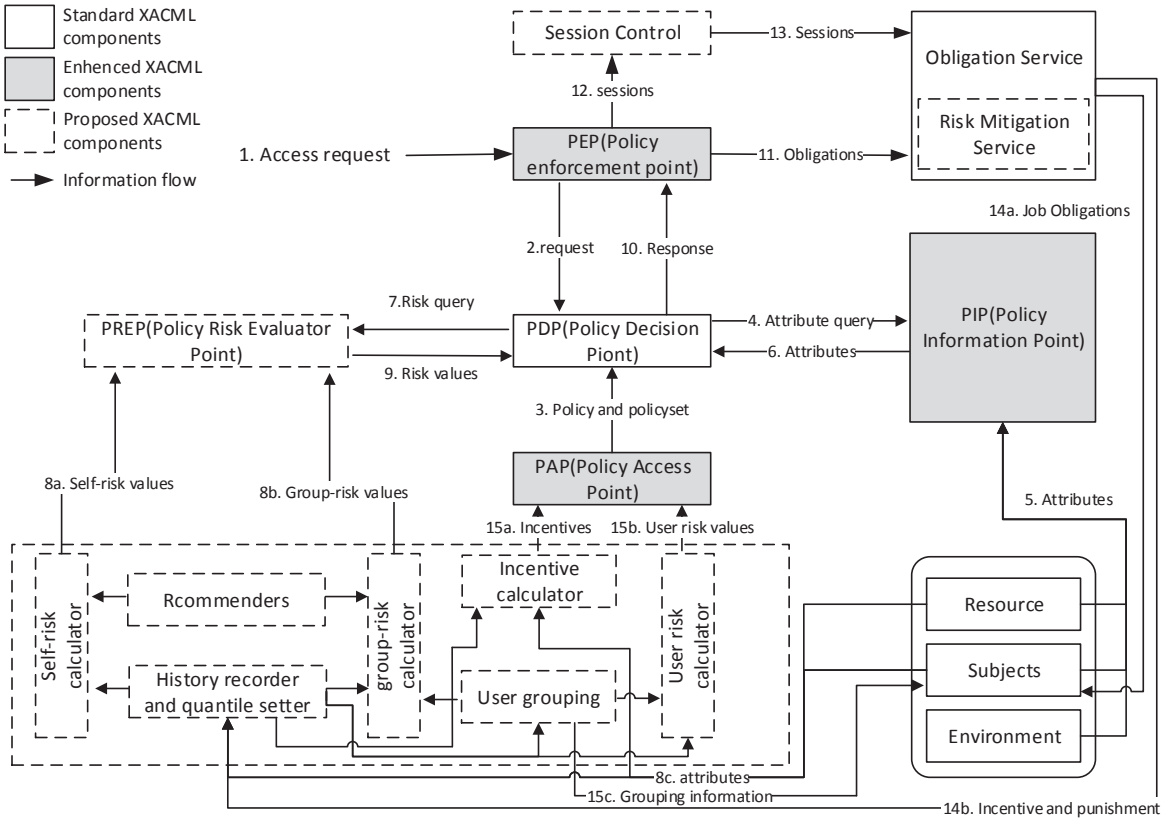

图 7.1: 基于XACML的风险自适应访问控制模型处理流程

在所提出的基于标准XACML风险访问控制框架中，所有访问请求均由经过身份验证的用户发送，我们称此类用户为访问主体。从步骤1到步骤6，其过程类似

于Shaikh等[114] 和Verma[119]所述的过程。一旦收到所有必需的信息，PDP就将有关当前请求的风险查询发送到PREP (步骤7)。PREP根据用户的过去行为和历史行为的风险值来评估风险值(步骤8)。每个请求都有两个风险值，一个是根据当前用户自己的过去行为评估的自我风险值，另一个是根据所有用户的过去行为以及当前用户属于同一组所有用户评估的群组风险值。若系统没有足够的历史数据，则PREP将根据系统平均风险水平评估两个隐私风险值。与该访问请求相关的当前风险值将返回到PDP (步骤9)。根据风险值，PDP做出决定，并将此决定转发给PEP，由PEP执行(步骤10)。无论是允许访问还是拒绝访问，PEP都会通知(步骤11) 职责服务，该服务将决定是否需要风险缓解服务。在强制执行的延迟时间内，会话控制组件监视请求者的行为，并管理访问会话(步骤12)。若在该会话中访问行为的隐私风险太高，则会话控制通知职责服务组件并控制该会话中的请求(例如，终止会话) (步骤13)。职责服务将决定是激励还是惩罚用户，并更新主体的属性(例如工作职责) (步骤14)。PREP定期通过激励机制重新分配预算配额，重新将用户标识为正常用户或有风险的用户，并将用户分类到为更合适的群组中(步骤15)。

7.4.2　请求风险值和请求决策

7.4.2.1　请求风险值

本章中，动态评估访问请求风险值的方法是根据请求者的过去行为以及基础请求者所属组的所有成员而设计的。对于特定的用户组，该组中的每个用户都按照相似的工作职责划分到该组中，其工作职责在短时间段内相对稳定，且会在长时间周期范围自然演变。对于特定的用户，其所属的组可能会随时间改变。因此，应该根据用户本人和组的短时间访问行为特征来评估特定组中用户的访问请求风险，可以根据用户本人和组的长时间访问行为特征来识别用户风险。本节仅关注对特定用户的访问请求隐私风险评估。直观地，一访问请求的目的是访问一个时间周期内没有被访问过的数据数据集，则即使该数据数据集在以前被该用户访问过，该请求的访问请求的隐私风险值也很高。我们将该思想应用于对访问请求的隐私风险评估中，基于信息论相关概念，并对其进行改进，以设计本章用以进行访问请求隐私风险值量化的函数。

令$u \in U$ 是已认证用户集U, 且u 属于用户组g ，该用户组g 是U 的子集。如定义7.1和7.2所述，u 的请求q 有一定的隐私风险，表示为*用户自风险* sr *和组风险* gr 。

令$(q_1, q_2, ..., q_{n-2}, q_{n-1})$ 为用户u的前$n-1$次访问请求，而$r_1, r_2, ..., r_{n-2}, r_{n-1}$ 分别为这些请求的访问数据集。令q_n 是用户当前的访问请求，该访问请求所要访问的数据集为r_n。若将每个访问请求和访问数据集对(q_n, r_n) 视为随机事件，则该对(q_i, r_i) 的信息量可以通过**自信息**表示。则当前访问请求的访问隐私自风险sr 可表示为

$$sr(u, q_n) = I(q_n, r_n) \tag{7.1}$$

由公式7.1 中可知, 可由r_n 中预期访问的数据集的概率分布计算得到rs。此外，由于不同的数据集具有相同的标签，因此其可能具有相同的敏感信息。故而，在不同的情况下应使用不同的分类方法对数据进行标签化分类。可以将关系数据库中的数据分类为相同的数据，以使这些数据具有相同的信息；在电子医疗信息系统中，具有相同信息的医疗数据应按标签分类(例如ICD-9或ICD-10代码)。

为方便起见，后文将不再对访问请求q 和其预期访问的数据集r 进行区分, 即，每个不同的访问请求都试图访问具有不同信息的不同数据。假设访问请求集Q_u 中有k 个不同的请求$q_1, q_1, ..., q_k$ ，其中包括前$n-1$ 次访问请求和的u 的当前访问请求q_n ，以及概率分别为$p_1, p_2, ..., p_k$。若在k 个不同的请求中q_n 与q_i 相同，则方程7.1 可以简化为

$$sr(u, q_n) = I(q_i) = -logp_i \tag{7.2}$$

公式7.1 和7.2 都在具有足够的历史访问请求行为时，才对用户u 有效，若无有足够的历史访问行为历史供u进行计算, 则可以使用某个默认值(例如1) 或整个历史数据。

$$sr(u, q_n) = \begin{cases} I(q_i) = -logp_i, & \text{是否有足够的历史数据;} \\ Avg(I(u, q)), & \text{若历史还不够;} \\ 1, & \text{若没有可用的历史数据。} \end{cases} \tag{7.3}$$

由公式7.3可知，rs 的计算依赖于用户u 自己过去$n-1$ 次访问行为的马尔可夫链，且马尔科夫链的长度可以根据需要针对每个用户进行动态和个性化设置。这样，可以通过调整参数 n 的大小，适当地平衡用户u 的短期历史和长期历史行为对隐私风险值的影响。

令$sr(u, q_1), sr(u, q_2), ..., sr(u, q_{n-2}), sr(u, q_{n-1})$ 为过去$n-1$ 次允许请求u 的隐私自风险值，并令$sr(u, q)$ 为u 当前(第n次) 请求q 的当前访问请求的隐私自风险值。令$\varepsilon_s \in (0, 1)$ 为分位数，通过定义7.1 可以方便地将q 定义为**自风险请求** 或**自正常请求** 。

类似地，可以通过该马尔可夫方法得到当前用户u 的当前访问请求的组风险值。令$q_1, q_1, ..., q_l$ 是访问请求集Q_g 中的元素，它表示组g 过去的$m-1$ 次允许访问请求和$u \in g$ 的当前访问请求q_m，$p_1, p_2, ..., p_l$ 分别为历史访问请求数据集的标签化概率分布。若q_m 与Q_g 中的q_i 相同，则$gr(g, q_m)$ 可计算为

$$sr(g, q_m) = \begin{cases} I(q_i) = -logp_i, & \text{若有足够的历史数据;} \\ Avg(I(g, q)), & \text{若历史还不够;} \\ 1, & \text{若没有可用的历史数据。} \end{cases} \tag{7.4}$$

类似地，通过定义7.2 可将$u \in g$ 的访问请求q 识别为**组风险请求**或**组正常请求** 。

7.4.2.2　访问控制决策

自风险值$sr(u,q)$ 和组风险值$gr(g,q)$ 都是访问决策的基础。根据定义7.1 和定义7.2, 可将所有用户的访问请求分为四类，即访问请求q 有四个不同的风险级别。故，数据服务提供者或系统可以根据请求的风险级别做出访问控制决策，即

$$decision = \begin{cases} p, & 若q为自正常访问请求，且为群组正常访问请求; \\ p(rm), & 若q为自风险访问请求，但为群组正常访问请求; \\ d, & 若q为自风险访问请求，且为群组风险访问请求; \\ d(p), & 若q为自正常访问请求，但为群组风险访问请求。 \end{cases} \tag{7.5}$$

其中，p表示因为访问请求时正常的，访问请求没有隐私风险，授权该访问请求；$p(rm)$ 表示该访问请求隐私风险较低，用户通过一定风险消减措施之后，可以授权该请求进行数据访问；d 表示由于该访问请求隐私风险过高而拒绝访问；$d(p)$ 表示该访问请求隐私风险太高，应当惩罚并限制用户访问包含隐私的敏感数据集。

公式7.5中对访问请求的访问控制决策的确定基于以下原因。若请求既是自身正常请求又是组正常请求，则用户和组在过去一段时间内频繁访问该访问请求的请求访问数据集，因此该请求是正常的而且没有风险。若某个请求是自风险请求，且是组正常请求，则表示该组中的其他用户（非用户本人）经常访问了预期数据，这些数据与该组的工作职责相关，但用户几乎不访问，且对该用户的访问风险很小，应该在系统采取某些适当的风险缓解措施后授予访问权限。若某个请求是自风险请求，且是组风险请求，则该组几乎不会访问预期数据，这些数据与该组的工作职责无关，因此访问请求应被拒绝。若某请求是一个自正常请求，且是一个组风险请求，则该组几乎不会访问预期数据，且这些数据与该组的工作职责无关，但该用户已多次访问数据，因此应拒绝访问此请求，并要加重惩罚以限制该用户访问。

7.4.3　用户分类与激励机制

本节首先基于用户和用户组历史访问请求，提出可定期地将用户$u \in g$ 识别为好奇用户还是诚实用户的方法。然后，提出可定期确定用户如何从一个组迁移到另一个组的方法；最后，设计了一种激励机制，以监督用户访问行为，抑制风险请求和风险用户。特别地，本节的所有方法，都基于类马尔科夫模型和信息论。

7.4.3.1　用户的风险值和用户分类

对于特定用户组中的用户，可在假设7.3.1和假设7.3.2 下通过定义7.3 将用户识别为好奇用户或诚实用户。但实际上很难找到θ_g 的特定函数，我们通过使用组g 的访问模式来近似刻画函数θ_g 。信息熵可用来表示信息集的不确定性，故而我们采用香农熵

来表示组和用户的访问模式，用户访问行为的熵越高，用户越好奇。

令T 为周期时间，$Q_{g,T}=(q_1,q_2,...,q_{s_g})$ 为T 中u 组所有用户的访问请求，$Q_{g,T}$ 遵循分布$P(g,T)=\begin{pmatrix} q_{g,1},q_{g,2},...,q_{g,n_g} \\ p_{g,1},p_{g,2},...,p_{g,n_g} \end{pmatrix}$。令$Q_{u,T}=(q_1,q_2,...,q_{s_u})$ 为时间T 中来自用户$u\in g$ 的访问请求，$Q_{u,T}$ 遵循分布$P(u,T)=\begin{pmatrix} q_{u,1},q_{u,2},...,q_{u,n_u} \\ p_{u,1},p_{u,2},...,p_{u,n_u} \end{pmatrix}$。

然后可以计算出用户$u\in g$ 在时间段T 中的风险值$risk(u,T)$ 为

$$risk(u,T)=max\{\frac{H(P(u,T))-H(P(g,T))}{H(P(g,T))},0\} \tag{7.6}$$

其中，等式7.6表示在过去的时间段T 中，用户风险随熵的增加而线性增加。但实际上，始终存在阈值ϕ, 使得用户A和用户B的风险相似，当$H(P(A,T))>H(P(B,T))>\phi$ 时，甚至$H(P(A,T))-H(P(B,T))$ 非常大。然后可以将公式7.6 中的风险值计算改进为

$$risk'(u,T)=\alpha^{max\{H(P(u,T))-H(P(g,T)),0\}} \tag{7.7}$$

其中，$\alpha\in(0,1)$, 而风险的结果$risk'(u,T)$ 将是$[\alpha,1)$ 中的实数。公式7.7 中所述函数是平滑的，在实际场景中更合适。

因此，一个用户$u\in g$ 可以由过去一段时间T中的风险值$risk(u,T)$ 或$risk'(u,T)$ 来标识。若$risk(u,T)>0$ 或$risk'(u,T)>\alpha$, 我们称u 在过去一段时间T 中是好奇用户，我们称u 为诚实用户，前提是$risk(u,T)=0$ or $risk'(u,T)=\alpha$. 形式上,

$$type(u,T)=\begin{cases} c, & \text{iff } risk(u,T)>0 \text{ or } risk'(u,T)>\alpha; \\ h, & \text{iff } risk(u,T)=0 \text{ or } risk'(u,T)=\alpha. \end{cases} \tag{7.8}$$

公式 7.8 为一个周期时间内的用户分类提供了基础，但是我们并不总是在短时间内将一个人分类为好人还是坏人。实际上，在某些情况下我们需要对一个人进行长时间的调查，这里我们对用户$u\in g$ 的风险值进行多次评估，然后形成u 的用户隐私风险值链。设T_n 为当前期间，$T_0,T_1,T_2,...,T_{n-1}$ 为过去n 个时间周期，n 个时间周期中，用户$u\in g$ 的用户风险值可分别通过$risk(u,T_0),risk(u,T_1),risk(u,T_2),...,risk(u,T_{n-1})$ (or $risk'(u,T_0),risk'(u,T_1),risk'(u,T_2),...,risk'(u,T_{n-1})$)分别计算得到。因此，可根据过去的$n$ 个风险值u 来识别当前期间的用户类型是诚实用户还是好奇用户，即

$$type(u,T(n))=\begin{cases} c, & \text{if } conut(risk(u,T_i)>0)>n/2; \\ h, & \text{if } conut(risk(u,T_i)>0)\le n/2. \end{cases} \tag{7.9}$$

此外，还可以用如下公式表示，

$$type(u,T(n))=\begin{cases} c, & \text{if } conut(risk'(u,T_i)>0)>\alpha; \\ h, & \text{if } conut(risk'(u,T_i)>0)\leq\alpha. \end{cases} \tag{7.10}$$

若u 在过去n 个周期中始终是一个好奇用户，我们称$u\in g$ 在过去n 个周期中是一个好奇用户，否则，他是一个诚实的用户。

7.4.3.2 组中的用户迁移

某个组织中的成员具有不同的工作职责，可以按相似的职责将其分组。随着时间的变化，特定成员可能会随着其职责的改变而从A组迁移到B组，且新职责比A组更接近B组中的用户。在所提出的访问控制模型的用户，其可随着工作职责的变化而在用户组间迁移，且可通过观察访问行为定期将特定用户分类为最合适的用户组中。

首先，我们定义特定用户和用户组之间的距离。直观地，对于用户和组的工作职责，职责越相似，距离就越近。特别是，若特定用户的工作职责与组(即该用户是该组的成员)的工作职责相同，则距离为零。从访问行为模式的角度来看，对于诚实用户而言，若该用户在最合适的组中被识别，则不会存在访问风险，否则，即使他是诚实用户也始终具有正风险值。

定义 7.4. *设T 为周期时间, u 为用户，g 为一个组. 假设u 是g 的成员,则t 中g 的风险值$risk(u,T)$ 或$'risk(u,T)$ 可以通过公式7.6 和7.7, 则我们称$d(u,g,T)=risk(u,T)$ or $d(u,g,T)=risk'(u,T)$ 是T 中u 和g 的**距离**。*

为方便起见，这里仅讨论$risk(u,T)$ 的公式。

断言7.1 (用户组距离)**.** *若u 是诚实用户，且g 是时段T 中最适合u 的组，则有$d(u,g,T)=0$ (或若采用$risk'$ ，则有$d(u,g,T)=\alpha$)。*

断言7.2. *若u 是诚实用户，且可以观察到在时间段T 中的访问行为。则总存在一个组$g\in G$ ，使得$d(u,g,T)=0$.*

由于用户访问行为是连续的且用户迁移过程很慢，故在识别用户是否迁移时，应该多个周期内考察访问行为。若特定的用户正在迁移，则其访问请求的隐私风险值在多个周期内持续性增加，意味着当前组不适合他，或者他确实是好奇用户(若在这种情况下，对他的惩罚是严重的，请参阅第 7.4.3.3节)。然后，我们定义迁移用户如下。

定义 7.5. *设$T_0,T_1,...,T_{n-1}$ 为过去的n 个周期, 而$risk(u,T_0),risk(u,T_1),risk(u,T_2),...,risk(u,T_{n-1})$ 分别为n 个时期$u\in g$ 的用户风险值。若存在周期T_i 使得$risk(u,T_0)=risk(u,T_1)=...=risk(u,T_{i-1})=0<risk(u,T_i)\leq risk(u,T_{i+1})\leq...\leq risk(u,T_{n-1})$, 那我们称$u$ 是一个**迁移用户**.*

注意"≤"的关系"=" 不能全部成立。应当对正在迁移的用户重新分组，使其划分到最合适的用户组。与诚实用户u 从g 迁移出来相反，若g' 是目标组，则u 与g' 之间的距离会越来越近，直到为零。

定义 7.6. *设$T_0, T_1, ..., T_{n-1}$ 为过去的n 个周期，$u \in g$ 为迁移用户。若存在$g' \in G/g$ 使得$d(u,g,T_0) = d(u,g,T_1) = ... = d(u,g,T_i) \geq d(u,g,T_{i+1}) \geq ... \geq d(u,g,T_{n-1}) = 0$, 则称$g'$ 为当前周期u 的**目标用户组**。*

若可以找到u 的目标组g'，则我们将u 识别为新用户组的成员，并用g' 更改u 的组信息，否则，将采用第7.4.3.3 节中介绍的激励机制，并不断观察访问行为。

7.4.3.3 激励机制

在银行的信用卡体系中，初始信用额是一个对普通消费者来说足够的常数。一旦某人得到了初始信用卡，银行就会评估该特定人的每一种消费行为，确定该消费行为是否违法，并拒绝该违法行为；在每个周期(例如一个月或六个月), 银行都会识别此人是否有风险，并根据该时间段内他的行为适当调整其下一个期间的信用额度；有时，银行会通过长期观察信贷行为来识别人，例如五年。受信用卡系统的启发，在本节中为风险自适应访问控制系统提出一种访问控制激励机制。

初始化 不同组的初始风险配额不同，且初始风险配额将被初始化为访问控制系统中的每个风险配额。另外，初始风险配额将由用户在请求访问时消耗，且初始风险配额对于一段时间内的诚实用户而言已足够。我们将$u \in g$ 特定为g 组的用户，g 的初始风险配额为$qt_{g,init}$ (这意味着组g 中包括u 的每个人都具有相同的$qt_{g,init}$)。g 的新用户将由相同的$qt_{g,init}$ 初始化，风险配额将根据u 的历史访问行为在新的时间段内重新分配给u。注意，一旦访问控制系统被初始化，组g 的初始风险配额就可以随着g 的工作职责的变化而改变。

消耗量 在一段时间内，每个访问请求将消耗一定数量的$qt_{g,init}$。风险配额将在下一个时期重新分配。风险配额消耗的增加取决于访问请求的决定。正如我们在第7.4.2节中所述，访问请求有4种不同的决策类型，因此有4种减少访问消耗的数量类型。令q 为周期T 中用户$u \in g$ 的访问请求。若决策$decision(q) = p$，则风险消耗量为c_p；若决策$decision(q) = p(rm)$ 且风险缓解措施确定为q，则风险消耗量为c_p。若决策$decision(q) = p(rm)$，而没有风险缓解措施q，则风险消耗量为$c_{p(rm)}$；若决策$decision(q) = d$，则风险消耗量为c_d；若决策$decision(q) = d(p)$，则风险消耗量为$c_{d(p)}$；其中$c_p <= c_{p(rm)} < c_d < c_{d(p)}$. 若在时段$T$ 中u 的请求正常，则u 的风险配额将始终减少到接近零的正数，且若T 中拒绝了u 的某些访问请求，则必须将风险配额减少到零。拒绝的请求越多，风险配额用尽的时间就越早。

风险配额重新分配 对于新的时间段，应该根据过去时间段内的访问行为重新分配组g 中每个用户的风险配额。在这里，我们提出了三种风险配额重新分配方法，一种

基于最后一个时期，一种基于最后一个时期和过去n 个时期，第三种是前两个时期的组合。

- **单周期方法** 设$u \in g$ 为g 组的用户，当前时期为T, 该时期u 的风险份额为$qt_{u,T}$ 。设$qt_{u,T'}$ 是u 在最后一个时期T' 的风险配额。然后根据等式7.6 和7.8, 得到

$$qt_{u,T} = \begin{cases} qt_{g,init}, & \text{if } type(u,T') = h; \\ qt_{u,T'} \cdot (1 - risk(u,T')), & \text{if } type(u,T') = c. \end{cases} \tag{7.11}$$

  而且，可以基于公式 7.7 和公式7.8得到公式7.11 的替代方程式。

- **多周期方法** 令$T_0, T_1, ..., T_{n-1}$ 为过去的n 个周期，而$risk(u,T_0), risk(u,T_1), risk(u,T_2), ...,$ $risk(u,T_{n-1})$ 分别为n 个周期内u 的用户风险值。因此T' 与T_{n-1} 相同，而$risk(u,T')$ 与$risk(u,T_{n-1})$ 相同。$u \in g$ 的新风险定额可以通过以下公式得到

$$qt_{u,T} = \begin{cases} qt_{g,init}, & \text{if } type(u,T(n)) = h; \\ qt_{u,T'} \cdot (1 - \frac{\sum_{i=0}^{n-1} risk(u,T_i))}{n}), & \text{if } type(u,T(n)) = c. \end{cases} \tag{7.12}$$

- **组合方法** 有时，我们应该权衡短期历史行为和长期历史的影响。将**单周期方法**和**多周期方法**相结合的加权方法非常有效。设$\omega_1, \omega_2 \in (0,1)$ 且$\omega_1 + \omega_2 = 1$, 则可计算出当前周期T 的风险配额$qt_{u,T}$

$$\begin{aligned} qt_{u,T} = qt_{u,T'} \cdot (\omega_1 (1 - \frac{\sum_{i=0}^{n-1} risk(u,T_i))}{n}) \\ + \omega_2 (1 - risk(u,T'))) \end{aligned} \tag{7.13}$$

可以将上述三种方法中的用户风险值$risk(\cdot,\cdot)$ 替换为公式7.7 中特定的$risk'(\cdot,\cdot)$ 。

7.4.4　其他改进的组件

如第 7.4.1 节中的图7.1 所示，与标准XACML相比，本章提出的风险自适应访问控制模型中包含三个新组件和三个增强组件。PREP的详细信息已在7.4.2 和7.4.3节中讨论，其他组件将在本节中讨论。

会话控制 在此会话控制组件中，通过执行时间的属性来管理策略执行点阶段的应用。策略的执行并非总是实时的(例如，下载文件或调用程序来完成某些任务), 然后可以量化此会话中的访问行为所造成的隐私损害。因此，会话会监视当前会话中发生的这些隐私损害，以确保策略允许风险级别。一旦隐私侵犯发生超出允许的风险范围，访问会话将被访问控制系统中断。

风险消减服务 风险缓解服务是职责服务中添加的组件，它提供了一些缓解风险的措施。该组件有助于访问控制系统降低访问请求的风险。PDP需要降低风险的服务后，将验证一些其他增强安全性的措施(例如，审核，认证) 。

政策执行点 通过一些新的附加功能，增强了策略执行点，例如添加了会话模型。这样，PEP就可以与外部应用程序和职责服务组件进行交互，从而方便地管理外部应用程序的状态并降低访问请求的风险。

点接入点 会根据用户的风险值为PAP提供动态访问策略模型，且这些策略将定期重置或调整。

政策信息点 增强的PIP中还有更多属性，这些属性对于风险量化很有用。例如，除了时间，位置和访问度量外，还添加了风险配额，分组信息等。

7.5　讨论与分析

由于传统的访问控制系统不是基于风险的，故本节仅与风险访问控制相关的研究成果进行讨论和对比，如表7.1所示。

表 7.1: 自适应隐私风险访问控制模型与相关工作对比

	Shaikh等[114]	Wang与Jin[49]	Khambhammettu等[117]	Chen等[?]	Dantos等[120]	本章模型
风险自适应	是	否	否	否	否	是
支持XACML	否	否	否	是	是	是
分类对象	主体-客体	主体-客体	主体-客体	-	-	客体
历史访问行为	是	是	否	否	否	是
激励机制	是	否	否	否	否	是

基于风险的访问控制研究变得越来越多，其中很多成果是将风险引入到多级安全性保障[47,113] 和角色访问控制中[115-116]。但是，基于云的大规模信息系统中潜在的安全性和隐私要求具备更好适应性风险的访问控制模型，例如文献[49,114,117] 中所述。

首先，本章提出的方案实施起来非常方便。该方案通过一些新的增强组件扩展了XACML标准，以支持风险自适应访问控制。Chen和Jason 等[?] 讨论了如何将XACML标准扩展到基于风险的访问控制中，文献[120] 的新近工作表明XACML描述的基于风险的访问控制在云环境中是可实现的和有效的。相对地，本章提出的风险自适应访问控制模型完全符合XACML标准，而无需引入额外的元素。因此，本章提出的模型和Shaikh 等[114]的模型可在现实场景中实现；不同的是，本章所提的方案是一个完整的访问控制模型，Shaikh 等[114]仅提出了一个访问控制模型的访问决策机制。

其次，本章的方法对于现实生活中的场景更为实用。风险评估是风险基础访问控制系统的核心，所有现有工作[49,114,117] 通过使用”threat(subject, object)-impact(object, action)”, ”trust-threat”, ”trust level-risk level” 来量化访问请求或访问行为的风险值。管理

员必须使用相同的方法对主题和对象(有时甚至是目的和动作) 进行分类，而这种方法很难设计或实现。此外，这些工作中的风险评估过程有些主观。本章所提出的风险访问模型中，仅需要对访问客体进行分类，可以通过标记或标签化很容易实现。无需识别特定访问主体的特定角色或工作职责，访问控制系统可以识别特定组中的用户所承担的某些职责与该组中其他用户的职责相似，而无需专门知道什么是工作职责。实际上，该模型中的风险量化方法更容易计算访问请求和用户的隐私风险值。

第三，本章所提模型中对访问请求和用户的识别更加精确。几乎现有的工作(如文献[49,114]) 会评估用户或请求的风险值，然后根据历史访问行为对请求做出决策并识别用户。除了Shaiare更精确的要求和用户的风险值外，所有这些工作都没有考虑到短期历史访问行为和长期历史访问行为间的平衡。本章所提出的隐私风险值都是通过类马尔可夫模型计算的，平衡了短期历史访问行为和长期历史访问行为的影响。然后，通过将当前访问请求与用户自身及其所属组的访问历史进行比较，基于用户自身隐私风险和群组隐私风险值做出决策。通过将一个用户的访问/请求模式与其所属的组的访问/请求模式进行比较，对用户类别进行识别。这样，访问控制决策就变得更加合理，用户类型识别也更加精确。

第四，本文所提模型中的激励机制更加有效。除Shaikh和Logrippo[114]外，相关工作中未考虑任何激励机制。文献[114]的作者提出了一种以电子现金支付为灵感的“奖罚”方法，但并未描述通用机制。在本章工作中，提出了一种类似于信用卡体系的精细激励机制。隐私风险配额是根据用户的请求和访问行为定期分配给用户的。若根据过去或过去一段时间的历史行为将其识别为好奇的用户，则其激励机制将降低其隐私风险配额；若特定用户的一个请求被确定为有风险，则隐私风险配额将被消耗得多。访问请求的风险越大，则隐私风险配额将被消耗的越多。然后，我们的激励机制可用于监督访问请求和用户，并限制有风险的请求和好奇的用户。

7.6　小结

本章提出了一种类马尔科夫风险自适应访问控制模型，该模型可提供动态访问控制，以便在访问信息系统中的数据或信息时仅提供用户工作职责所需的信息，保护数据集中的隐私信息不被数据应用职责相关的访问者越权访问，从而保护数据隐私。在所提出的模型中，设计了一个基于标准XACML的修改框架，定义了三个附加组件，并增强了标准XACML框架的三个组件。为了考虑用户在访问控制系统中的访问请求风险，根据工作职责将所有用户分为不同的非相交组。通过将请求与用户和组的历史访问行为进行比较，可以计算出对特定用户组中用户的访问请求的风险值。此外，我们通过基于马尔可夫的方法定期地将用户识别为诚实用户或好奇用户，且该方法可以权衡近期历史和悠久历史的权重。最后，提出了一种基于信用体系的激励机制，监督所有用户履行其工作职责。所提出的访问控制模型对于基于云的庞大信息系统非常有效，

因为所有策略，访问请求风险值(历史数据的长度), 用户标识(历史数据的周期), 以及激励措施都是自适应的。而且，仅需标记存储的数据(访问客体) 而无需标记用户(访问主体) 或信任计算。

第八章　基于两方博弈的理性隐私风险访问控制模型

本章运用*Shannon*信息论和博弈论，提出了基于风险适应性的理性访问模型以实现数据共享场景中的保护隐私和数据应用需求间的平衡。在定义了隐私风险和隐私侵犯访问的概念之后，提出了基于博弈论风险的访问控制模型框架和工作流程。此外，还提出了量化访问请求和用户的隐私风险值计算公式，通过使用多轮两人博弈来构造和分析所提出的访问控制博弈模型。分析表明，在基于风险的访问控制的每一轮博弈中都存在子博弈精炼纳什均衡，可以通过限制侵犯隐私的访问请求来保护隐私。分析和比较表明，该方法比已有的工作更有优势，需要更少的辅助信息，提供更多的风险适应性和隐私保护能力。

8.1　概述

访问控制机制是解决信息和计算机领域中安全和隐私问题的基本技术。在当今的大规模，跨域和动态计算环境中，人们对隐私的关注日益增加，因此迫切需要灵活，细粒度，动态和自适应的访问模型。但是，传统的访问模型，例如自由访问控制（DAC）[121]，强制访问控制（MAC）[122]和基于角色的访问控制（RBAC）[123]及其改进方案不能满足这样复杂、分布式的计算环境和系统的要求。尽管基于属性的访问控制（ABAC）[124]比传统的访问模型更灵活，更细粒度，并且更适合现代系统（例如云计算和大数据平台），仍然存在一些挑战[125-126]。这些挑战源于日益增加的复杂性属性和用户，ABAC难以管理属性和策略，难以动态地监控和调整访问行为，因此仍然存在安全和隐私泄露的风险。

考虑医疗信息系统（Health-care Information System, HIS）的场景，一旦HIS识别出医生或护士后，他（她）的访问策略将通过预定义的属性确定的和静态的，并且他（她）可以访问HIS中的所有敏感和私人医疗数据。根据他（她）的工作职责和职责，他（她）会访问过多的不必要的隐私数据，但是系统不会采取任何对策来监视和调整用户的访问权限。因此，侵犯患者隐私的行为时有发生，类似的情况也发生在机密信息系统，军事信息系统，社交网络等方面。针对这些问题，为了克服传统访问模型（如DAC、MAC和RBAC）和ABAC的不足，在访问控制中引入了风险[7,47]和信任[127-128]，基于风险的访问控制（RaBAC）[47]具有更强的隐私意识和适应性[7,49,113]。

访问主体始终与系统同时竞争并协作以访问客体。一方面，访问主体希望从系统访问更多资源（包括正常所需的数据和额外的敏感数据）以获得有趣或商业上的利益。另一方面，访问主体必须与系统进行协作（尽可能遵循访问策略），以便他（她）可以

获得更多访问机会。相反，系统希望识别所有异常和恶意访问，且系统还希望与访问主体合作以吸引更多访问主体和访问请求。主体与系统之间的关系类似于博弈论[129]，需要利用该数学方法解决系统中理性参与者之间的冲突与合作。博弈论在安全和隐私领域中发挥着重要作用[56,130]。而且，通过结合不同的功能，将博弈论引入到访问控制机制的设计中[62-65,131]。在已有工作中，它适用于有限场景[62,65]或辅助信息过多的场景[63-64,131]。此外，将博弈论与访问控制结合起来的工作几乎都集中在安全性问题上（如文献[64]是用于同时具有信任和风险评估的安全性）而不是隐私，因此将访问控制与博弈论结合仍有很大的研究空间，特别是用于以数据和用户为中心环境中的隐私保护。

为了克服访问控制模型中授权用户的隐私侵犯以及现有工作存在的不足问题。在本章中，我们将信息熵和博弈论应用于基于风险的访问控制中，设计了基于风险适应性的访问控制模型，用于以数据和用户为中心的信息系统中的隐私保护。在提出的访问控制模型中，利用Shannon信息论设计了访问请求和用户的隐私风险风险值计算方法，通过通过引入新的组件提出了理性风险访问控制框架和流程，并对基于风险的访问控制博弈过程进行了分析。通过达到纳什均衡的，博弈双方不在有愿望改变访问控制的策略选择，进而限制侵犯隐私的访问请求，有效地保护了隐私敏感资源。与之前的工作相比，本章提出的方法具有更多优势，具体创新如下。

- 通过量化意图访问数据资源和已访问资源间的距离定义了隐私风险和隐私侵犯访问两个新的概念:。
- 提出了一个基于风险自适应的访问控制（RaBAC）的博弈论框架，并给出了基于xacml的访问控制流程。该框架涉及用户上下文，资源上下文，访问历史记录，风险历史记录和博弈历史记录。
- 应用信息度量和自定义功能来评估访问请求和用户的风险值。
- 分析了服务提供者和用户之间的多轮博弈模型，并得到了每轮的子博弈纳什均衡，在这种状态下，可以有效地限制对隐私数据的访问。

8.2　基于风险的访问控制模型

Cheng等[47] 提出了一种用于多级安全的风险量化方法访问控制模型，Ni等[113]通过将访问风险量化和模糊推理用于基于风险的访问控制，改进了文献[47]的工作。不同与传统访问控制模型，该访问控制模型在访问控制决策过程中应用了风险的定义，还引入了操作需求 和情景因子的概念来评估访问风险。在大多数文献[47,113,132-133]中，风险由主体s和访问客体o之间的函数$f(\cdot,\cdot)$定义。Cheng等[47]使用了访问主体与访问客体之间安全等级“差距”来定义风险，即$risk(s,o)=Val(o)\cdot P(s,o)$，其中$Val(o)$是披露访

问客体时受损的价值估算值，$P(s,o)$ 是安全事件披露的可能性。此外，所有风险的定量定义都是基本相同，类似于[47]的公式。风险量化的数学公式为

$$Risk = Likehood \cdot Impact \tag{8.1}$$

其中*Risk*是对当前访问请求的一个量化值，*Likehood* 表示事件发生的可能性，*Impact* 表示事件发生的潜在损害价值。

在基于风险的访问控制模型中，总是有三个常见的组件，包括访问控制管理器，风险量化和上下文检索。在图8.1中，展示了文献[134]中基于风险的访问控制模型基本组件概览。访问控制管理器组件接收访问请求，收集并分析用户的访问信息，然后将这些信息发送到风险量化组件。上下文检索组件收集上下文信息并发送给风险量化组件；风险量化组件通过使用从访问控制管理器和上下文检索组件收集的数据来评估每个访问请求的风险值，然后将风险值返回给访问控制管理器进行决策。基于风险的访问控制模型的核心问题是如何设计一种细粒度且适应性强的风险量化方法，而一种可适应的风险量化基础访问控制称为基于风险适应性的访问控制（Risk adaptable Based Access Control，RaBAC）。

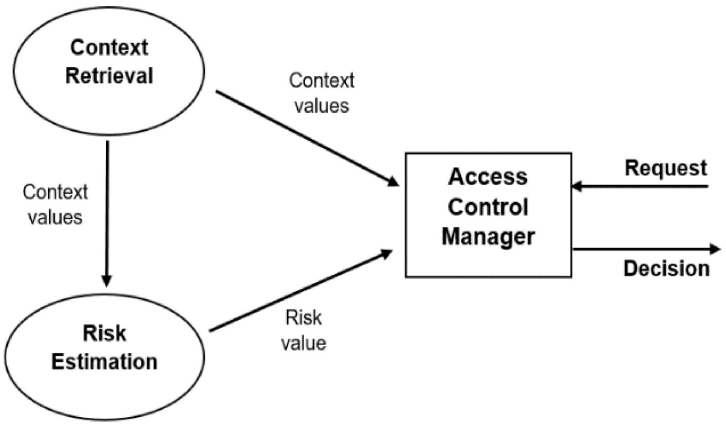

图 8.1: 基于风险的访问控制概述[134]

本章中，我们通过引入新的适应性风险量化方法和博弈论方法，扩展了基于风险的访问控制基本模型。具体来说，风险估算过程与公式8.1中的模型有所不同，并应用博弈论提出了一个新的组件。所提出的基于博弈论的风险自适应访问控制模型框架将在第8.4节中介绍。

8.3　符号和模型

在由服务提供商**S**（即系统）拥有的大规模用户**U**（即访问主体）和隐私敏感资源（即访问客体**O**）组成的系统中，所有用户都希望尽可能多地访问资源（甚至违反隐私

权政策），并且希望尽可能多地访问所有资源。但是，用户必须履行自己的职责，并且不希望资源或服务提供商识别其恶意访问行为；资源（和/或服务提供商）希望尽早且尽可能多地识别恶意访问行为。因此，用户和服务提供商之间存在访问合作和隐私冲突。用户和资源都是自私的，因为他们希望获得最大的利益，他们将在每次访问中做出最佳策略选择以最大化自己的利益。对于特定用户$u \in \mathbf{U}$，其隐私侵犯行为与其他用户的隐私侵犯行为不同，因为他们的职责彼此不同。但是，用户组g中总是有一些用户，这些用户在系统中具有相同或相似的职责（例如，所有胸外科医生在医院的HIS中必须遵循类似的职责）。用户组g中的用户u的访问请求q_u想要访问某些资源$o_{u,q} \subset \mathbf{O}$，$o_g \subset \mathbf{O}$ 是组g的所有访问资源的资源集，若$o_{u,q}$和o_g之间的距离小于用户/访问主体s的阈值t_u，则访问请求q_u不侵犯隐私；否则，q_u侵犯了隐私。这意味着，若访问请求不遵循具有类似职责的用户访问模式，则该请求会侵犯隐私。这种侵犯隐私的定义是合理的。因为同一组中的所有用户将以相似的方式执行其职责，因此遵循这些职责的所有访问都将以相似的方式执行。一旦访问不遵循职责，则模式将有所不同，并且此访问侵犯了隐私。在此，我们将$o_{u,q}$与o_g之间的距离$d(o_{u,q}, o_g)$定义为访问请求q的隐私风险r_q。

定义 8.1 (隐私风险). *$o_{u,q}$和o_g之间的距离$d(o_{u,q}, o_g)$是隐私访问请求q的风险r_q，其中$o_{u,q}$表示用户$u \in g$的访问请求q的目标资源集，o_g表示用户组g的访问资源集。*

定义 8.2 (隐私侵犯访问). *给定用户 u 的隐私阈值t_u和用户u的访问请求q。若$r_q > t_u$，则q为隐私侵犯访问；否则，q是普通访问。*

注意，可以根据不同用户的历史访问行为，将定义8.2中的隐私阈值设置为不同的值。特定用户的隐私阈值可以根据其历史访问行为（例如，使用贝叶斯方法或马尔可夫方法）在不同时期内变化。

在访问活动过程中，在用户**U**和访问客体**O**之间存在博弈（实际上是由服务提供者**S**而不是访问客体来博弈）。在博弈中，参与者集$\mathbf{A} = \{A_1, A_2, ..., A_n\}$由用户**U**和服务提供商**S**组成，每个参与者A_i都有一个策略集St_{A_i}，其中包含A_i的所有潜在动作。对于一次访问过程中的所有参与者，都有一个支付函数$U_{A_1,A_2,...,A_n}$。因此，$< \mathbf{A}, \{St_{A_i}\}, U_{A_1,A_2,...,A_n} >$是访问控制博弈模型。在该模型中，策略和收益值与用户**U**的访问隐私有关。

8.4　基于风险自适应的访问控制

在本节中，我们利用博弈论提出了一个基于风险适应性访问控制模型的框架，并给出了该框架的详细工作流程。

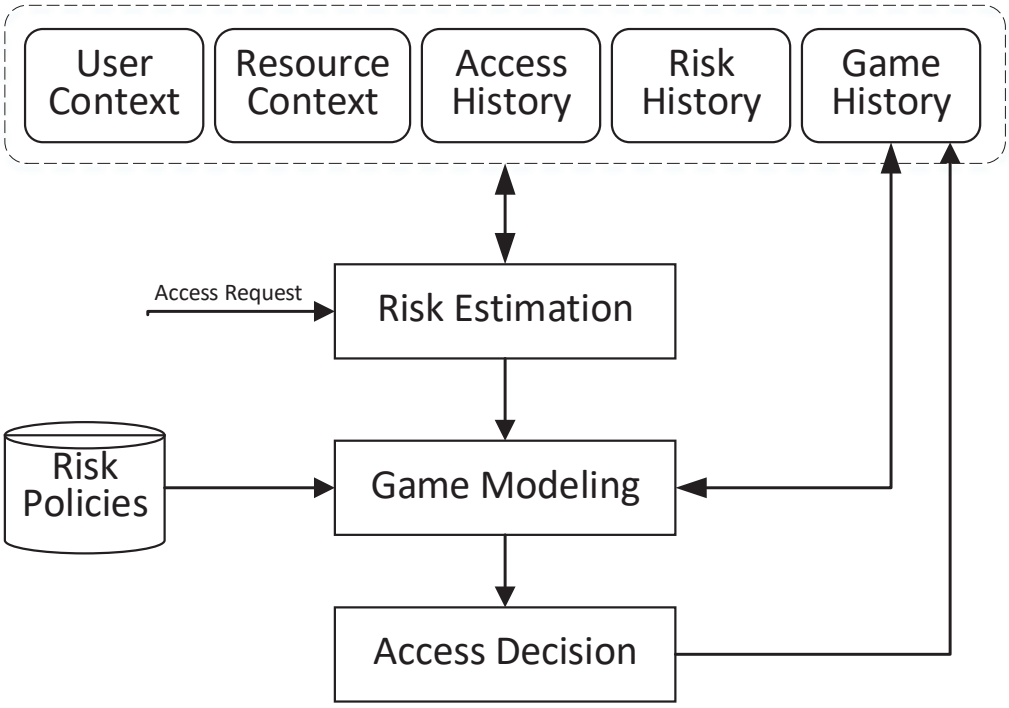

图 8.2: 基于博弈论风险适应性访问控制框架(RaBAC)

8.4.1　RaBAC框架

基于博弈论风险适应性的访问控制模型框架如图 8.2所示。存储资源系统记录所有用户**S**的所有用户上下文，所有资源**O**的资源上下文，用户**S**的访问历史记录，每个访问请求q的风险历史记录，以及博弈参与者**A**中的博弈历史记录。收到访问请求q后，系统会通过使用用户上下文，资源上下文、访问历史记录和风险历史记录来自适应地评估q的隐私风险r_q，并更新风险历史记录（风险量化模块）;然后，系统尝试通过识别q是否是违反隐私的行为来识别请求访问q的用户u的访问策略A_u，系统会根据用户的访问策略执行最佳策略A_u以获取最大利益，并更新博弈历史记录（博弈建模模块）；系统采取的最佳策略是接收到的访问请求q的访问决策（访问决策模块）。如第 8.3节中所述，可以定期更新“风险策略”模块中每个用户的风险阈值。在此框架中，风险量化和博弈建模是核心模块，风险评估模块旨在实现对访问控制的适应性隐私风险评估，博弈建模模块旨在实现针对访问控制的最佳策略选择。

8.4.2　RaBAC的工作流程

本节基于第 8.4.1节中提出的框架，提出基于博弈的风险适应性访问控制模型的工作流程。

在XACML的标准框架中，有四个组件，策略执行点（PEP），策略决策点（PDP），策略访问点（PAP）和策略信息点（PIP）。策略执行点（PEP）收到用户的访问请求

后，它将请求传递给策略决策点（PDP），然后PDP向策略访问点（PAP）和策略信息点（PIP）请求其他信息，然后进行决定接受还是拒绝该请求。另外，策略执行点（PEP）难以处理与请求者的交互，策略访问点（PAP）是静态的。职责服务和策略信息点（PIP）都缺乏风险管理。

在我们提出的模型中，对PEP，PIP和PAP进行了改进，并添加了新的三个组件，即博弈建模，策略风险评估点（PREP），会话控制和风险缓解服务。然后，一旦PDP接收到来自经过身份验证的用户的访问请求，并且在做出决定之前，它会请求与指定用户和历史记录相关的风险值，并构建一个博弈模型来做出决定。此外，在由博弈建模组件执行决策后，一些反馈信息将提供给职责服务。PREP可以实现对访问请求和用户的适应性隐私风险量化，博弈建模组件可以在用户（访问客体）和系统（访问客体）之间实现最佳访问策略选择。

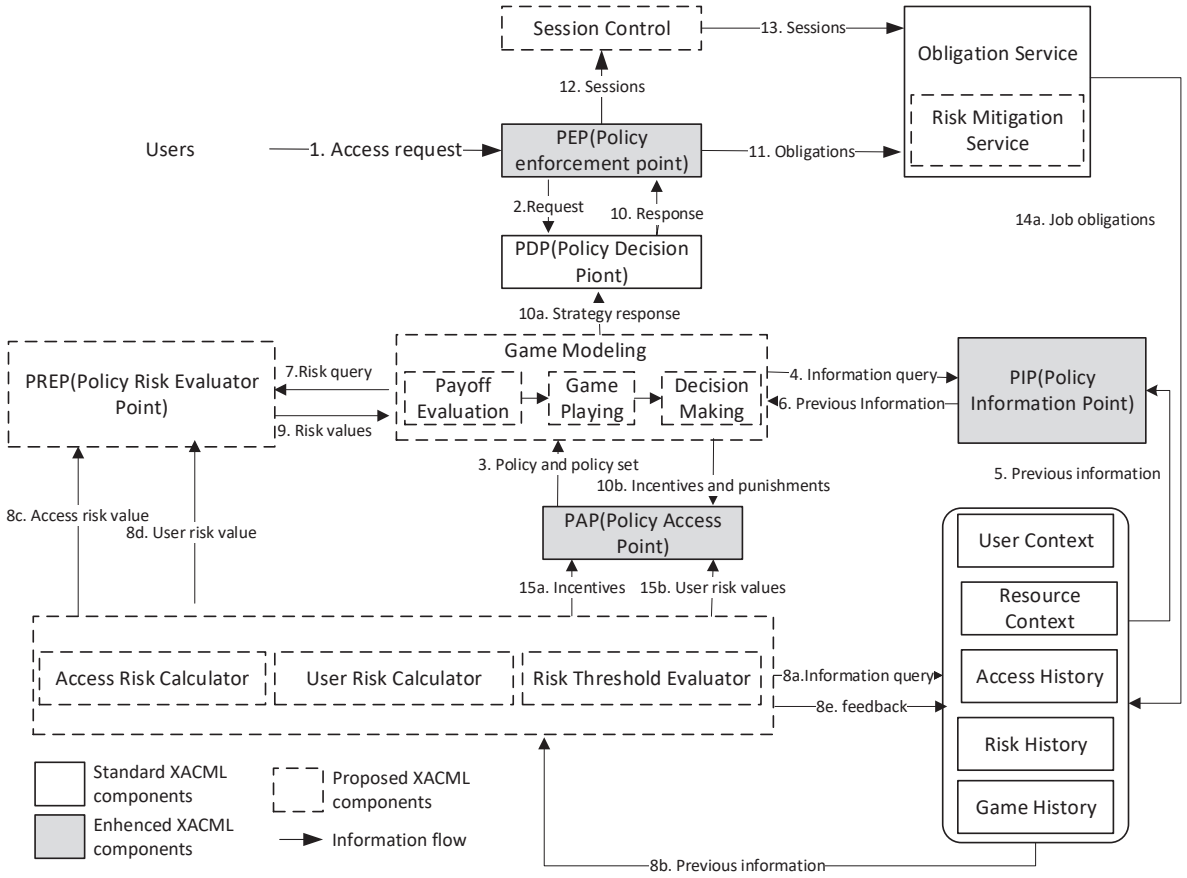

图 8.3: 基于XACML的理性RaBAC的处理流程

所提出的理性RaBAC的过程流程如图 8.3所示，基于标准可扩展访问控制标记语言（XACML）提出了此框架，并展示了所提出的理性RaBAC的处理流程。该图中，所有新组件均以虚线突出显示，所有增强的组件均以浅灰色突出显示。工作流基于标准XACML，所有访问请求均由经过身份验证的用户发送。从步骤1到6，组件传递请求

并收集先前的信息以进行访问控制；在查询了风险值之后（步骤7），策略风险评估器点（PREP）量化访问的隐私风险值和用户风险值（步骤8）。注意，PREP由访问风险计算器，用户风险计算器和风险阈值评估器组成。每个请求都有一个风险值和用户风险值，并且会根据基础用户的过去行为（例如，用户上下文，资源上下文，访问历史记录和风险历史记录）评估这两个值。若系统没有足够的历史记录，则PREP将根据建议评估两个值。与特定请求相关联的当前风险值返回到博弈建模（步骤9）。基于风险值、风险值和历史博弈行为，博弈建模为系统做出决策（例如，授予访问权限或拒绝访问权限）。将此决定转发给PEP，由其执行访问控制决策（步骤10）。无论是允许访问还是拒绝访问，PEP都会通知（步骤11）职责服务组件，该服务将决定是否需要风险缓解服务。在强制执行的延迟时间内，会话控制组件监视用户的行为，并管理访问会话（步骤12）。若在此会话中访问行为的风险过高，则会话控制会通知职责服务组件并控制此会话中的请求（步骤13）。职责服务将决定是奖励还是惩罚用户，并更新用户的特征（步骤14）。PAP定期更新激励对策和用户的用户风险值（步骤15）。

8.5　私隐风险评估

风险评估是基于风险的访问控制的核心问题，设计一种适用于风险评估的方法十分重要，由此才能实现基于风险适应性的访问控制模型。在本节中，为了能够实现适应性隐私保护需求，分别提出了针对访问请求和用户的适应性隐私风险量化方法。这些方法是图 8.3中PREP组件的细节设计与实现。

8.5.1　访问请求的隐私风险

除了我们在上一节中提出的框架之外，一个问题是如何评估来自用户的每个访问请求的隐私风险。对于来自用户u的特定访问请求q_u，可以通过遵循定义 8.1来估算隐私风险 r_{q_u}

这是一个用户组g，其中$u \in g$，g中的所有用户都执行相似的职责，并且他们通过遵守职责来访问相似的资源。假设在特定时期t（例如24小时或1周），g的用户总共访问了基础系统n次，并且访问请求为$Q^g_{pre} = (q^g_1, q^g_2, ..., q^g_n)$，每个请求$q^u_i$旨在访问资源集$R^g_i$，其中$1 \leq i \leq n$。现在，$q_u$是$u$的当前访问请求，而$R_u$是预期资源集。因此，可以通过使用$R_{q_u}$的信息和$R^g_i$的平均信息之间的距离来量化*privacy risk* r_{q_u}，如下

$$r_{q_u} = \frac{|Infor(R_{q_u}) - \frac{\sum_{i=1}^{n} Infor(R^g_i)}{n}|}{\frac{\sum_{i=1}^{n} Infor(R^g_i)}{n}}, \tag{8.2}$$

其中$Infor(\cdot)$表示资源集$\cdot$的信息。在一段时间内，组g中的所有用户访问资源都遵循一个分布。可以通过每个访问请求中资源的访问频率来构造此分布。因此，访问资

源集$R^g = \bigcup_{i=1}^{n} R_i^g = \{x_1, x_2, \cdots, x_m\}$遵循分布

$$\begin{pmatrix} X \\ P(X) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_m \\ p(x_1) & p(x_2) & \cdots & p(x_m) \end{pmatrix}, \tag{8.3}$$

其中$p(x_j) = frequency(x_j) / \sum_{k=1}^{m} frequency(x_k)$，而$frequency(x_j)$表示$R_1^g, R_2^g, \cdots, R_n^g$中$x_j$的访问计数。因此，$R_i^g = \{x_1^{R_i^g}, x_2^{R_i^g}, \cdots, x_t^{R_i^g}\} \subset R^g$，有

$$Infor(R_i^g) = -\sum_{j=1}^{t} log(p(x_j^{R_i^g})). \tag{8.4}$$

对于当前访问请求q_u的预期资源集R_{q_u}，可以将其分为两个子集：$R_{q_u}^* = R_{q_u} / R^g$ and $R_{q_u}^{**} = R_{q_u} \cap R^g = \{x_1^{R_{qu}^{**}}, x_2^{R_{qu}^{**}}, \cdots, x_r^{R_{qu}^{**}}\}$，和

$$\begin{aligned} Infor(R_{q_u}) &= Infor(R_{q_u}^*) + Infor(R_{q_u}^{**}) \\ &= -\|R_{q_u}^*\| \cdot log(min(P(X))) - \sum_{j=1}^{r} log(p(x_j^{R_{qu}^{**}})), \end{aligned} \tag{8.5}$$

其中$||R_{q_u}^*||$表示$R_{q_u}^*$的顺序。在等式8.5中，若$R_{q_u}^* \neq \emptyset$，则$R_{q_u}^*$的任何元素都不属于R^g，并且我们使用R_g代表它们。

在等式中8.2，$r_{q_u} \geq 0$，并且r_{q_u}越大，q_u的隐私风险就越高。我们可以在每个周期或每次访问中为用户u设置阈值$r_{q_u}^{th}$。由定义8.2，若$r_{q_u} > r_{q_u}^{th}$，则q_u是违反隐私的访问；否则，q_u是普通访问，并且可以根据u的历史访问行为在每个周期或每次访问中更新$r_{q_u}^{th}$。

8.5.2　用户风险计算

在每个周期的开始，都有一个由服务提供商签署的用户u的初始风险值r_u^0。每次访问后，将根据基础访问来更新用户u的风险值。假设用户u第$i-1$次访问后的风险值为r_u^{i-1}，并且q_u是u的当前访问请求，则该风险u的值将更新为r_u^i。若q_u是违反隐私的访问，则u的风险值将增加，反之则降低。并且该值快速增加而缓慢减小。这在我们的日常生活中自然而然，存在特定人的风险，若他的表现不好，则风险会增加，而若表现良好，则风险会降低。即使他做了一些新的好事，他周围的人也会保持警惕，风险值也不会迅速下降。若他做了一些新的坏事，周围的人会更加警惕他，风险会迅速增加。在这里，我们将用户的风险设置为

$$r_u^i = \begin{cases} r_u^{i-1}(1 - \dfrac{\alpha}{xr_{max}}), & \text{if } q_u \text{ is a normal access;} \\ r_u^{i-1}(1 + \dfrac{\beta}{r_{max}})), & \text{otherwise.} \end{cases} \tag{8.6}$$

在等式8.6中，α和β是因子，s是连续正常访问的计数，r_{max}是最大的用户风险。

8.6 博弈理论模型

8.6.1 RaBAC的博弈模型

博弈论是一种重要的数学工具，可用于与冲突和合作的参与者进行决策[?]。在访问控制系统中，服务提供商（系统）和用户（或多个用户）对不同的利益感兴趣，并且他们必须彼此合作以实现自己的利益。在这项工作中，我们假设服务提供商（系统）和用户是理性的，并且将基于风险适应性的访问控制建模为一种隐私保护的博弈模型，其中涉及参与者，参与者的策略和支付功能的参与者。在这个博弈中，有两个参与者，服务提供者s和用户u。服务提供商拥有对隐私敏感的资源（即访问客体），并希望授予正常访问权限并拒绝侵犯隐私的访问权限；用户是主体，谁希望为经济或其他利益而尽可能多地访问这些访问客体。用户u有两种策略，执行普通访问N和执行违反隐私的访问V；服务提供商有两种策略，分别授予访问权限G和拒绝访问权限D。 8.1显示了具有不同策略的参与者的支付功能。

表 8.1: 服务提供商和用户之间的支付矩阵

		User	
		N	V
Service Provider	G	$U_s^{G,N}, U_u^{G,N}$	$U_s^{G,V}, U_u^{G,V}$
	D	$U_s^{D,N}, U_u^{D,N}$	$U_s^{D,V}, U_u^{D,V}$

因此，基于风险适应性的访问控制的博弈模型可以由元组$< s,u,A_s,A_u,U_{s,u} >$定义，其中s是服务提供者，u是用户$A_s = \{G,D\}$是s的策略集，$A_u = \{N,V\}$是u的策略集，而$U_{s,u} = \{U_s^{G,N}, U_s^{G,V}, U_s^{D,N}, U_s^{D,V}, U_u^{G,N}, U_u^{G,V}, U_u^{D,N}, U_u^{D,V}\}$是具有不同策略的参与者的收益函数集。该博弈是一个多阶段博弈，在每次迭代中，博弈者彼此了解并了解策略，同时，收益还取决于策略，历史访问和历史博弈策略。因此，该博弈具有以下特征。

- 两个博弈者的博弈：在每次访问迭代中，博弈者都是服务提供者和用户。
- 有限策略博弈：服务提供商和用户，分别具有两个可选策略。
- 非零和合作博弈：若服务提供商和用户彼此合作，则均可获胜。例如，若用户执行常规访问并且服务提供商准予访问，则它们将共同受益。

- 静态博弈：在每次迭代之前，两个博弈者都不知道彼此的策略。
- 完美的信息博弈：博弈者知道他们在较早的访问迭代中选择了哪些策略。
- 不完整的信息博弈：在此博弈中，用户出于不同的兴趣爱好而具有不同的类型，并且服务提供商只是根据访问要求知道用户类型的分布。在不同的访问迭代中，收益是不同的。

8.6.2 博弈模型分析

在表 8.1中，支付函数如下所示，并且我们分析了支付的组成部分。

- $U_s^{G,N} > 0$是授予正常访问权限时服务提供商的实用程序。该实用程序是服务提供商通过授予常规访问权限而获得的收益，并且该收益取决于基础访问权q_u和用户的风险值r_u。然后$U_s^{G,N} = Sbenefit_g^n \times (r_{max} - r_u)$，其中$Sbenefit_g^n$是服务提供商授予正常访问权限的基本好处，而$(r_{max} - r_u)$是因素。用户风险越低，服务提供商将获得更多的利益。
- $U_s^{G,V} < 0$是授予隐私侵犯访问权限时服务提供商的实用程序。此实用程序是由于授予基本的隐私违规访问而导致的隐私丢失，并且受用户风险和访问风险的影响。然后$U_s^{G,V} = Sloss_g^v \times r_u \times r_{q_u}$。
- $U_s^{D,V} = 0$是拒绝隐私侵犯访问时服务提供商的实用程序。
- $U_u^{G,N}$是用户被授予正常访问权限时的实用程序。此实用程序是正常访问带来的收益，并受用户风险值影响，然后$U_u^{G,N} = Ubenefit_g^n \times (r_{max} - r_u)$。
- $U_u^{G,V} > 0$是授予用户隐私权访问权限时的实用程序。该实用程序包括几个部分，正常利益和通过授予基本访问权而带来的额外利益，并受用户和访问权的当前风险的影响。然后$U_u^{G,V} = Ubenefit_g^n \times (r_{max} - r_u) + Uextra_g^v \times r_u \times r_{q_u}$
- $U_u^{D,N} = 0$是拒绝用户正常访问时的实用程序。
- $U_u^{D,V} < 0$是当用户的隐私违规访问被拒绝时的实用程序。该实用程序是服务提供商对用户的一种惩罚，并受到用户和访问风险的影响。然后$U_u^{D,V} = Upunish \times r_u \times r_{q_u}$。

在此多阶段博弈中，我们可以分离每个阶段之间的战略关系，并将每个子博弈视为一个独立博弈。假设此博弈中有T个阶段，并且$\sigma_1^*, \sigma_2^*, \cdots, \sigma_T^*$是独立阶段博弈的纳什均衡策略的有序序列，然后存在子博弈的完美均衡，并且均衡路径由$\sigma_1^*, \sigma_2^*, \cdots, \sigma_T^*$生

成。在每个阶段的博弈中，我们都会解决最佳策略。我们假设博弈中服务提供者的混合策略是$(p,1-p)$，其中服务提供者以概率p授予访问请求，并以概率$1-p$拒绝访问请求；并且用户的混合策略是$(q,1-q)$，其中q是用户执行正常访问的概率，而$1-q$是执行隐私的概率用户违反访问权限。因此，用户的预期效用为

$$\begin{aligned} U_u &= (1-q)(p\times U_u^{G,N}+(1-p)\times U_u^{D,N})+q(p\times U_u^{G,V}+(1-p)\times U_u^{D,V}) \\ &= (1-q)\times p\times Ubenefit_g^n\times(r_{max}-r_u)+q[p(Ubenefit_g^n\times(r_{max}-r_u) \\ &+ Uextra_g^v r_u r_{q_u})+(1-p)Upunishr_u r_{q_u}]. \end{aligned} \tag{8.7}$$

通过求解微分方程$\frac{\partial U_n}{\partial q}=0$, we obtain $(p^*,1-p^*)$，我们得到$(p^*,1-p^*)$，其中

$$p^*=\frac{Upunish}{Upunish-Uextra_g^v}. \tag{8.8}$$

因此，$(p^*,1-p^*)$是服务提供商混合策略的纳什均衡。在这种情况下，服务提供商希望惩罚并减少隐私侵犯访问。同样，我们可以为用户获得混合策略$(q^*,1-q^*)$的纳什均衡，其中

$$q^*=\frac{Sloss_g^v r_u r_{q_u}}{Sloss_g^v r_u r_{q_u}+(Sloss_d^n-Sbenefit_g^n)(r_{max}-r_u)}. \tag{8.9}$$

在这种情况下，服务提供商和用户都可以获得最大的收益，并且每个阶段的博弈都可以达到纳什均衡。因此，用户将要执行正常访问，而服务提供商将准许用户的正常访问请求。因此，服务提供商通过限制隐私侵害访问来保留信息资源中涉及的隐私。

8.7　比较与分析

尽管有文献[7,49,62-65,113-114,131? ? ? ?]报道了与风险或博弈论相关的不同访问控制模型，但我们的工作与这些报告和收益比它们更大。比较显示在图 8.2中。

表 8.2: 所提出模型与已有工作的对比

Literature	Purpose of Access Control	Risk Estimation	Players of Game	Game Model
Ni et al [113]	Security protection	Static security risk	-	-
Shaikh et al [114]	Security protection	Dynamic risk and trust	-	-
dos Santos et al [?]	Cloud security protection	Multi-factor aggregation risk	-	-
Ding et al [?]	Cloud data security protection	Dynamic risk via entropy and Markov	-	-
Wang and Jin [49]	Privacy preserving of medical information	Static privacy risk	-	-
Zhen et al [?]	Privacy preserving of medical information	Dynamic risk via entropy	-	-
Zhang et al [7]	Privacy preserving of medical information	Dynamic privacy risk via conditional probability and Markov	-	-
Liu et al [63]	Access security of multi-femtocell networks	-	Multi players	Stackelberg game
Gao et al [65]	Cloud data security protection	-	Two players	Repeat game
Zhang et al [131]	Security protection	Trust	Two players	Non-zero-sum multi-stage game
Wang et al [?]	Security protection	Dynamic trust	Two players	Non-zero-sum multi-stage game
Hu et al [62]	Privacy preserving of social network	Static privacy risk	Multi players	Multi-control game
Helil et al [64]	General access control scenarios	Dynamic security risk	Two players	Non-zero-sum cooperative game
This work	Data privacy preserving	Dynamic privacy risk via information and Markov	Two players	Non-zero-sum multi-stage game

在表 8.2中，几个工作[7,49,113? ? ? -114]设计了基于混合风险的非混合访问控制。但是，Niel等人[113]和Shaikh等人[114]的目标是分别通过量化静态安全风险和动态风险来保护系统的安全。dos Santos等人[?]和Ding等人[?]提出了基于风险自适应的访问控制模型，以通过不同的动态风险估算方法维护云安全性。我们的模型是为了在开放和数据集中式系统中保护隐私而不是安全保护，它适用于本地和云系统。尽管一些作者[7,49?]提出了用于保护隐私的基于风险的不同访问模型，但是这些模型仅适用于医疗保健系统，并且可以保留病历的隐私，这些工作改进了风险量化的方法。我们的模型不仅可以应用于医疗保健系统，还可以应用于其他方案（例如，分类信息系统，数据集中系统）。此外，我们的隐私风险值包括通过Shannon信息和Markov访问请求和用户，而不是通过熵[?]和条件概率[7]的静态隐私风险[49]。此外，所有这些工作都是非博弈论方法，我们的工作是基于风险适应性的访问控制的博弈论方法。在我们提出的访问控制模型中，所有参与者都是理性和自私的，他们在每次访问迭代中都做出了最佳选择。

还有一些基于博弈论的访问控制模型[62-65,131?]。但是只有Hu等人[62]和Helil等人[64]的工作是基于风险的访问控制模型，而Liu等人[63]和Gao等人[65]只是利用博弈论扩展了传统的访问控制，并应用于多毫微微小区网络和云数据访问控制方面，Zhang等人[131]和Wang等人[?]专注于通过信任而不是风险进行安全保护。甚至Zhang等人和Wang等人的模型都是两人非零和多阶段博弈，与我们的模型相同，其应用场景和量化方法也有所不同，例如我们的模型用于数据隐私保护，并基于一种可调整的隐私风险量化方法。除此之外，这些工作[63,65,131?]都不是基于风险的访问控制，而我们的模型是基于风险适应性的访问控制。

最相似的报告是[62]和[64]，它们是基于风险和博弈论的访问控制模型。但是这些作品与我们的作品不同。Hu等[62]提出了一种用于通过静态隐私风险量化在社交网络中保护隐私的多方控制博弈。我们的工作不是针对社交网络，博弈模型与Hu等人[62]不同，[62]的作者根据用户关系设计了静态隐私风险，而我们模型中的隐私风险则根据用户的历史访问权限是动态的和自适应的行为。在[64]中，作者针对一般访问控制方案提出了基于风险信任的访问控制的两人非零和合作博弈分析。这项工作不是为了保护隐私，并且该模型基于历史访问通过用户的信任值量化了许可风险。虽然我们的工作是在开放和数据集中的情况下保护隐私，并根据访问请求和用户的直接量化隐私风险。此外，我们还为访问控制模型提出了一个基于XACML的框架和详细的工作流程。

8.8　小结

在这项工作中，出于保护访问控制系统中隐私的目的，我们提出了一种基于风险适应性的访问控制模型，并将此访问控制建模为一个多阶段的两人博弈。在该模型中，引入了一些新的组件，例如风险评估和博弈建模，并通过使用Shannon信息来量化访问风险和用户风险。最后，我们为每次访问迭代获得了子博弈的纳什均衡，服务提供商

和用户都希望在这种状态下表现良好，并且通过限制侵犯隐私的访问请求来保护隐私敏感的资源。比较表明，此访问控制模型比以前的工作受益更多，并且实现了良好的隐私保护性能。

第九章　总结及展望

9.1　结论

9.2　展望

参考文献

[1] SWEENEY L. k-anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5):557-570.

[2] NABEEL M, BERTINO E. Privacy preserving delegated access control in public clouds [J]. IEEE Trans. Knowl. Data Eng., 2014, 26(9):2268-2280.

[3] 黄刘生, 田苗苗, 黄河. 大数据隐私保护密码技术研究综述[J]. 软件学报, 2015, 26 (4):945-959.

[4] MACHANAVAJJHALA A, KIFER D, GEHRKE J, et al. *L*-diversity: Privacy beyond *k*-anonymity[J]. TKDD, 2007, 1(1):3.

[5] LI N, LI T, VENKATASUBRAMANIAN S. t-closeness: Privacy beyond k-anonymity and l-diversity[C]//ICDE. [S.l.]: IEEE Computer Society, 2007: 106-115.

[6] DWORK C. Differential privacy[C]//Lecture Notes in Computer Science: volume 4052 ICALP (2). [S.l.]: Springer, 2006: 1-12.

[7] ZHANG W, LI H, ZHANG M, et al. Privacy-aware risk-adaptive access control in health information systems using topic models[C]//SACMAT. [S.l.]: ACM, 2018: 61-67.

[8] REITER M K, RUBIN A D. Crowds: Anonymity for web transactions[J]. ACM Trans. Inf. Syst. Secur., 1998, 1(1):66-92.

[9] EDMAN M, YENER B. On anonymity in an electronic society: A survey of anonymous communication systems[J]. ACM Comput. Surv., 2009, 42(1):5:1-5:35.

[10] NIU B, LI Q, ZHU X, et al. Achieving k-anonymity in privacy-aware location-based services[C]//INFOCOM. [S.l.]: IEEE, 2014: 754-762.

[11] CAMPAN A, TRUTA T M. Data and structural k-anonymity in social networks[C]// Lecture Notes in Computer Science: volume 5456 PinKDD. [S.l.]: Springer, 2008: 33-54.

[12] WONG R C, LI J, FU A W, et al. (α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing[C]//KDD. [S.l.]: ACM, 2006: 754-759.

[13] YING X, PAN K, WU X, et al. Comparisons of randomization and k-degree anonymization schemes for privacy preserving social network publishing[C]//SNAKDD. [S.l.]: ACM, 2009: 10.

[14] LI N, LI T, VENKATASUBRAMANIAN S. Closeness: A new privacy measure for data publishing[J]. IEEE Trans. Knowl. Data Eng., 2010, 22(7):943-956.

[15] 林欣, 李善平, 杨朝晖. LBS中连续查询攻击算法及匿名性度量[J]. 软件学报, 2009, 20(4):1058-1068.

[16] XU T, CAI Y. Location anonymity in continuous location-based services[C]//GIS. [S.l.]: ACM, 2007: 39.

[17] 王彩梅, 郭亚军, 郭艳华, 等. 位置服务中用户轨迹的隐私度量[J]. 软件学报, 2012, 23(02):352-360.

[18] CUFF P, YU L. Differential privacy as a mutual information constraint[C]//ACM Conference on Computer and Communications Security. [S.l.]: ACM, 2016: 43-54.

[19] WANG W, YING L, ZHANG J. On the relation between identifiability, differential privacy, and mutual-information privacy[J]. IEEE Trans. Information Theory, 2016, 62 (9):5018-5029.

[20] KAIROUZ P, OH S, VISWANATH P. Extremal mechanisms for local differential privacy[C]//NIPS. [S.l.: s.n.], 2014: 2879-2887.

[21] MIRONOV I. Rényi differential privacy[C]//CSF. [S.l.]: IEEE Computer Society, 2017: 263-275.

[22] HOLOHAN N, ANTONATOS S, BRAGHIN S, et al. (k, ε)-anonymity: k-anonymity with ε-differential privacy[J]. CoRR, 2017, abs/1710.01615.

[23] LI N, QARDAJI W H, SU D, et al. Membership privacy: a unifying framework for privacy definitions[C]//ACM Conference on Computer and Communications Security. [S.l.]: ACM, 2013: 889-900.

[24] 熊金波, 王敏燊, 田有亮, 等. 面向云数据的隐私度量研究进展[J]. 软件学报, 2018, 29(7):1963-1980.

[25] WAGNER I, ECKHOFF D. Technical privacy metrics: A systematic survey[J]. ACM Comput. Surv., 2018, 51(3):57:1-57:38.

[26] SHOKRI R, THEODORAKOPOULOS G, BOUDEC J L, et al. Quantifying location privacy[C]//IEEE Symposium on Security and Privacy. [S.l.]: IEEE Computer Society, 2011: 247-262.

[27] MA C Y T, YAU D K Y. On information-theoretic measures for quantifying privacy protection of time-series data[C]//AsiaCCS. [S.l.]: ACM, 2015: 427-438.

[28] ZHAO Y, WAGNER I. Evaluating privacy metrics for graph anonymization and de-anonymization[C]//AsiaCCS. [S.l.]: ACM, 2018: 817-819.

[29] 俞艺涵, 付钰, 吴晓平. 基于Shannon信息熵与BP神经网络的隐私数据度量与分级模型[J]. 通信学报, 2018, 39(12):10-17.

[30] HUMBERT M, AYDAY E, HUBAUX J P, et al. Addressing the concerns of the lacks family: Quantification of kin genomic privacy[C]//CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York, NY, USA: ACM, 2013: 1141-1152.

[31] OLTEANU A, HUGUENIN K, SHOKRI R, et al. Quantifying interdependent privacy risks with location data[J]. IEEE Trans. Mob. Comput., 2017, 16(3):829-842.

[32] DEZNABI I, MOBAYEN M, JAFARI N, et al. An inference attack on genomic data using kinship, complex correlations, and phenotype information[J]. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2018, 15(4):1333 - 1343.

[33] MANOUSAKAS D, MASCOLO C, BERESFORD A R, et al. Quantifying privacy loss of human mobility graph topology[J]. PoPETs, 2018, 2018(3):5-21.

[34] CAO Y, YOSHIKAWA M, XIAO Y, et al. Quantifying differential privacy in continuous data release under temporal correlations[J]. IEEE Trans. Knowl. Data Eng., 2019, 31 (7):1281-1295.

[35] SHOKRI R, STRONATI M, SONG C, et al. Membership inference attacks against machine learning models[C]//IEEE Symposium on Security and Privacy. [S.l.]: IEEE Computer Society, 2017: 3-18.

[36] RAHMAN M A, RAHMAN T, LAGANIÈRE R, et al. Membership inference attack against differentially private deep learning model[J]. Transactions on Data Privacy, 2018, 11(1):61-79.

[37] CHEU A, SMITH A D, ULLMAN J, et al. Distributed differential privacy via shuffling [C]//Lecture Notes in Computer Science: volume 11476 EUROCRYPT (1). [S.l.]: Springer, 2019: 375-403.

[38] XU C, REN J, ZHANG D, et al. Ganobfuscator: Mitigating information leakage under GAN via differential privacy[J]. IEEE Trans. Information Forensics and Security, 2019, 14(9):2358-2371.

[39] YU L, LIU L, PU C, et al. Differentially private model publishing for deep learning[C]// IEEE Symposium on Security and Privacy. [S.l.]: IEEE, 2019: 332-349.

[40] WANG Q, ZHANG Y, LU X, et al. Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy[J]. IEEE Trans. Dependable Sec. Comput., 2018, 15(4):591-606.

[41] 李昊, 张敏, 冯登国, 等. 大数据访问控制研究[J]. 计算机学报, 2017, 40(1):72-91.

[42] NI Q, TROMBETTA A, BERTINO E, et al. Privacy-aware role based access control [C]//SACMAT. [S.l.]: ACM, 2007: 41-50.

[43] EDEMACU K, PARK H K, JANG B, et al. Privacy provision in collaborative ehealth with attribute-based encryption: Survey, challenges and future directions[J]. IEEE Access, 2019, 7:89614-89636.

[44] WANG Y, TIAN L, CHEN Z. Game analysis of access control based on user behavior trust[J]. Information, 2019, 10(4):132.

[45] LIU D, LI N, WANG X, et al. Beyond risk-based access control: Towards incentive-based access control[C]//Lecture Notes in Computer Science: volume 7035 Financial Cryptography. [S.l.]: Springer, 2011: 102-112.

[46] AMINI M, OSANLOO F. Purpose-based privacy preserving access control for secure service provision and composition[J]. IEEE Trans. Services Computing, 2019, 12(4): 604-620.

[47] 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.

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

[49] WANG Q, JIN H. Quantified risk-adaptive access control for patient privacy protection in health information systems[C]//AsiaCCS. [S.l.]: ACM, 2011: 406-410.

[50] LI T, LI N. On the tradeoff between privacy and utility in data publishing[C]//KDD. [S.l.]: ACM, 2009: 517-526.

[51] SUI X, BOUTILIER C. Efficiency and privacy tradeoffs in mechanism design[C]// AAAI. [S.l.]: AAAI Press, 2011.

[52] GUO S, CHEN K. Mining privacy settings to find optimal privacy-utility tradeoffs for social network services[C]//SocialCom/PASSAT. [S.l.]: IEEE Computer Society, 2012: 656-665.

[53] SANKAR L, RAJAGOPALAN S R, POOR H V. Utility-privacy tradeoffs in databases: An information-theoretic approach[J]. IEEE Trans. Information Forensics and Security, 2013, 8(6):838-852.

[54] KALANTARI K, SANKAR L, SARWATE A D. Robust privacy-utility tradeoffs under differential privacy and hamming distortion[J]. IEEE Trans. Information Forensics and Security, 2018, 13(11):2816-2830.

[55] HE Z, LI J. Modeling snp-trait associations and realizing privacy-utility tradeoff in genomic data publishing[C]//Lecture Notes in Computer Science: volume 11490 ISBRA. [S.l.]: Springer, 2019: 65-72.

[56] ZHU Q, RASS S. Game theory meets network security: A tutorial[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. [S.l.: s.n.], 2018: 2163-2165.

[57] FREUDIGER J, MANSHAEI M H, HUBAUX J, et al. On non-cooperative location privacy: a game-theoretic analysis[C]//ACM Conference on Computer and Communications Security. [S.l.]: ACM, 2009: 324-337.

[58] SANTOS F, HUMBERT M, SHOKRI R, et al. Collaborative location privacy with rational users[C]//Lecture Notes in Computer Science: volume 7037 GameSec. [S.l.]: Springer, 2011: 163-181.

[59] WANG W, ZHANG Q. A stochastic game for privacy preserving context sensing on mobile phone[C]//INFOCOM. [S.l.]: IEEE, 2014: 2328-2336.

[60] SHOKRI R, THEODORAKOPOULOS G, TRONCOSO C. Privacy games along location traces: A game-theoretic framework for optimizing location privacy[J]. ACM Trans. Priv. Secur., 2017, 19(4):11:1-11:31.

[61] DU J, JIANG C, CHEN K, et al. Community-structured evolutionary game for privacy protection in social networks[J]. IEEE Trans. Information Forensics and Security, 2018, 13(3):574-589.

[62] HU H, AHN G, ZHAO Z, et al. Game theoretic analysis of multiparty access control in online social networks[C]//SACMAT. [S.l.]: ACM, 2014: 93-102.

[63] 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.

[64] 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.

[65] 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.

[66] Shannon C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948, 27(3):379-423.

[67] STONE J V. Information theory: A tutorial introduction[J]. CoRR, 2018, abs/1802.05968.

[68] The Genomes Project Consortium. A global reference for human genetic variation[J]. Nature, 2015, 526:68.

[69] U.S. Equal Employment Opportunity Commission. Genetic information nondiscrimination act of 2008[M]. [S.l.]: Eeoc.gov, 2008.

[70] SWEENEY L, ABU A, WINN J. Identifying participants in the personal genome project by name[Z/OL]. Data Privacy Lab, IQSS, Harvard University, 2013. http://dataprivacylab.org/projects/pgp/.

[71] GYMREK M, MCGUIRE A L, GOLAN D, et al. Identifying personal genomes by surname inference[J]. Science, 2013, 339(6117):321-324.

[72] CAI R, HAO Z, WINSLETT M, et al. Deterministic identification of specific individuals from gwas results[J]. Bioinformatics, 2015, 31(11):1701-1707.

[73] SHRINGARPURE S, BUSTAMANTE C. Privacy Risks from Genomic Data-Sharing Beacons[J]. American Journal of Human Genetics, 2015, 97(5):631-646.

[74] WALSH S, LIU F, BALLANTYNE K N, et al. Irisplex: A sensitive dna tool for accurate prediction of blue and brown eye colour in the absence of ancestry information[J]. Forensic Science International: Genetics, 2011, 5(3):170 - 180.

[75] ROHLFS R V, FULLERTON S M, WEIR B S. Familial identification: Population structure and relationship distinguishability[J]. PLOS Genetics, 2012, 8(2):e1002469.

[76] HESS P. Controversial geneticist warns: We can read your face in your dna.[M]. [S.l.]: Eeoc.gov, 2017.

[77] SCUTTI S. What the golden state killer case means for your genetic privacy[M]. [S.l.]: CNN, 2018.

[78] SHI X, WU X. An overview of human genetic privacy[J]. Annals of the New York Academy of Sciences, 2017, 1387(1):61-72.

[79] SAMANI S S, HUANG Z, AYDAY E, et al. Quantifying genomic privacy via inference attack with high-order snv correlations[C]//SPW '15: Proceedings of the 2015 IEEE Security and Privacy Workshops. Washington, DC, USA: IEEE Computer Society, 2015: 32-40.

[80] HOWIE B N, DONNELLY P, MARCHINI J. A flexible and accurate genotype imputation method for the next generation of genome-wide association studies[J]. PLOS Genetics, 2009, 5(6):1-15.

[81] En.wikipedia.org. Inference attack[EB/OL]. 2018[21 May 2018]. https://en.wikipedia.org/wiki/Inference_attack.

[82] NARAIN S, VO-HUU T D, BLOCK K, et al. Inferring user routes and locations using zero-permission mobile sensors[C]//IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016. [S.l.: s.n.], 2016: 397-413.

[83] GONG N Z, LIU B. You are who you know and how you behave: Attribute inference attacks via users' social friends and behaviors[C]//25th *USENIX* Security Symposium (*USENIX* Security 16). [S.l.: s.n.], 2016: 979-995.

[84] GANJU K, WANG Q, YANG W, et al. Property inference attacks on fully connected neural networks using permutation invariant representations[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. [S.l.: s.n.], 2018: 619-633.

[85] POULIOT D, WRIGHT C V. The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016. [S.l.: s.n.], 2016: 1341-1352.

[86] WANG R, LI Y F, WANG X, et al. Learning your identity and disease from research papers: Information leaks in genome wide association study[C]//CCS '09: Proceedings of the 16th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2009: 534-544.

[87] HE Z, LI Y, LI J, et al. Addressing the threats of inference attacks on traits and genotypes from individual genomic data[C]//Bioinformatics Research and Applications - 13th International Symposium, ISBRA 2017, Honolulu, HI, USA, May 29 - June 2, 2017, Proceedings. [S.l.: s.n.], 2017: 223-233.

[88] AYDAY E, HUMBERT M. Inference attacks against kin genomic privacy[J]. IEEE Security & Privacy, 2017, 15(5):29-37.

[89] HOMER N, SZELINGER S, REDMAN M, et al. Resolving individuals contributing trace amounts of dna to highly complex mixtures using high-density snp genotyping microarrays[J]. PLOS Genetics, 2008, 4(8):1-9.

[90] MAILMAN M D, FEOLO M, JIN Y, et al. The ncbi dbgap database of genotypes and phenotypes[J]. Nature genetics, 2007, 39(10):1181.

[91] The National Human Genome Research Institute. Privacy in genomics[EB/OL]. 2015 [April 21, 2015]. https://www.genome.gov/27561246/privacy-in-genomics.

[92] WANG Y, WEN J, WU X, et al. Infringement of individual privacy via mining differentially private gwas statistics[C]//WANG Y, YU G, ZHANG Y, et al. Big Data Computing and Communications. Cham: Springer International Publishing, 2016: 355-366.

[93] HARMANCI A, GERSTEIN M. Quantification of private information leakage from phenotype-genotype data: linking attacks[J]. Nature Methods, 2016, 13(3):251-256.

[94] SCHADT E E, WOO S, HAO K. Bayesian method to predict individual SNP genotypes from gene expression data[J]. Nature Genetics, 2012, 44(5):603-608.

[95] LIBBRECHT M W, NOBLE W S. Machine learning applications in genetics and genomics[J]. Nature Reviews Genetics, 2015, 16(6):321-332.

[96] DURBIN R, EDDY S R, KROGH A, et al. Biological sequence analysis: probabilistic models of proteins and nucleic acids[M]. [S.l.]: Cambridge university press, 1998.

[97] RABINER L R. A tutorial on hidden Markov models and selected applications in speech recognition[J]. Proceedings of the IEEE, 1989, 77(2):257-286.

[98] STAMP M. A revealing introduction to hidden Markov models[J]. Department of Computer Science San Jose State University, 2004:26-56.

[99] HU J, BROWN M K, TURIN W. Hmm based online handwriting recognition[J]. IEEE Transactions on pattern analysis and machine intelligence, 1996, 18(10):1039-1045.

[100] LONG J, SHELHAMER E, DARRELL T. Fully convolutional networks for semantic segmentation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 39(4):640-651.

[101] NYHOLT D R, YU C E, VISSCHER P M. On Jim Watson's APOE status: genetic information is hard to hide[J]. European Journal of Human Genetics, 2009, 17(2):147-149.

[102]]IGSR2019 The International Genome Sample Resource (IGSR). IGSR: The international genome sample resource[EB/OL]. [January 30, 2015]. http://www.internationalgenome.org/.

[103] HOWIE B, MARCHINI J. IMPUTE2[EB/OL]. 2014[23 Dec 2014]. https://mathgen.stats.ox.ac.uk/impute/impute_v2.html#reference.

[104] AYDAY E, RAISARO J L, HUBAUX J. Personal use of the genomic data: Privacy vs. storage cost[C]//2013 IEEE Global Communications Conference, GLOBECOM 2013, Atlanta, GA, USA, December 9-13, 2013. [S.l.: s.n.], 2013: 2723-2729.

[105] WAGNER I. Evaluating the strength of genomic privacy metrics[J]. ACM Trans. Priv. Secur., 2017, 20(1):2:1-2:34.

[106] MARCHINI J, HOWIE B, MYERS S, et al. A new multipoint method for genome-wide association studies by imputation of genotypes[J]. Nature Genetics, 2007, 39(7): 906-913.

[107] The International Genome Sample Resource (IGSR). Which populations are part of your study?[EB/OL]. 2015[January 30, 2015]. http://www.internationalgenome.org/category/population/.

[108] THORISSON G A, SMITH A V, KRISHNAN L, et al. The international hapmap project web site[J]. Genome research, 2005, 15(11):1592-1593.

[109] QIAN J. ACLA: A framework for access control list (ACL) analysis and optimization[C]//IFIP Conference Proceedings: volume 192 Communications and Multimedia Security. [S.l.]: Kluwer, 2001.

[110] JUNG Y, JOSHI J B D. Cribac: Community-centric role interaction based access control model[J]. Computers & Security, 2012, 31(4):497-523.

[111] ZHANG Q, MU Y, ZHANG M. Attribute-based authentication for multi-agent systems with dynamic groups[J]. Computer Communications, 2011, 34(3):436-446.

[112] HUANG D, TSAI W, TSENG Y. Policy management for secure data access control in vehicular networks[J]. J. Network Syst. Manage., 2011, 19(4):448-471.

[113] NI Q, BERTINO E, LOBO J. Risk-based access control systems built on fuzzy inferences[C]//AsiaCCS. [S.l.]: ACM, 2010: 250-260.

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

[115] CHOI D, KIM D, PARK S. A framework for context sensitive risk-based access control in medical information systems[J]. Comp. Math. Methods in Medicine, 2015, 2015: 265132:1-265132:9.

[116] CHEN L, CRAMPTON J. Risk-aware role-based access control[C]//Lecture Notes in Computer Science: volume 7170 STM. [S.l.]: Springer, 2011: 140-156.

[117] KHAMBHAMMETTU H, BOULARES S, ADI K, et al. A framework for risk assessment in access control systems[J]. Computer Security, 2013, 39:86-103.

[118] 惠榛, 李昊, 张敏, 等. 面向医疗大数据的风险自适应的访问控制模型[J]. 通信学报, 2015, 36(12):190-199.

[119] VERMA M. Xml security: Control information access with xacml[R]. [S.l.]: IBM, 2004.

[120] DOS SANTOS D R, WESTPHALL C M, WESTPHALL C B. A dynamic risk-based access control architecture for cloud computing[C]//NOMS. [S.l.]: IEEE, 2014: 1-9.

[121] LAMPSON B W. Protection[J]. ACM SIGOPS Operating Systems Review, 1974, 8(1): 18-24.

[122] BELL D E, LAPADULA L J. Secure computer systems: Mathematical foundations[R]. [S.l.]: Miter Corp Bedford Ma, 1973.

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

[124] KUHN D R, COYNE E J, WEIL T R. Adding attributes to role-based access control[J]. Computer, 2010, 43(6):79-81.

[125] 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.

[126] PACI F, SQUICCIARINI A C, ZANNONE N. Survey on access control for community-centered collaborative systems[J]. ACM Computing Surveys (CSUR), 2018, 51(1):6:1-6:38.

[127] 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.

[128] PUSTCHI N, SANDHU R. Mt-abac: A multi-tenant attribute-based access control model with tenant trust[C]//QIU M, XU S, YUNG M, et al. Network and System Security. Cham: Springer International Publishing, 2015: 206-220.

[129] GIBBONS R. Game theory for applied economists[M]. Princeton: Princeton University Press, 1992.

[130] DO C T, TRAN N H, HONG C S, et al. Game theory for cyber security and privacy[J]. ACM Computing Surveys (CSUR), 2017, 50(2):30:1-30:37.

[131] ZHANG Y, HE J, ZHAO B, et al. Towards more pro-active access control in computer systems and networks[J]. Computers and Security, 2015, 49(C):132-146.

[132] 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.

[133] BIJON K Z, KRISHNAN R, SANDHU R. Risk-aware rbac sessions[C]// VENKATAKRISHNAN V, GOSWAMI D. Information Systems Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 59-74.

[134] DIEP N N, HUNG L X, ZHUNG Y, et al. Enforcing access control using risk assessment [C]//Fourth European Conference on Universal Multiservice Networks (ECUMN'07). [S.l.: s.n.], 2007: 419-424.