Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Cybersecurity—Review

实现隐私保护个性化推荐服务

王聪 [a,b,*]，郑宜峰 [a,b]，蒋精华 [a,c]，任奎 [d]

[a] Department of Computer Science, City University of Hong Kong, Hong Kong, China
[b] City University of Hong Kong, Shenzhen Research Institute, Shenzhen, Guangdong 518057, China
[c] Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China
[d] Institute of Cyber Security Research, Zhejiang University, Hangzhou, Zhejiang 310058, China

ARTICLE INFO

Article history:
Received 21 June 2017
Revised 26 September 2017
Accepted 12 February 2018
Available online 16 February 2018

关键词
隐私保护
个性化推荐服务
针对性推送
协同过滤
机器学习

摘要

推荐系统对于向用户提供个性化服务至关重要。通过个性化的推荐服务，用户可以享受各种有针对性的推荐，如电影、书籍、广告、餐馆等。此外，个性化推荐服务极大地推动了在线业务收入的增长。尽管存在诸多好处，但采用个性化推荐服务通常需要收集用户的个人数据以进行处理和分析，会让用户怀疑个人隐私遭到严重侵犯。因此，在尊重用户隐私的前提下开发实用的隐私保护技术来维护个性化推荐服务提供的数据尤为重要。在本文中，我们提供了与隐私保护的个性化推荐服务相关文献的综合调查。我们介绍了个性化推荐系统的总体架构、其中的隐私问题以及集中于隐私保护个性化推荐服务的现有研究。根据个性化推荐和隐私保护的核心支撑技术，我们对现有研究进行了分类，并对其优缺点进行了深入的讨论和对比，特别是针对隐私和推荐的准确性。与此同时，我们也确定了一些未来的研究方向。

1. 引言

如今，推荐系统日益普及并被广泛应用于在线服务。推荐系统的广泛使用允许用户享受针对电影、书籍、广告、餐馆、酒店等的各种个性化推荐。同时，个性化推荐服务也极大地推动了网上业务收入的增长。例如，最近的研究表明，消费者在亚马逊（Amazon）购买的商品中有35%以及他们在网飞（Netfix）上看到的商品的75%都来源于个性化推荐[1]。研究公司Marketing Sherpa进行的一项研究表明，在通过电子商务网站购物产生的收入中，11.5%都来自通过个性化推荐购买的产品[2]。

为了支持个性化推荐，现有的系统通常采用基于协作过滤（CFB）的推荐或基于内容（CB）的推荐[3]。CFB推荐系统通常基于用户之间的相似性来进行推荐。例如，一部电影的用户评级可以通过其他类似用户的评级/决定（经由某些度量分类）来预测。CB推荐系统通常通过比较推荐物的属性和用户的个人偏好/行为数据的属性来进行推荐。例如，广告网络可以将与广告相关联的关键字与指示用户偏好的关键字进行比较，以便提供个性化广告。为了从这些系统获得个性化推荐，用户通常需要将其个人数据提供给推荐人进行处

* Corresponding author.
E-mail address: congwang@cityu.edu.hk (C. Wang)

英文原文: Engineering 2018, 4(1): 21–28
引用本文: Cong Wang, Yifeng Zheng, Jinghua Jiang, Kui Ren. Toward Privacy-Preserving Personalized Recommendation Services. *Engineering*: https://doi.org/10.1016/j.eng.2018.02.005

理和分析。

尽管个性化推荐十分有用，但直接向推荐者展示用户的隐私数据会给用户带来隐私风险[4–6]：①提供的数据可能导致向推荐人泄露用户的个人利益；②所提供的数据可能会被推荐人滥用，例如，推荐人为了获利而在未经用户同意的情况下将数据卖给第三方 [4]；③由于推荐方的安全漏洞，所提供的数据可能会被攻击者蓄意盗取[5,6]。因此，为推荐系统开发隐私保护技术非常重要，这样既可以保留推荐系统的数据，同时也能尊重用户的隐私。

在本文中，我们调查了与隐私保护相关的个性化推荐服务的相关文献。我们首先介绍当今社会推荐系统的总体架构和其中的隐私问题；然后对现有解决方案进行全面的调查，以支持隐私保护个性化推荐服务。如上所述，推荐系统采用的机制通常是CFB或CB。基于这种观察，我们首先将现有解决方案分为两大类：①隐私保护CFB推荐；②隐私保护CB推荐。在第一类中，根据所采用的具体明文技术，现有研究可进一步分为基于隐私保护的邻近用户方法和基于隐私保护机器学习的方法；在第二类中，根据具体的应用设置，现有研究可进一步分类为隐私保护定向广告和隐私保护定向优惠券推送。因此，总共有4个明确的类别。

在描述每个类别中具有代表性的现有工作时，我们的关键点是根据隐私保护的基本安全策略/技术对其进行进一步分类，例如，一些研究依赖于诸如同态加密和乱码电路（GC）的密码技术，而另一些则采用模糊处理技术。在这一趋势领域的大量工作中，我们仔细挑选了引用率高的描述当前流行技术的代表性工作，以及提供重大新兴技术的文献。我们的目标是尽可能全面地覆盖每个类别，以号召该领域的进一步积极研究。

本文的其余部分安排如下：第2部分介绍了推荐系统的总体架构和隐私问题；第3部分介绍了关于隐私保护CFB推荐的现有研究；第4部分介绍了保护隐私的CB推荐的现有研究；第5部分讨论了一些未来的研究方向；第6部分总结全文。

2. 推荐系统

2.1. 系统模型

推荐系统旨在通过采用有效的方法收集和处理用户的个人数据，从而为用户提供准确的建议[7]。个性化推荐服务的系统模型如图1所示。它包含两个主要对象：用户和推荐者。每个用户在其本地设备（如智能手机）上都有一些个人数据，表明他的个人兴趣/喜好。推荐人收集和处理用户的个人数据，并为用户提供个性化推荐。生成的建议可以以各种方式提供给用户或向用户显示，如通过消息和弹出窗口。

为了处理收集的用户数据以进行推荐，推荐者可以采用不同的技术。粗略地说，根据采用的技术，推荐系统可以分为两类：CFB推荐系统和CB推荐系统。如前所述，CFB推荐系统根据用户之间的相似性推荐项目。也就是说，向特定用户推荐的项目是具有相似偏好的其他用户所感兴趣的项目[3]。相反，CB推荐系统基于项目的性质来执行推荐，其可以通过某些显性特征（如属性和特性）来描述。

为了利用用户之间的相似性，CFB推荐系统通常采用基于隐私保护的邻近用户的方法或基于机器学习的方法。基于隐私保护的邻近用户的方法直接计算用户之间的相似关系[8]，并利用这种关系来生成个性化的推荐；相反，基于机器学习的方法首先从收集的用户数据中学习数学模型，然后应用该模型生成个性化推荐。

2.2. 隐私问题

推荐人收集的个人数据越多，用户可以获得的建议也就越准确。推荐人收集的用户数据可能包括有关用户身份、人口统计资料、行为数据、购买历史记录、评级记录等信息[9]。这些信息会对隐私非常敏感。例如，人口统计资料是指顾客的人口特征，如年龄、性别、体重和教育程度；行为数据是指客户的动态数据，如位置、活动状态和浏览历史；评级历史是指顾客在物品上提供的投票。向推荐人明确提供这些信息会造成不良的隐私风险。例如，用户数据可能会在未经用户同意的情况下被推荐人出售给第三方，甚至可能被歹徒伺机盗取。因此，保护推荐系统中的用户数据至关重要。

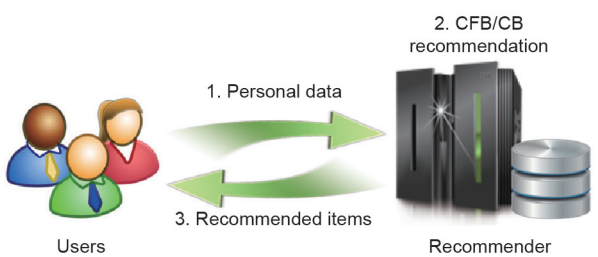

图1. 个性化推荐服务的系统模型。推荐人可以采用基于协作过滤（CFB）的技术或基于内容（CB）的技术。

3. 隐私保护 CFB 推荐

CFB推荐系统通常基于用户之间的相似性度量推荐事物[3]。为了在保护用户隐私的同时支持CFB建议的功能，我们已经开展了许多有关保护隐私的CFB推荐。由于CFB推荐系统通常采用基于隐私保护的邻近用户的方法或基于机器学习的方法，因此我们将这些现有的研究分为两类：基于隐私保护的邻近用户的方法和基于隐私保护机器学习的方法。

3.1. 基于隐私保护的邻近用户的方法

在基于隐私保护的邻近用户的方法支撑下的现有解决方案通常采用两种主要类别的技术。第一类是密码技术[4,6,10,11]，第二类是随机化技术[12–14]。基于密码技术的解决方案通常需要很大的高负荷运算，这可能不太适合大规模数据。但是，这种方法可以在保证推荐准确性的同时在语义安全下为用户数据提供强有力的保护。基于随机化技术的解决方案将随机扰动应用于用户的隐私保护数据，例如通过添加适当的噪声；此过程通常为用户隐私牺牲准确性。但这种方法的运算负荷较低，并且比基于密码技术的方法快得多。在下文中，我们描述了一些有代表性的、基于密码技术的解决方案的代表研究[4,6,10,11]和基于随机化技术的解决方案[12–14]。

Erkin等[6]提出了使用部分同态加密（PHE）和安全多方计算（SMC）协议的高效隐私保护推荐系统。他们的设计通过PHE加密用户的隐私保护数据（即用户对项目的评级），因此推荐人无法访问原始评级，同时仍然能够处理数据以生成隐私保护推荐。更具体地说，为了避免用户与推荐者的主动交互，他们的设计引入了半信任的第三方来帮助推荐者完成加密域中的推荐。推荐人或第三方都不能获取用户的隐私保护数据。有了这种架构，用户只需将他们的加密数据上传到推荐人手中，随后保持离线状态。推荐人会与第三方执行密码协议以生成个性化推荐。由于直接应用PHE会导致高昂的计算和通信开销，Erkin等[6]进一步设计了打包技术，在加密之前紧凑地打包多个数值，从而大大提高了整个系统的性能。

后来，Badsha等[10]提出了一种基于ElGamal密码体制的推荐系统，它是PHE的一种。与参考文献[6]中的研究相比，他们的设计没有引入额外的协助方，但所有用户都需要积极与推荐服务器协作，以便为目标用户生成隐私保护推荐。最近，Badsha等[11]设计了一个新的推荐系统，该系统依赖于Boneh-Goh-Nissim（BGN）同态密码系统。与参考文献[6]中的研究类似，他们的设计采用了额外的服务器来协助；但是，推荐服务器和附加服务器之间不会进行交互。附加服务器仅在需要时帮助用户解密密文。想要获得隐私保护推荐的用户必须与推荐/附加服务器进行有效交互。也就是说，用户不能简单地将其隐私保护数据发送给推荐服务器进行处理，从而直接获得个性化推荐。

与上述研究不同，Li等[4]基于用户群的思想提出了一个名为YANA的隐私保护推荐系统（“you are not alone”的简称，意为“你并不孤单”）。在YANA中，用户被划分成具有不同兴趣的群体，并通过特定兴趣的虚拟用户与推荐人进行交互。这样，单个用户的个人兴趣信息就会对服务器保密。他们还提出了一套SMC协议和推荐策略，以在推荐流程中保护个人用户隐私免受其他小组成员侵害。YANA采用的想法类似于隐私保护数据发布中的k-匿名和l-多样性。然而，在k-匿名和l-多样性中，中央服务器能明码收集用户数据，然后将所收集的数据匿名化，以防止第三方识别个别用户。在隐私保护个性化推荐的情况下，收集用户数据的服务器通常是不可信的，因此用户应该以分布式并且隐私保护的方式进行分组和维护。

Polat和Du[12]提出应用数据随机化技术来保护用户数据，而不采用昂贵的加密技术。特别的是，每个用户在将个人数据发送给推荐人之前，都会通过添加随机噪声扰乱其个人数据。由于推荐人只收到噪声数据，因此无法获得有关用户的准确信息。只要用户数量足够大，推荐人仍然可以基于汇总信息生成个性化推荐，这些信息可以从加扰的用户数据中获得，而且有较高的准确性。然而，一些研究[15–17]表明，这种提出的扰动技术仍然可能泄露用户隐私保护数据的相关信息。

Shokri等[13]提出了一种新的混淆机制以模糊处理来自不可信服务器的用户项目连接。在该系统中，假设有一个中央推荐服务器存储用户的在线配置文件并为用户提供建议。用户也存储了各自本地命名的离线档案。推荐服务器仅根据在线配置文件生成个性化推荐。当用户更新最近评级的项目时，每个用户都将其在线个人资料与其离线个人资料独立同步。为了保护隐私，除了用户的实际评级外，用户还会将其他用户的项目信息添加到其个人资料中。具体来说，用户任意选择一些同龄人以及关于所选同龄人的离线档案的某些信息，并将他们

的一些项目添加到其档案中。因此，用户的实际配置文件对服务器是隐藏的，因为服务器不知道用户实际评价了哪些项目。该混淆机制仍然可以更准确地显示用户的兴趣。同时，混淆机制在推荐准确性方面还是存在一定的取舍。

针对实用的可扩展性，Chow等[14]后来提出了一个新的隐私保护协作过滤系统来容纳大量的用户。在该系统中，通过正确使用局部敏感哈希（LSH）技术，用户首先基于相互相似性进行聚类。这与参考文献[12]中的研究不同，他们的研究中类似的用户可通过噪声等级被识别。接下来，根据同一集群中类似用户的总评级生成个性化推荐。这种设计通过修改现有的LSH技术，以保护隐私的方式创建一个原始类似的用户群。Chow等[14]也在隐私保护生成个性化推荐的过程中加入了人工评级。

更具体地说，该设计包括聚类步骤和推荐步骤。在聚类步骤中，推荐者将LSH算法分配给用户。使用这种散列函数，用户之间的相似性可以通过它们评级的LSH值之间的匹配来衡量。为了计算LSH值，每个用户都会进行一些预处理，例如，通过减去平均值来标准化他们的评级，LSH值随后被上传到推荐者。在推荐步骤中，推荐人在无法看到明码用户数据的情况下，计算所有LSH值相同的用户的平均评级。为了保护用户的隐私，Chow等[14]提出让用户向推荐人发送混淆评级，这仍然可以让推荐人计算平均评级。具体来说，即通过为随机选择的电影添加人为评级来进行混淆。人工评级与真实评级数量的比例是可调系统参数，这也决定了隐私-效用的权衡。较高的比例意味着较强的隐私，但准确性却较低。

3.2. 基于隐私保护机器学习的方法

其他研究探索了隐私保护基于机器学习的推荐。这些研究的基本思想是首先以保护隐私的方式对收集的用户数据进行机器学习模型训练，然后应用该模型生成个性化的推荐。这些研究中通常采用的机器学习技术包括矩阵分解（MF）和岭回归（RR）。为了保护隐私，这些工作通常依赖于加密技术，包括PHE、完全同态加密（FHE）和GCs。在下文中，我们将介绍一些有代表性的工作。

Nikolaenko等[18] 针对推荐系统提出了隐私保护MF设计。MF技术旨在通过用户评级中学习项目配置文件和用户配置文件。给定一个项目配置文件和一个用户配置文件（其中一个是向量），然后可以通过向量的内积来进行评级预测。在此设计中，推荐人收集加密的用户评级，与第三方[称为加密服务提供商（CSP）]一起运行隐私保护MF协议。该协议的安全目标主要是确保推荐人和CSP都不能学习用户评级。在协议执行结束时，将生成项目配置文件，然后利用该配置文件为未评估项目上的用户进行预测。需要注意，由于公开项目配置文件和用户配置文件可能很容易侵犯用户隐私，因此此协议不会在推荐人一方生成用户配置文件。

为了支持保护隐私的MF，Nikolaenko等[18]采用了结合PHE和GC的混合方法。在这种方法中，用户评级由CSP的公共密钥下的部分同态密码系统加密。收集所有加密的用户评级后，推荐人将加密域中的随机掩码添加到用户评级中，并将得到的密文发送给CSP，CSP解密密文并获得被屏蔽的用户评级。随后CSP准备一个GC，将输入掩码用户评级和随机掩码的乱码值作为输入值。在回路内部，首先通过从掩蔽的用户评级中去除掩模来恢复用户评级，随后执行MF。在基于构建的GC运行协议后，会生成项目配置文件。

获得项目配置文件后，生成隐私保护预测的方式如下：推荐人将项目配置文件发送给用户，该用户首先通过解决优化问题恢复自己的配置文件。拥有项目配置文件和其自己的配置文件后，用户就可以生成本地预测以评估未分级项目。除了这个基本的方法，Nikolaenko等[18]还提出了一种机制来要求推荐人以隐私保护的方式为用户提供预测。

作为提高参考文献[18]中工作效率的后续研究，Kim等[19]提出了一种基于FHE的高效隐私保护MF协议。他们采用了与参考文献[18]中相似的体系结构，引入CSP来协助推荐人执行基于梯度下降法的MF。在该协议中，CSP拥有两个密钥对：一个是部分同态密码系统，另一个是完全同态密码系统。每个用户在部分同态密码系统的公钥下对其评级进行加密，并将密文发送给推荐者，推荐者随后使用基于随机掩码的CSP运行协议，以将部分同态密文转换为完全同态密文。接下来，推荐者和CSP基于FHE和随机掩码，联合执行基于梯度下降的MF以产生加密的项目简档和用户简档。由于梯度下降本质上需要矢量的内积，所以直接应用FHE效率不高。因此，Kim等[19]引入了一种新颖的数据结构，以充分利用FHE密文中单指令多数据（SIMD）操作所支持的时间段。也就是说，它允许一个同态操作在梯度下降期间对矢量进行多种操作。

考虑到披露用户评价的项目可能会泄露诸如性别等个人信息，Kim等[19]通过注入虚拟评级，然后在加密域中运行以消除虚拟评级的影响，进一步增强了他们的设计使用用户输入的指标。值得注意，虽然参考文献[18]也提到了这种方法，但它没有被包括在其中用于效率问题的设计中。

与参考文献[18]和[19]中的研究不同，Nikolaenko等[20]研究了另一种具有隐私保护功能的机器学习技术：隐私保护RR。在基于RR的推荐中，推荐人收集不同项目的许多用户的偏好和评级，并对数据运行学习算法。学习算法生成一个模型，可用于预测新用户对特定项目的评级。Nikolaenko等[20]设计了一个协议，使推荐人能够在没有看到明码用户数据的情况下学习模型。

在此系统架构中，引入了第三方CSP与推荐人合作以完成学习过程。与参考文献[18]中的工作类似，Nikolaenko等[20]通过结合同态加密和GC来设计隐私保护RR协议。提议的协议包含两个阶段。在第一阶段，每个用户在CSP的公共密钥下加密其数据记录，并将密文发送给推荐人。然后推荐者利用同态加密的同态加法性质来执行跨不同用户数据的聚合。这样的聚合是可行的，因为它们重新制定了RR问题，导致大量减少用于进一步处理的数据量。在第二阶段，推荐人为加密域中的加密聚合数据添加随机掩码，并将密文发送给CSP，CSP执行解密并获得掩蔽的汇总数据。为了安全地找出模型，CSP构建了一个GC，其中掩码聚合数据和随机掩码的乱码值作为输入值。在基于构建的GC的协议运行之后，该模型被生成并且可以被进一步用于对推荐进行预测。这项工作没有具体说明如何安全地应用学习模型来生成个性化建议。

作为提高参考文献[20]中工作效率的后续工作，Hu等[21]提出了一种新的隐私保护RR协议，该协议纯粹基于PHE和随机掩码，并且在推荐者和第三方之间运行。为了实现高效率，他们高度利用PHE的打包支持属性，如Paillier密码系统。特别的是，他们设计了一个打包安全乘法协议，可以在加密域中同时计算多对私密输入的乘积。

基于这种打包的安全乘法协议，Hu等[21]进一步将RR问题重新表达为求解线性方程的问题。然后他们提出采用高斯消除法或Jacobi迭代法来有效地导出学习模型。在此设计中，模型是在加密域中生成的，推荐人无法获取模型。在获得加密模型之后，推荐者将其发送给同样从第三方接收解密密钥的用户。用户可以解密模型并在本地应用模型。

4. 隐私保护 CB 推荐

CB推荐系统根据物品的属性推荐物品。CB推荐服务的两个常见应用是定向广告和定向优惠券发放。在有针对性的广告中，广告网络会收集用户的个人信息并将匹配的广告发送给目标用户。在有针对性的优惠券发放中，供应商拟根据用户的行为配置文件向可能成为忠实常客的特定用户提供有针对性的优惠券。接下来，我们将介绍如何保护每个应用程序中的用户隐私。

4.1. 隐私保护定向广告

诸多研究提出了实现有针对性的广告投放和保护用户个人信息的解决方案。这些研究中通常采用的隐私保护机制包括局部定位[22,23]、博弈论[23]、匿名化[24–26]、密码技术[27]和模糊化[28,29]。在下文中，我们将介绍一些有代表性的研究。

Toubiana等[22]提出采用本地定位策略同时实现行为定位和隐私，并提出了一个名为Adnostic的隐私保护定向广告架构。更具体地说，Adnostic首先预先获取广告列表并在用户访问发布商的页面之前将其存储在本地。当用户浏览发布者的页面时，广告网络将n列广告发送给用户。用户检查最相关的广告是否已经存在于预先获取的列表中。如果所选广告已经存储在本地，浏览器会立即显示它，这会导致页面显示速度加快；否则，用户需要从广告网络下载所选广告进行显示。需要注意的是，无论所选广告是否已存储，Adnostic都会下载所有未预先获取的列出广告，以避免信息泄漏到广告网络。在不可知情况下，n是可配置的参数，较大的值可以实现更精确的目标定位，但会导致网络带宽消耗更多，反之亦然。Adnostic建议n的适当值为20。

在Adnostic中，存在所提取的广告均无法精确地匹配用户偏好的风险，因为广告网络仅向用户提供少量广告。因此，为了覆盖广泛的用户兴趣，应该从广告网络中检索给定兴趣分段系统的每一段至少一个广告。他们对现有的在线行为广告系统进行的调查发现，现有系统中使用的细分受众群的数量在25到100个之间，这给传播广告的数量带来了上限。

后来，Wang等[23]提出了一种设计，该设计还执行针对用户的本地设备。然而，他们的重点是提供激励措

施，让用户点击他们感兴趣的广告，但可能会导致潜在的隐私风险。他们特别提出了一个隐私意识的补偿框架，以通过控制隐私风险来促进有针对性的广告。在他们的框架中，Wang等[23]认为用户、广告经纪人和广告商是理性和利己的实体，他们都只关心自己的利益。为了鼓励用户点击有趣的广告，广告网络为用户隐私广告点击漏洞提供了一定的补偿。这可以有效提高点击率并为广告网络和广告客户创造更多收入。Wang等[23]进一步将该框架建模为3阶段Stackelberg博弈，其中所有实体都被认为是利己的，并且都有通过选择最优策略来最大化自己的公用事业的目标。他们通过分析用户，广告网络和广告商之间的合作和竞争关系，获得纳什均衡。同时，Wang等[23]分析了共享整个市场的广告商之间的竞争。此外，他们将市场分享场景模拟为非合作博弈，并证明存在纳什均衡。简言之，他们提出的框架为广告网络和广告商在实践中强制实施补偿政策以及为用户提供有针对性的广告服务提供了强有力的动力。

Guha等[24]没有在用户的本地设备上执行定位，而是提出了一种被称为Privad的隐私保护广告架构，该架构涉及一个称为经销商的额外方，以保护用户隐私。在Privad中，为了防止广告网络了解客户的身份，经销商匿名了客户和广告网络之间的通信。为了防止经销商学习用户的档案，客户端和广告网络之间的通信被加密，并且只有客户端和广告网络才能正确解密所传输的消息。但是，这样的架构有潜在的局限性：经销商需要始终保持在线状态。这是不可取的，因为在实践中，最好不经常与经销商联系。后来，Backes等[25]提出了一个名为ObliviAd的可证实的安全架构，用于隐私保护在线行为广告，该架构利用了基于安全硬件的隐私保护信息检索（PIR）技术。ObliviAd使用运行在广告网络端的安全协处理器（SC）上的未知的随机存取存储器（ORAM）实现PIR，允许用户检索最符合其个人资料的广告，而不会泄露任何隐私保护个人信息。特别是当用户访问网页时，ObliviAd首先将加密的用户配置文件发送给SC，SC再根据指定的广告网络算法安全地搜索广告并选择最适合用户配置文件的广告子集。搜索和选择方案建立在ORAM协议之上，可以防止广告网络了解有关所选广告的任何信息。为了支持每个关键字有多个不同广告的情况，Backes等[25]进一步修改了使用的ORAM方案。之后，SC以加密形式向用户发送选定的广告。

与参考文献[24]、[25]中的研究不同，Artail和Farhat [26]探讨了隐私保护非本地定位，但没有引入额外的第三方。他们的架构依赖于用户之间的合作来向彼此发出请求和分发广告，并实施洗牌算法来隐藏个人用户彼此的兴趣以及来自广告网络的身份信息。首先，为了在请求广告时隐藏来自广告网络的身份信息，每个用户基于*ad hoc*网络中的洗牌机制聚合其兴趣后，通过其中一个对等用户发送。选定的对等用户充当代理，以匿名方式将广告网络与所收到的汇总兴趣进行联系。收到广告后，选定用户通过*ad hoc*以与收集相同的方式将它们分发给用户。其次，由于用户可能相互不信任，汇总的兴趣不应该泄漏隐私保护信息给对方。在他们的设计中，Artail和Farhat [26]结合了非对称密码系统和洗牌机制来保护个人用户的偏好。

Jiang等[27]没有依赖用户合作，而是利用隐私保护流搜索（PSS）技术来设计另一个隐私保护型定向广告系统，该系统可以在不引入额外第三方的情况下提供隐私保护和准确定位。在此系统中，用户配置文件是从用户的行为数据和本地移动设备上的传感器数据中推断出来的。用户使用该配置文件构建加密广告请求，然后将其发送到不受信任的广告网络中。广告网络处理所有广告上的加密配置文件，并在不知道任何基础内容的情况下返回加密匹配广告。用户使用其私钥恢复匹配的广告。通过这种方式，广告网络可以向具有强大隐私保护的用户提供准确的匹配广告。然而，直接使用PSS来获取安全和准确的移动广告会导致严重的实用性问题。也就是说，这将导致资源受限的移动设备产生高计算和通信开销。因此，Jiang等[27]进一步提出了改善系统计算和通信性能的机制。他们特别提出使用分层结构来表示用户和广告偏好，并利用广告网络中的广告拍卖。他们还建议鼓励用户提供广泛的类别来缩小匹配广告的搜索范围，这可以节省广告网络的计算成本。他们还通过利用预取和缓存机制来使广告加载延迟降至最低，这可以帮助分摊计算和通信成本。

其他研究也利用混淆技术来实现隐私保护定向广告。在参考文献[28]中，Hardt和Nath指出，优化以下3个设计目标在定向广告系统中是不可行的：隐私、效率和广告相关性。因此，他们为定向广告系统中的广告选择制定了优化问题。所提出的优化问题包括3个重要变量。第一个变量是隐私，也就是说，用户与广告网络共享的信息量；第二个变量是带宽效率，指有多少广告发送给用户；第三个变量是效用，也就是传递给用户的广告的相关性。更具体地说，所提出的框架赋予用户决定

与广告网络共享的个人信息量的权利。根据从用户收集的信息，广告网络为用户选择一组广告，但是通信开销受到限制。在从广告网络接收到广告时，用户的本地设备通过分析该用户的所有隐私保护信息来选择最相关的一个显示。因此，他们的框架面临以下挑战：如何以适当的方式选择一组已投放的广告，以便可变效用可以最大化，同时满足可变隐私和带宽效率的限制。Hardt和Nath[28]表明，找到最优广告集合是一个非确定性多项式时间（NP）难题，因此需采用近似技术来解决优化问题。

在一项独立的研究中，Davidson等[29]指出，个性化支持应由操作系统（OS）内的统一系统提供，而不是由单个应用程序提供。一方面，当收集来自所有应用和操作系统交互的用户偏好信息时，与任何指定的应用单独获取信息相比，可以实现相当高的准确度；另一方面，用户通常信任操作系统，因此可信计算库不会通过执行个性化来扩展。为了支持用户端个性化的操作系统支持，Davidson等[29]提出了一个名为MoRePriv的操作系统服务。为了平衡隐私和个性化，MoRePriv将用户的个人配置文件概括为粗粒度配置文件，该配置文件限制了隐私信息泄漏造成的损害。MoRePriv首先捕获操作系统内用户的多个关于用户的（敏感）信息流，如用户的电子邮件、短消息服务（SMS）等，这可能会指示用户的偏好。MoRePriv随后通过解析和分类该信息来推断用户的兴趣。 MoRePriv提供了一组应用程序编程接口（API），可以使第三方应用程序有限地访问用户配置文件。

4.2. 隐私保护定向优惠券发放

虽然文献中包含了大量关于隐私保护定向广告的研究，但是关于安全定位优惠券发放的研究很少。与私有定向广告相比，定向优惠券投放带来了额外的安全风险。首先，它要求将有针对性的优惠券投放给符合条件的用户，这些用户的行为档案可以准确地满足供应商的定位资料，这是为了防止利用优惠券进行攻击；其次，在整个有针对性的优惠券发放程序中，除符合条件的非资格用户外，不符合条件的用户不应了解有关供应商的定位资料的任何内容，否则，有资格的用户可能会尝试利用他们学习的信息获得目标优惠券[30–32]。在文献中，定向优惠券发放的安全策略/技术包括本地定位[30,31]和密码技术（即PHE和GC）[32]。

Partridge等[30]第一次提出了名为PiCoDa的隐私保护定向优惠券发放框架。PiCoDa采用本地定位策略实现用户隐私保护。为了验证用户是否有资格获得定向的优惠券，他们使用LSH技术来测试用户的行为配置文件是否与供应商的目标配置文件大致相符。因此，如果用户的行为配置文件的LSH值与供应商的目标配置文件的LSH值相同，则用户能够导出用于解密目标优惠券的密钥。这项工作的主要局限性是由于LSH中存在误报，部分非合格用户可能能够获得目标优惠券。这可能违反供应商的利益。

Rane和Uzun [31]后来提出了针对隐私保护定向优惠券发放的另一种设计。他们采用了与参考文献 [30]（即本地瞄准）中相同的安全策略，但没有采用LSH来测试用户的资格，而是提出了应用纠错码来对用户的行为描述文件和供应商的目标描述文件进行编码。这种新的机制不会出现之前的设计误报问题。然而，代价是有关供应商的定位配置文件的一些信息泄露给用户。Jiang等[32]最近提出了一种针对隐私保护定向优惠券发放的新设计，该设计结合了同态加密和GC技术，确保仅将有针对性的优惠券准确地发放给合格用户，同时实现用户隐私和供应商保护。

5. 未来研究方向

（1）针对恶意用户的鲁棒性。现有的大多数隐私保护个性化推荐服务都假定用户诚实地参与整个过程。但实际上某些用户可能是恶意的，会故意向推荐人提供无效数据以破坏系统。这将会是一个严重的威胁，并且在关于保护隐私的个性化推荐服务的现有研究中大部分都未被探讨。针对这种威胁的防御可能具有挑战性，特别是当推荐人仅接收到加密的用户数据时。为确保服务质量，开发隐私保护推荐系统的验证技术势在必行，以便提供针对恶意用户的数据伪造攻击的鲁棒性。一个可能的方向是利用一些加密技术，如数字签名和承诺书，迫使用户生成承诺数据。

（2）防止恶意推荐的安全性。大多数关于隐私保护推荐的现有研究中隐含的假设是推荐人推荐的内容是良性的，并且不会造成任何伤害。但是，移动设备上的一些媒体推荐项目（如广告）包含JavaScrip、图片或视频。这些项目通常会访问外部存储——不同的移动应用程序存储其文件的共享位置。最近的一些研究[33,34]表明，这些媒体推荐项目可以用来推断隐私敏感信息，如性别和社交圈。为了抵御新出现的恶意推荐威胁，在移动设

备上提供独立的执行环境并赋予其满足媒体推荐项目的全部使用要求的能力是不可或缺的。另外，大多数引入第三方的现有研究都认为第三方是半诚实的。但是，这样的假设在实践中并不总是成立，第三方可能在执行恶意行为的同时协助推荐人执行隐私保护个性化推荐。发展有效的机制来抵御这种恶意的对手也至关重要。

（3）移动设备导向的成本效益。随着移动设备的普及，移动个性化推荐服务正变得越来越普遍。但移动设备通常受资源限制，特别是在电池和带宽方面。为了在保护用户隐私的同时，在移动个性化推荐服务中实现令人满意的用户体验，安全设计应该在移动设备上施加轻量的成本。因此，值得在推荐服务中继续开发用于移动设备的轻量级隐私保护技术的研究。一种可能的方向是整合诸如用户网络流量分析[35]和社交网络[36]等技术，以提出新的创新隐私保护解决方案。另一个方向可以是利用诸如英特尔软件防护扩展（Intel SGX）等先进的可信硬件来设计轻量级的隐私保护解决方案，该软件可能以最小的性能开销提供安全计算。此外，在进行隐私保护移动个性化推荐服务安全设计的绩效评估时，有必要考虑移动设备的能源成本，而不是将评估限制在计算和通讯成本上。这是因为电池能量是移动设备最宝贵的资源之一，是直接影响用户体验的实用因素。

6. 结论

在本文中，我们查阅了与隐私保护个性化推荐服务有关的文献。本文首先介绍了个性化推荐服务的系统架构、常用的推荐技术以及个性化推荐服务带来的隐私问题。然后，我们描述了用于个性化推荐服务的现有隐私保护技术，其分为两大类：保护隐私的CFB推荐和保护隐私CB推荐。而后我们进一步将保护隐私的CFB推荐分为基于隐私保护的邻近用户的方法和基于隐私

表 1 对隐私保护个性化建议工作的比较

Category	Techniques	Additional party	Active user participation	Computation overhead	Inter-user interaction	User data protection	Accuracy loss	Ref.
NBCF	PHE, SMC	Yes	Yes	High	No	Strong	No	[6]
NBCF	PHE	No	No	High	No	Strong	No	[10]
NBCF	PHE	Yes	Yes	High	No	Strong	No	[11]
NBCF	SMC	No	Yes	High	Yes	Strong	No	[4]
NBCF	Perturbation	No	No	Low	No	Weak	Yes	[12]
NBCF	Obfuscation	No	Yes	Low	Yes	Weak	Yes	[13]
NBCF	LSH, artificial ratings	No	No	Low	No	Weak	Yes	[14]
MLBCF	MF, PHE, GC	Yes	No	High	No	Strong	No	[18]
MLBCF	MF, FHE	Yes	No	High	No	Strong	No	[19]
MLBCF	RR, PHE, GC	Yes	No	High	No	Strong	No	[20]
MLBCF	RR, PHE	Yes	No	High	No	Strong	No	[21]
CBRTA	Local targeting	No	No	Low	No	Strong	Yes	[22]
CBRTA	Local targeting, game theory	No	No	Low	No	Strong	Yes	[23]
CBRTA	Anonymization, PKE	Yes	No	High	No	Strong	No	[24]
CBRTA	ORAM	Yes	No	High	No	Strong	No	[25]
CBRTA	Anonymization, PKE	No	Yes	High	Yes	Strong	No	[26]
CBRTA	PSS	No	No	High	No	Strong	No	[27]
CBRTA	Obfuscation	Yes	No	Low	No	Weak	Yes	[28]
CBRTA	Obfuscation	No	No	Low	No	Weak	Yes	[29]
CBRTCD	LSH, local targeting	No	No	Low	No	Strong	Yes	[30]
CBRTCD	Fuzzy commitment	No	No	Low	No	Strong	No	[31]
CBRTCD	PHE, GC	Yes	No	High	No	Strong	No	[32]

NBCF: neighborhood-based collaborative filtering; MLBCF: machine learning-based collaborative filtering; CBRTA: content-based recommendation for targeted advertising; CBRTCD: content-based recommendation for targeted coupon delivery; PHE: partially homomorphic encryption; FHE: fully homomorphic encryption; GC: garbled circuit; MF: matrix factorization; RR: ridge regression; SMC: secure multiparty computation; PKE: public-key encryption; LSH: locality-sensitive hashing; ORAM: oblivious random-access memory; PSS: private stream searching.
The indicator "Active user participation" is marked "Yes" if more than one round of user-server interaction is needed upon a request for private recommendations or if inter-user interaction is required. The indicator "User data protection" is marked "Strong" if user data are held locally or protected via cryptographic techniques. The indicator "Computation overhead" is marked "High" if cryptographic operations are involved.

保护机器学习的方法，并继而将隐私保护CB推荐分类为隐私保护定向广告和隐私保护定向优惠券发放。表1[4,6,10–14,18–32]对所描述的关于隐私保护建议的现有工作进行了比较。最后，我们就未来的研究方向进行了一些讨论。

Acknowledgements

This work was supported in part by the Research Grants Council of Hong Kong (CityU 11276816, CityU 11212717, and CityU C1008-16G), the Innovation and Technology Commission of Hong Kong (ITS/168/17), and the National Natural Science Foundation of China (61572412 and 61772236).

Compliance with ethics guidelines

Cong Wang, Yifeng Zheng, Jinghua Jiang, and Kui Ren declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Mackenzie I, Meyer C, Noble S. How retailers can keep up with consumers [Internet]. Chicago: McKinsey & Company; 1996–2018 [cited 2017 Mar 22]. Available from: http://www.mckinsey.com/industries/retail/our-insights/how-retailers-can-keep-up-with-consumers.
[2] Hassler J. The power of personalized product recommendations [Internet]. Carrollton: Intelliverse; 2018 [updated 2017 Aug 22; cited 2017 Mar 22]. Available from: http://www.intelliverse.com/blog/the-power-ofpersonalized-product-recommendations/.
[3] Leskovec J, Rajaraman A, Ullman J. Mining of massive datasets. 2nd ed. Cambridge: Cambridge University Press; 2014.
[4] Li D, Lv Q, Shang L, Gu N. Efficient privacy-preserving content recommendation for online social communities. Neurocomputing 2017;219:440–54.
[5] Ramakrishnan N, Keller BJ, Mirza BJ, Grama AY, Karypis G. Privacy risks in recommender systems. IEEE Internet Comput 2001;5(6):54–62.
[6] Erkin Z, Veugen T, Toft T, Lagendijk RL. Generating private recommendations efficiently using homomorphic encryption and data packing. IEEE Trans Inf Foren Sec 2012;7(3):1053–66.
[7] Xu K, Yan Z. Privacy protection in mobile recommender systems: A survey. In: Wang G, Ray I, Alcaraz Calero J, Thampi S, editors Proceedings of the 9th International Conference on Security, Privacy and Anonymity in Computation, Communication, and Storage; 2016 Nov 16–18; Zhangjiajie, China. Cham: Springer; 2016. p. 305–18.
[8] Koren Y, Bell R, Volinsky C. Matrix factorization techniques for recommender systems. Computer 2009;42(8):30–7.
[9] Aïmeur E, Brassard G, Fernandez JM, Onana FSM. Alambic: A privacypreserving recommender system for electronic commerce. Int J Inf Secur 2008;7(5):307–34.
[10] Badsha S, Yi X, Khalil I. A practical privacy-preserving recommender system. Data Sci Eng 2016;1(3):161–77.
[11] Badsha S, Yi X, Khalil I, Bertino E. Privacy preserving user-based recommender system. In: Proceedings of the 37th IEEE International Conference on Distributed Computing Systems; 2017 Jun 5–8; Atlanta, GA, USA. Los Alamitos: IEEE Computer Society Press; 2017. p. 1074–83.
[12] Polat H, Du W. Privacy-preserving collaborative filtering using randomized perturbation techniques. In: Proceedings of the 3rd IEEE International Conference on Data Mining; 2003 Nov 19–22; Melbourne, FL, USA. Los Alamitos: IEEE Computer Society Press; 2003. p. 625–8.
[13] Shokri R, Pedarsani P, Theodorakopoulos G, Hubaux JP. Preserving privacy in collaborative filtering through distributed aggregation of offline profiles. In: Proceedings of the 3rd ACM Conference on Recommender Systems; 2009 Oct 23–25; New York, NY, USA. New York: Association for Computing Machinery, Inc.; 2009. p. 157–64.
[14] Chow R, Pathak MA, Wang C. A practical system for privacy-preserving collaborative filtering. In: Proceedings of the 12th IEEE International Conference on Data Mining Workshops; 2012 Dec 10; Brussels, Belgium. Los Alamitos: IEEE Computer Society Press; 2012. p. 547–54.
[15] Huang Z, Du W, Chen B. Deriving private information from randomized data. In: Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data; 2005 Jun 14–16; Baltimore, MD, USA. New York: Association for Computing Machinery, Inc.; 2005. p. 37–48.
[16] Zhang S, Ford J, Makedon F. Deriving private information from randomly perturbed ratings. In: Ghosh J, Lambert D, Skillicorn D, Srivastava J, editors Proceedings of the 2006 SIAM International Conference on Data Mining; 2006 Apr 20–22; Bethesda, MD, USA. Philadelphia: Society for Industrial and Applied Mathematics; 2006. p. 59–69.
[17] Aggarwal CC. On randomization, public information and the curse of dimensionality. In: Proceedings of the 23rd International Conference on Data Engineering; 2007 Apr 15–20; Istanbul, Turkey. Los Alamitos: IEEE Computer Society Press; 2007. p. 136–45.
[18] Nikolaenko V, Ioannidis S, Weinsberg U, Joye M, Taft N, Boneh D. Privacypreserving matrix factorization. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security; 2013 Nov 4–8; Berlin, Germany. New York: Association for Computing Machinery, Inc.; 2013. p. 801–12.
[19] Kim S, Kim J, Koo D, Kim Y, Yoon H, Shin J. Efficient privacy-preserving matrix factorization via fully homomorphic encryption: Extended abstract. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security; 2016 May 30–Jun 3; Xi'an, China. New York: Association for Computing Machinery, Inc.; 2016. p. 617–28.
[20] Nikolaenko V, Weinsberg U, Ioannidis S, Joye M, Boneh D, Taft N. Privacypreserving ridge regression on hundreds of millions of records. In: Proceeding of the 2013 IEEE Symposium on Security and Privacy; 2013 May 19–22; Berkeley, CA, USA. Los Alamitos: IEEE Computer Society Press; 2013. p. 334–48.
[21] Hu S, Wang Q, Wang J, Chow SSM, Zou Q. Securing fast learning! Ridge regression over encrypted big data. In: Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA; 2016 Aug 23–26; Tianjin, China. Los Alamitos: IEEE Computer Society Press; 2016. p. 19–26.
[22] Toubiana V, Narayanan A, Boneh D, Nissenbaum H, Barocas S. Adnostic: Privacy preserving targeted advertising. In: Proceedings of the 2010 Network and Distributed System Security Symposium; 2010 Feb 28–Mar 3; San Diego, CA, USA. Reston: Internet Society; 2010. p. 1–16.
[23] Wang W, Yang L, Chen Y, Zhang Q. A privacy-aware framework for targeted advertising. Comput Netw 2015;79:17–29.
[24] Guha S, Cheng B, Francis P. Privad: Practical privacy in online advertising. In: Proceedings of the 8th USENIX Conference on Networked Systems Design and Implementation; 2011 Mar 30–Apr 1; Boston, MA, USA. Berkeley: USENIX Association; 2011. p. 169–82.
[25] Backes M, Kate A, Maffei M, Pecina K. ObliviAd: Provably secure and practical online behavioral advertising. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy; 2012 May 20–23; San Francisco, CA, USA. Los Alamitos: IEEE Computer Society Press; 2012. p. 257–71.
[26] Artail H, Farhat R. A privacy-preserving framework for managing mobile ad requests and billing information. IEEE Trans Mobile Comput 2015;14(8):1560–72.
[27] Jiang J, Gui X, Shi Z, Yuan X, Wang C. Towards secure and practical targeted mobile advertising. In: Proceedings of the 11th International Conference on Mobile Ad-hoc and Sensor Networks; 2015 Dec 16–18; Shenzhen, China. Los Alamitos: IEEE Computer Society Press; 2015. p. 79–88.
[28] Hardt M, Nath S. Privacy-aware personalization for mobile advertising. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security; 2012 Oct 16–18; Raleigh, NC, USA. New York: Association for Computing Machinery, Inc.; 2012. p. 662–73.
[29] Davidson D, Fredrikson M, Livshits B. MoRePriv: Mobile OS support for application personalization and privacy. In: Proceedings of the 30th Annual Computer Security Applications Conference; 2014 Dec 8–12; New Orleans, LA, USA. New York: Association for Computing Machinery, Inc.; 2014. p. 236–45.
[30] Partridge K, Pathak MA, Uzun E, Wang C. PiCoDa: Privacy-preserving smart coupon delivery architecture. In: Proceedings of 5th Workshop on Hot Topics in Privacy Enhancing Technologies; 2012 Jul 11–13; Vigo, Spain; 2012. p. 95–108.
[31] Rane S, Uzun E. A fuzzy commitment approach to privacy preserving behavioral targeting. In: Proceedings of the ACM MobiCom Workshop on Security and Privacy in Mobile Environments; 2014 Sep 11; Maui, HI, USA. New York: Association for Computing Machinery, Inc.; 2014. p. 31–6.
[32] Jiang J, Zheng Y, Yuan X, Shi Z, Gui X, Wang C, et al. Towards secure and accurate targeted mobile coupon delivery. IEEE Access 2016;4:8116–26.
[33] Wu D, Chang RKC. Analyzing Android browser apps for file:// vulnerabilities. In: Chow SSM, Camenisch J, Hui LCK, Yiu SM, editors Proceedings of the 17th International Conference on Information Security; 2014 Oct 12–14; Hong Kong, China. Cham: Springer; 2014. p. 345–63.
[34] Son S, Kim D, Shmatikov V. What mobile ads know about mobile users. In: Proceedings of 2016 Network and Distributed System Security Symposium; 2016 Feb 21–24; San Diego, CA, USA. Reston: Internet Society; 2016. p. 1–14.
[35] Su X, Zhang D, Li W, Li W. Android app recommendation approach based on

network traffic measurement and analysis. In: Proceedings of the IEEE Symposium on Computers and Communication; 2015 Jul 6–9; Larnaca, Cyprus. Piscataway: Institute of Electrical and Electronic Engineers, Inc.; 2015. p. 988–94.

[36] Li F, He Y, Niu B, Li H, Wang H. Match-MORE: An efficient private matching scheme using friends-of-friends' recommendation. In: Proceedings of the 2016 International Conference on Computing, Networking and Communications; 2016 Feb 15–18; Kauai, HI, USA. Piscataway: Institute