个性化推荐系统隐私保护策略研究进展

王国霞，王丽君，刘贺平
（北京科技大学 自动化学院，北京 100083）

摘　要：个性化推荐系统能较好地帮助用户获得个人所需的信息，但它要获得好的推荐效果，需要收集大量的用户个人信息；这些信息可能泄露个人隐私，用户会因对隐私泄露的担心而放弃对推荐系统的信任，所以大量的研究集中于如何在获得高效推荐的同时保护用户的个人隐私。主要就个性化推荐系统中使用的隐私保护技术进行了综述，在给出了隐私和隐私保护定义的同时讨论了隐私保护的相关技术，包括隐私策略描述语言和目前使用的隐私保护技术。最后尝试给出了今后的研究重点和方向。

关键词：个性化；推荐系统；隐私；隐私保护；隐私保护技术
中图分类号：TP315　　**文献标志码**：A　　**文章编号**：1001-3695(2012)06-2001-08
doi:10.3969/j.issn.1001-3695.2012.06.001

Study progress of privacy protection techniques used in personalized recommendation system

WANG Guo-xia, WANG Li-jun, LIU He-ping
(*School of Automation*, *University of Science & Technology Beijing*, *Beijing* 100083, *China*)

Abstract: Personalized recommendation systems can help users to get the information that they really want, but good recommendation depends on a great deal of information about users. Those information maybe arouse the users' concern about their privacy which lead to lose the users' trust in recommendation systems, so a lot of study focused on the privacy protection techniques. These techniques can protect users privacy, at the same time, recommendation systems can get good recommendations. This paper mainly discussed privacy protection techniques applied in personalized recommendation systems, and gave the definition of privacy and privacy protection. It discussed some privacy protection techniques including privacy policy languages and privacy protection techniques used at present. At last it summaried the key points and directions of this study in the future.

Key words: personalization; recommendation system; privacy; privacy protection; privacy protection technique

0　引言

互联网的出现和普及给用户带来了大量的信息，满足了用户在信息时代对信息的需求，但随着网络的迅速发展，网上信息量大幅增长，从而引发了两个问题，即信息超载和资源迷向。这两个问题使得用户不知道如何确切表达自己的信息需求和无法确切知道自己真正需要的信息是什么。尽管 Google、百度等搜索引擎的出现在一定程度上解决了上述问题，但它们在用户使用同一个关键字搜索信息时，得到的结果是相同的，无法满足用户个性化和多元化的需求，从而出现了个性化推荐系统。该系统是根据用户的信息需求、兴趣等将用户感兴趣的信息、产品等推荐给用户的个性化信息推荐系统。与搜索引擎相比，推荐系统通过研究用户的兴趣偏好进行个性化计算，由系统发现用户的兴趣点，从而引导用户发现自己的信息需求。

一个好的推荐系统要获取高度个性化的、准确高效的推荐，就必须要充分了解和掌握用户的个性化信息及需求。推荐的个性化程度和准确度越高，要求对用户的个性化信息掌握得越多、越准确越好，但获取和使用这些个性化信息会导致用户对个人隐私泄露的担心。例如，在注册某一网站账户时登记的个人电话被泄露或盗用，又或搜索引擎记录了用户的搜索关键词给用户下次的使用提供了个性化的搜索方案，但当用户发现自己的搜索历史被别人发现并利用等诸多现象就会引发用户对个性化推荐的反感和不信任，这将导致个性化推荐系统和个人隐私之间的矛盾，即一方面个性化系统的准确和高效需要大量用户的个性化信息，而另一方面获取和使用用户的个性化信息会导致个人隐私泄露的担心。文献[1]首次提出了该矛盾。隐私保护策略就是研究如何在两者之间找到平衡，即在用户获得准确高效的个性化推荐的同时还能有效保护用户的个人隐私。

1　个性化推荐和隐私保护

推荐系统的定义有很多，但被广泛接受的推荐系统的概念和定义是 Resnick 等人[2]在 1997 年给出的："它是利用电子商务网站向客户提供商品信息和建议，帮助用户决定应该购买什么产品，模拟销售人员帮助客户完成购买过程"。

个性化推荐系统有三个重要的模块：用户建模模块和推荐对象建模模块、推荐算法模块。通用的推荐系统模型流程如图

收稿日期：2011-11-14；**修回日期**：2011-12-29

作者简介：王国霞(1975-)，女，讲师，博士研究生，主要研究方向为个性化信息获取(my_zhg0127@sina.com)；王丽君(1971-)，女，讲师，主要研究方向为自抗扰控制、混沌优化、模糊控制等先进控制技术及智能优化技术在冶金、电力行业的理论与应用；刘贺平(1951-)，男，教授，博导，主要研究方向为智能化信息处理与控制、自适应控制等.

1所示[3]。推荐系统把用户模型中兴趣需求信息和推荐对象模型中的特征信息进行匹配,同时使用相应的推荐算法进行计算筛选,找到用户可能感兴趣的推荐对象推荐给用户。个性化推荐在很多领域都表现出它的优势,尤其是在电子商务领域得到了很多经销商和用户的青睐。

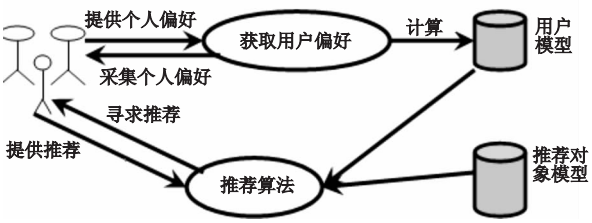

图1 推荐系统通用模型

推荐的个性化程度和准确度越高,要求对用户的个性化信息掌握得越多、越准确越好,还要能准确地表达给系统并能随着它们的变化而及时修正。个性化信息包括用户的基本属性信息,如用户的姓名、年龄、职业、收入、学历等,还有用户输入搜索关键词、用户输入的感兴趣的主题、频道、用户的反馈信息(感兴趣、不感兴趣的信息等)等,用户浏览网站的内容和行为也能很好地反映用户的个性化偏好和需求。

个性化服务的过程中会导致用户隐私担心的地方主要有三个阶段[4]。

a)用户的建模。这一阶段要获取用户的个性化信息偏好和需求,建立用户模型。获取个性化偏好和需求的方法有用户主动提供的显式方式,如注册时用户名等基本属性、用户输入查询关键词、用户给出的喜好反馈等;还有通过跟踪用户行为之后推理得到隐式方式,如跟踪用户浏览网页的行为(如点击次数、浏览时间、标记书签等)。获取个性化信息后得到用户模型(user profiles)。之后,还要采用合适的数据结构来表示用户的个性化信息需求,以方便系统处理和使用,再使用该模型进行匹配计算;然后还要根据用户的个性化需求变化更新用户模型。

这一阶段中会产生的隐私担心有[5]不正当的接近(improper access)、不正当收集(improper collection)、不正当监控(improper monitoring)、不正当的分析(improper analysis)、不正当合并数据(improper merge data)、不正当传输数据(improper transfer data)、不正当的数据存储(improper storage)、身份欺骗(identity fraud)等。

b)计算。这个阶段要进行相似性计算,依此进行后期的推荐。产生的隐私担心有[5]不正当的分析、不正当合并数据、不正当传输数据、身份欺骗等。

c)产生推荐结果。这一阶段就是进行匹配计算后得到推荐结果。该阶段会产生的隐私担心有不正当的分析、不正当合并数据、不正当传输数据、误导推荐(solicitation)等。

三个阶段可能产生的隐私担心如表1所示,其中√表示可能产生此项隐私。用户对个人隐私的担忧会给个性化系统带来很多深层次的影响,一方面用户不愿意信任个性化推荐系统,从而不愿意甚至放弃使用它,另一方面就是用户不愿意向系统提供个性化信息,也不愿意被系统跟踪监视,从而导致个性化推荐系统无法得到足够数据进而影响推荐的准确度。文献[6]对这些影响进行了调查并给出了一定的结果:a)担心个人数据的隐私或安全的用户比例为70% ~89.5%;b)拒绝向网站提供个人信息的用户比例为82% ~95%;c)从不向网站提供个人信息的用户比例为27%;d)在注册时,向网站提供虚假个人数据的用户比例为24% ~40%;e)担心个人数据被用于非初始目的的地方的用户比例为89% ~90%;f)担心网站会同别的网站分享个人数据的用户比例为83%。

表1 推荐过程中可能产生的隐私担心

阶段		控制数据							保护身份识别	保护身份隐藏
		不适当的获取	不适当的收集	不适当的监视	不适当的分析	不适当的融合	不适当的传输	不适当的存储	身份欺骗	误导推荐
用户建模	跟踪和监控	√	√	√						
	用户主动给出	√	√					√		
	推理				√	√				
	分析建模				√	√	√	√	√	
计算					√	√	√	√	√	
产生推荐					√	√	√	√		√

针对用户个人数据的收集过程中使用的跟踪和cookies,用户也会有不同的态度。

a)担心被跟踪的用户的比例为54% ~63%;b)担心有人知道自己访问了什么网站的用户比例为31%;c)当知道被多个网站跟踪会感到不安的用户比例为91%;d)接受cookies的用户比例为62%;e)拒绝自己计算机上的cookies的用户比例为10% ~25%;f)定期删除cookies的用户比例为53%。

从上述的调查结果可见,由于用户对隐私的担心,使得他们大多拒绝给出个人数据,这会大大降低个性化推荐系统的推荐精度,从而影响到个性化推荐系统的使用。

隐私即隐蔽不愿公开的私事,Westin教授[7]给出隐私的定义为个人、团体或某机构有权控制、编辑、管理并删除关于自己的信息,还有权决定何时、以何种方式以及何种程度将个人信息公开给他人。

上述对隐私的定义中重点强调的是信息所有者对其的控制权,而不是完全密封不能使用。因此结合网络中对信息的使用情况,文献[8]给出隐私的定义为隐私是与个人相关的具有不被他人搜集、保留和处分的权利的信息资料集合,并且它能够按照所有者的意愿在特定时间、以特定方式、在特定程度上被公开。

从上述定义可以看出,在个性化服务的三个阶段中都涉及到了个人的隐私,如收集的个人基本信息、个人兴趣偏好、个人浏览行为和内容,未经用户许可对个人信息进行处理、传输、存储、计算等。

关于隐私保护这一概念,因保护隐私的出发点不同而出现的不同定义有三种:

a)privacy protection。保护个人隐私不被外界怀有不良用心的黑客等攻击威胁,侧重的是对隐私的保护。

b)privacy preservation。在使用有关个人隐私的信息时充分考虑信息所有者对其态度,对隐私进行有限的使用。该定义侧重的是使用过程中对隐私所有者的尊重和对信息的有限使用。

c)privacy enhance。在个人隐私使用过程中充分尊重所有者的态度,在对其有限使用的过程中充分增加它的价值。该定义侧重在保护隐私的前提下增加其价值,这一概念多用于个性化服务系统中。

文献[8]也给出了隐私保护定义:隐私保护是对个人隐私

采取一系列的安全手段防止其泄露和被滥用的行为。该定义指出隐私保护的对象主体是个人隐私,其包含的内容是使用一系列的安全措施来保障个人隐私安全的这一行为,而其目的则是防止个人隐私遭到泄露以及被滥用。

文献[9]认为隐私保护有三种类型,分别是保护能辨别个人身份的信息、保护用户隐藏(seclusion)自己的权利和保护用户控制自己信息数据的权利(如收集什么数据、为什么给出个人信息、自己的数据如何使用、数据能被什么人使用分享等)。

目前,很多国家都制定了相应的法律来保护公民的隐私。如美国 1970 年的公平信用报告法和 1974 年的隐私法成为制定隐私保护法的开端。之后,欧洲的一些国家如瑞典、德国、法国等相继制定了自己的隐私保护法律。1980 年经济合作与发展组织(OECD)也制定了保护隐私和过境个人数据指导法案。亚太经济合作体(APEC)也于 2004 年制定了隐私保护框架。针对目前存在的国家法律和企业条例,文献[9]对其进行了总结,罗列了一系列对提高个性化信息服务的隐私保护措施有用的原则,如表 2 所示。其中"X"表示该框架有对应的原则。

表 2　各国法律条例提到的隐私问题

principle	specification						
	OECD guidelines (OECD. 1980)	EU directive on data protecion (EU. 1995)	German telemedia law (DETML. 2007)	APEC privacy framework (APEC – FIP. 2004)	FTC safe harbor principles (FTC. 2000c)	FTC fair info practice (FTC. 2000b)	ACM principles (USACM. 2006)
notice/awareness	X	X	X	X	X	X	X
minimization							X
purpose specification	X	X	X	X	X		X
collection limitation		X	X	X	X		
use limitation	X	X	X	X	X		X
onward transfer		X	X		X		
choice/consent	X	X	X	X	X	X	X
access/participation	X	X	X	X	X	X	X
integrity/accuracy	X	X	X	X	X	X	X
security	X	X	X	X	X	X	X
enforcement/redress		X	X		X	X	
匿名相关的原则							
anonymity							
pseudonymity		X	X				
unobservability							
unlinkability							
deniability							
其他提高隐私保护的原则							
user preference							
negotiation							
seclusion							
ease of adoption							
ease of compliance							
usability							
responsiveness							

2　隐私保护策略表述

隐私保护策略是网站要全面描述的对用户个人信息的收集、使用等方面采用的保护策略,目的是让用户明确网站的隐私保护策略,所以网站的隐私保护策略通常采用了冗长的文字描述呈现在用户面前。而隐私保护策略表达是采用机读的方式来表达网站的隐私保护策略。

2.1　P3P

P3P 即隐私偏好设定平台(platform for privacy preference project),是由万维网联盟 W3C(World Wide Web Consortium)于 2002 年开发完成的,并且得到了很多机构的认可并广泛使用。雅虎、新浪等高访问率网站已经接受了 P3P 标准;AOL、AT&T、Engage 科技等公司已宣布其网站将支持 P3P;IBM 公司还发行了 P3P 策略编辑器,以便于网站管理人员按照 XML 格式来描述保密和参数选择策略;浏览器巨头之一的微软也已经在新版浏览器 IE 6.0 内加装 P3P 程序,此举将大幅扩增 P3P 技术的应用范围,迫使想吸引 IE 用户的网站采纳 P3P 技术。

P3P 可以使 Web 站点有一种标准的、机器可读的、XML 描述的隐私保护策略文件,包括隐私信息的收集、存储和使用等方面的描述语法和语义。网络用户根据个人需要可在 P3P 软件(用户代理)中设定隐私偏好参数,受访的 Web 站点会把 XML 策略引用文件发送到用户代理;用户代理可以自动或半自动地把 Web 站点的隐私策略和用户的隐私偏好参数匹配,若匹配,说明用户的隐私偏好和站点的隐私策略相符合,用户可以顺利访问 Web 站点;否则,用户有权决定是否放弃对网站的访问,或修改个人隐私偏好参数以继续对网站的访问,这一过程通常以对话框的形式出现,以方便用户作出选择。P3P 策略可用于整个网站,也可是网站的某部分。

P3P 的工作过程中需要如下几个组件的参与[10]:

a)XML 和 Web 站点中支持 P3P 的组件。XML 是一种标准的机器可读的语言,它使用标准 P3P 隐私词汇来描述 Web 站点隐私保护策略[11]。Web 站点中支持 P3P 的组件用于创建和配置 P3P 的 XML 文件以及配置 Web 服务器以发布响应报头,该 XML 文件叫做 P3P 策略引用文件。

b)用户代理。该组件是一种能够获取和识别 P3P 策略并且能够为互联网用户提供帮助的工具[12],它给用户提供的帮助主要有显示与 Web 站点隐私策略相关的标志或文本;把用户自己设定的隐私偏好和站点的隐私策略进行匹配,以判断该站点的隐私策略是否符合用户的隐私偏好,从而可以帮助用户决定是否访问该站点;也可根据 Web 站点的隐私策略有选择性地阻止 cookie。

用户代理可以是一个独立的工具,也可以嵌入到浏览器等其他的软件中。它可按需运行也可持续运行,可以仅提供信息也可自动采取行动。

c)基于 HTTP 的 P3P 握手协议。该协议使得用户代理检索站点的隐私策略,并与用户的隐私偏好进行匹配,只有两者一致时,用户代理才可以向 Web 站点的服务器请求其他的信息。该协议工作过程如图 2 所示[10]。

图2　P3P握手协议工作过程

尽管 P3P 已经非常流行,世界上多数的站点都支持 P3P,但在实际的使用过程中,P3P 存在着诸多的问题。

a)P3P 在实际使用过程中犹如纸上谈兵,不能起到真正的隐私保护作用。原因之一在于 P3P 仅通过隐私策略宣布站点

遵循的隐私保护策略,缺乏真正的技术措施来保证其隐私策略得以顺利实施,用户也没有任何措施判断站点是否能按照其隐私策略来执行[4]。原因二在于P3P的隐私策略既不是政府法律,也不是行业条例,对站点或是某些心怀叵测的人来说,不具备任何的约束力。所以P3P并不是隐私保护的万金油,站点和用户不能仅依靠P3P作为隐私保护的保障。

b)P3P的1.1版本不能因用户而异,也不能因网站而异,即P3P不能为不同用户提供不同的隐私策略,但在未来的新版本中将会考虑到这一点,给以改进;同时,每个网站因业务不同,其隐私保护策略也会不同,但P3P还无法做到因站点不同而隐私策略也不同。所以,目前网站中隐私策略大多采用用户可读的隐私策略文件和P3P隐私策略共存的方式。

c)P3P的应用在某种程度上阻碍了网站对信息的收集,从而影响到其服务质量。对个性化系统而言,其个性化无法实现;对用户而言,一方面是因P3P保护措施不到位,导致用户的隐私无法得到真正的保护,同时因某些良性站点不兼容P3P而无法让使用诸如IE6的用户看到。

在讨论P3P时,不得不提到的两种语言就是Applet和XPref,它们都是在客户端用来描述用户隐私偏好的XML。

Applet语言对于熟悉Java语言的人来说不算陌生,但这里的Applet是用来在客户端采用规则的方法描述用户的隐私偏好,如图3[13]所示为某段Applet描述的用户隐私偏好。Applet中的规则会由用户代理和站点的P3P隐私策略进行匹配,依此决定用户对站点的访问。

```
〈appel:RULESET〉
  〈appel:RULE behavior="block"〉规则1
    〈POLICY〉
      〈STATEMENT〉
        〈PURPOSE appel:connective="or"〉
          〈contact/〉
          〈telemarketing/〉
        〈/PURPOSE〉
      〈/STATEMENT〉
    〈/POLICY〉
  〈/appel:RULE〉

  〈appel:RULE behavior="request"/〉
    〈appel:OTHERWISE/〉  规则2
  〈/appel:RULE〉
〈/appel:RULESET〉
```

图3 Applet语言示例

尽管Applet拥有很多优点,如体积小、可读性强、表达方式采用XML标准化的语言等,但Applet在用户的隐私偏好和站点的P3P策略进行匹配时,在Applet规则和隐私策略之间只能进行逻辑运算,这样会有很大的缺点,如当隐私策略中某项阐述与Applet规则中某一规则不匹配,就会导致两者的不匹配,即使其他隐私策略都与规则相符。所以Applet仅在表述不能接受的隐私偏好时能起到较好作用,在表述能接受的隐私偏好时就不能起到很好的作用[13]。

另外一种在客户端用于隐私偏好描述的语言是XPref,该语言基于XPath语言的XML,它是为了克服Applet语言的缺点而出现的。XPref和Applet的区别在于Applet使用规则中的子元素来与P3P中的策略进行匹配,而XPref中使用XPath表达式来与P3P中的策略进行匹配,当XPath表达式返回结果为空值时表示用户的隐私偏好与P3P的隐私策略不匹配。XPref完成了此项改动后,其在描述可接受和不可接受的隐私偏好时都能发挥好的作用。如图4是用XPref描述用户隐私偏好[13]。

```
〈RULESET〉
  〈RULE behavior="request"
     condition="/POLICY [
       every $pname in
       STATEMENT/PURPOSE/* satisfies
         (name($pname) = "current" or
          name($pname) = "pseudo-analysis")
       ]" /〉

  〈RULE behavior="block" condition="true"/〉
〈/RULESET〉
```

图4 Xpref示例

2.2 EPAL

EPAL(enterprise privacy authorization language)由IBM开发完成[14],目的是为了企业描述内部在处理掌握的用户数据时采用的隐私策略。该语言描述的策略能被企业的管理系统应用并自动遵守,并且也是采用XML格式的文件。

EPAL采用规则的方法描述隐私策略,对规则描述时采用EPAL的词汇来描述。每一个隐私规则[9]中包括规定(ruling)、数据使用者、数据使用方法(action)、数据类别(data category)、使用目的等,也可能包括使用条件和遵守的规则。隐私规则按照优先级进行降级排序。在使用时,系统把EPAL隐私规则和发来的请求进行匹配,匹配结果决定请求是允许或是拒绝。

EPAL与P3P的区别[9]包括以下几方面:

a)作用的范围不同。P3P是对外公共隐私策略,而EPAL是企业内部的隐私策略,通常不会对外公布。同时P3P是以保护数据为中心的,而EPAL是以控制访问数据为中心的。

b)保障措施不同。P3P仅仅告知自己的隐私策略,没有相应的技术措施来保证其隐私策略的实施,而EPAL的隐私策略会有企业的系统来保障其实施。同时,P3P没有考虑国家法律和条例或者不具有法律的约束力,而EPAL把法律和企业条例考虑在隐私策略内。

c)隐私定义方法不同。P3P的隐私策略是提前定义好的,而EPAL的隐私策略在定义时是抽象的,只有在实际使用时会映射为具体的策略。P3P的隐私策略因规则不同相互冲突,而EPAL可以。

d)P3P策略擅长正面的描述(即什么是允许的),而EPAL对正面和负面(即什么不允许)的描述都比较擅长。

2.3 XACML

XACML(extensible access control markup language)也是一种基于XML的标记语言。在2003年OASIS定义了该语言的1.0版本,2005年OASIS发布了2.0版本[15]。XACML不仅能对访问控制的规则和策略进行描述,也能对访问控制的请求和响应乃至整个访问控制过程进行描述。

XACML最重要的一个元素就是策略文件,它是一个策略规则的集合,该集合中包括了一组访问控制规则,每条规则[16]中包括有条件(condition)、效果(effect)和目标(target)。其总的条件是关于属性的描述,评估的结果有真、假或不确定;效果是符合规则的预期后果,可以是许可或拒绝;目标帮助确定规则是否与请求有关,请求的相关性决定了是否要为请求评估该策略。隐私策略的典型格式[17]如下:

〈policy〉
〈target〉〈/target〉
〈rule effect = "Permit/Deny"〉
〈target〉…〈/target〉

〈condition〉□〈/condition 〉
〈/rule 〉
〈obligations〉
〈obligation fulfilOn = Permit/Deny〉〈/obligation〉
〈/policy〉

XACML 的工作过程大致如下:

策略管理点(policy administration point,PAP)制定策略。当一个访问请求发送给策略加强点[16~18](policy enforcement point,PEP),PEP 创建决策请求,并通过上下文处理器把决策请求发送给策略决策点(policy decision point,PDP);PDP 把上下文处理器收集来的主体、资源、动作和环境的属性值进行计算评估,并根据结果生成授权决定(拒绝或接受),然后把该决定发送给 PEP;PEP 根据收到的授权决定执行,如果允许访问,则 PEP 允许访问者访问资源,否则禁止访问资源。

XACML 同 EPAL 一样是一种描述企业内部隐私策略的语言,同样都采用 XML 标准语言,但 XACML 具有很好的通用性、重用性和可移植性、可分布性以及可扩展性[15,19],使得 XAML 不仅在访问控制策略,而且在隐私策略方面较 EPAL 更具优越性。

3　隐私保护技术

最近这些年,个性化系统中隐私保护研究逐渐受到大家的重视,不同隐私保护技术也不断地被提出来。

3.1　从系统的体系结构方面考虑

推荐系统的体系结构研究的着眼点大多都集中在用户的信息收集和用户描述文件(user profile)放在系统的什么位置,以此来认定系统是什么样的体系结构。

最初的个性化推荐系统都是基于服务器的,逻辑上用户信息的收集、建模以及用户描述文件的存放都在服务器端,通常服务器和 Web 服务器共享一台硬件设备。基于服务器端的推荐系统除了增加 Web 服务器的开销并受到其功能限制外,对用户的隐私存在极大的威胁。这是因为用户的个人信息全部存放在服务器端,用户基本上无法看到或控制自己的个人数据,并且无论是系统的管理者还是系统的入侵者都能比较方便地获取存放在服务器上的用户数据[19~22]。鉴于此,众多研究者对推荐系统的体系结构提出了很多改进方法,把集中式的结构变为分布式的体系结构。文献[23]首先提出了基于分布式体系结构的推荐系统。

1)基于客户端的推荐系统

用户的个人信息数据存放在用户个人客户端,只有用户可以完全操控自己的数据,这就可以很好地保护个人隐私。文献[24]提出了一种分布式的推荐系统,系统中存在两种用户描述文件,一个线下用户描述文件,存储在客户端;另一个是线上用户描述文件,存储在服务器端,该描述文件是线下描述文件的一部分,是对线下描述文件通过聚合混淆了真实数据形成的,并且线上描述文件还要和线下描述文件保持同步。在对用户进行推荐时,利用线上描述文件进行个性化推荐。文献[25]提出了基于客户端的广告推荐系统。文献[26]提出了在客户端建立树状的用户描述文件算法,即建立分层的用户描述文件,高层次的用户描述文件中存储的是概括性的兴趣偏好,而低层的用户描述文件存储的是具体的比较有针对性的兴趣偏好,通过用户自己设定的参数来决定用户的哪些数据是要被保护的,从而达到保护用户隐私的目的。

2)基于 P2P 的推荐系统

文献[19~22,27]提出了基于 P2P 的推荐系统。在 P2P 的推荐系统中,每个用户的计算机要同时担任客户端和服务器的角色,用户的个人数据存放在用户的计算机中,用户可以完全操控个人数据。文献[23]首先提出了一种基于 P2P 的为移动客户提供产品推荐的系统,客户采用智能体模拟,但其在智能体间的通信采用泛洪的方式,导致通信费用昂贵,文献[28]对此提出了改进意见。文献[27]也提出了基于 P2P 的推荐系统,并就五种分布式体系结构的推荐系统进行了比较。由于上述几种 P2P 的推荐系统还是需要通过网络传输个人数据,具有隐私暴露的危险,文献[19,20]提出了基于 P2P 的推荐系统,融合了数据的聚合和加密技术,保证了用户的数据不会暴露。文献[21,22]提出了一种仅给出用户部分数据而得到精确推荐的 P2P 推荐系统。

3)基于代理的推荐系统

在这一结构中,用户信息的收集、用户建模和推荐服务都在代理端实现。典型的代理端个性化服务系统有明尼苏达大学的 GroupLens、斯坦福大学的 Fab[29] 等。与这一结构相似的情况就是基于第三方(third party)的推荐,把用户的数据交给第三方处理,如文献[27,30,31],但体系结构依然存在个人数据在网络传输的问题,而且个人信息集中在了代理端,还会存在个人隐私的问题。

3.2　采用伪装的方法保护隐私

所谓的伪装就是把用户真实的个人数据进行伪装后用于个性化推荐。这一方式通常用于协同推荐系统中。

文献[32,33]提出了采用随机扰动技术(RPT)伪装用户的真实数据。随机扰动技术是一种常用的数据隐藏方法,为了隐藏数据 a,就在 a 上加上一个随机数 r,这样外界看到的是 $a+r$。即用户的真实数据加上一个随机数后才送给服务器用于协同推荐,服务器和其他的任何用户都无法知道用户的真实数据,但当用户的数据足够多时,用户的集体信息用于推荐计算时依然可以获得精确的推荐,从而既可保护用户隐私,又可获得精确的推荐。文献[34]应用同样的方法在数据挖掘过程中保护隐私;文献[35]提出了扰动强度的概念和度量方法,对基于随机扰动技术的协同推荐进行了改进;文献[36]提出了一种综合 DWT 和随机扰动技术的协同过滤系统;文献[37]把随机扰动技术用于基于 NMF 的协同推荐,也取得了较好的效果。

另外一种伪装用户个人数据的方法是模糊化处理(obfuscation)。文献[21,22]提出了一个分布式的协同推荐系统,该系统中用户描述文件存放在客户端,同时,用户个人数据的一部分被一些其他的数据代替,作者证明了较多的用户描述文件被模糊化处理后用于协同推荐时仍能产生精确的推荐。之后,他们又把该方法用于另外的一个推荐系统,也取得了较好的推荐效果。文献[38]同时运用了模糊化处理和匿名方法来保护隐私。

3.3　聚合的方法保护隐私

文献[19,20]在分布式的体系结构下使用了聚合(aggregation)的方法,用户组成相应的团体,并对团体内用户数据进行运算得到一个聚合数据,该数据作为公共的数据使用,用户使用该数据以及个人数据进行计算,获得推荐。在这一方法下,

用户对个人数据具有完全控制权。文献[21]也是在分布式体系结构下提出了:用户间进行接触交流时,把各自的部分数据进行交换,每个用户再把收到的数据和自己的数据进行聚合,之后进行计算得到推荐。这些方法都能防止用户的数据暴露。

与聚合相似的一个保护隐私的办法是建立团体模型,即首先根据用户的数据找到共同的兴趣偏好,相似者形成一个团体,用户获得的推荐是以团体为单位的。文献[19,27,39]等都应用了这一方法。

3.4 匿名技术保护隐私

所谓匿名(pseudonymous)技术就是用户在获得个性化推荐时,不要求其真实身份,可以以匿名的方式使用系统,同样也可以获得个性化信息。通常系统允许一个用户可以用多个身份进入,这样就可以保护用户在不同活动时的身份。大量的个性化系统采用这一技术来保护用户隐私,如文献[27,30,31,40~42]等都提出了匿名的个性化系统。

匿名化的方法中还有一种方法受到了广泛的关注,就是k-匿名模型。1998年,Samarati和Sweeney[43,44]提出了k-匿名模型,该模型能够防止链接攻击所造成的隐私泄露问题,此后k-匿名模型被应用到很多领域的隐私保护。该模型的基本思想是数据中每个元组都存在一定数量(至少为k个)的、在准标志属性上取值相同的元组。这样,即使攻击者通过与其他数据进行链接也无法唯一地标志出各元组所有者的身份,仅能以不超过$1/k$的概率标志元组所属个体的身份,从而降低了隐私泄露的风险。k-匿名模型中可以通过调整参数k的大小达到对隐私不同程度的保护,k越大,隐私保护越强。之后又出现了很多该模型的改进模型,如文献[45]提出的l-多样性模型、文献[46]提出的(a,k)-匿名模型、文献[47]提出的t-接近模型、文献[48]提出的(k,e)匿名模型、文献[49]提出的个性化隐私匿名模型、文献[50]提出的(k,l)-匿名模型等。

用匿名技术来保护隐私也受到了较多的质疑,比如用户在匿名使用推荐系统时,通常要求使用电子邮件地址注册,通过电子邮件很容易识别用户的身份特征;再有就是如果有购物付款等行为时,用户依然需要提供个人真实身份,那么个人隐私的保护就无从谈起了。文献[51]提出了匿名技术对保护个人隐私存在的不足,并给出了实验证明。

3.5 加密技术保护个人隐私

加密技术是一种常用的安全保密措施,可在进行推荐计算时应用该技术来保护用户的个人隐私。数据加密就是通过密码机制实现对原始数据的不可见性和数据的无损失性,可以达到隐私保护和推荐精确无损的目的。文献[19,20]在用户聚合模型的计算时就应用了同态加密技术以保证用户个人数据传输时的安全。文献[27]使用同态加密技术保护个人隐私,同时也没有损失推荐精度。

3.6 社会网络分析方法保护隐私

基于社会网络分析方法的个性化推荐得到了很多研究者的关注,文献[52~56]对基于社会网络分析的个性化推荐进行了研究。文献[57]提出了基于社会网络分析进行隐私保护的方法,该文中用户把个性化查询要求发送给他的邻居,邻居或邻居的邻居把查询发送给搜索引擎,这样搜索引擎便无从知道该查询的准确来历,从而保护用户的隐私。这一方法可以认为是匿名和伪装保护隐私的引申。文献[52]也提出了一种基于社会网络分析方法保护隐私的个性化推荐系统。

3.7 其他方法

文献[58]采用分布式的体系结构,并采用了相关性的方法来计算相似性。该方法不需要关注用户个体的评分数据,只关心他们的评分数据和平均评分值之间的关系,从而可以保护用户的个人隐私。文献[59,60]提出了基于任务的推荐系统,使得用户不必给出个人历史评分也可得到推荐,从而保护隐私。

对上述的隐私保护方法加以分析,它们符合隐私保护原则的情况如表3所示。

表3 隐私保护技术关注到的隐私原则

principle	C/S	P2P	代理	伪装	聚合	匿合	加密	SNA
notice/awareness								
minimization								
purposes specification								
collection limitation								
use limitation								
onward transfer	√				√		√	
choice/consent							√	
access/participation	√	√						
integrity/accuracy							√	
security				√	√		√	
enforcement/Redress				√	√	√	√	√
匿名相关的原则								
anonymity	√	√		√	√	√	√	√
pseudonymity	√	√		√	√	√	√	√
unobservability						√	√	
unlinkability						√	√	
deniability						√		
其他提高隐私保护的原则								
user preference								
negotiation								
seclusion				√	√			
ease of adoption	√	√						
ease of compliance	√	√						
usability	√	√		√				
responsiveness	√	√						
personalization quality		√		√	√			

4 存在问题及未来研究重点

通过分析上述隐私保护技术可以看到,尽管有比较多的隐私保护方法出现,但未来需要进一步研究的问题还是比较多。

a)透明性。个性化研究中,过分重视用户个人信息的获取,忽视了用户对个人数据的控制权,研究相关技术来保证用户对个人数据的获取和使用的透明性,从而使得用户更加主动地提供个人数据,进而提高个性化系统的性能。

b)实时性。这一点是指用户兴趣偏好以及对隐私的要求会随着时间、场合、心情、需求的变化而变化。目前的隐私保护技术中没有考虑到这一点,所以可研究能随时跟踪捕捉到用户隐私要求的变化,并能随之而改变其隐私策略的技术。

c)针对性。文献[61]在研究中发现,不同用户对隐私的态度是不同,从而可以把用户分成三类,即隐私严苛者、隐私无关者和隐私实用者。隐私严苛者对自己个人的任何信息都非常在意其安全性;而隐私无关者则对个人数据的安全性关注不是很高,对隐私的态度比较温和;隐私实用者对个人数据会根据个人需要而给出,如果了解了个人数据的用途会选择给出个人数据。目前的隐私保护技术中没有关注到不同用户对隐私

态度的不同,研究针对不同的用户而采取不同技术保护措施的系统是未来的一个研究方向。

d)敏感性。研究表明用户对不同类型的个人数据的敏感度是不同的,如对身份信息、储蓄信息、信用信息等比较敏感,而对职业、爱好、学历等不太敏感。目前的隐私保护技术中没有考虑到敏感数据和不敏感数据的区别,研究对不同类型的信息采用不同的隐私保护策略,从而提高对敏感数据的敏感性也是未来的研究重点。

e)充分性。目前大多数网站都兼容了 P3P 等隐私保护技术,但 P3P 等隐私保护技术还存在一定的不完备性,不能充分表达用户的隐私保护需求。同时,这些隐私保护技术缺乏相应的技术和法律措施来保证其隐私保护策略的实施,对用户而言,表达的隐私保护需求是否得以实现不可而知。因此,研究相应的能充分描述用户隐私要求的隐私描述语言以及相关的技术保证措施,是未来的一个研究方向。同时,研究便于使用户了解和掌握个人隐私保护需求是否得以实现的方法和措施也是一个研究方向。

关于个性化隐私保护已经成为研究者关注的一个热点,隐私保护不局限于个性化推荐,其他领域的隐私保护也都逐步走进了研究者的视野当中。

参考文献:

[1] KOBSA A. User modeling in dialog systems: potentials and hazards [C]//Proc of IFIP/GI Conference on Opportunities and Risks of Artificial Intelligence Systems. 1989:147-165.

[2] RESINICK P, VARIAN H R. Recommender systems[J]. Communications of the ACM,1997,40(3):56-58.

[3] 许海玲. 互联网推荐系统比较研究[J]. 软件学报,2009,20(2):350-362.

[4] WANG Yang, KOBSA A. Technical solutions for privacy-enhanced personalization[J]. Intelligent User Interiaces,2009,5704(949):353-376.

[5] WANG Huai-qing, LEE M K O, WANG Chen. Consumer privacy concerns about Internet marketing [J]. Communications of the ACM,1998,41(3):63-70.

[6] KOBSA A. Privacy-enhanced Web personalization [M]//BRUSILOVSKY P, KOBSA A, NEJDL W. The Adaptive Web: Methods and Strategies of Web Personalization. Berlin: Springer-Verlag,2007:628-670.

[7] WESTIN A F. Privacy and freedom[M]. [S. l.]: The Bodley Head Ltd,1970.

[8] 臧镇. 个性化搜索中隐私保护的关键问题研究[D]. 杭州:浙江大学,2008.

[9] WANG Yang, KOBSA A. Privacy-enhancing technologies [M]// GUPTA M, SHARMAN R. Handbook of Research on Social and Organizational Liabilities in Information Security. Hershey: IGI Global, 2009:203-227.

[10] 陈娟. P3P 的隐私政策变更风险及其对策研究[D]. 大连:东北财经大学,2005.

[11] 袁志斌. 基于 P3P 的网络隐私保护[J]. 电脑与电信,2008(6):15-16.

[12] 蔡莉. 基于 P3P 的隐私策略评估系统的设计与实现[J]. 云南大学学报:自然科学版,2006,28(S2):45-50.

[13] AGRAWAL R, KIERNAN J, SRIKANT R, *et al*. XPref: a preference language for P3P[J]. Computer Networks,2005,48(5):809-827.

[14] ASHLEY P,HADA S,KARJOTH G,*et al*. Enterprise privacy authorization language(EPAL), RZ345(#93951)[R]. [S. l.]: IBM Corporation,2003.

[15] 谢舒婷. 基于 XACML 流媒体服务器的 Web 访问控制模型[J]. 计算机技术与发展,2010,20(9):136-140.

[16] 张晓波. 基于 XACML 的角色访问控制机制的研究与实现[D]. 长春:吉林大学,2008.

[17] 贾雯. 基于 XACML 的普适计算下的访问控制的研究与实现[D]. 长春:东北师范大学,2007.

[18] 邓凯,裴浩. 基于 XACML 和 SAML 的 Shibboleth 隐私保护方法的探索分析[J]. 计算机应用与软件,2009,26(1):267-284.

[19] CANNY J. Collaborative filtering with privacy[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society,2002:45-57.

[20] CANNY J. Collaborative filtering with privacy via factor analysis [C]//Proc of the 25th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM Press,2002:238-245.

[21] BERKOVSKY S, EYTANI Y, KUFLIK T, *et al*. Privacy-enhanced collaborative filtering[C]//Proc of user Modeling Workshop on Privacy-Enhanced Personalization. 2005:75-83.

[22] BERKOVSKY S, KUFLIK T. Hierarchical neighborhood topology for privacy enhanced collaborative filtering[C]//Proc of CHI Workshop on Privacy-Enhanced Personalization. 2006:6-13.

[23] TVEIT A. Peer-to-peer based recommendations for mobile commerce [C]//Proc of the 1st International Workshop on Mobile Commerce. New York: ACM Press,2001:26-29.

[24] SHOKRI R, PEDARSANI R,THEODORAKOPOULOS G, *et al*. Preserving privacy in collaborative filtering through distributed aggregation of offline profiles[C]//Proc of the 3rd ACM Conference on Recommender Systems. New York: ACM Press,2009:157-164.

[25] BILENKO M, RICHARDSON M. Predictive client-side profiles for personalized advertising[C]//Proc of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press,2011:413-421.

[26] XU Ya-bo, WANG Ke, ZHANG Ben-yu, *et al*. Privacy-enhancing personalized Web search[C]//Proc of the 16th International Conference on World Wide Web. New York: ACM Press,2007:591-600.

[27] MILLER B, KONSTAN J, RIEDL J. PockLens: toward a personal recommender system[J]. ACM Trans on Information Systems, 2004,22(3):437-476.

[28] OLSSON T. Decentralised social filtering based on trust[C]//Proc of AAAI Recommender Systems Workshop. 1998:84-88.

[29] BALABANOVIC M, SHOHAM Y. Fab: content-based collaborative recommendation[J]. Communications of the ACM,1997,40(3):66-72.

[30] GABBER E, GIBBONS P B, MATIAS Y, *et al*. How to make personalized Web browsing simple, secure, and anonymous[C]//Proc of the 1st International Conference on Financial Cryptography. London: Springer-Verlag,1997:17-31.

[31] GILBURD B, SCHUSTER A, WOLFF R. *k*-TPP: a new privacy model for large-scale distributed environments[C]//Proc of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Date Mining. New York: ACM Press,2004:563-568.

[32] POLAT H, DU Wen-liang. Privacy-preserving collaborative filtering

using randomized perturbation techniques[C]//Proc of the 3rd Internation Conference on Data Mining. Washington DC: IEEE Computer Society,2003:625-628.

[33] POLAT H, DU Wen-liang. SVD-based collaborative filtering with privacy[C]//Proc of ACM Symposium on Applied Computing. New York: ACM Press,2004:791-795.

[34] AGRAWAL R, SRIKANT R. Privacy-preserving data mining[C]//Proc of ACM SIGMOD International Conference on Management of Data. New York: ACM Press,2000:439-450.

[35]张付志,刘亭,封素石.一种改进的隐私保持协同过滤推荐算法[J].计算机工程,2010,36(16):126-134.

[36] BILGE A, POLAT H. An improved privacy-preserving DWT-based collaborative filtering scheme[J]. Expert Systems with Applications,2011,39(3): 3841-3854.

[37] LI Tao, GAO Chao, DU Jing-lin. An NMF-based privacy-preserving recommendation algorithm[C]//Proc of the 1st International Conference on Information Science and Engineering. 2009:754-757.

[38] KOTOULAS S, STEGERS R. A scalable architecture for peer privacy on the Web[C]//Proc of the 6th European Semantic Web Conference. 2009.

[39] HUBERMAN B A, FRANKLIN M, HOGG T. Enhancing privacy and trust in electronic communities[C]//Proc of the 1st ACM Conference on Electronic Commerce. New York: ACM Press,1999: 78-86.

[40] ISHITANI L, ALMEIDA V, Jr WAGNER M. Masks: bringing anonymity and personalization together[J]. IEEE Security & Privacy Magazine,2003,1(3):18-23.

[41] KOBSA A. A component architecture for dynamically managing privacy in personalized Web-based systems[C]//Proc of the 3rd International Workshop on Privacy Enhancing Technologies. 2003:177-188.

[42] HITCHENS M, KAY J, KUMMERFELD B, *et al*. Secure identity management for pseudo anonymous service access[C]//Proc of the 2nd International Conference on Security in Pervasive Computing. 2005:48-55.

[43] SAMARATI P, SWEENEY L. Generalizing data to provide an onymity when disclosing information[C]//Proc of the 17th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. New York: ACM Press,1998:188.

[44] SAMARATI P, SWEENEY L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression[C]//Proc of IEEE Symposium on Research in Security and Privacy. 1998.

[45] MACHANAVAJJHALA A, KIFER D, GEHRKE J, *et al*. l-diversity: privacy beyond k-anonymity[J]. ACM Trans on Knowledge Discovery,2007,1(1):1-56.

[46] WONG C R W,LI Jiu-yong,FU A W C,*et al*. (a,k)-anonymity:an enhanced k-anonymity model for privacy preserving data publishing [C]//Proc of the 12th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York: ACM Press,2006:754-759.

[47] LI Ning-hui, LI Tian-cheng, VENKATASUBRRAMANIAN S. t-closeness: privaey beyond k-anonymity and l-diversity[C]//Proc of the 23rd International Conference on Data Engineering. 2007:106-115.

[48] ZHANG Qing, KOUDAS N, SRIVASTAVA D, *et al*. Aggregate query answering on anonymized tables[C]//Proc of the 23rd IEEE International Conference on Data Engineering. 2007:116-125.

[49] XIAO Xiao-kui, TAO Yu-fen. Personalized privacy preservation [C]//Proc of ACM SIGMOD International Conference on Management of Data. New York: ACM Press,2006:229-240.

[50] YE Xiao-jun, ZHANG Ya-wei, LIU Ming. A personalized(a,k)-anonymity model[C]//Proc of the 9th International Conference on Web-age Information Management. 2008:341-348.

[51] RAO J R, ROHATGI P. Can pseudonymity really guarantee privacy [C]//Proc of the 9th USENIX Security Symposium. 2000:85-96.

[52] HOENS T R, BLANTON M, CHAWLA N. A private and reliable recmmendation system using a social network[C]//Proc of the 2nd International Conferenceon Social Computing. Washington DC: IEEE Computer Society,2010:816-825.

[53] KWON K, CHO J, PARK Y. Multidimensional credibility model for neighbor selection in collaborative recommendation[J]. Expert Systems with Applications,2009,36(3):7114-7122.

[54] POUWELSE J A, GARBACKI P, WANG J, *et al*. TRIBLER: a social-based peer-to-peer systems[J]. Concurrency and Compution: Practice and Expperience,2008,20(2):1-11.

[55] FAN Bei, LIU Lu, LI Ming, *et al*. Knowledge recommendation based on social network theory[C]//Proc of IEEE Symposium on Advanced Management of Information for Globalized Enterprises. 2008:1-3.

[56] PENNOCK D M, HORVITZ E, GILES C. Social choice theory and recommender systems: analysis of the axiomatic foundations of collaborative filtering[C]//Proc of the 17th National Conference on Artificial Intelligence. [S.l.]: AAAI Press,2000:729-734.

[57] VIEJO A, JORDI C R. Using social networks to distort users' profiles generated by Web search engines[J]. Computer Networks, 2010,54(9):1343-1357.

[58] LATHIA N, HAILES S, CAPRA L. Private distributed collaborative filtering using estimated concordance measures[C]//Proc of ACM Conference on Recommender System. New York: ACM Press,2007: 1-8.

[59] HERLOCKER J, KONSTAN J. Content independent task focused recommendation[J]. IEEE Internet Computing,2001,5(6):40-47.

[60] CRANOR L F. I didn't buy it for myself: privacy and ecommerce personalization[C]//Proc of ACM Workshop on Privacy in the Electronic Society. New York: ACM Press,2003:111-117.

[61] LOUIS H, WESTIN A F. Harris-equifax consumer privacy survey [M]. Atlanta, GA: Equifax Inc,1991.

[62] KALELI C, POLAT H. P2P collaborative filtering with privacy[J]. Turkish Journal of Electrical Engineering & Computer Sciences, 2010,18(1):101-116.

[63] BERKOVSKY S, EYTANI Y, KUFLIK T, *et al*. Enhancing privacy while preserving the accuracy of collaborative filtering[C]//Proc of Workshop on Recommender Systems. New York: ACM Press,2006: 49-53.

[64] MALIN B, SWEENEY L, NEWTON E. Trail re-identification: learning who you are from where you have been, LIDAP-WP12[R]. Pittsburgh: Carnegie Mellon University,2003.

[65] ARLEIN R M, JAI B, JAKOBSSON M, *et al*. Privacy-preserving global customization[C]//Proc of the 2nd ACM Conference on Electronic Commerce. New York: ACM Press,2000:176-184.

[66] LI Jie-xing, TAO Yu-fei, XIAO Xiao-kui. Preservation of proximity privacy in publishing numerical sensitive data[C]//Proc of ACM SIGMOD International Conference on Management of Data. New York: ACM Press,2007:473-486.