基于密文检索的位置服务用户隐私保护方案

刘树波 李艳敏 刘梦君
(武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)
(武汉大学计算机学院 武汉 430072)

摘 要 在基于位置服务系统中,为用户提供高质量服务的同时如何很好地保护用户的隐私(身份、行踪以及偏好等)仍然是一个挑战。针对这一挑战,提出了基于密文检索的位置服务用户隐私保护方案。在本方案中,位置服务提供商将其服务数据以及数据向量索引以密文的形式外包给云端,移动用户通过密文查询请求向云端查询所需服务,云端通过用户的查询以及服务数据索引计算出匹配度高的服务数据并返回给用户,整个交互过程都是以密文形式进行,云端以及外界得不到任何明文信息。本方案不依赖集中匿名器和用户协作,最后通过理论以及实验分析表明,本方案以低的计算开销有效地保护了用户的身份、位置以及查询偏好隐私。

关键词 基于位置服务,隐私保护,密文检索,匹配度
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.4.019

Privacy-preserving for Location-based Service over Encrypted Data Search

LIU Shu-bo LI Yan-min LIU Meng-jun
(Key Laboratory of Airspace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China)
(School of Computer, Wuhan University, Wuhan 430072, China)

Abstract In location-based service system, it is a vital problem to protect user's privacy including identity privacy, location privacy and preference privacy, and gain high quality service for users at the same time. This paper proposed a privacy-preserving scheme based on encrypted data search. Location-based service provider outsources its encrypted data and index to cloud server who executes user's LBS queries and returns the top-K results to user according to matching score. The scheme does not rely on user's cooperation and any trusted third party. Finally theoretical and experimental analysis shows that the proposed scheme can effectively protect user's identity, location and preference privacy with a lower computation and communication overhead.

Keywords Location-based service, Privacy-preserving, Searchable encryption, Matching score

1 引言

无线通信技术和定位技术的发展以及移动设备的普及,催生了LBS应用。LBS是指用户通过向位置服务提供商(Location-based Service Provider, LBSP)提供自己的位置信息,得到相应的服务查询结果的服务,比如移动用户查询其附近的加油站、医院、餐馆、公交站或娱乐场所等。而日益普及的移动互联网,更是使得LBS成为了人们生活中不可或缺的一部分。

然而,用户在享受LBS带来的极大便利的同时也面临着个人隐私泄露的风险。恶意的位置服务提供商或其他攻击者根据用户位置和查询内容,运用数据挖掘和机器学习等方法,可以获得用户的隐私信息,从而给用户的隐私带来严重威胁。因而在LBS系统中,如何保护用户的隐私一直是研究的热点。从国内外已取得的研究成果来看,大量的研究都是基于隐匿技术,比如假地址技术[1-4]、隐匿空间技术[5-8]、假名技术以及匿名组[9-11]等隐匿技术,这些技术都是将用户的信息隐藏在一些虚假信息中。现有隐匿技术的研究都是借鉴了数据库中的K-匿名机制[12-17],其原理是通过将用户信息隐藏在至少$K-1$个难以区分的用户中,使得攻击者不能分辨出某条信息究竟是K个用户中的哪一个用户的,从而保护了用户的隐私。K匿名技术的关键是集中式的匿名器,用户的请求先经过完全可信的匿名器完成K匿名处理再发给LBSP。在这种方案中,匿名器在查询高峰时容易成为系统的瓶颈,而且匿名器容易成为攻击者的重点攻击目标,一旦匿名器被攻破,系统中的用户将无隐私可言。

为了不依赖匿名器,学者们[12,14,16]提出了分布式的K-匿名技术,文献[16]通过P2P模式,汇聚区域内一定数量用户的位置查询请求,实现K匿名位置查询服务。并且,通过这种分布式汇聚方式,可以有效地保护各个用户的服务偏好隐私。然而,P2P模式中用户间会产生大量的交互,并且移动用户需要完成K匿名处理,这将消耗移动用户大量的资源,制约了分布式的K-匿名技术的发展。

云计算的兴起、云端强大的存储以及计算能力为LBS隐

到稿日期:2014-07-28 返修日期:2014-09-30
刘树波(1970—),男,教授,博士生导师,主要研究方向为信息安全、物联网、嵌入式系统,E-mail:liu.shubo@whu.edu.cn(通信作者);李艳敏(1989—),女,硕士生,主要研究方向为信息安全、网络安全,E-mail:joymin19@foxmail.com;刘梦君(1988—),男,博士生,主要研究方向为无线传感器网络安全、嵌入式系统。

私保护提供了新的思路。文献[18]通过将 LBS 服务数据外包到云端之上，利用云端强大的资源为用户提供位置查询服务，并且保护了用户位置隐私。然而，其并没考虑用户查询偏好的隐私保护，并且在处理用户查询请求时云端需要对所有的服务数据进行大量的线性对计算，以找出满足用户请求的服务数据，这大大浪费了云端的计算资源。因此，在将 LBS 服务数据外包到云端这种模式下，以较小的移动终端和云端代价，同时保障用户的位置和查询偏好隐私，仍然是一个巨大的挑战。

为了解决这个挑战，本文提出了基于 KNN 向量分解技术的云端密文检索 LBS 用户隐私保护方案。在本方案中，用户将查询请求映射成请求向量，而 LBS 将服务数据同样映射成数据向量，并使用 KNN 向量分解技术将请求向量和数据向量进行分解、分别形成数据索引以及密文查询请求。云端只需通过用户的密文查询请求以及服务数据的索引，就可计算符合用户需求的服务数据。与现有的 LBS 隐私保护方案相比，本文提出的方案有如下优点：

1)本方案不依赖可信第三方，同时可单独进行查询服务；

2)云端在不获知用户查询偏好的情况下即可进行服务查询，而且查询过程还具有较高的效率；

3)移动端进行查询并对结果进行处理时需要的计算开销很小。

2 相关工作

目前国内外很多学者和研究人员针对 LBS 系统中的用户隐私保护做了大量的工作。主要包括假地址技术、基于可信第三方的 K-匿名技术、P2P 架构下的 K 匿名技术以及数据外包技术。

文献[13]提出的 K-匿名保护方式保护了用户的位置隐私和身份隐私，不过需要引入可信第三方作为匿名器。当用户向 LBSP 发送服务请求时，先把位置信息发给匿名器，匿名器将用户的精确位置泛化为一个具有 K-匿名性质的匿名区，这个区域内至少有 K 个用户并且该区域的面积不能小于一定的阈值。然后再根据该匿名区域向 LBSP 请求位置服务，LBSP 将该区域内的所有候选结果返回给用户，让用户自己挑选所需要的。该方案虽然能够在很大程度上解决用户位置隐私保护问题，但需要依赖可信匿名器，同时因为 LBSP 无法给用户精确的反馈，故需浪费用户一定的通信及计算开销。

针对上述问题，很多学者[12,14,16]引入了 P2P 的思想，取消了可信匿名器，通过用户彼此间的合作来完成匿名，从而解决了集中式匿名器瓶颈问题。文献[16]提出了一种 P2P 架构下的 K 匿名方案，有效地保护了用户的位置隐私、身份隐私以及查询偏好隐私。在用户通信范围内，需要请求 LBSP 服务的用户之间彼此合作，大于等于 K 个用户时将他们的服务请求(包括位置信息以及请求的具体内容)聚合在一起，这个服务请求必须包含大于等于 L 种服务，即至少 K 个用户请求至少 L 种服务，攻击者或 LBSP 无法确定某一条请求具体是哪个用户发出的，从而保护了用户的隐私。然后将聚合请求发给 LBSP，LBSP 处理完聚合请求后将结果返回给用户，用户各自再从中获得自己所需要的服务。虽然该方案在不依赖集中匿名器的同时还保护了用户的身份、位置以及查询偏好隐私，但用户端需完成请求聚合，其中的计算开销和通信开销对移动设备来说是个挑战，并且在没有 K 个用户提出 L 种服务请求时(现实生活中这种情况很常见)用户需要等待，从而影响用户的服务体验。

文献[18]提出了一种不依赖可信第三方同时也无需用户协作的新的 LBS 用户隐私保护框架，该框架将 LBSP 的服务数据经属性加密后再外包到云服务器，用户直接向云服务器请求相关服务。该框架虽然保护了用户的位置隐私，但是并没考虑用户查询偏好的隐私保护，并且用户不能根据自己的需求来获得特定的服务。同时 LBSP 外包数据时没有为数据生成相关索引，故云服务器在处理用户的服务请求时需对每个服务数据都进行大量的线性对加密运算，大大浪费了云端的计算资源。

3 模型及假设

3.1 系统模型

如图 1 所示，该系统主要由密钥分发中心(KDC)、位置服务提供商(LBSP)、云服务器(CSS)以及移动用户 4 个部分组成。

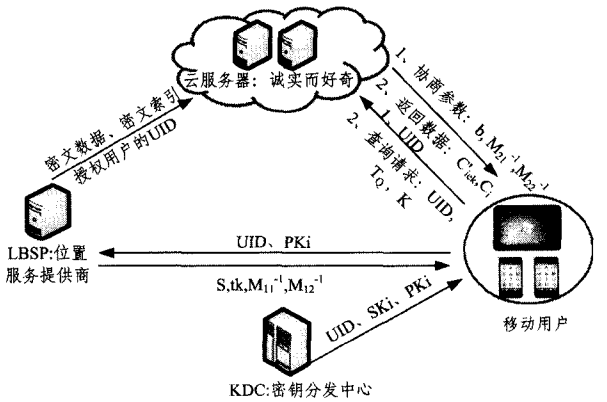

图 1 系统模型

1)KDC 负责管理系统中的用户，如图 1 所示，它为系统中每一个用户分发公私钥对$\{SK_i, PK_i\}$以及一个唯一的用户编号 UID，通过安全可信通道(如 SSL 套接字)分发给用户。

2)LBSP 将其服务所覆盖的范围区域化形成 n_1 个区域 $L=\{L_1, L_2, L_3, \cdots, L_{n_1}\}$，然后根据其所有的服务数据 $F=\{F_1, F_2, F_3, \cdots, F_m\}$提取出 n_2 个关键字 $W=\{W_1, W_2, W_3 \cdots W_{n_2}\}$，比如“美食”、“团购”、“KTV”、“电影”、“公交”、“医院”、“酒店”等。将 F 逐一加密得到 $C=\{C_1, C_2, C_3, \cdots, C_m\}$，然后将 C 以及 F 所对应的密文索引 $I=\{I_1, I_2, I_3, \cdots, I_m\}$外包给云服务器。

3)移动用户刚加入系统时需要由 KDC 为自己分配相关密钥，查询服务时在需要获得 LBSP 授权的同时还需要根据自己的位置信息以及查询关键字生成密文查询请求 T_Q，然后向云服务器请求自己所需要的服务，收到查询结果后需要解密得到明文数据以获得服务。

4)云服务器负责管理 LBSP 的外包数据，同时完成合法用户的服务查询请求，根据用户的查询请求及数据的索引计算最能满足用户查询请求的 top-k 个数据文件并将结果返回给用户。

3.2 安全模型及设计目标

本系统中我们主要考虑移动用户位置和查询偏好隐私，以及位置服务提供商的数据安全。系统中云服务器是诚实而好奇的，它会忠实地正确执行系统中的协议，但会基于其所接

触的数据，最大化窥探或分析用户和 LBSP 的私密信息。

围绕以上安全需求，设计目标主要包括：

1)用户的身份隐私保护，即用户的真实身份信息不被泄露；

2)用户的查询偏好隐私保护，即用户查询过什么服务、对什么感兴趣不被泄露；

3)用户的位置隐私保护，即用户的精确位置不被外界获知；

4)LBSP 的服务数据安全，即 LBSP 的服务数据不能被云服务器以及非法用户获得。

3.3 相关定义

定义 1 二进制数据向量 D，根据服务数据所服务的区域以及包含的关键字而形成，每个 F_i 对应一个 D_i，m 个文件对应的数据向量为 $D=\{D_1,D_2,D_3,\cdots,D_m\}$。而任意的 D_i 都跟地理位置区域集合 L 及关键字集合 W 对应。当 $1\leqslant j\leqslant n_1$ 时，$D_{ij}=1$，表示该数据服务范围涵盖 L_j 区域，等于 0 则不涵盖；当 $n_1\leqslant j\leqslant n(n=n_1+n_2)$ 时，$D_{ij}=1$ 表示该服务数据包含 W_j 这个关键字，反之则不包含。

定义 2 二进制用户请求向量 Q，根据用户所在的位置及所查询的关键字而形成，Q 中的每一位与数据向量 D 是一一对应的。

4 预备知识

4.1 双线性映射

设 G_1 和 G_2 是两个阶为素数 q 的循环群，双线性映射 e：$G_1\times G_2\rightarrow G_2$ 满足如下的性质：

1)双线性：对于任意 $P,Q\in G_1$ 和 $a,b\in Z_P$ 满足 $e(aP,bQ)=e(P,Q)^{ab}$。

2)非退化性：存在 $P\in G_1$ 使得 $e(P,P)\neq 1$。

3)可计算性：对于任意的 $P,Q\in G_1$，存在一个高效的算法计算 $e(P,Q)$。

4.2 代理重加密

代理重加密(Proxy Re-Encryption，PRE)是一种基于密文的密钥转换机制，是由 Blaze 等[19]在 1998 年的欧洲密码学年会上首次提出的。PRE 的主要思想是半可信代理将 A 加密的密文转化为 B 可解的密文，并且在完成转换过程中，半可信代理得不到任何明文数据以及 A、B 双方的私钥信息。

4.3 安全的 KNN[16]向量分解

根据 n 维二进制分解向量 S，将 n 维向量 P 分解为 2 个 n 维向量 Pa 和 Pb，分解规则如下：

对 $\forall i\in(1,n)$ 有

1)当 $S_i=0$ 时，不分解 P，即 $Pa_i=Pb_i=P_i$；

2)当 $S_i=1$ 时，分解 P，选择一个随机数 t，令 $Pa_i=t$，$Pb_i=P_i-Pa_i$，即 $Pa_i+Pb_i=P_i$。

当然也可以反过来，即 $S_i=0$ 时，分解 P；$S_i=1$ 时，不分解 P。本文需要对数据向量 D 和查询向量 Q 进行分解，而分解这两向量时规则是相反的，即 $S_i=0$ 时分解 D 不分解 Q，$S_i=1$ 时分解 Q 不分解 D。因为这样能保证向量 D、Q 经分解成为 Da、Db 和 Qa、Qb 后仍可计算 D 和 Q 的向量积 $D\cdot Q=Da\cdot Qa+Db\cdot Qb$。如给定 $D=(x_1,x_2)$ 和 $Q=(y_1,y_2)$，将 D 解为 $Da=(x_1,x_{21})$ 和 $Db=(x_1,x_{22})$，将 Q 分解为 $Qa=(y_{11},y_2)$ 和 $Qb=(y_{12},y_2)$，其中 $x_{21}+x_{22}=x_2$，$y_{11}+y_{12}=y_2$，则，$Da\cdot Qa+Db\cdot Qb=x_1y_{11}+x_{21}y_2+x_1y_{12}+x_{22}y_2=x_1(y_{11}+y_{12})+y_2(x_{21}+x_{22})=D\cdot Q$。

5 方案描述

5.1 设计思想

根据 3.2 节的设计目标，为了不让 LBSP 获得用户的位置以及查询偏好隐私，故将 LBS 服务数据外包到云端，利用云端强大的资源为用户执行位置服务查询请求，中断用户与 LBSP 的直接交互。与此同时，将 LBSP 的服务数据外包到云端，为了保护其数据的安全，故需让服务数据在本地进行加密处理再以密文的形式外包到云端。但这样给用户查询所需服务造成了一定的困难，故采用了向量索引技术[21]为 LBS 服务数据建立索引 I，它有效地提取了数据的关键信息并且能进行高效率的查询匹配运算。最后为了不让外界以及云端获得用户的隐私故将用户的位置以及查询内容映射成二进制向量 Q，利用 KNN 向量分解技术以及矩阵加密技术对 Q 进行加密处理得到密文查询请求 T_Q。用户查询服务时，云端根据用户的查询请求 T_Q 以及服务数据索引 I 计算出最满足用户请求的 K 个文件，并将结果返回给用户，用户得到结果后自己解密得到明文服务数据。

5.2 方案交互过程

本方案主要包括系统初始化、服务数据外包、用户授权、查询请求的生成以及服务数据的查询共 5 个部分：

1)系统初始化，LBSP 选择一个安全参数 λ，运行 $Setup(1^\lambda)$ 生成系统参数 (q,g,G,G_T,e)，其中 G 和 G_T 是 q 阶循环群，g 是 G 的生成元，再随机选择 $\alpha\in Z_q^*$，公开 (g,e)，保密 α。

2)服务数据外包，这个过程主要包括数据文件的加密和文件索引的建立。LBSP 首先从文件集 F 中提取 L 及 W，然后随机生成 $(n+2)$ 的二进制向量 S 以及两个 $(n+2)(n+2)$ 的非奇异对角矩阵 $\{M_{11},M_{12}\}$ 并对外保密。数据外包以单个文件为单位。下面以 F_i 为例说明数据外包的过程，首先生成 F_i 对应的 D_i，确定 F_i 服务区域并同时提取该文件的关键词集将这些信息映射到 n 维二进制数据向量 D_i 中，D_i 与 L 及 W 的关系如表 1 所列，D_i 的每一位跟 L 及 W 对应，为 1 表示包含，为 0 表示不包含。然后分解 D_i，随机选择 ε_i(ε_i 服从正态分布 $N(0,\sigma^2)$)，将 D_i 扩展为 $n+2$ 维，形成新的 $D_i=(D_i,1,\varepsilon_i)$，利用 S 将 D_i 分解为 2 个 $n+2$ 维向量 D_{ia} 和 D_{ib}，计算文件索引 $I_i=\{M_{11}^{\mathrm{T}}D_{ia},M_{12}^{\mathrm{T}}D_{ib}\}$。然后用对称加密算法加密明文数据，在密钥空间选取密钥 ek_i，用 ek_i 加密数据 F_i 形成 C_i，即 $C_i=ENC_{ek_i}(F_i)$，用 α 加密 ek_i 即 $C_{ek_i}=ENC_\alpha(ek_i)=e(g,g)^\alpha ek_i$，最后将 F_i 外包给云服务器，具体格式如表 2 所列。

表 1 D_i 与 L 及 W 的关系说明表

	L_1	L_2	…	L_{n_1}	W_1	W_2	…	W_{n_2}
D_i	0	1	…	0	1	1	…	0

表 2 外包数据格式

FID	$I_i=\{M_{11}^{\mathrm{T}}D_{ia},M_{12}^{\mathrm{T}}D_{ib}\}$	$C_{ek_i}=ENC_\alpha(ek_i)$	$C_i=ENC_{ek_i}(F_i)$

3)用户授权与注销，用户 U_i 需要查询服务时，首先 KDC 为其生成相关密钥对 SK_i、PK_i，KDC 随即选取 $sk_i\in Z_q^*$，$pk_i=g^{*_i}$，同时 KDC 为用户分配一个用户编号 UID，将密钥对和 UID 通过安全信道发给用户。用户将自己的公钥 PK_i 和 UID 发给 LBSP 向其请求授权，LBSP 收到用户请求后，首先计算该用户的传递密钥 $tk=pk_i^\alpha=g^{*_i\cdot\alpha}$，最后 LBSP 通过安

全信道将$\{tk,S,M_{11}^{-1},M_{12}^{-1}\}$发给用户，将{UID}发给云服务器。当用户退出服务程序时，则该用户的 UID 被视为无效，从用户列表中删除。

4)查询请求的生成，用户需要查询服务时，首先发送 UID 给云服务器，云服务器收到 UID 后查用户列表验证用户的合法性，通过验证则为该用户随机生成两个$(n+2)(n+2)$的非奇异对角矩阵$\{M_{21},M_{22}\}$以及随机选取$b\in Zq$，然后将$\{M_{21}^{-1},M_{22}^{-1},b\}$通过安全信道给过用户，云服务器同时为该用户建索引 $I_i=\{M_{21}^{T},M_{22}^{T}\}\cdot I_i=\{M_{21}^{T},M_{22}^{T}\}\cdot\{M_{11}^{T}D_{ia},M_{12}^{T}D_{ia}\}=\{M_{21}^{T}(M_{11}^{T}D_{ia}),M_{22}^{T}(M_{12}^{T}D_{ib})\}$，用户收到$\{M_{21}^{-1},M_{22}^{-1},b\}$后，通过自身设备确定所处位置区域，然后根据输入的查询关键字，将位置信息及关键字信息映射成 n 维请求向量 Q，其过程与数据向量形成过程是一样的。选取两随机数 r 和 t 将 Q 扩展为$(n+2)$维，形成新的$Q=(rQ,t,r)$，然后根据 S 将 Q 分解为 2 个$(n+2)$维的向量 Q_a 和 Q_b，该分解规则跟数据向量 D 的相反。计算密文查询请求 T_Q，$T_Q=\{M_{21}^{-1}(M_{11}^{-1}Q_a),M_{22}^{-1}(M_{12}^{-1}Q_b)\}$。将$\{UID,T_Q,K\}$发给云服务器请求相应服务，$K$ 代表只取 K 个匹配度高的文件。

5)服务数据的查询，文件数据跟查询请求的匹配程度直接用 $D\cdot Q$ 来度量[21]，其匹配度与 $D\cdot Q$ 成正比。故云服务器收到用户的查询请求后，依次计算每个文件的匹配度 $Score=T_Q\cdot I_i$，$Score$ 与 $D\cdot Q$ 成线性关系，故我们可以用 $Score$ 来度量文件数据与查询请求的匹配程度。

$$\begin{aligned}Score&=T_Q\cdot I_i\\&=\{M_{21}^{-1}(M_{11}^{-1}Q_a),M_{22}^{-1}(M_{12}^{-1}Q_b)\}\cdot\{M_{21}^{T}(M_{11}^{T}D_{ia}),M_{22}^{T}(M_{12}^{T}D_{ib})\}\\&=Q_a\cdot D_{ib}+Q_b\cdot D_{ib}\\&=D\cdot Q=r(D\cdot Q)+t+r\varepsilon_i\\&=r(D\cdot Q+\varepsilon_i)+t\end{aligned}$$

根据 $Score$ 得到前 K 个匹配度最高的文件，然后利用 b 依次计算这 K 个文件的 C'_{ek_i}：

$$C'_{ek_i}=C_{ek_i}e(g,g)^b=e(g,g)^{\alpha}\cdot e(g,g)^b\cdot ek_i$$

最后将这 K 个文件对应的$\{C'_{ek_i},C_i\}$发给用户，用户收到后首先利用自己的$\{sk_i,b\}$解密得到 ek_i，$ek_i=\dfrac{C'_{ek_i}}{e(g,g)^b\cdot e(tk,g)^{\frac{1}{sk_i}}}=\dfrac{e(g,g)^{\alpha}\cdot e(g,g)^b\cdot ek_i}{e(g,g)^b\cdot e(g^{sk_i\cdot\alpha},g)^{\frac{1}{sk_i}}}=\dfrac{e(g,g)^{\alpha}\cdot ek_i}{e(g,g)^{\alpha}}=ek_i$，然后用 ek_i 解密得到所需的服务数据 $F_i=DEC_{ek_i}(C_i)$。

6 方案分析

6.1 安全性分析

本方案不仅需要保护用户身份、查询以及位置隐私还需要保护 LBSP 的数据安全。

1)用户的身份隐私，KDC 负责管理用户，为每个用户分配相应的 UID。这个 UID 只是系统中的用户编号，不代表任何用户个人的信息，故外界无法利用 UID 推断出用户任何的真实身份信息。

2)用户的查询以及位置隐私，本方案将用户的查询内容以及位置信息都映射到请求向量 Q 中，并且引入了随机数对 Q 进行维度扩展以及分解操作，分解向量 S 对外保密。最后还利用对外保密的 4 个矩阵对分解后的向量进行加密操作，形成最后的密文查询请求 T_Q，文献[20]已经证明了向量分解后用矩阵进行加密的方法安全性。同时为了防止 LBSP 或其它用户截取用户的 T_Q 从而获取到用户的信息，云服务器为每个用户都生成了两个特定的矩阵$\{M_{21},M_{22}\}$并对外保密，，所以即便 LBSP 和其它用户截取了某个用户 T_Q，但因为不知道$\{M_{21},M_{22}\}$，所以也无法推断出用户的查询请求向量 Q 从而无法获得用户的信息。而在云服务器给用户返回结果时，因为数据已经进行了重加密，故 LBSP 也无法解密从而无法知道用户查询了什么服务。而用户的查询请求是以密文提交给云服务器的，云服务器在处理用户查询请求时，操作的也是密文，所以云服务器也无法获得用户的查询以及位置隐私。

3)LBSP 的外包数据始终是以密文形式存放在云服务器中，$\{r,M_{11},M_{12}\}$对云服务器都是保密的，故服务器无法获取 LBSP 的任何明文信息。

6.2 性能分析

我们主要从用户的角度出发来进行性能分析：1)用户所接收的服务质量主要包括所接收的服务数据的精度和服务器响应用户查询的时间；2)用户需承担的计算以及通信的开销，下面从这两个方面来进行分析。

根据 $Score=r(D\cdot Q+\varepsilon_i)+t$ 可知服务数据的精度受 ε_i 影响，我们由 Score 可得到服务器给用户返回的 K 个服务数据，同时由 $D\cdot Q$ 可得到真实的 K' 个服务数据，故用户所接收到的服务数据的精度 $Pk=(K\wedge K')/K$ 即真实的 K' 个文件在云服务器返回的 K 个文件中所占的比例。由实验我们得到 Pk 与 K 的关系如图 2 所示，从图可以看到无论 K 多大，Pk 都在 90%以上，即服务器返回给用户的服务数据 90%以上都满足用户的需求。

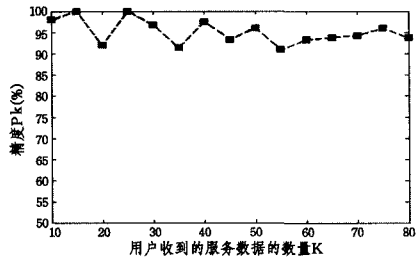

图 2 用户收到服务数据的精度

由方案的查询阶段可知服务器从接收到用户的 T_Q 后所需的时间开销包括找出 top-k 以及对 top-k 文件的 C_{ek_i} 进行重加密，操作完便将结果返回给用户。针对服务器处理查询的效率，我们对本方案做了实验，实验使用 Java 作为软件平台，硬件平台为浪潮双核服务器，操作系统为 64 位 Window Server 2088 R2 Enterprise，CPU 为 Xeon(R) E5-2420，主频为 1.9GHz，内存为 32GB。实验的结果如图 3 所示，其中服务数据总数量 $m=10000$，$K=30$，从图中可以看出，$n=10000$ 时云服务器给予的响应时间也仅需 2.5 秒。

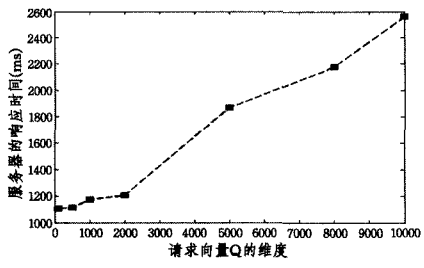

图 3 服务器的响应时间

用户的通信开销主要是在注册阶段需要接收相关的参数$\{M_{11}+M_{12}+S\}$、第一次跟云服务器发请求时需要接收$\{M_{21}+M_{22}\}$以及在查询服务阶段需接收云服务器返回的服务数

据$\{C'_{eki}, C_i\}$。本方案采用的是非奇异矩阵，其大小直接由 n（$n=n_1+n_2$）决定，不过在整个过程中用户只需进行一次注册，同时用户只有第一次跟云服务器请求服务时需要获得相关$\{M_{21}+M_{22}\}$，在后续的请求服务时都不再需要。用户的计算开销主要是在查询阶段进行矩阵与向量的乘法运算，生产密文查询请求 T_Q，以及接收到服务数据后需进行简单的线性对运算获得 ek_i，再利用对称加密算法解密文件得到最终的 F_i。对于用户的通信与计算开销总结如表 3 所列。同时对移动用户端生成 T_Q 的时间开销做了实验，实验使用 Java 作为软件平台，硬件平台为魅族 MX2，操作系统为 Android 4.1，四核 CPU 主频为 1638MHz，内存为 2GB。实验结果如图 4 所示，从图可看到，当 $n=10000$ 时需 0.469 秒，这个时间完全在用户可接受的范围内。

表 3　用户端性能分析表（$|X|$ 表示大小即 X 所占的比特数）

阶段	带宽开销		计算开销	
用户授权	$\|M_{11}\|+\|M_{12}\|+\|S\|$	O(n)	0	0
查询请求的生成	第一次发请求：$\|M_{21}\|+\|M_{22}\|+\|b\|+\|T_Q\|$ 其他：$\|T_Q\|$	第一次发请求：O(n) 其他：O(1)	T_Q	O(1)
服务数据的查询	$K*(C'_{eki}, C_i)$	O(K)	$K*(ek_i, F_i)$	O(K)

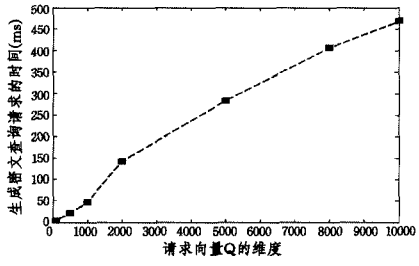

图 4　用户端查询生成查询请求 T_Q 的效率

结束语　本文为 LBS 系统中的用户提出了一种基于密文检索的隐私保护方案，通过引入云服务器，将 LBSP 的服务数据以密文形式外包给云服务器同时还为数据建立了索引，用户在查询服务时不但不会泄露用户隐私，同时还能快速地查询到所需的服务数据。本方案不依赖可信第三方和用户协作，保护了用户的身份、位置、查询偏好隐私，最后通过理论与实验分析表明，用户通过该方案付出的通信与计算开销较小。

参 考 文 献

[1] Leitner M, Curtis. A first step towards a framework for presenting the location of confidential point data on maps-results of an empirical perceptual study[J]. International Journal of Geographical Information Science, 2006, 20(7): 813-822

[2] Shankar P, Ganapathy V, Iftode L. Privately querying location-based services with Sybilquery[C]// Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp, ACM). 2009: 31-40

[3] Chang Wei, Wu Jie, Tan Chiu-Chiang. Enhancing mobile social network privacy[C]// Proceedings of the IEEE Global Communications Conference (Globecom). 2011: 1-5

[4] Wei Wei, Xu Feng-yuan, Li Qun. Flexible Privacy-preserving location sharing in mobile online social networks[C]// Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM). 2012: 2616-2620

[5] Gedik B, Liu Ling. Location privacy in mobile systems: A personalized anonymization model[C]// Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS). 2005: 620-629

[6] Chow Chi-Yin, Mokbel M F, Walid G. The new Casper: Query processing for location services without compromising privacy [C]// Proceedings of the 32nd International Conference on Ver Large Data Base. 2006: 763-774

[7] Chow Chi-Yin, Mokbel M F, He Tian. A privacy-preserving location monitoring system for wireless sensor networks[J]. IEEE Transactions on Mobile Computing, 2010: 94-107

[8] Chow Chi-Yin, Mokbel M F, Leong V. On Efficient and Scalable Support of Continuous Queries in Mobile Peer-to-Peer Environments[J]. IEEE Transactions on Mobile Computing, 2011, 10 (10): 1473-1487

[9] Beresford A R, Stajano F. Location privacy in pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(1): 46-55

[10] Pfitzmann A, Kohntopp M. Anonymity, unobservability, and pseudonymity-a proposal for terminology[C]// Designing privacy enhancing technologies. 2001: 1-9

[11] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router[C]// Proceedings of the 13th USENIX Security Symposium (Security'04). 2004: 303-320

[12] Chow Chi-Yin, Mokbel M F, Liu Xuan. A peer-to-peer spatial cloaking algorithm for anonymous location-based services[C]// Proc of the 14th ACM International Symposium on Advances in Geographic Information Systerms. NewYork: ACM Press, 2006: 171-178

[13] Mokbel M F, Chow Chi-Yin, Aref W G. The new casper: aprivacy-aware location-based database server[OL]. http://www-users. cs. umn. edu

[14] Ghinita G, Kalnis P, Skiadopoulos S. A mobile peer-to-peer system for anomymous location-based queries[C]// Proc. of the 10th International Symposium on Advances in Spatial and Temporal Databases. Berlin: Springer-Verlag, 2007: 519-523

[15] Kalnis P, Ghinita G, Mouratidis K, et al. Preventing location-based identity inference in anonymous spatial queries[C]// IEEE Trans. Knowl. Data Eng.. 2007: 1719-1733

[16] Lu Rong-xing, Lin Xiao-dong, Shi Zhi-guo, et al. PLAM: A privacy-preserving framework for local-area mobile social networks [C] // Proceedings of the 33st IEEE International Conference on Computer Communications. 2014

[17] Niu Ben, Li Qing-hua, Zhu Xiao-yan, et al. Achieving k-anonymity in Privacy-Aware Location-Based Services[C]// Proceedings of the 33st IEEE International Conference on Computer Communications. 2014

[18] Shao Jun, Lu Rong-xing, Lin Xiao-dong. FINE: A fine-grained privacy-preserving location-based service framework for mobile devices[C]// Proceedings of the 33st IEEE International Conference on Computer Communications. 2014

[19] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography[C]// Proceedings of Eurocrypt. 1998, 1403: 127-144

[20] Wong W K, Cheung D W, Kao B. Secure knn computation on encrypted databases[C]// Proceedings of the 35th SIGMOD International Conference on Management of Data. 2009: 139-152

[21] Cao N, Wang C, Li M, et al. Privacy-preserving Multi-keyword ranked search over encrypted cloud data[C]// IEEE INFOCOM. 2011: 829-837