(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113158087 B
(45)授权公告日 2024.07.09

(21)申请号 202110384135.2

(22)申请日 2021.04.09

(65)同一申请的已公布的文献号
申请公布号 CN 113158087 A

(43)申请公布日 2021.07.23

(73)专利权人 深圳前海微众银行股份有限公司
地址 518027 广东省深圳市前海深港合作区前湾一路1号A栋201室
专利权人 西安电子科技大学

(72)发明人 苗银宾 童秋云 范瑞彬 张开翔 李辉忠 严强 李成博

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 宋正伟

(51)Int.Cl.
G06F 16/9537(2019.01)
G06F 16/951(2019.01)
G06F 16/33(2019.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

(56)对比文件
CN 104731860 A,2015.06.24
CN 110222012 A,2019.09.10
CN 110362652 A,2019.10.22
CN 111212084 A,2020.05.29

审查员 王晓嫚

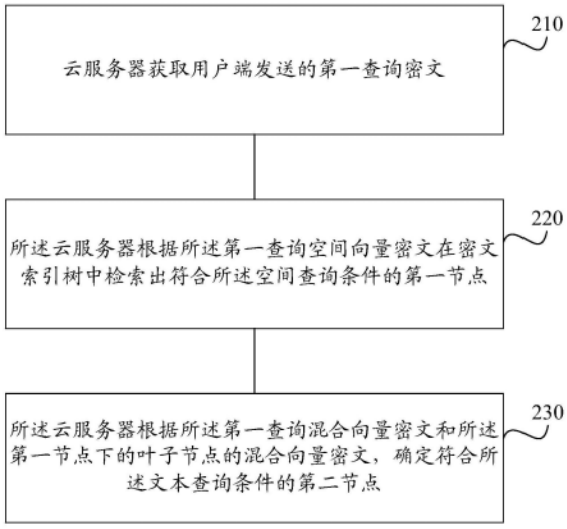
权利要求书3页 说明书20页 附图5页

(54)发明名称

一种空间文本的查询方法及装置

(57)摘要

本发明公开了一种空间文本的查询方法及装置,包括:云服务器获取用户端发送的第一查询密文,其中,第一查询密文包括第一查询空间向量密文和第一查询混合向量密文,第一查询空间向量密文是根据查询请求中的空间查询条件生成的,第一查询混合向量密文是根据查询请求中的文本查询条件和空间查询条件生成的,根据第一查询空间向量密文在密文索引树中检索出第一节点,根据第一查询混合向量密文和第一节点下的叶子节点的混合向量密文,确定符合文本查询条件的第二节点,避免查询结果受权重的影响,使查询结果在查询范围内,防止查询结果与查询位置距离过远的问题,提升了空间文本查询的准确度,提升了用户的查询体验。



CN 113158087 B

1.一种空间文本的查询方法,其特征在于,包括:

云服务器获取用户端发送的第一查询密文;所述第一查询密文包括第一查询空间向量密文和第一查询混合向量密文;所述第一查询空间向量密文是根据查询请求中的空间查询条件生成的;所述第一查询混合向量密文是根据所述查询请求中的文本查询条件和所述空间查询条件生成的;

所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点;所述密文索引树是数据拥有者根据各明文空间文本构建的;所述密文索引树中的非叶子节点存储有基于明文空间文本中的空间信息生成的空间向量密文,叶子节点存储有基于明文空间文本中的空间信息和文本信息生成的混合向量密文;所述第一节点为非叶子节点;

所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点;所述第二节点为叶子节点;所述第二节点用于作为查询结果。

2.如权利要求1所述的方法,其特征在于,所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点,包括:

所述云服务器根据预设检索顺序,针对所述密文索引树中的任一节点,在确定所述节点为非叶子节点时,根据所述第一查询空间向量密文和所述节点的空间向量密文确定与所述第一查询空间向量密文相交的所述第一节点。

3.如权利要求2所述的方法,其特征在于,根据所述第一查询空间向量密文和所述节点的空间向量密文确定与所述第一查询空间向量密文相交的所述第一节点,包括:

所述云服务器根据所述第一查询空间向量密文和所述节点的空间向量密文确定多个第一内积值;

所述云服务器在确定所述多个第一内积值均大于空间阈值时,根据所述节点的各第一孩子节点的空间向量密文和所述第一查询空间向量密文,在所述各第一孩子节点中确定出与所述第一查询空间向量密文在空间位置上相交的第二孩子节点,直至确定出与所述第一查询空间向量密文相交的所述第一节点;所述第一节点为叶子节点的父节点;

所述云服务器在确定所述多个第一内积值未均大于空间阈值时,确定所述节点的父节点下与所述第一查询空间向量密文在空间位置上相交的其他孩子节点,直至确定出与所述第一查询空间向量密文相交的所述第一节点。

4.如权利要求1所述的方法,其特征在于,所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点,包括:

针对所述第一节点下的任一叶子节点,所述云服务器根据所述第一查询混合向量密文和所述叶子节点的混合向量密文确定多个第二内积值;

所述云服务器在确定所述多个第二内积值均大于空间阈值,且所述多个第二内积值的和大于相似度阈值时,将所述叶子节点确定为所述第二节点。

5.如权利要求1至4任一项所述的方法,其特征在于,所述第一查询密文是所述用户端基于第一用户密钥加密的;

所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点之前,还包括:

所述云服务器根据所述用户端的第二用户密钥,对所述第一查询密文进行加密,确定第二查询密文;所述第二查询密文包括第二查询空间向量密文和第二查询混合向量密文;

所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点,包括:

所述云服务器根据所述第二查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点;

所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点,包括:

所述云服务器根据所述第二查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点。

6.如权利要求1所述的方法,其特征在于,所述第二节点用于作为查询结果,包括:

所述云服务器将所述第二节点对应的空间文本编号发送至边缘服务器,以指示所述边缘服务器根据所述空间文本编号查询出所述空间文本编号对应的密钥密文和空间文本密文,并根据所述空间文本编号对应的密钥密文确定所述空间文本编号对应空间文本密文的中间量;

所述云服务器将所述第二节点的空间文本密文和中间量作为所述查询结果。

7.一种空间文本的查询方法,其特征在于,包括:

用户端基于查询请求中的空间查询条件生成第一查询空间向量密文;

所述用户端基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文;

所述用户端将第一查询密文发送至云服务器;所述第一查询密文包括所述第一查询空间向量密文和所述第一查询混合向量密文;

所述用户端基于所述云服务器的查询结果,确定所述查询请求对应的明文空间文本;

其中,所述第一查询空间向量密文用于所述云服务器在密文索引树中检索出符合所述空间查询条件的第一节点;所述密文索引树是数据拥有者根据各明文空间文本构建的;所述密文索引树中的非叶子节点存储有基于明文空间文本中的空间信息生成的空间向量密文,叶子节点存储有基于明文空间文本中的空间信息和文本信息生成的混合向量密文;所述第一节点为非叶子节点;

所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文用于所述云服务器确定符合所述文本查询条件的第二节点;所述第二节点为叶子节点;所述第二节点用于作为所述查询结果。

8.如权利要求7所述的方法,其特征在于,所述空间查询条件包括指示空间范围的第一位置点和第二位置点;

用户端基于查询请求中的空间查询条件生成第一查询空间向量密文,包括:

所述用户端生成第一随机向量和第二随机向量;

所述用户端根据第一比特向量中各比特位的元素值,按照第一方式对所述第一随机向量的前K位进行与所述第一位置点相关的赋值;根据第二比特向量中各比特位的元素值,按

照第二方式对所述第一随机向量的后L位进行与第一位置点相关的赋值,得到所述第一查询空间向量密文的第一子向量密文;所述第一比特向量和所述第二比特向量是数据拥有者随机生成的;

所述用户端根据所述第一比特向量中各比特位的元素值,按照第三方式对所述第二随机向量的前K位进行与所述第二位置点相关的赋值;根据所述第二比特向量中各比特位的元素值,按照第四方式对所述第二随机向量的后L位进行与所述第二位置点相关的赋值,得到所述第一查询空间向量密文的第二子向量密文。

9.如权利要求7所述的方法,其特征在于,所述用户端基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文,包括:

所述用户端生成第三随机向量和第四随机向量;

所述用户端根据第三比特向量中各比特位的元素值,基于所述空间查询条件为所述第三随机向量的前N1位和所述第四随机向量的前N1位进行赋值;所述第三比特向量是数据拥有者随机生成的;

所述用户端根据随机选取的关键字是否位于所述文本查询条件中的查询关键字中,通过随机数为所述第三随机向量的后N2位和所述第四随机向量的后N2位进行赋值。

10.如权利要求7所述的方法,其特征在于,所述用户端基于所述云服务器的查询结果,确定所述查询请求对应的明文空间文本,包括:

所述用户端接收边缘服务器发送的空间文本密文和中间量;所述空间文本密文和中间量是边缘服务器根据所述云服务器发送的空间文本编号确定的;

所述用户端根据对所述中间量进行解密,确定所述空间文本密文的对称密钥;

所述用户端根据所述空间文本密文的对称密钥对所述空间文本密文进行解密,得到所述查询请求对应的明文空间文本。

一种空间文本的查询方法及装置

技术领域

[0001] 本发明涉及金融科技(Fintech)领域,尤其涉及一种空间文本的查询方法及装置。

背景技术

[0002] 随着计算机技术的发展,越来越多的技术(例如:区块链、云计算或大数据)应用在金融领域,传统金融业正在逐步向金融科技转变,大数据技术也不例外,但由于金融、支付行业的安全性、实时性要求,也对大数据技术中文本信息查询提出了更高的要求。

[0003] 随着基于位置的服务在移动互联网中的广泛应用,近年来基于空间(如地理位置—上海)和文本(如查询关键字—川菜)的查询服务也在工业界和学术界引起了越来越多的关注。在针对空间文本查询时,主要利用了查询请求中的文本相关度和空间距离来确定查询结果。具体的,将查询请求的文本相关度和空间距离按照预设的权重进行整合,得到查询向量,再通过得到的查询向量在预设的空间向量中确定出符合条件的查询结果。

[0004] 然而,现有技术中的方案受权重的影响,导致用户进行查询时,得到的查询结果准确率低,不尽人意。例如,查询结果的文本信息与查询请求的文本信息之间的相关度较高,但查询结果的空间地点距离查询请求的查询位置(如用户查询时的经纬度值)较远。

[0005] 因此,需要一种空间文本的查询方法,使查询结果在查询范围内,且文本信息相关度较高。

发明内容

[0006] 本发明实施例提供一种空间文本的查询方法及装置,用于提升空间文本查询的准确度,提升用户的查询体验。

[0007] 第一方面,本发明实施例提供一种空间文本的查询方法,包括:

[0008] 云服务器获取用户端发送的第一查询密文;所述第一查询密文包括第一查询空间向量密文和第一查询混合向量密文;所述第一查询空间向量密文是根据查询请求中的空间查询条件生成的;所述第一查询混合向量密文是根据所述查询请求中的文本查询条件和所述空间查询条件生成的;

[0009] 所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点;所述密文索引树是数据拥有者根据各明文空间文本构建的;所述密文索引树中的非叶子节点存储有基于明文空间文本中的空间信息生成的空间向量密文,叶子节点存储有基于明文空间文本中的空间信息和文本信息生成的混合向量密文;所述第一节点为非叶子节点;

[0010] 所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点;所述第二节点为叶子节点;所述第二节点用于作为查询结果。

[0011] 上述技术方案中,根据第一查询密文的第一查询空间信息密文可以在密文索引树中确定出在查询范围内的所有第一节点,即非叶子节点,再根据第一查询混合向量密文在

非叶子节点中确定出查询范围内所有第二节点,其中,第二节点为查询范围内的叶子节点,并确定出第一查询混合向量密文与各第二节点的相关度,进而确定出查询结果,避免了查询结果受权重的影响,且防止了查询结果与查询位置距离过远的问题,提升了空间文本查询的准确度,使查询结果在查询范围内的基础上,仅根据文本信息的相关度进行确定,提升了用户的查询体验。

[0012] 可选的,所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点,包括:

[0013] 所述云服务器根据预设检索顺序,针对所述密文索引树中的任一节点,在确定所述节点为非叶子节点时,根据所述第一查询空间向量密文和所述节点的空间向量密文确定与所述第一查询空间向量密文相交的所述第一节点。

[0014] 上述技术方案中,云服务器根据预设检索顺序进行检索,以提高检索效率,缩短确定查询结果的时间,将与第一查询空间向量密文相交非叶子节点作为第一节点,以保证第一节点与第一查询空间向量密文在空间位置上相交,防止了查询结果与查询位置距离过远的问题。

[0015] 可选的,根据所述第一查询空间向量密文和所述节点的空间向量密文确定与所述第一查询空间向量密文相交的所述第一节点,包括:

[0016] 所述云服务器根据所述第一查询空间向量密文和所述节点的空间向量密文确定多个第一内积值;

[0017] 所述云服务器在确定所述多个第一内积值均大于空间阈值时,根据所述节点的各第一孩子节点的空间向量密文和所述第一查询空间向量密文,在所述各第一孩子节点中确定出与所述第一查询空间向量密文在空间位置上相交的第二孩子节点,直至确定出与所述第一查询空间向量密文相交的所述第一节点;所述第一节点为叶子节点的父节点;

[0018] 所述云服务器在确定所述多个第一内积值未均大于空间阈值时,确定所述节点的父节点下与所述第一查询空间向量密文在空间位置上相交的其他孩子节点,直至确定出与所述第一查询空间向量密文相交的所述第一节点。

[0019] 上述技术方案中,基于密文索引树的结构,由上至下的进行检索,依次确定出与第一查询空间向量密文在空间位置上相交的叶子节点的父节点,以提高检索效率,通过具体的内积值来确定第一节点是否与第一查询空间向量密文在空间位置上相交,以增加查询结果的准确度。

[0020] 可选的,所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点,包括:

[0021] 针对所述第一节点下的任一叶子节点,所述云服务器根据所述第一查询混合向量密文和所述叶子节点的混合向量密文确定多个第二内积值;

[0022] 所述云服务器在确定所述多个第二内积值均大于空间阈值,且所述多个第二内积值的和大于相似度阈值时,将所述叶子节点确定为所述第二节点。

[0023] 上述技术方案中,与第一查询空间向量密文在空间位置上相交的第一节点中,来确定在第一查询空间向量密文内的第二节点,而不是通过所有叶子节点遍历进行确定第二节点,可以减少云服务器的计算量,提高检索效率,缩短确定查询结果的时间,因为第二节点为第一查询空间向量密文内的叶子节点,因此防止了查询结果与查询范围距离过远的问

题,提升了空间文本查询的准确度,因为确定第二节点的文本查询条件为相似度阈值,因此避免了查询结果受权重的影响,使查询结果在查询范围内的基础上,仅根据文本信息的相关度进行确定,提升了用户的查询体验。

[0024] 可选的,所述第一查询密文是所述用户端基于第一用户密钥加密的;

[0025] 所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点之前,还包括:

[0026] 所述云服务器根据所述用户端的第二用户密钥,对所述第一查询密文进行加密,确定所述第二查询密文;所述第二查询密文包括第二查询空间向量密文和第二查询混合向量密文;

[0027] 所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点,包括:

[0028] 所述云服务器根据所述第二查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点;

[0029] 所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点,包括:

[0030] 所述云服务器根据所述第二查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点。

[0031] 上述技术方案中,云服务器在获取第一查询密文之后,再次进行加密,得到第二查询密文,以实现多用户均可以与云服务器交互进行查询的场景。

[0032] 可选的,所述第二节点用于作为查询结果,包括:

[0033] 所述云服务器将所述第二节点对应的空间文本编号发送至边缘服务器,以指示所述边缘服务器根据所述空间文本编号查询出所述空间文本编号对应的密钥密文和空间文本密文,并根据所述空间文本编号对应的密钥密文确定所述空间文本编号对应空间文本密文的中间量;

[0034] 所述云服务器将所述第二节点的空间文本密文和中间量作为所述查询结果。

[0035] 上述技术方案中,中间量是边缘服务器根据边缘私钥和边缘服务器存储的密钥密文进行计算得到的,边缘私钥是可信第三方系统发送至边缘服务器的,用户端根据用户私钥对中间量进行解密,得到对称密钥,再根据对称密钥对空间文本密文进行解密,得到明文。以此通过将空间文本编号发送至边缘服务器,以指示边缘服务器进行辅助计算,以减少用户端的计算量,实现用户端轻量级的计算,减少用户端的资源消耗。

[0036] 第二方面,本发明实施例提供一种空间文本的查询方法,包括:

[0037] 用户端基于查询请求中的空间查询条件生成第一查询空间向量密文;

[0038] 所述用户端基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文;

[0039] 所述用户端将第一查询密文发送至云服务器;所述第一查询密文包括所述第一查询空间向量密文和所述第一查询混合向量密文;

[0040] 所述用户端基于所述云服务器的查询结果,确定所述查询请求对应的明文空间文本。

[0041] 上述技术方案中,用户端对查询请求进行加密,以防止明文形式的查询请求泄露。

[0042] 因为第一查询密文包括第一查询空间向量密文和第一查询混合向量密文,以使云服务器在确定查询结果时,避免查询结果受权重的影响,防止查询结果与查询位置距离过远的问题。

[0043] 可选的,所述空间查询条件包括指示空间范围的第一位置点和第二位置点;

[0044] 用户端基于查询请求中的空间查询条件生成第一查询空间向量密文,包括:

[0045] 所述用户端生成第一随机向量和第二随机向量;

[0046] 所述用户端根据第一比特向量中各比特位的元素值,按照第一方式对所述第一随机向量的前K位进行与所述第一位置点相关的赋值;根据第二比特向量中各比特位的元素值,按照第二方式对所述第一随机向量的后L位进行与第一位置点相关的赋值,得到所述第一查询空间向量密文的第一子向量密文;所述第一比特向量和所述第二比特向量是数据拥有者随机生成的;

[0047] 所述用户端根据所述第一比特向量中各比特位的元素值,按照第三方式对所述第二随机向量的前K位进行与所述第二位置点相关的赋值;根据所述第二比特向量中各比特位的元素值,按照第四方式对所述第二随机向量的后L位进行与所述第二位置点相关的赋值,得到所述第一查询空间向量密文的第二子向量密文。

[0048] 上述技术方案中,根据第一位置点和第二置位点,以确定出查询空间范围,从而使云服务器确定出在空间范围内的第二节点,使查询结果在查询范围内的基础上,仅根据文本信息的相关度进行确定,提升了用户的查询体验。

[0049] 可选的,所述用户端基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文,包括:

[0050] 所述用户端生成第三随机向量和第四随机向量;

[0051] 所述用户端根据第三比特向量中各比特位的元素值,基于所述空间查询条件为所述第三随机向量的前N1位和所述第四随机向量的前N1位进行赋值;所述第三比特向量是数据拥有者随机生成的;

[0052] 所述用户端根据随机选取的关键字是否位于所述文本查询条件中的查询关键字中,通过随机数为所述第三随机向量的后N2位和所述第四随机向量的后N2位进行赋值。

[0053] 上述技术方案中,第一查询混合向量密文中包括文本查询条件信息,从而使云服务器确定查询结果时,根据文本信息的相关度进行确定,提升了空间文本查询的准确度。

[0054] 可选的,所述用户端基于所述云服务器的查询结果,确定所述查询请求对应的明文空间文本,包括:

[0055] 所述用户端接收边缘服务器发送的空间文本密文和中间量;所述空间文本密文和中间量是边缘服务器根据所述云服务器发送的空间文本编号确定的;

[0056] 所述用户端根据对所述中间量进行解密,确定所述空间文本密文的对称密钥;

[0057] 所述用户端根据所述空间文本密文的对称密钥对所述空间文本密文进行解密,得到所述查询请求对应的明文空间文本。

[0058] 上述技术方案中,用户端对查询结果进行解密所需要的中间量是边缘服务器计算的,以此减少了用户端的计算量,实现用户端轻量级的计算,减少了用户端的资源消耗。

[0059] 第三方面,本发明实施例提供一种空间文本的查询装置,包括:

[0060] 获取模块,用于获取用户端发送的第一查询密文;所述第一查询密文包括第一查

询空间向量密文和第一查询混合向量密文;所述第一查询空间向量密文是根据查询请求中的空间查询条件生成的;所述第一查询混合向量密文是根据所述查询请求中的文本查询条件和所述空间查询条件生成的;

[0061] 处理模块,用于根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点;所述密文索引树是数据拥有者根据各明文空间文本构建的;所述密文索引树中的非叶子节点存储有基于明文空间文本中的空间信息生成的空间向量密文,叶子节点存储有基于明文空间文本中的空间信息和文本信息生成的混合向量密文;所述第一节点为非叶子节点;

[0062] 根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点;所述第二节点为叶子节点;所述第二节点用于作为查询结果。

[0063] 可选的,所述处理模块具体用于:

[0064] 根据预设检索顺序,针对所述密文索引树中的任一节点,在确定所述节点为非叶子节点时,根据所述第一查询空间向量密文和所述节点的空间向量密文确定与所述第一查询空间向量密文相交的所述第一节点。

[0065] 可选的,所述处理模块具体用于:

[0066] 根据所述第一查询空间向量密文和所述节点的空间向量密文确定多个第一内积值;

[0067] 在确定所述多个第一内积值均大于空间阈值时,根据所述节点的各第一孩子节点的空间向量密文和所述第一查询空间向量密文,在所述各第一孩子节点中确定出与所述第一查询空间向量密文在空间位置上相交的第二孩子节点,直至确定出与所述第一查询空间向量密文相交的所述第一节点;所述第一节点为叶子节点的父节点;

[0068] 在确定所述多个第一内积值未均大于空间阈值时,确定所述节点的父节点下与所述第一查询空间向量密文在空间位置上相交的其他孩子节点,直至确定出与所述第一查询空间向量密文相交的所述第一节点。

[0069] 可选的,所述处理模块具体用于:

[0070] 针对所述第一节点下的任一叶子节点,根据所述第一查询混合向量密文和所述叶子节点的混合向量密文确定多个第二内积值;

[0071] 在确定所述多个第二内积值均大于空间阈值,且所述多个第二内积值的和大于相似度阈值时,将所述叶子节点确定为所述第二节点。

[0072] 可选的,所述第一查询密文是所述用户端基于第一用户密钥加密的;

[0073] 所述处理模块还用于:

[0074] 根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点之前,根据所述用户端的第二用户密钥,对所述第一查询密文进行加密,确定所述第二查询密文;所述第二查询密文包括第二查询空间向量密文和第二查询混合向量密文;

[0075] 所述处理模块具体用于:

[0076] 根据所述第二查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点;

[0077] 根据所述第二查询混合向量密文和所述第一节点下的叶子节点的混合向量密文，确定符合所述文本查询条件的第二节点。

[0078] 可选的，所述处理模块具体用于：

[0079] 将所述第二节点对应的空间文本编号发送至边缘服务器，以指示所述边缘服务器根据所述空间文本编号查询出所述空间文本编号对应的密钥密文和空间文本密文，并根据所述空间文本编号对应的密钥密文确定所述空间文本编号对应空间文本密文的中间量；

[0080] 将所述第二节点的空间文本密文和中间量作为所述查询结果。

[0081] 第四方面，本发明实施例提供一种空间文本的查询装置，包括：

[0082] 生成单元，用于基于查询请求中的空间查询条件生成第一查询空间向量密文；

[0083] 基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文；

[0084] 发送单元，用于将第一查询密文发送至云服务器；所述第一查询密文包括所述第一查询空间向量密文和所述第一查询混合向量密文；

[0085] 解密单元，用于基于所述云服务器的查询结果，确定所述查询请求对应的明文空间文本。

[0086] 可选的，所述空间查询条件包括指示空间范围的第一位置点和第二位置点；

[0087] 所述生成单元具体用于：

[0088] 生成第一随机向量和第二随机向量；

[0089] 根据第一比特向量中各比特位的元素值，按照第一方式对所述第一随机向量的前K位进行与所述第一位置点相关的赋值；根据第二比特向量中各比特位的元素值，按照第二方式对所述第一随机向量的后L位进行与第一位置点相关的赋值，得到所述第一查询空间向量密文的第一子向量密文；所述第一比特向量和所述第二比特向量是数据拥有者随机生成的；

[0090] 根据所述第一比特向量中各比特位的元素值，按照第三方式对所述第二随机向量的前K位进行与所述第二位置点相关的赋值；根据所述第二比特向量中各比特位的元素值，按照第四方式对所述第二随机向量的后L位进行与所述第二位置点相关的赋值，得到所述第一查询空间向量密文的第二子向量密文。

[0091] 可选的，所述生成单元具体用于：

[0092] 生成第三随机向量和第四随机向量；

[0093] 根据第三比特向量中各比特位的元素值，基于所述空间查询条件为所述第三随机向量的前N1位和所述第四随机向量的前N1位进行赋值；所述第三比特向量是数据拥有者随机生成的；

[0094] 根据随机选取的关键字是否位于所述文本查询条件中的查询关键字中，通过随机数为所述第三随机向量的后N2位和所述第四随机向量的后N2位进行赋值。

[0095] 可选的，所述解密单元具体用于：

[0096] 接收边缘服务器发送的空间文本密文和中间量；所述空间文本密文和中间量是边缘服务器根据所述云服务器发送的空间文本编号确定的；

[0097] 根据对所述中间量进行解密，确定所述空间文本密文的对称密钥；

[0098] 根据所述空间文本密文的对称密钥对所述空间文本密文进行解密，得到所述查询

请求对应的明文空间文本。

[0099] 第五方面,本发明实施例还提供一种计算机设备,包括:

[0100] 存储器,用于存储程序指令;

[0101] 处理器,用于调用所述存储器中存储的程序指令,按照获得的程序执行上述空间文本的查询方法。

[0102] 第六方面,本发明实施例还提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机可执行指令,所述计算机可执行指令用于使计算机执行上述空间文本的查询方法。

附图说明

[0103] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简要介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域的普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0104] 图1为本发明实施例提供的一种系统架构示意图;

[0105] 图2为本发明实施例提供的一种空间文本的查询方法的流程示意图;

[0106] 图3为本发明实施例提供的一种密文索引树的示意图;

[0107] 图4为本发明实施例提供的一种用户端针对空间文本的查询方法的流程示意图;

[0108] 图5为本发明实施例提供的一种待查询的空间范围的示意图;

[0109] 图6为本发明实施例提供的一种空间文本的查询方法的示意图;

[0110] 图7为本发明实施例提供的一种空间文本的查询装置的结构示意图;

[0111] 图8为本发明实施例提供的一种空间文本的查询装置的结构示意图。

具体实施方式

[0112] 为了使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明作进一步地详细描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

[0113] 在现有技术中,空间关键字的查询方法一般是针对查询位置进行查询,例如,用户A在某一具体位置发起了查询请求,则该位置为查询请求的查询位置,该查询位置一般为经纬度坐标值,即查询点。

[0114] 针对于查询点查询时,需要确定出该查询点与预先根据明文空间文本数据构建的索引树中各最小外包矩形的最小空间距离,然后再根据各最小外包矩形中存在的空间文本对应的关键字和查询请求的关键字,确定出各空间文本与查询请求的关键字相似度。最后根据预设权重、空间距离和关键字相似度确定出查询值,根据查询值的大小确定查询结果,例如,将最大查询值对应的空间文本(相当于索引树中的叶子节点)作为查询结果。其中,索引树是数据拥有者根据明文空间文本进行构建的,最小外包矩形为非叶子节点的空间范围。

[0115] 但上述方法存在的问题是,查询值与预设权重相关,例如,对空间距离所预设的权

重较小,对关键字相似度所预设的权重较大时,则查询结果易出现与查询请求中的关键字相似的节点,但该节点与该查询请求的查询位置距离较远。或者在对空间距离所预设的权重较大,对关键字相似度所预设的权重较小时,则查询结果易出现与该查询请求的查询位置距离相近,但查询结果与查询请求中的关键字不相似,从而导致查询结果准确度低,影响了用户的查询体验。

[0116] 且在目前的方法中,在对查询结果进行解密时,由用户端根据用户私钥对密钥密文进行解密得到对称密钥,从而对查询结果进行解密,因此对用户端也造成了资源开销大的问题。

[0117] 因此,现需要一种空间关键字的查询方法,针对于查询范围的查询请求,仅根据查询关键字的相似度来确定查询范围内的节点,以提升查询结果的准确度,并引入边缘服务器,用于在构建索引树和用户端对查询结果进行解密时进行辅助计算,以实现轻量级的计算,减少用户端的资源消耗。

[0118] 图1示例性的示出了本发明实施例所适用的一种系统架构,该系统架构包括可信第三方系统110、数据拥有者120、边缘服务器130、云服务器140和用户端150。

[0119] 其中,可信第三方系统110用于生成用户私钥、边缘私钥和密钥,用户私钥是根据用户的唯一标识信息确定的,用户的唯一标识信息如IP地址、网络账号、身份信息等。边缘私钥用于计算出空间文本密文的中间量。密钥用于用户端150和云服务器140对查询指令进行加密。

[0120] 数据拥有者120,用于根据用户端150的数量生成对应数量的对称密钥,利用对称密钥对明文空间文本进行加密,得到空间文本密文集,还根据文空间文本构建明文索引树,并对其加密,得到初始密文索引树。

[0121] 边缘服务器130,用于对访问结构进行加密,进而相当于对数据拥有者120生成的对称密钥进行加密,得到临时对称密钥密文,以减少数据拥有者的计算量。

[0122] 需要说明的是,图1中给出的两个边缘服务器130可以为同一个也可以为两个不同的边缘服务器,在此不做具体限定。

[0123] 云服务器140,用于对数据拥有者120加密的初始密文索引树进行加密,得到最终的密文索引树,还用于针对用户端150发送的第一查询密文进行加密,得到第二查询密文,进一步根据第二查询密文得到查询结果,并将查询结果发送至用户端150。

[0124] 用户端150,用于生成第一查询密文,并在接收到查询结果之后,解密出明文数据。

[0125] 需要说明的是,上述图1所示的结构仅是一种示例,本发明实施例对此不做限定。

[0126] 基于上述描述,图2示例性的示出了本发明实施例提供的一种空间文本的查询方法的流程示意图,该流程可由空间文本的查询装置执行。

[0127] 如图2所示,该流程具体包括:

[0128] 步骤210,云服务器获取用户端发送的第一查询密文。

[0129] 本发明实施例中,第一查询密文包括第一查询空间向量密文和第一查询混合向量密文,第一查询空间向量密文是根据查询请求中的空间查询条件生成的,第一查询混合向量密文是根据查询请求中的文本查询条件和空间查询条件生成的。

[0130] 其中,第一查询空间向量指示了查询请求中待查询的空间范围,第一查询混合向量密文不仅包括了查询请求中待查询的空间范围,还包括了查询请求中的关键字,用于确

定各叶子节点与查询请求中关键字的相似度。

[0131] 在一种可实施的方式中,查询请求中的待查询的空间范围可以根据用户的查询位置生成,如以用户查询位置的经纬度值为中心生成的正方形为待查询的空间范围。

[0132] 在另一种可实施的方式中,待查询的空间范围是由用户直接输入的两个空间位置形成的矩形范围。

[0133] 步骤220,所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点。

[0134] 本发明实施例中,密文索引树是数据拥有者根据各明文空间文本构建的,密文索引树中的非叶子节点存储有基于明文空间文本中的空间信息生成的空间向量密文,叶子节点存储有基于明文空间文本中的空间信息和文本信息生成的混合向量密文,第一节点为非叶子节点。

[0135] 其中,密文索引树是加密后的明文索引树,明文索引树是数据拥有者以各明文空间文本为叶子节点构建的,在明文索引树中,除叶子节点外,均是非叶子节点,非叶子节点存在空间范围,即空间信息,进而生成空间向量密文,空间向量密文可以表示非叶子节点存在的空间范围,同理,叶子节点相当于位置信息,即空间点,与文本信息生成的混合向量密文可以表示叶子节点所在的空间位置及文本信息。

[0136] 进一步地,第一查询空间向量密文可以表示查询请求中待查询的空间范围,非叶子节点的空间向量密文可以表示非叶子节点存在的空间范围,因此,通过向量之间的计算可以确定出与第一查询空间向量密文在空间位置上相交的非叶子节点,即第一节点。

[0137] 步骤230,所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文,确定符合所述文本查询条件的第二节点。

[0138] 本发明实施例中,第二节点为叶子节点,第二节点用于作为查询结果。根据上述混合向量密文所知,每个叶子节点均存在混合向量密文,包括空间信息和文本信息,而第一查询混合向量密文中包括了查询请求中的关键字信息和查询空间范围,进而通过叶子节点的空间信息和查询范围确定出在查询请求的空间范围内的叶子节点,并确定出各叶子节点与查询请求之间的相似度。

[0139] 进一步地,在步骤220中,云服务器根据第一查询空间向量密文在密文索引树中检索出符合空间查询条件的第一节点之前,还会对第一查询密文进行加密,实现多用户与云服务器进行交互查询的应用场景。具体的,云服务器根据用户端的第二用户密钥,对第一查询密文进行加密,确定第二查询密文,其中,第二查询密文包括第二查询空间向量密文和第二查询混合向量密文。

[0140] 举例来说,可信第三方系统针对用户端生成了第二用户密钥$K_{EN,2}$,并发送给了云服务器,云服务器在接收到第一查询密文$Eq=\{q_{l,1},q_{l,2},q_{r,1},q_{r,2},b_{l,1},b_{l,2},b_{r,1},b_{r,2}\}$之后,根据第二用户密钥$K_{EN,2}$对第一查询密文Eq进行加密得到第二查询密文$Eq^*=\{q^*_{l,1},q^*_{l,2},q^*_{r,1},q^*_{r,2},b^*_{l,1},b^*_{l,2},b^*_{r,1},b^*_{r,2}\}$。

[0141] 需要说明的是,可信第三方系统是针对用户端生成的第二用户密钥,相当于各用户端的第二用户密钥是不同的。

[0142] 在步骤220中,云服务器根据第二查询空间向量密文在密文索引树中检索出符合空间查询条件的第一节点。

[0143] 在步骤230中,云服务器根据第二查询混合向量密文和第一节点下的叶子节点的混合向量密文,确定符合文本查询条件的第二节点。

[0144] 需要说明的是,第二查询密文仅是加密后的第一查询密文,并不会改变第一查询密文的空间信息和文本信息。

[0145] 在步骤220中,一种可实施的方式可以包括,云服务器根据随机的方式来对索引树中的节点进行判断是否为非叶子节点。

[0146] 又一种可实施的方式包括,云服务器根据预设检索顺序,针对密文索引树中的任一节点,在确定节点为非叶子节点时,根据第一查询空间向量密文和节点的空间向量密文确定与第一查询空间向量密文相交的第一节点。

[0147] 其中,预设检索顺序可以为由密文索引树中的叶子节点至根节点,在本发明实施例中,预设检索顺序为由密文索引树中的根节点至叶子节点进行判断。以图3进行举例,图3示例性的示出了一种密文索引树的示意图,由根据R1进行判断,确定R1是否为非叶子节点。

[0148] 在确定节点为非叶子节点后,确定与第一查询空间向量密文相交的第一节点,具体的,云服务器根据第一查询空间向量密文和节点的空间向量密文确定多个第一内积值;在确定多个第一内积值均大于空间阈值时,根据节点的各第一孩子节点的空间向量密文和第一查询空间向量密文,在各第一孩子节点中确定出与第一查询空间向量密文在空间位置上相交的第二孩子节点,直至确定出与第一查询空间向量密文相交的第一节点,其中,第一节点为叶子节点的父节点。

[0149] 云服务器在确定多个第一内积值未均大于空间阈值时,确定节点的父节点下与第一查询空间向量密文在空间位置上相交的其他孩子节点,直至确定出与第一查询空间向量密文相交的第一节点。

[0150] 结合以上描述的内容举例来说,云服务器在得到第一查询空间向量密文之后,云服务器根据第二用户密钥$K_{EN,2}$对第一查询空间向量密文进行加密,得到第二查询密文$Eq^*=\{q^*_{l,1},q^*_{l,2},q^*_{r,1},q^*_{r,2},b^*_{l,1},b^*_{l,2},b^*_{r,1},b^*_{r,2}\}$,其中,第二查询密文的第二查询空间向量密文为$q^*=\{b^*_{l,1},b^*_{l,2},b^*_{r,1},b^*_{r,2}\}$,节点的空间向量密文为$d_{R1}^*=\{d^*_{l,1},d^*_{l,2},d^*_{r,1},d^*_{r,2}\}$,因此,得到四个内积值为$in_1=b^*_{l,1}\times d^*_{l,1}$,$in_2=b^*_{l,2}\times d^*_{l,2}$,$in_3=b^*_{r,1}\times d^*_{r,1}$,$in_4=b^*_{r,2}\times d^*_{r,2}$。

[0151] 然后在确定四个表示空间信息的内积值(in_1,in_2,in_3,in_4)均大于0(空间阈值)时,确定根节点R1与第二查询空间向量密文在空间位置上相交。

[0152] 然后再确定根节点R1下的孩子节点(R2和R3),以R2为例,根据上述内计算法,在确定节点R2的四个内积值均大于0时,因为R2为叶子节点(R4和R5)的父节点,以此,节点R2为第一节点。

[0153] 若确定节点R2不满足上述条件,即节点R2的四个内积值中,有一个、两个、三个或四个内积值不大于0时,确定节点R2与第二查询空间向量密文在空间位置上不相交,此时,返回节点R2父节点,即节点R1,再次确定节点R1下的其他孩子节点(R3)是否满足上述条件,以此类推,确定出所有满足条件的节点,作为第一节点。

[0154] 在一种可实施的方式中,在确定出与第二查询空间向量密文在空间位置上相交的非叶子节点之后,根据上述非叶子节点下的叶子节点的混合向量密文和第二查询混合向量密文直接确定出上述非叶子节点下的各叶子节点与查询请求的相似度。

[0155] 在另一种可实施的方式中,即本发明实施例步骤230中,在确定出与第二查询空间向量密文在空间位置上相交的非叶子节点之后,首先需要先确定出在第二查询空间向量密文范围内的叶子节点,再确定出满足条件的叶子节点与查询请求的相似度。

[0156] 在一种可实现的方式中,根据相似度的大小对满足条件的叶子节点进行排序,将排序前N名的叶子节点作为第二节点,其中N是人为预设的数,如5、10等。

[0157] 在另一种可实施的方式中,针对第一节点下的任一叶子节点,云服务器根据第一查询混合向量密文和叶子节点的混合向量密文确定多个第二内积值,在确定所述多个第二内积值均大于空间阈值,且多个第二内积值的和大于相似度阈值时,将叶子节点确定为第二节点。

[0158] 本发明实施例中,云服务器根据第一查询密文先加密生成了第二查询密文,然后根据第二查询密文的第二查询混合向量密文和叶子节点的混合向量密文确定第二节点。

[0159] 结合上述例子,举例说明,第二查询密文$Eq^*=\{q^*_{l,1},q^*_{l,2},q^*_{r,1},q^*_{r,2},b^*_{l,1},b^*_{l,2},b^*_{r,1},b^*_{r,2}\}$,其中,第二查询密文的第二查询混合向量密文为$q^*=\{q^*_{l,1},q^*_{l,2},q^*_{r,1},q^*_{r,2}\}$,叶子节点的混合向量密文为$p_{R7}^*=\{p^*_1,p^*_2\}$,然后确定出四个表示空间信息和文本信息的内积值,$in^*_1=p^*_1\times q^*_{l,1}$,$in^*_2=p^*_2\times q^*_{l,2}$,$in^*_3=p^*_1\times q^*_{r,1}$,$in^*_4=p^*_2\times q^*_{r,2}$。

[0160] 在确定四个表示空间信息的内积值($in^*_1,in^*_2,in^*_3,in^*_4$)均大于0(空间阈值)时,确定叶子节点R7在空间位置上,在第二查询空间向量密文内。此时,将叶子节点R7作为满足条件的节点。

[0161] 若某一叶子节点内积值($in^*_1,in^*_2,in^*_3,in^*_4$)中存在不大于0的内积值时,则表示该叶子节点不在第二查询空间向量密文内,即该叶子节点为不满足条件的节点。

[0162] 在满足的叶子节点中,确定出各满足条件的叶子节点的相似度值,在一种可实施的方式中,根据满足条件的叶子节点预设权重确定相似度值。

[0163] 在另一种可实施的方式中,根据满足条件的叶子节点的内积值确定其相似度值,例如,将内积值($in^*_1,in^*_2,in^*_3,in^*_4$)的和作为叶子节点相似度值,然后将相似度值大于s(相似度阈值)在满足条件的叶子节点中确定出第二节点。其中,s可以是人为根据经验预设的值,如6、7等。

[0164] 需要说明的是,在一种可实施的方式中,云服务器在获取用户端发送的第一查询密文之后,对用户端进行验证,根据预设的访问结构验证其是否属于已授权用户,若用户端为未授权的用户,则不允许用户端进行查询操作,其中,访问结构可以是用户在数据拥有者、边缘服务器或云服务器预设的。

[0165] 在另一种可实施的方式中,预设的访问结构针对于单个明文空间文本,即叶子节点。相当于在确定出第二节点之后,判断第二节点是否授权于用户端,即各第二节点对不同用户端进行了授权,以增加验证方法的灵活性,明文空间文本的安全性。

[0166] 例如,数据拥有者针对第二节点A仅对用户端A进行了授权,数据拥有者针对第二节点B仅对用户端B进行了授权,若在用户端B发起的查询请求时,查询的第二节点包括第二节点A,但在将第二节点A作为用户端B发起的查询请求对应的查询结果之前,确定数据拥有者针对第二节点A未对用户端B进行授权,则第二节点A不可作为查询结果。

[0167] 在本发明实施例中,查询结果包括第二节点的空间文本密文和中间量,其中密钥密文和空间文本密文是云服务器查询的,中间量是边缘服务器计算的。

[0168] 具体的,云服务器将第二节点对应的空间文本编号发送至边缘服务器,以指示边缘服务器根据空间文本编号查询出空间文本编号对应的密钥密文和空间文本密文,并根据空间文本编号对应的密钥密文确定空间文本编号对应空间文本密文的中间量,云服务器将第二节点的空间文本密文和中间量作为查询结果。

[0169] 为了更好的解释上述技术方案中第一查询密文的由来,以及查询结果的用法,图4示例性的示出了一种用户端针对空间文本的查询方法的流程示意图,如图4所示,具体流程包括:

[0170] 步骤410,用户端基于查询请求中的空间查询条件生成第一查询空间向量密文。

[0171] 本发明实施例中,查询请求包括待查询的空间范围及关键字,例如空间范围是由两个位置点确定的矩形范围,两个位置点包括经纬度信息。

[0172] 具体的,所述用户端生成第一随机向量和第二随机向量;

[0173] 用户端根据第一比特向量中各比特位的元素值,按照第一方式对第一随机向量的前K位进行与第一位置点相关的赋值,再根据第二比特向量中各比特位的元素值,按照第二方式对第一随机向量的后L位进行与第一位置点相关的赋值,得到第一查询空间向量密文的第一子向量密文,其中,第一比特向量和第二比特向量是数据拥有者随机生成的。

[0174] 然后根据第一比特向量中各比特位的元素值,按照第三方式对第二随机向量的前K位进行与所述第二位置点相关的赋值,再根据第二比特向量中各比特位的元素值,按照第四方式对第二随机向量的后L位进行与第二位置点相关的赋值,得到第一查询空间向量密文的第二子向量密文。

[0175] 其中,第一方式和第二方式的区别在于比特位的元素值是否为预设值,若是则执行第一方式,否则执行第二方式。

[0176] 举例来说,图5示例性的示出了一种待查询的空间范围的示意图,例如,在图5所示的空间范围中,位置点1(即第一位置点或第二位置点)和位置点2包括经、纬度值,其中,针对不同的位置点,使用不同的编码算法得到向量密文,例如针对左下角的位置点1使用第一编码算法,针对右上角的位置点2使用第二编码算法。

[0177] 以位置点1的经度值或纬度值为例,第一编码算法为:生成预设维数(K+L)的随机向量,在第一比特向量中任意选取一个未选取过的第t_{l1}个元素值t_{i1},在确定元素值t_{i1}为0时,将1(预设值)赋予在随机向量对应位置上,在确定元素值t_{i1}不为0时,将位置点1的经度值或纬度值g1赋予在随机向量对应位置上。例如随机向量是4维的随机向量{K1,K2,L1,L2},在$t_{l1}=1$,且$t_{i1}=0$时,随机向量变为{1,K2,L1,L2}。在$t_{l1}=1$,且$t_{i1}\neq0$时,随机向量变为{g1,K2,L1,L2}。其中,t_{l1}的取值范围为{1,……,K+L/2}。

[0178] 然后随机确定出(K+L/4)个随机数,其中,(K+L/4)个随机数的和大于0。然后在第二比特向量中任意选取一个未选取过的第t_{l2}个元素值t_{i2},在确定元素值t_{i2}为0时,将第1个随机数yi_1的值赋予在随机向量对应位置上,在确定元素值t_{i2}不为0时,将第1个随机数与位置点1的经度值或纬度值g1的积赋予在随机向量对应位置上。其中,t_{l2}的取值范围为{1,……,K+L/2},t_{l2}在随机向量对应的位置为$K+L/2+t_{l2}$。例如,随机向量为{K1,K2,L1,L2},在$t_{l2}=1$,且$t_{i2}=0$时,随机向量变为{K1,K2,yi_1,L2}。在$t_{l2}=1$,且$t_{i2}\neq0$时,随机向量变为{g1,K2,($yi_1\times g1$),L2}。以此类推,在选取一个未选取过的第$t_{l2}+1$个元素值t_{i2+1},时根据第2个随机数进行赋值,以此得到具体的随机向量。

[0179] 以位置点2的经度值或纬度值为例,第二编码算法为:随机确定出(K+L/4)个随机数,其中,(K+L/4)个随机数的和大于0。然后在第一比特向量中任意选取一个未选取过的第t_{r1}个元素值t_{j1},在确定元素值t_{j1}为0时,将第1个随机数yi_2与位置点2的经度值或纬度值g2的积赋予在随机向量对应位置上,在确定元素值t_{j1}不为0时,将第1个随机数yi_2的相反数赋予在随机向量对应位置上。其中,t_{r1}的取值范围为{1,……,K+L/2}例如,随机向量为{K1,K2,L1,L2},在$t_{r1}=1$,且$t_{j1}=0$时,随机向量变为{($yi_2\times g2$),K2,L1,L2}。在$t_{r1}=1$,且$t_{j1}\neq 0$时,随机向量变为{$-yi_2$,K2,L1,L2}。

[0180] 然后在第二比特向量中任意选取一个未选取过的第t_{r2}个元素值t_{j2},在确定元素值t_{j2}为0时,将g2赋予在随机向量对应位置上,在确定元素值t_{j2}不为0时,将-1赋予在随机向量对应位置上。例如随机向量为{K1,K2,L1,L2},在$t_{r2}=1$,且$t_{j2}=0$时,随机向量变为{1,K2,g2,L2}。在$t_{r2}=1$,且$t_i\neq 0$时,随机向量变为{g1,K2,-1,L2}。其中,t_{r2}的取值范围为{1,……,K+L/2},t_{r2}在随机向量对应的位置为$K+L/2+t_{r2}$。

[0181] 步骤420,所述用户端基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文。

[0182] 本发明实施例中,第一查询混合向量密文中包括了查询请求的查询位置信息和文本信息,其中,文本信息为关键字信息,关键字可以为多个。例如查询川菜和火锅,其中川菜和火锅为两个关键字。

[0183] 具体的,用户端生成第三随机向量和第四随机向量;

[0184] 用户端根据第三比特向量中各比特位的元素值,基于空间查询条件为第三随机向量的前N1位和第四随机向量的前N1位进行赋值,然后根据随机选取的关键字是否位于文本查询条件中的查询关键字中,通过随机数为第三随机向量的后N2位和第四随机向量的后N2位进行赋值,其中,第三比特向量是数据拥有者随机生成的。

[0185] 结合上述图5举例来说,将位置点1和位置点2的经度值作为两个随机数v1和v2。然后根据第三随机向量或第四随机向量的维数确定出多个随机数,如第三随机向量的维数为N1+N2,则生成N1/2个随机数,且保证N1/2个随机数的和大于或等于空间文本数据到矩形查询范围(位置点1和位置点2形成的矩形)的最小距离MD,以反映范围条件和相似度值。其中,第三随机向量的维数和第四随机向量的维数相同。

[0186] 然后在第三比特向量s`中任意选取一个未选取过的第t_{w1}个元素值t_{b1},在确定元素值t_{b1}为1时,将第1个随机数wb1赋予在第三随机向量对应位置上,将第1个随机数的相反数赋予在第四随机向量对应位置上。在确定元素值t_{b1}不为0时,第1个随机数wb1分别与-v1和v2相乘,将对应的积赋予在第三随机向量和第四随机向量对应位置上。

[0187] 例如第三随机向量为{N1a,N1b,N2a,N2b},第四随机向量为{N1`a,N1`b,N2`a,N2`b},在$t_{w1}=1$,且$t_{b1}=1$时,第三随机向量变为{wb1,N1b,N2a,N2b},第四随机向量为{-wb1,N1`b,N2`a,N2`b}。在$t_{w1}=1$,且$t_{b1}\neq 1$时,第三随机向量变为{$wb1\times -v1$,N1b,N2a,N2b},第四随机向量为{$wb1\times v2$,N1`b,N2`a,N2`b}。其中,t_{w1}的取值范围为{1,……,N1}。

[0188] 然后再从关键字中(针对密文索引树中的所有关键字)随机选取一个未选过的第t_{w2}个关键字t_{b2},确定关键字t_{b2}是否存在于查询关键字中,若是,则随机选一个随机数sj1,将sj1赋予在第三随机向量对应位置上,将1与sj1的差值赋予在第四随机向量对应位置上。否则随机选一个随机数sj2,将sj2赋予在第三随机向量对应位置上,将0与sj2的差值赋予

在第四随机向量对应位置上。

[0189] 例如,在$t_{w2}=1$,且关键字t_{b2}存在于预设的查询关键字中时,第三随机向量为{N1a,N1b,sj1,N2b},第四随机向量为{N1`a,N1`b,1-sj1,N2`b}。在$t_{w2}=1$,且关键字$t_{b2}$不存在于预设的查询关键字中时,第三随机向量为{N1a,N1b,sj2,N2b},第四随机向量为{N1`a,N1`b,0-sj2,N2`b}。其中,t_{w2}的取值范围为{1,……,N2}。t_{w2}在随机向量对应的位置为$N1+t_{w2}$。

[0190] 需要说明的是,在确定第一查询密文之前,用户端可以先将查询请求中空间查询条件的第一位置点和第二位置点的经、纬度增加,相当于在查询请求的空间范围基础上,扩大预设经、纬度,得到扩大后的空间范围。

[0191] 步骤430,所述用户端将第一查询密文发送至云服务器;所述第一查询密文包括所述第一查询空间向量密文和所述第一查询混合向量密文。

[0192] 本发明实施例中,用户端在根据查询请求得到第一查询空间向量密文和第一查询混合向量密文之后,根据第三方可信系统针对用户端生成的第一用户密钥对第一查询空间向量密文和第一查询混合向量密文进行加密,进而得到第一查询密文。

[0193] 举例来说,可信第三方系统针对用户端生成了第一用户密钥$K_{EN,1}$,并发送给用户端,用户端在生成第一查询空间向量密文$E`b=\{b`_{1,1},b`_{1,2},b`_{r,1},b`_{r,2}\}$和第一查询混合向量密文$E`q=\{q`_{1,1},q`_{1,2},q`_{r,1},q`_{r,2}\}$之后,使用第一用户密钥$K_{EN,1}$第一查询空间向量密文E`b和第一查询混合向量密文E`q进行加密,得到第一查询密文$Eq=\{q_{1,1},q_{1,2},q_{r,1},q_{r,2},b_{1,1},b_{1,2},b_{r,1},b_{r,2}\}$。

[0194] 需要说明的是,可信第三方系统是针对用户端生成的第一用户密钥,相当于各用户端的第一用户密钥是不同的。

[0195] 步骤440,所述用户端基于所述云服务器的查询结果,确定所述查询请求对应的明文空间文本。

[0196] 本发明实施例中,云服务器的查询结果包括空间文本密文和中间量,用户端根据查询结果得到空间文本密文对应的明文。

[0197] 具体的,用户端接收边缘服务器发送的空间文本密文和中间量,再根据自身的用户私钥对中间量进行解密,确定出空间文本密文的对称密钥,最后根据对称密钥对空间文本密文进行解密,得到查询请求对应的明文空间文本。因为在现有技术中,是用户端根据用户私钥直接对密文密钥进行解密得到对称密钥的,导致用户端的计算量较大,过多的消耗计算资源,通过引入边缘服务器,由边缘服务器在保证安全性的基础上,将确定对称密钥的过程分为两步,第一步是边缘服务器根据密钥密文和边缘私钥确定中间量,第二步是用户端根据中间量和用户私钥确定对称密钥,因为其中一步是边缘服务器计算的,以此减少用户端的计算量,降低用户端的计算资源,使用户端实现轻量级的查询。

[0198] 其中,中间量是边缘服务器根据边缘私钥得到的,用户私钥和边缘私钥是可信第三方系统生成的,例如,可信第三方系统生成公共参数$pp=(G,G_T,e,p,g,g_0,g_1,g_2,e(g,g)^{\alpha},g^{\beta},g^{\gamma})$和主秘钥$msk=(\alpha,\beta,\gamma)$,其中G是p阶加法循环群,$g,g_0,g_1,g_2$是G的生成元,$G_T$是p阶乘法循环群,e是双线性映射$G\times G\rightarrow G_T$,$\alpha$表示第一随机数:$\alpha\in Z_p$,$\beta$表示第二随机数:$\beta\in Z_p$,$\gamma$表示第三随机数:$\gamma\in Z_p$,$Z_p$表示p阶整数域,p表示一个大素数。

[0199] 然后在Z_p上随机构造一个Shamir(t,n)-门限秘密共享实例f,并保存f(0)和t-1个

f上的点{(a_1,z_1),……,(a_{t-1},z_{t-1})},其中,a_1,……,$a_{t-1}\in Z_p$。再利用概率加密算法,对新加入的用户端的唯一标识信息id_{EN}进行加密,得到密文a,将密文a带入f,得到相应的函数值z=f(a)。其中,概率加密算法随机性加密算法的使用,当加密相同的信息几次后,会产生不同的密文。

[0200] 再利用概率加密算法加密a||z,得到密文$c\in Z_p$,其中,"||"表示连接符号,最后根据新加入的用户端的属性集,生成用户私钥$sk_{EN}=g^{(\alpha+(\gamma+c)r)/\beta}$和边缘私钥$sk_{FN}=(K`,L,L`,\{K_{j,1,},K_{j,2}\}_{j\in[1,K]})$,并将用户私钥$sk_{EN}$发送给用户端,将边缘私钥$sk_{FN}$发送给用户端所接入的边缘服务器,其中,K`表示第一边缘私钥分量:K`=c,L表示第二边缘私钥分量,$L=g^r$,L`表示第三边缘私钥分量,$L`=g^{\gamma r}$,$K_{j,1}$,表示第四边缘私钥分量,$K_{j,1},=g^{rj}$,$K_{j,2}$表示第五边缘私钥分量,$K_{j,2}=\left(g_0^{A_j}g_1\right)^{r_j}g_2^{-(\gamma+c)r}$。

[0201] 在目前的方法中,加密明文空间文本得到空间文本密文以及用于解密空间文本密文的密钥对应的密钥密文均是由数据拥有者计算的,无疑造成了数据拥有者的资源开销大的问题。

[0202] 而在本发明中,对于密钥密文由数据拥有者和边缘服务器共同完成,以实现数据拥有者轻量级的计算,减少数据拥有者的资源消耗。

[0203] 进一步地,数据拥有者针对明文空间文本生成对称密钥,并根据所述对称密钥对所述明文空间文本进行加密,得到空间文本密文。

[0204] 例如,明文空间文本{如,包括某餐厅的文本信息和空间信息,即关键字(菜系类型,餐厅主题等)和空间位置(经纬度)}的数量为m个,则数据拥有者生成m个对称密钥sk_t,利用sk_t对明文空间文本集(包括所有明文空间文本)O_t进行加密,得到空间文本密文集c_t,其中t的取值范围是{1,……,m}。

[0205] 数据拥有者针对各明文空间文本建立访问结构,来确定每个明文空间文本(即密文索引树中的叶子节点)的已授权用户。

[0206] 在一种可实施的方式中,数据拥有者将访问结构发送至云服务器,以使云服务器针对用户端查询到的第二节点时,由云服务来确定第二节点是否授权于用户端。

[0207] 在另一种可实施的方式中,数据拥有者将访问结构发送至边缘服务器,以使云服务器针对用户端查询到的第二节点时,指示边缘服务器根据访问结构确定第二节点是否授权于用户端。以减少云服务器的计算量,降低云服务器的资源消耗。

[0208] 边缘服务器针对数据拥有者的对称密钥根据预设算法,对数据拥有者的对称密钥进行加密,得到临时密钥密文,并将临时密钥密文发送至数据拥有者,其中预设算法可以为随机算法等,在此不做限定。

[0209] 数据拥有者在得到临时密钥密文后,选取随机数,对临时密钥密文进行加密,得到用于解密空间文本密文的密钥对应的密钥密文。因为在此过程中,引入边缘服务器辅助计算,以此实现了数据拥有者轻量级的计算,降低了数据拥有者的资源消耗。

[0210] 在本发明实施例中,密文索引树可以为四叉树、R树等结构,在此不做限定。

[0211] 结合以上描述,以密文索引树为R树举例,数据拥有者将明文空间文本O_t作为叶子节点,即每个明文空间文本均为一个叶子节点,针对每个叶子节点,数据拥有者建立叶子节点的混合向量密文。其中,叶子节点的混合向量密文包括空间信息和文本信息,空间信息包

括叶子节点的位置信息,如经、纬度信息,文本信息包括叶子节点的各关键字,如该叶子节点为“东北餐馆”以及“情侣主题餐馆”。

[0212] 在构建叶子节点的混合向量密文之前,数据拥有者根据所有的明文空间文本预设关键字,其中,关键字的数量为N2个。

[0213] 数据拥有者随机生成第三比特向量以及N1+N2维数的第五随机向量和第六随机向量;再根据第三比特向量中各比特位的元素值,基于预设条件为第五随机向量的前N1位和第六随机向量的前N1位进行赋值。

[0214] 再根据随机选取的关键字是否位于叶子节点中的关键字中,通过随机数为第五随机向量的后N2位和第六随机向量的后N2位进行赋值。

[0215] 举例来说,生成第三比特向量s`和第五随机向量{Na1,Nb1,Na2,Nb2},第六随机向量{N`a1,N`b1,N`a2,N`b2}。

[0216] 针对任一叶子节点,在第三比特向量s`中任意选取一个未选取过的第t_{y1}个元素值t_{z1},在确定元素值t_{z1}为0时(预设条件),将1赋予在第五随机向量和第六随机向量对应的位置上。在确定元素值t_{z1}不为0时,将叶子节点的经度值xi赋予在第五随机向量对应位置上,将叶子节点的纬度值yi赋予在第六随机向量对应位置上。

[0217] 例如,在$t_{y1}=1$,且$t_{z1}=0$时,第五随机向量为{1,Nb1,Na2,Nb2},第六随机向量为{1,N`b1,N`a2,N`b2}。在$t_{y1}=1$,且$t_{z1}\neq0$时,第五随机向量{xi,Nb1,Na2,Nb2},第六随机向量{yi,N`b1,N`a2,N`b2}。其中,t_{z1}的取值范围为{1,……,N1}。

[0218] 然后再从关键字中(R树中的所有预设关键字)随机选取一个未选过的第t_{y2}个关键字t_{z2},确定关键字t_{z2}是否存在于叶子节点的关键字(如该叶子节点的关键字包括川菜和火锅)中,若是,则随机选一个随机数sy1,将sy1赋予在第五随机向量对应位置上,将1与sy1的差值赋予在第六随机向量对应位置上。否则随机选一个随机数sy2,将sy2赋予在第五随机向量对应位置上,将0与sy2的差值赋予在第二随机向量对应位置上。

[0219] 例如,在$t_{y2}=1$,且关键字t_{z2}存在于该叶子节点的关键字中时(如选取的关键字为“火锅”),第五随机向量{Na1,Nb1,sy1,Nb2},第六随机向量{N`a1,N`b1,1-sy1,N`b2}。在$t_{y2}=1$,且关键字$t_{z2}$不存在于该叶子节点的关键字中时,第五随机向量{Na1,Nb1,sy0,Nb2},第六随机向量{N`a1,N`b1,0-sy2,N`b2}。其中,t_{y2}的取值范围为{1,……,N2}。t_{y2}在随机向量对应的位置为$N1+t_{y2}$。

[0220] 数据拥有者针对R树中的任一非叶子节点,根据上述第一编码算法和第二编码算法,确定出非叶子节点的空间向量密文,具体算法这里不作赘述。

[0221] 根据上述确定出的数据,数据拥有者接收可信第三方系统发送的拥有者密钥,根据拥有者密钥对R树(包括叶子节点混合向量密文和非叶子节点的空间向量密文)进行加密,得到初始密文索引树。

[0222] 然后将初始密文索引树、密钥密文和空间文本密文发送至云服务器,以使云服务器对初始密文索引树进行重加密,得到最终的密文索引树,进而查询出符合查询请求的第二节点。

[0223] 为了更好的阐述上述技术方案,图6示例性的示出了一种空间文本的查询方法的示意图,如图6所示,可信第三方系统针对数据拥有者生成第一拥有者密钥和第二拥有者密钥,针对用户端生成用户私钥、边缘私钥、第一用户密钥和第二用户密钥。

[0224] 数据拥有者根据对称密钥,对各明文空间文本进行初始加密,得到各空间文本密文,进而得到空间文本密文集。针对各明文空间文本建立访问结构,并将访问结构和空间文本密文集发送至边缘服务器1。

[0225] 边缘服务器1根据共享秘密算法对上述访问结构进行加密,进而相当于对称密钥进行加密,得到各明文空间文本的临时密钥密文,并返回给数据拥有者。

[0226] 数据拥有者在得到各临时密钥密文之后,选取随机数,对临时密钥密文进行加密,得到各密钥密文,进而得到密钥密文集。

[0227] 数据拥有者根据各明文空间文本构建明文索引树,然后再根据第一拥有者密钥对明文索引树进行初始加密,得到初始密文索引树,然后将空间文本密文集、密钥密文集和初始密文索引树发送至云服务器。

[0228] 云服务器在接收到数据拥有者发送的空间文本密文集、密钥密文集和初始密文索引树之后,根据第二拥有者密钥对初始密文索引树进行重加密,得到最终的密文索引树,并将空间文本密文集、密钥密文集发送至与用户端相交互的边缘服务器2。

[0229] 用户端发起查询请求,根据第一用户密钥对查询请求进行加密,得到查询请求的第一查询空间向量密文和第一查询混合向量密文,并发送至云服务器。

[0230] 云服务器在得到查询请求的第一查询空间向量密文和第一查询混合向量密文之后,根据第二用户密钥对其进行加密,得到查询请求的第二查询空间向量密文和第二查询混合向量密文。

[0231] 云服务器根据查询请求的第二查询空间向量密文在密文索引树中确定出与之相交的第一节点,根据查询请求的第二查询混合向量密文确定出在查询请求的空间范围内且用户端为授权用户的第二节点,并将第二节点对应的空间文本密文的空间文本编号发送至边缘服务器2。

[0232] 边缘服务器2根据空间文本编号查询出第二节点对应的密钥密文和空间文本密文,再根据边缘私钥和第二节点对应的密钥密文确定出中间量,最后将中间量和第二节点对应的空间文本密文发送至用户端。

[0233] 用户端根据用户私钥对中间量进行解密,得到对称密钥,再根据对称密钥对空间文本密文进行解密,得到明文空间文本。

[0234] 本发明实施例中,根据第一查询空间信息密文可以在密文索引树中确定出在查询位置内的所有第二节点,再根据第一查询混合向量密文在第二节点中确定出查询范围内第一节点,并确定出第一查询混合向量密文与各第一节点的相关度,进而确定出查询结果,避免了查询结果受权重的影响,提升了空间文本查询的准确度,边缘服务器1辅助计算出临时密钥密文,以实现数据拥有者轻量级的计算,降低了数据拥有者的资源消耗。边缘服务器2辅助计算出中间量,以实现用户端轻量级的计算,降低了用户端的资源消耗。

[0235] 基于相同的技术构思,图7示例性的示出了本发明实施例提供的一种空间文本的查询装置的结构示意图,该装置可以执行空间文本的查询方法的流程。

[0236] 如图7所示,该装置具体包括:

[0237] 获取模块710,用于获取用户端发送的第一查询密文;所述第一查询密文包括第一查询空间向量密文和第一查询混合向量密文;所述第一查询空间向量密文是根据查询请求中的空间查询条件生成的;所述第一查询混合向量密文是根据所述查询请求中的文本查询

条件和所述空间查询条件生成的；

[0238] 处理模块720，用于根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点；所述密文索引树是数据拥有者根据各明文空间文本构建的；所述密文索引树中的非叶子节点存储有基于明文空间文本中的空间信息生成的空间向量密文，叶子节点存储有基于明文空间文本中的空间信息和文本信息生成的混合向量密文；所述第一节点为非叶子节点；

[0239] 根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文，确定符合所述文本查询条件的第二节点；所述第二节点为叶子节点；所述第二节点用于作为查询结果。

[0240] 可选的，所述处理模块720具体用于：

[0241] 根据预设检索顺序，针对所述密文索引树中的任一节点，在确定所述节点为非叶子节点时，根据所述第一查询空间向量密文和所述节点的空间向量密文确定与所述第一查询空间向量密文相交的所述第一节点。

[0242] 可选的，所述处理模块720具体用于：

[0243] 根据所述第一查询空间向量密文和所述节点的空间向量密文确定多个第一内积值；

[0244] 在确定所述多个第一内积值均大于空间阈值时，根据所述节点的各第一孩子节点的空间向量密文和所述第一查询空间向量密文，在所述各第一孩子节点中确定出与所述第一查询空间向量密文在空间位置上相交的第二孩子节点，直至确定出与所述第一查询空间向量密文相交的所述第一节点；所述第一节点为叶子节点的父节点；

[0245] 在确定所述多个第一内积值未均大于空间阈值时，确定所述节点的父节点下与所述第一查询空间向量密文在空间位置上相交的其他孩子节点，直至确定出与所述第一查询空间向量密文相交的所述第一节点。

[0246] 可选的，所述处理模块720具体用于：

[0247] 针对所述第一节点下的任一叶子节点，根据所述第一查询混合向量密文和所述叶子节点的混合向量密文确定多个第二内积值；

[0248] 在确定所述多个第二内积值均大于空间阈值，且所述多个第二内积值的和大于相似度阈值时，将所述叶子节点确定为所述第二节点。

[0249] 可选的，所述第一查询密文是所述用户端基于第一用户密钥加密的；

[0250] 所述处理模块720还用于：

[0251] 根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点之前，根据所述用户端的第二用户密钥，对所述第一查询密文进行加密，确定所述第二查询密文；所述第二查询密文包括第二查询空间向量密文和第二查询混合向量密文；

[0252] 所述处理模块720具体用于：

[0253] 根据所述第二查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点；

[0254] 根据所述第二查询混合向量密文和所述第一节点下的叶子节点的混合向量密文，确定符合所述文本查询条件的第二节点。

[0255] 可选的,所述处理模块720具体用于:

[0256] 将所述第二节点对应的空间文本编号发送至边缘服务器,以指示所述边缘服务器根据所述空间文本编号查询出所述空间文本编号对应的密钥密文和空间文本密文,并根据所述空间文本编号对应的密钥密文确定所述空间文本编号对应空间文本密文的中间量;

[0257] 将所述第二节点的空间文本密文和中间量作为所述查询结果。

[0258] 基于相同的技术构思,图8示例性的示出了本发明实施例提供的一种空间文本的查询装置的结构示意图,该装置可以执行空间文本的查询方法的流程。

[0259] 如图8所示,该装置具体包括:

[0260] 生成单元810,用于基于查询请求中的空间查询条件生成第一查询空间向量密文;

[0261] 基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文;

[0262] 发送单元820,用于将第一查询密文发送至云服务器;所述第一查询密文包括所述第一查询空间向量密文和所述第一查询混合向量密文;

[0263] 解密单元830,用于基于所述云服务器的查询结果,确定所述查询请求对应的明文空间文本。

[0264] 可选的,所述空间查询条件包括指示空间范围的第一位置点和第二位置点;

[0265] 所述生成单元810具体用于:

[0266] 生成第一随机向量和第二随机向量;

[0267] 根据第一比特向量中各比特位的元素值,按照第一方式对所述第一随机向量的前K位进行与所述第一位置点相关的赋值;根据第二比特向量中各比特位的元素值,按照第二方式对所述第一随机向量的后L位进行与第一位置点相关的赋值,得到所述第一查询空间向量密文的第一子向量密文;所述第一比特向量和所述第二比特向量是数据拥有者随机生成的;

[0268] 根据所述第一比特向量中各比特位的元素值,按照第三方式对所述第二随机向量的前K位进行与所述第二位置点相关的赋值;根据所述第二比特向量中各比特位的元素值,按照第四方式对所述第二随机向量的后L位进行与所述第二位置点相关的赋值,得到所述第一查询空间向量密文的第二子向量密文。

[0269] 可选的,所述生成单元810具体用于:

[0270] 生成第三随机向量和第四随机向量;

[0271] 根据第三比特向量中各比特位的元素值,基于所述空间查询条件为所述第三随机向量的前N1位和所述第四随机向量的前N1位进行赋值;所述第三比特向量是数据拥有者随机生成的;

[0272] 根据随机选取的关键字是否位于所述文本查询条件中的查询关键字中,通过随机数为所述第三随机向量的后N2位和所述第四随机向量的后N2位进行赋值。

[0273] 可选的,所述解密单元830具体用于:

[0274] 接收边缘服务器发送的空间文本密文和中间量;所述空间文本密文和中间量是边缘服务器根据所述云服务器发送的空间文本编号确定的;

[0275] 根据对所述中间量进行解密,确定所述空间文本密文的对称密钥;

[0276] 根据所述空间文本密文的对称密钥对所述空间文本密文进行解密,得到所述查询

请求对应的明文空间文本。

[0277] 基于相同的技术构思,本发明实施例还提供一种计算机设备,包括:

[0278] 存储器,用于存储程序指令;

[0279] 处理器,用于调用所述存储器中存储的程序指令,按照获得的程序执行上述空间文本的查询方法。

[0280] 基于相同的技术构思,本发明实施例还提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机可执行指令,所述计算机可执行指令用于使计算机执行上述空间文本的查询方法。

[0281] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0282] 本申请是参照根据本申请的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0283] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0284] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0285] 显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

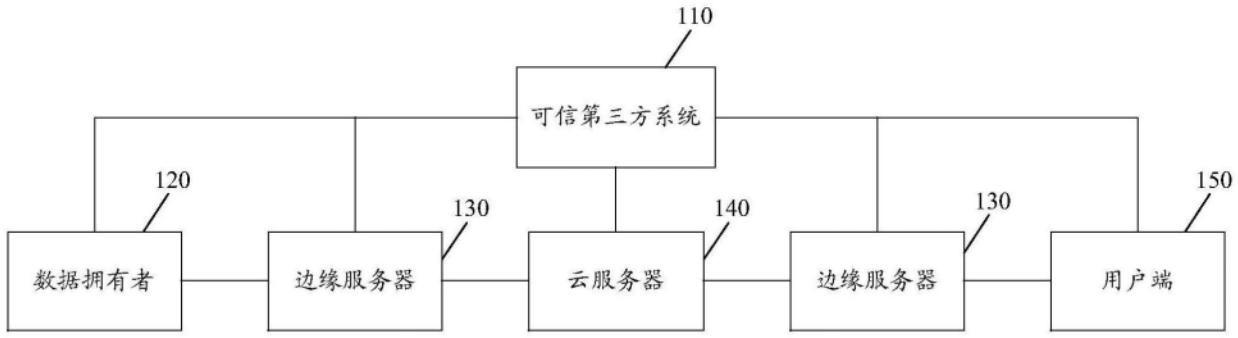

110
可信第三方系统
120
130
140
130
150
数据拥有者
边缘服务器
云服务器
边缘服务器
用户端

图1

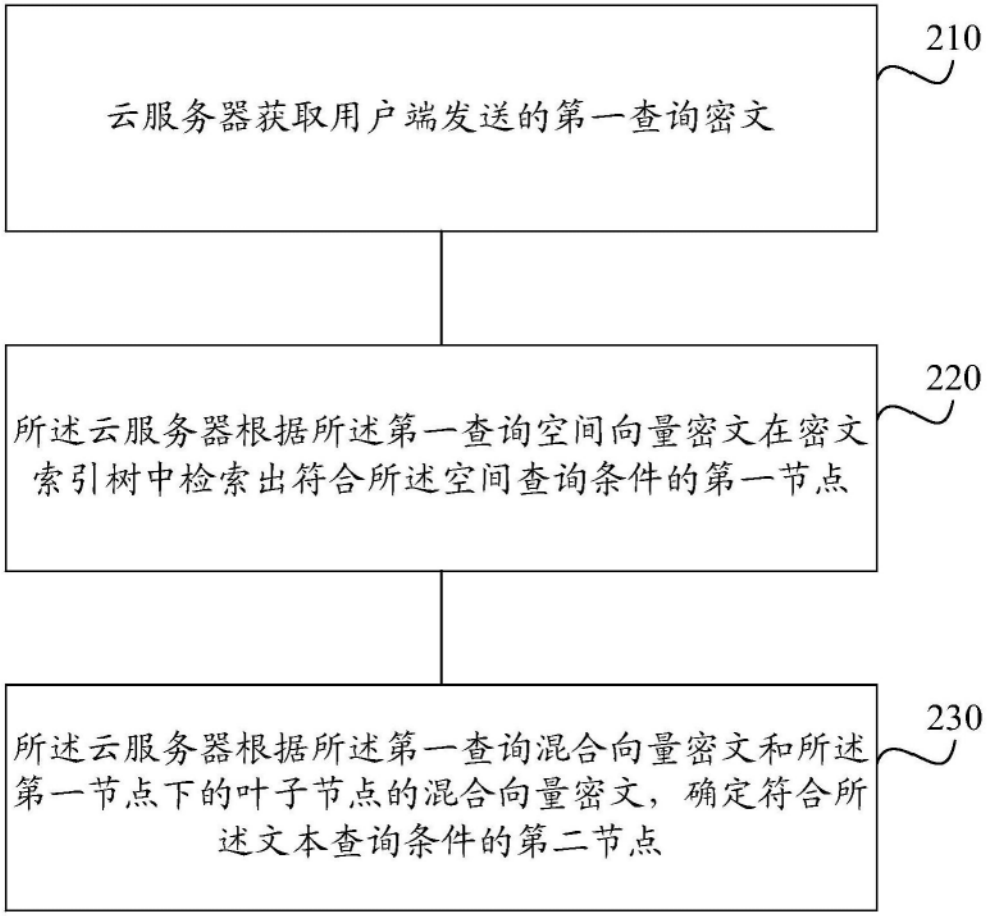

210
云服务器获取用户端发送的第一查询密文
220
所述云服务器根据所述第一查询空间向量密文在密文索引树中检索出符合所述空间查询条件的第一节点
230
所述云服务器根据所述第一查询混合向量密文和所述第一节点下的叶子节点的混合向量密文，确定符合所述文本查询条件的第二节点

图2

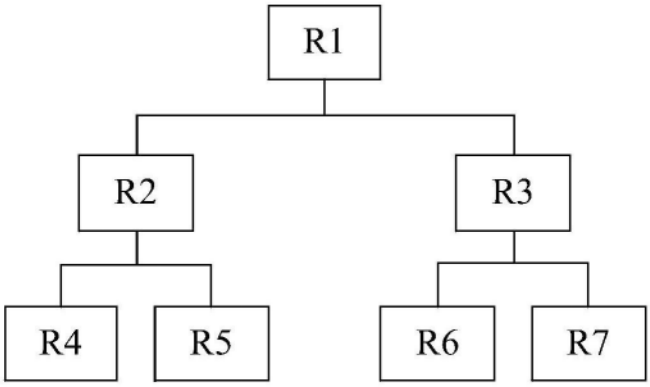


图3

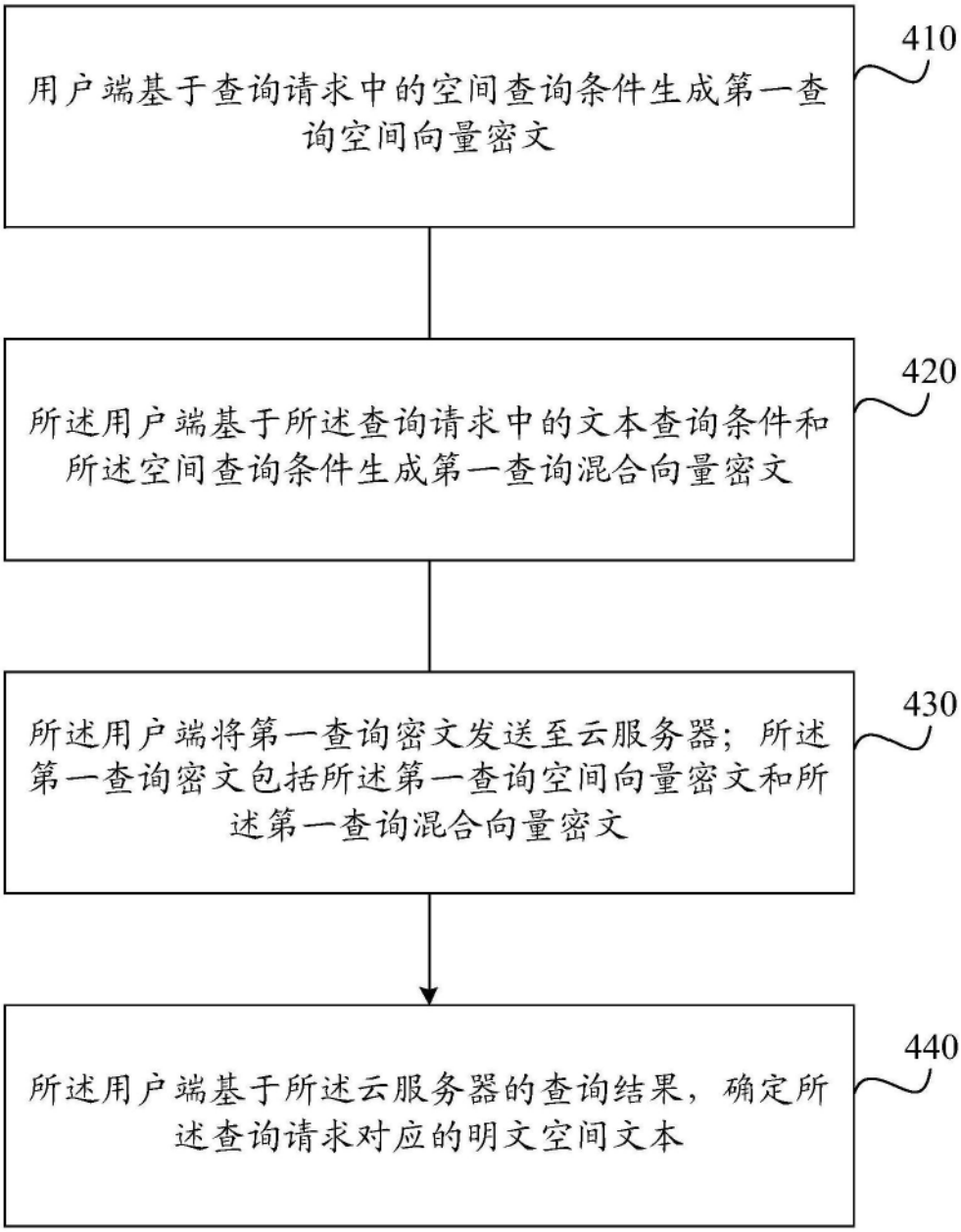

用户端基于查询请求中的空间查询条件生成第一查询空间向量密文
410
所述用户端基于所述查询请求中的文本查询条件和所述空间查询条件生成第一查询混合向量密文
420
所述用户端将第一查询密文发送至云服务器；所述第一查询密文包括所述第一查询空间向量密文和所述第一查询混合向量密文
430
所述用户端基于所述云服务器的查询结果，确定所述查询请求对应的明文空间文本
440

图4

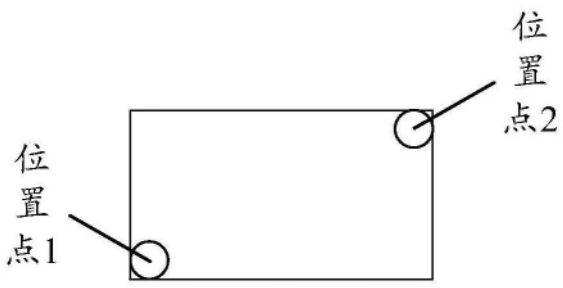

位置点2
位置点1

图5

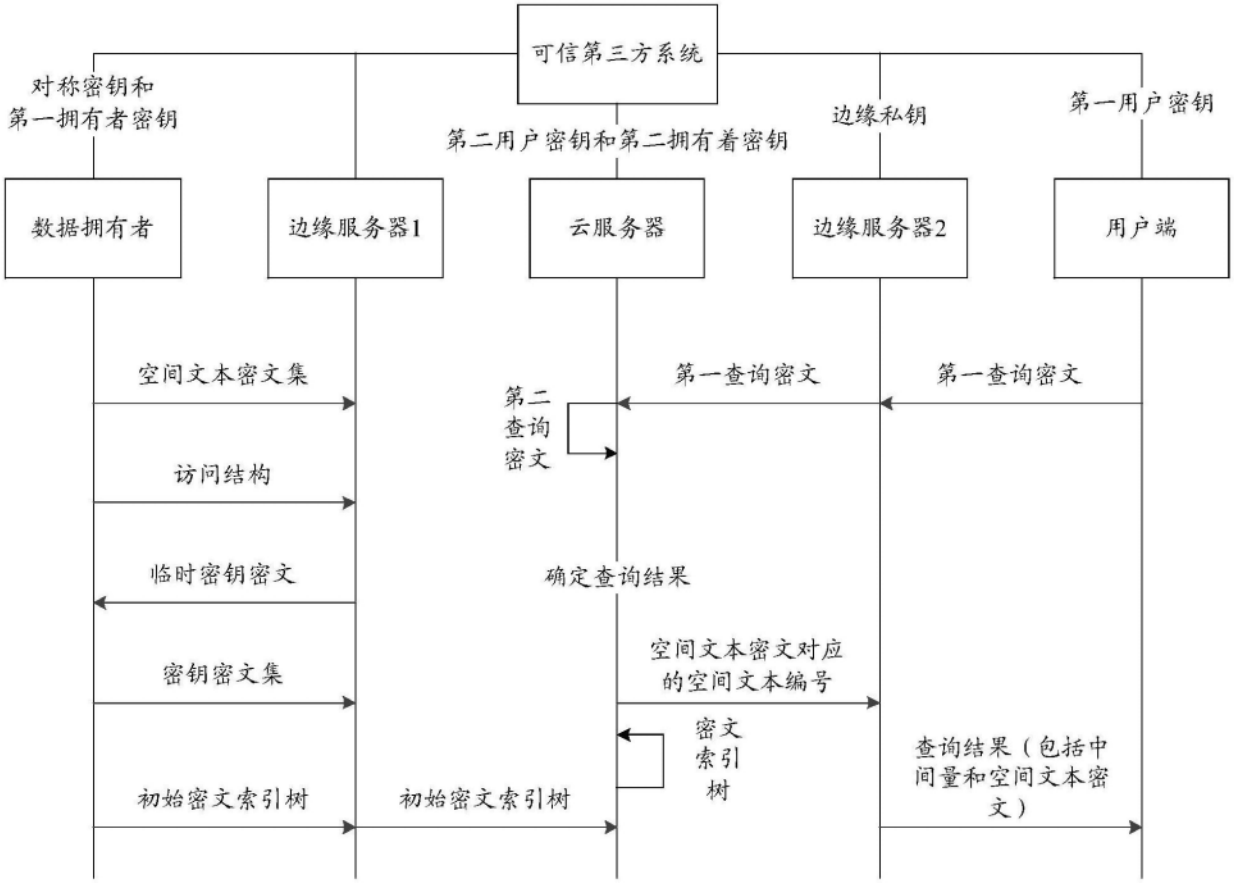

可信第三方系统
对称密钥和
第一拥有者密钥
第二用户密钥和第二拥有着密钥
边缘私钥
第一用户密钥
数据拥有者
边缘服务器1
云服务器
边缘服务器2
用户端
空间文本密文集
第一查询密文
第一查询密文
第二
查询
密文
访问结构
临时密钥密文
确定查询结果
密钥密文集
空间文本密文对应
的空间文本编号
密文
索引
树
查询结果（包括中
间量和空间文本密
文）
初始密文索引树
初始密文索引树

图6

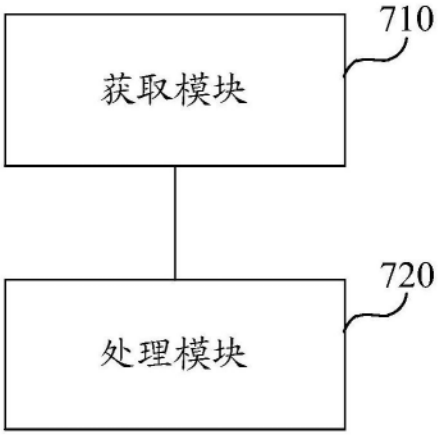

710
获取模块
720
处理模块

图7

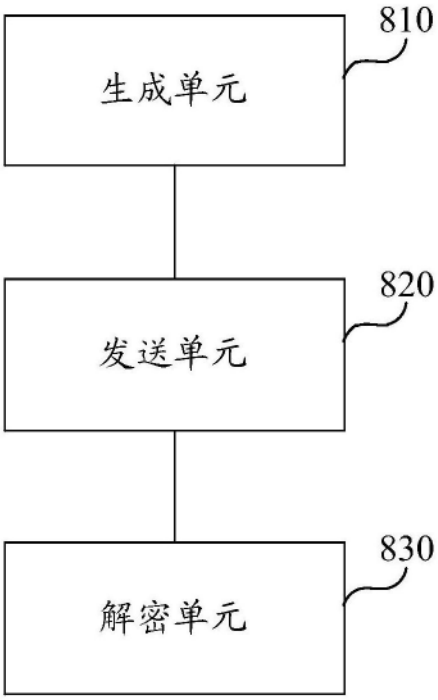


图8