文章编号:1674-2974(2022)04-0001-10 DOI:10.16339/j.cnki.hdxbzkb.2022279

云计算环境下数据安全与隐私保护研究综述

邓桦[1],宋甫元[1],付玲[2],欧露[1],尹辉[3],高毅[4],秦拯[1†]
(1. 湖南大学 信息科学与工程学院,湖南 长沙,410082;2. 中联重科股份有限公司,湖南 长沙,410013;
3. 长沙学院 计算机工程与应用数学学院,湖南 长沙,410022;
4. 益丰大药房连锁股份有限公司,湖南 长沙,410199)

摘 要:用户数据安全与隐私保护是云计算环境中最重要的问题之一,通常采用密码学技术保护数据安全与隐私.目前,基于密码学技术的数据安全查询、分享以及差分隐私保护是国内外的研究热点.本文主要针对密文查询、密文分享和差分隐私等当前国内外研究的现状进行综述,指出存在的问题与不足.在此基础上,重点介绍了文章作者团队在云计算环境下数据安全与隐私保护的最新研究成果.在密文查询方面,提出了空间关键字密文检索技术,实现了轻量级的访问控制和多关键字搜索;在密文分享方面,提出了跨密码系统的细粒度密文分享方法,使用户可以指定访问控制策略将加密数据分享给不同加密系统中的用户.最后,指出了当前研究中尚待解决的问题以及未来研究方向.

关键词:云计算;数据安全;可搜索加密;代理重加密;差分隐私保护
中图分类号:TP393 **文献标志码**:A

A Review of Data Security and Privacy Preserving in Cloud Computing Environment

DENG Hua[1],SONG Fuyuan[1],FU Ling[2],OU Lu[1],YIN Hui[3],GAO Yi[4],QIN Zheng[1†]
(1. College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082,China;
2. Zoomlion Heavy Industry Science&Technology Co. ,Ltd,Changsha 410013,China;
3. College of Computer Engineering and Applied Mathematics, Changsha University,Changsha 410022,China;
4. Yifeng Pharmacy Chain Co. ,Ltd,Changsha 410199,China)

Abstract: User data security and privacy preserving has been becoming one of the most crucial issues in cloud computing environment, where cryptographic technologies are taken as a useful solution to achieve these goals. Nowadays, secure data searching and sharing and differential privacy preserving have attracted much more attention. This paper reviews the state-of-the-art in the field of ciphertext search, ciphertext sharing and differential privacy, and identifies their inappropriateness. Then, a series of recent research results in ciphertext search and ciphertext sharing are presented. In the respect of ciphertext search,this paper introduces the encrypted spatial keyword searth method, which achieves lightweight access control and efficient keyword search. In the respect of ciphertext sharing, this paper proposes the cross-cryptosystem fine-grained data sharing scheme, in which a data owner can formulate an ac-

* **收稿日期**:2021-11-29
基金项目:国家自然科学基金资助项目(U20A20174), National Natural Science Foundation of China(U20A20174)
作者简介:邓桦(1984—),男,湖南郴州人,湖南大学副研究员,博士
† 通信联系人,E-mail:zqin@hnu.edu.cn

cess policy such that the part of encrypted data satisfying the access policy can be shared with the users in a different cryptosystem. Finally, this paper provides several open research issues and the trend in the future.

Key words: cloud computing; data security; searchable encryption; proxy re-encryption; differential privacy

云计算(Cloud Computing)是分布式计算、并行计算、效用计算、虚拟化、负载均衡等传统计算技术和网络技术发展融合的产物[1]. 云计算是以按需付费的模式,通过互联网提供可配置计算资源共享池(资源包括网络、服务器、存储、应用软件、服务等).

在使用云计算服务时,用户最为关心和担忧的问题是数据的安全和隐私是否得到了很好保护.当用户将数据外包给云服务提供商后,便失去了对数据的物理控制,数据的安全和隐私依赖于云服务提供商对数据采取的安全防护措施.如果安全措施被外部黑客或者云服务提供商内部人员破坏,用户的敏感数据有可能被泄露,数据的安全和隐私将被严重破坏[2].实现云计算数据安全与隐私保护的方式有很多,其中最主要的是使用密码学方法和技术.但是,这同时也带来了两个主要问题:一是数据被加密后,如何对密文态数据进行查询搜索以及如何将密文准确分享给指定用户;二是如何对数据进行差分隐私保护,防止用户从公开发布数据中挖掘敏感信息.

密文查询是指在不泄露明文信息的前提下对密文执行有效检索.可搜索加密是最主要的密文查询方法.目前研究较多的可搜索加密主要可以分为两类:对称可搜索加密和非对称可搜索加密.在可搜索加密过程中,用户可以通过提交查询陷门,委托云服务器在加密索引上进行查询匹配,并将对应的密文结果返回给用户.然而,现有的可搜索加密方案在安全性、效率、功能性等方面仍然存在一些不足.一方面,传统的隐私保护密文查询协议大多致力于抵御不可信云攻击,且需要依赖不合谋的双云模型进行隐私计算,或者依靠可信第三方对用户合法性进行认证,缺乏有效的访问控制策略,安全性有待加强;另一方面,现有的可搜索加密技术大部分基于繁重的密码算法设计,计算开销通常较大,且需要用户和云服务器进行多轮交互,极大地增加了用户端的通信开销.此外,现有的密文查询系统模型仅适用于单用户系统,并且只关注了单关键字精确查询.但是,在实际应用中,多用户模型多关键字相似性搜索更为普遍.目前缺乏在多用户模型中进行密文查询的有效方法.

密文分享一般是指数据所有者将被加密的数据分享给指定的用户.实现密文分享的算法包含对称加密和非对称加密.在实际应用中,通常先使用对称加密密钥加密数据,然后使用指定用户公钥加密对称密钥;解密时指定用户使用私钥获得对称密钥,最终恢复数据.因此,使用非对称加密算法能够直接决定哪些用户可以访问数据.目前研究比较多的非对称加密算法有身份基加密、广播加密、属性基加密等.在云计算中,数据所有者在完成对数据的加密后,即利用指定用户的公钥加密完对称密钥后,可能还需要将数据分享给指定用户之外的更多用户;但是由于这些用户没有掌握指定用户的私钥,因而无法直接访问数据.解决这类问题的较好方法是代理重加密,它可以将消息在当前公钥下的密文,转换为在另一个公钥下的密文.但是,现有代理重加密方案只能在相同的加密系统下使用,不同加密系统的用户无法直接分享密文.

差分隐私保护作为具有严格数学定义的隐私保护框架,可使得敌手不能够推断某个个体是否在数据库中,已被广泛应用于谷歌Chrome浏览器以及苹果iOS / macOS操作系统.专家学者运用差分隐私保护框架,在大数据相关性隐私保护以及深度学习方面,取得了很好的研究成果.考虑云计算环境下时序数据中普遍存在的相关性,专家学者提出马尔科夫退出机制、时域上相关的高斯白噪声机制等,可有效隐藏云数据中自相关性;设计相关噪声机制,可有效解决互相关性隐私泄露问题.此外,考虑深度学习中隐私泄露问题,专家学者提出具有隐私保护的分布式深度学习框架、差分隐私保护的随机梯度下降方法、以及基于集中式差分隐私保护框架的方法等,实现训练模型的差分隐私保护.

本文第1节介绍密文查询国内外研究现状和存在的问题,并介绍作者团队提出的空间关键字搜索技术;第2节介绍密文分享国内外研究现状和存在的问题,并介绍作者团队提出的跨密码系统密文转换技术;第3节介绍差分隐私国内外研究现状并对存在的问题进行阐述;第4节对本文工作进行总结和展望.

1 密文查询

密文查询一般是指在密文态数据中进行关键字搜索,同时不泄露明文的任何有用信息.实现密文查询的主要方法是可搜索加密技术.近年来,随着云计算数据外包模式的充分发展,如何以加密的方式保护云外包数据的机密性,同时又保证加密数据的可搜索性以及搜索效率,引起了研究人员的广泛研究.云计算环境下典型的可搜索加密系统模型如图1所示.该模型包括3个实体,即数据提供者、数据使用者和云服务提供商.数据提供者加密外包数据并为外包数据建立安全可搜索索引,将密文和安全索引发送给云服务器进行存储;如果一个授权的数据使用者想从云服务器中获取感兴趣的数据文件,他将使用一个授权的密钥加密查询关键字生成查询陷门,并将查询陷门发送给云服务器;云服务器利用查询陷门在加密的数据中进行检索,最后将匹配到的查询结果发送给数据使用者.

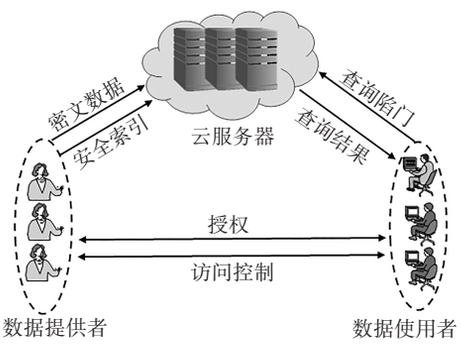

图1　基于云计算的可搜索加密系统模型

Fig.1　System model of searchable encryption in cloud computing

1.1 单关键字可搜索加密

Song等人提出了第一个实用的对称可搜索加密(Searchable Symmetric Encryption, SSE)方案[3],Chang和Mitzenmacher[4]提出了一个类似方案,但在安全性上第一次实现了前向安全.这两个方案的搜索时间与数据文件集合的规模呈线性关系.直到2006年,Curtomal等人[5]使用倒排索引结构提出了第一个次线性查询复杂度的SSE方案.该方案将文档组织成keyword-document对,其中使用伪随机函数加密关键词并存储在一个随机的哈希表中,文档标识符使用对称加密技术进行随机化,并保存在一个随机数组中,哈希表和数组组成倒排列表共同构成该数据集合的安全索引.该设计的优势是其搜索复杂度仅与查询结果集合的规模成正比,提高了查询效率.在后续的研究中,加密的倒排索引技术被广泛应用于可搜索加密方案的设计中.为了使可搜索加密技术能够在云计算环境中进行实际应用,SSE被进一步扩展成动态结构,即支持安全的数据动态更新,允许数据提供者删除已有数据或增加新数据,且不会破坏SSE方案的可搜索性,从而提高了可搜索加密的实用性[6-8].研究者针对传统动态可搜索加密方案在更新数据过程中由于文件注入攻击[9]泄露数据信息的问题,提出了动态可搜索加密的前向安全概念[10-12].前向安全能够保证更新数据不会泄露比一个预定义的泄露函数所表示的更多信息,用来抵御文件注入攻击.近年来,研究者们提出了后向安全的概念,它要求可搜索加密的搜索过程不能揭示已删除数据中的信息.图2所示为对称可搜索加密算法结构框架.

Setup

数据提供者:

1. 生成随机密钥K和一个空Map M;
2. 对词典中的每一个关键词w:
3. 生成密钥$K_1=F(k,w\|1)$和$K_2=F(k,w\|2)$,符号F表示一个伪随机函数,‖表示字符串连接.
4. 定义一个计数器c,初始值为0.
5. 对每一个包含关键词w的文档,用标识符id表示,计算
6. $l=F(K_1,c)$,d=Enc(K_2,id);
7. 将key-value对<l,d>加入到Map M中;
8. $c=c+1$.
9. 发送密钥K给数据使用者,输出M.

Search

数据使用者:

1. 给定搜索关键词w,数据使用者利用密钥K计算$K_1=F(k,w\|1)$和$K_2=F(k,w\|2)$;
2. 发送K_1和K_2给搜索服务器(比如云服务器).

云服务器

1. 生成一个空的列表List R,用于存储查询结构;
2. For c = 0 直到M.getValue返回空
3. $d=M$.getValue($F(K_1,c)$),id = Dec(K_2,d);
4. $c=c+1$;
5. 增加文件表示符id至列表R.
6. 发送R给数据使用者.

图2　对称可搜索加密算法框架示例

Fig.2　An example of symmetric searchable encryption

对称可搜索加密框架包括2个算法,**Setup**算法由数据提供者调用,其功能是对外包数据建立加密的可搜索索引(一般而言,数据本身采用语义安全的对称加密技术进行加密);**Search**是一个数据查询者和云服务器之间的交互协议,数据查询者加密查询关键字,并将查询陷门发送给云服务器,云服务器根据查询陷门在外包的加密索引中进行搜索并返回查询结果给数据使用者.Boneh等人[13]提出了公钥可搜索加密(Public Key Encryption with Keyword

Search,PEKS),允许数据提供者使用数据使用者的公钥建立安全索引,数据使用者使用自己的私钥加密查询关键字生成陷门.与SSE方案相比,PEKS查询效率相对较低,但能够构造更丰富的查询功能,如关键字连接查询、子集查询和范围查询等[14-15].

1.2 多关键字可搜索加密

近年来,为了提高可搜索加密在云计算环境下的实用性,研究者对多关键字排名查询进行了研究.文献[16]利用矩阵变换,提出了一种保内积加密方案.该方案能够保证加密索引与陷门的内积等价于原明文数据向量与查询向量的内积.基于安全k近邻(k-nearest neighbor, kNN)计算技术,研究者们陆续提出了很多改进的方案.Cao等人[17]首次基于安全kNN计算技术在加密的向量空间模型下构造了云环境下隐私保护的多关键字排名查询方案MRSE.MRSE需要一个全局词典,数据文件基于全局词典被转换为关键字索引向量,该索引向量被一个矩阵密钥$\boldsymbol{M}$加密后成为文件的安全索引.云服务器通过计算查询索引和查询令牌之间的"内积相似度"来实现隐私保护的多关键字密文排名查询,"内积相似度"越大表明文件和查询越相关.由于该方案没有考虑索引关键词和查询关键词的权重,Cao等人[18]改进了他们的方案,运用明文信息检索领域来衡量关键字查询相关性的TF×IDF规则,其中TF和IDF分别表示安全索引和查询令牌向量中关键字的权重.云服务器在查询时所计算的两个向量内积实际上是查询和文件的相关性得分,用以衡量查询和文件的相关度,最终实现精确的排名查询.Xu等人[19]首先指出Cao等人的方案不支持预定义词典的动态更新等问题.为了解决动态更新问题,他们提出将索引向量加密矩阵$\boldsymbol{M}$分割成很多小矩阵,当有关键字更新时,只需要局部更新发生变化的矩阵及对局部索引进行重新加密,这样可以避免索引完全重建.同时,小矩阵使索引加密和查询的计算复杂度也随之降低.Fu等人[20]实现了根据用户个人兴趣在加密的外包云数据上进行个性化查询的多关键字安全查询方案,进一步提高用户查询体验.他们使用语义本体词汇网络来表达用户的查询兴趣模型,而用户个人兴趣模型的建立仅仅通过分析用户的查询历史即可自动完成.Xia等人[21]提出了一种支持数据文件动态更新的多关键字排名查询方案.他们首先使用安全kNN算法加密数据文件索引和用户查询向量,然后把安全索引按规则组织成树形数据结构以支持数据文件的动态删除和插入,并设计了"贪婪深度优先查询"算法加速多关键字查询.

随着云计算技术的发展,多关键字搜索问题受到了学术界和工业界的广泛关注,促使多关键搜索技术在多个领域得到了全面应用,如基于位置的服务[22-24]、智慧医疗[25]、智慧城市[26]、智能交通[27]等.云计算环境下的多关键字搜索主要聚焦于如何构建有效索引,使得基于多关键字的加密索引和查询陷门能够正确匹配.多关键字搜索作为一种密文查询技术,能够根据用户的查询请求,在海量、异构、复杂数据中,查找到与之匹配的索引[16].近年来,已有较多的工作研究了云计算环境下的多关键字搜索问题.Wang等人[28]基于对称隐向量加密算法和位映射方法,将多关键字搜索问题转换为二进制向量匹配问题,提出了一种安全高效的基于空间关键字的布尔范围查询方案.Zheng等人[29]基于R-tree和矩阵加密技术提出了一种多关键字范围查询方案.Shu等人[30]基于矩阵变换和多项式函数性质,设计了一种多关键字任务推荐方案,实现了高效的任务匹配.Song等人[31]利用矩阵相似性和对称谓词加密算法,提出了一种众包环境下基于多关键字和位置的任务匹配方案.一旦多关键字维度过高时,密文查询效率将会受到极大限制.为了解决多关键字密文搜索效率低等问题,本研究团队基于对称谓词加密和向量聚合方法,将多关键字前缀相同的向量聚合为一个向量,提出了一种基于车载众包的多关键字任务匹配方案,实现了高效的任务匹配.此外,针对多关键字搜索中存在的用户非法访问和搜索效率低等问题,本研究团队提出了一种基于多项式函数和几何范围查询的空间关键字搜索方案,实现了轻量级的访问控制和高效的多关键字搜索[32].空间关键字搜索技术框架如图3所示.

空间关键字搜索主要包含8个阶段:在几何范围索引构建(GRQ.IndexBuild)阶段,数据拥有者根据空间位置集构建索引,并将位置索引发送给云服务器,用于几何范围查询;在范围查询陷门生成(GRQ.TrapGen)阶段,数据使用者根据拟合曲线的范围生成相应的陷门,并提交至云服务器;在几何范围查询(GRQ.Query)阶段,云服务器根据位置索引,匹配与范围陷门对应的位置;在空间关键字索引构建(MSSAC.IndexBuild)阶段,数据拥有者根据几何范围查询匹配到的位置,提取出该位置对应的空间关键字,并构建多关键字索引;在空间关键字陷门生成(MSSAC.TrapGen)阶段,数据使用者根据查询请求中的多关键字,生成查询陷门,并发送给云服务器;云服务器收到空间关键字查询请求后,首先对该用

户进行基于角色的访问认证,一旦该用户角色满足访问控制策略,则云服务器执行空间关键字搜索(MSSAC.Query);最后,云服务器将搜索得到的密文结果返回给通过认证的用户,该用户可以利用对称密钥解密该密文.

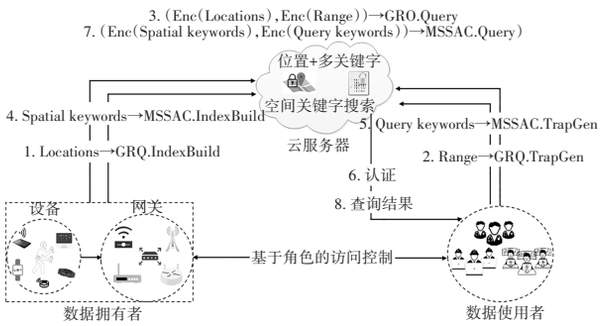

图3　空间关键字搜索技术框架图

Fig.3　Framework of spatial keyword query

2　密文分享

2.1　云计算中公钥加密方法

为保障云计算中数据安全和隐私,防止数据被非授权访问,用户可对外包数据进行加密保护.传统的公钥证书加密要求由一个公钥证书机构管理所有用户的公钥证书,数据所有者在加密数据前,需向公钥证书机构请求数据使用者的公钥证书.在云环境中,用户规模可能达到十万、百万数量级,传统公钥证书加密技术将导致高昂的证书管理开销.为解决公钥证书管理问题,Boneh 和 Franklin[33]于 2001 年提出了首个身份基加密方案,用户可以使用任意字符串(比如电子邮箱地址、手机号码)作为公钥,而无需再向第三方申请公钥证书.Boneh 和 Franklin 的研究成果使身份基加密技术迅速成为密码学领域的研究热点,各种身份基加密技术及扩展被不断提出,如层次身份基加密[34]、匿名身份基加密[35]、身份基广播加密[36]、身份基格式保护加密[37]、可穿刺身份基加密[38],等等.

传统公钥加密及身份基加密技术要求用户在加密时指定数据访问者,但在云环境中,数据访问者的身份往往不能预先确定.为解决这类问题,Sahai 和 Waters 提出了属性基加密方法[39],只有属性满足预定义访问控制策略的请求者才能访问数据.Goyal 等人[40]将属性基加密方法分为两类:密文策略属性基加密和密钥策略属性基加密.在密文策略属性基加密方法中,访问控制策略与密文关联,密钥与多个属性关联,用户能否解密密文的判断条件是其密钥关联的属性集合能否满足密文关联的访问控制策略.图 4 所示为密文策略属性基加密在云计算环境中的典型应用.数据所有者指定访问控制策略并利用该策略加密数据,然后将密文上传至云服务器;数据使用者从云服务器处下载密文,并且如果其密钥关联的属性集合满足数据所有者指定的访问控制策略,则可以解密密文.在密钥策略属性基加密方法中,访问控制策略与密钥关联,密文与属性集关联,如果密文的属性集满足密钥的访问控制策略,则该密钥可以解密密文.

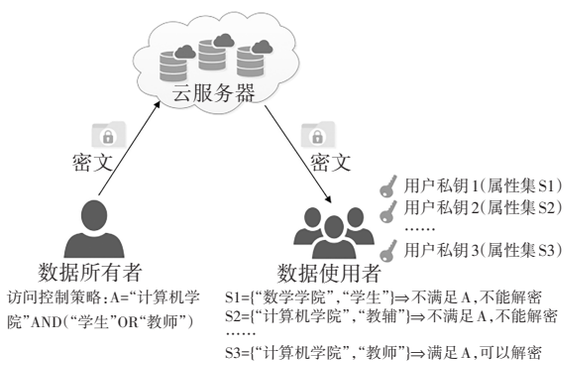

图4　密文策略属性基加密示例

Fig.4　An example of cipher text-policy attribute-based encryption

为提高属性基加密的安全性并减少密文或密钥存储开销,Attrapadung[41]提出了具有固定长度密文(密钥)的适应性安全密钥(密文)策略属性基加密方案.适应性安全是指在安全性模型中,敌手可以在获取系统公开参数以及选择的用户密钥之后才公布要攻击的访问控制结构(在密文策略属性基加密中)或者是属性集合(在密钥策略属性基加密中).基于上述安全性模型被证明安全的属性基加密方案具有较高的安全性,称之为适应性安全.但是,方案[41]是基于合数阶双线性群构造,因而算法运行效率比基于素数阶群构造的方案要低.为此,Attrapadung[42]提出了一种在素数阶双线性群中构造适应性安全属性基加密的方法,既保证较高安全性又提高了算法的效率.在属性基加密中,属性是构造密文和密钥的关键元素,有的属性基加密方案要求在系统初始化时设置好系统中所有的属性名称以及数量,这对于一些对属性使用灵活度要求较高的应用不太实际.为此,Chen 等人[43]提出了一种 large-universe 的属性基加密方法.在这种方法中,系统初始化时不设定属性及其数量,用户在加密时可以使用任意字符串作为属性来加密数据,这样一来,既提高了用户加密的灵

活程度,又减少了系统公开参数的存储空间.针对属性基加密中授权机构权力过大问题,Datta 等人[44]提出了一种多授权机构的属性基加密方案,任何用户都可生成自己的密钥.

2.2 云计算中密文分享方法

上述公钥加密方法虽然很好保护了数据隐私,但限制了数据的进一步共享.当出现加密时,未指定的用户申请访问数据会因其没有密钥而无法访问.代理重加密(Proxy re-encryption, PRE)技术可以解决云计算中的密文分享问题.基于代理重加密技术,数据所有者可以在不解密密文的情况下,授权代理(云服务提供商)将当前公钥下的密文转换成在新的公钥下的密文,并且不泄露有关明文的任何信息.这样一来,当有新用户(加密时未指定的用户)请求访问云端的加密数据时,数据所有者可以授权云服务器将密文转换成新用户公钥下的密文,使得新用户可以直接使用自身密钥访问数据.

Blaze 等人[45]设计了第一个代理重加密方案.Ateniese 等人[46]指出文献[45]中的代理重加密方案是双向的,即代理既能转换数据所有者的密文,也能转换指定用户的密文,因而不能保障指定用户的数据安全.Li 等人[47]提出了一种单向多跳的代理重加密方法,代理只能转换数据所有者的密文,且该密文可以被多次转换.为了控制密文被分享的次数,Cao 等人[48]设计了密文转换次数和路径可由数据所有者预先指定的单向代理重加密方法,将密文分享限制在一定范围内.针对代理重加密中的密钥泄露问题,Ge 等人[49]提出了一种可撤销代理重加密技术,允许代理撤销用户指定的访问者对转换密文的解密权限,保证密钥泄露情况下的数据安全.Fuchsbauer 等人[50]提出了一种适应性安全的代理重加密方案,允许敌手在获取公开参数及重加密密钥之后再公布其攻击目标,因而更符合真实的攻击场景.

在云计算中,数据所有者可能只想将一部分加密数据与其他用户共享,而传统代理重加密只能一次性分享所有的密文,安全性和灵活性均不太高.基于条件的代理重加密允许用户根据条件选择部分密文进行共享,使得指定用户只能访问符合预定义条件的数据.Xu 等人[51]提出了广播条件代理重加密方法,允许用户同时向多个授权访问者分享所选择的数据.Ge 等人[52]提出了一种细粒度的条件代理重加密方法,密文能否被转换不再是判断密文关联的条件是否与重加密密钥的条件相等,而是判断密文是否适用于重加密密钥关联的访问控制结构.Liang 等人[53]提出了一种属性基代理重加密方案,并且在标准模型下基于错误学习(Learning With Errors)假设证明了方案的安全性,因而可以抵抗量子攻击.云计算中用户众多,不同用户可能使用不同的加密系统上传和访问数据,如何将一种加密系统下的密文转换为另一个加密系统下的密文是更为困难的挑战.Jiang[54]等人提出了一种在传统公钥加密和身份基加密之间进行双向密文转换的方法,但是该方法要求可信第三方为每次转换生成一个转换密钥,当重加密并发数较高时会造成系统性能瓶颈.Döttling 和 Nishimaki 提出了一种通用代理重加密方案[55],可以将密文转换成另一种加密系统的密文,但是该方案依赖概率不可区分混淆函数和混淆电路,因而其算法复杂度较高.

针对云计算环境中密文高效分享问题,本文作者研究团队提出了跨密码系统的代理重加密方法,该方法通过重加密技术桥接两种不同的密码系统,使得用户可以访问被不同加密系统保护的数据[56].以身份基加密系统和身份基广播加密为例,数据所有者可以使用身份基加密系统加密数据,使得数据只能被自己或者一个授权用户访问.当需要将数据分享给更多的用户时,数据所有者可以生成转换密钥并把该密钥发送给云服务器;云服务器使用转换密钥将数据所有者的身份基加密密文转换为身份基广播加密密文,使得多个指定用户可以使用自身私钥解密.在生成转换密钥过程中,数据所有者可以指定一个分享策略,使得只有满足该策略的密文才能被转换.这样一来,数据所有者可以更加灵活地分享自己的加密数据.基于身份基加密和身份基广播加密的代理重加密系统框架如图5所示.

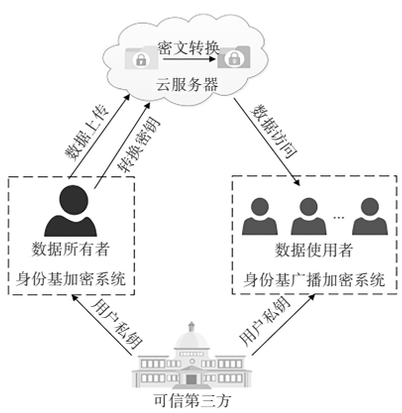

图5 跨密码系统密文分享系统框架

Fig.5 System model of cross-cryptosystem ciphertext sharing

1)初始化阶段.可信第三方基于双线性对 $e:G\times$

$G\rightarrow G_T$生成身份基加密系统与身份基广播加密系统的公开参数:PP=(g^a, u, u^a, h, h_1, h_2, …, h_m, $e(g, h)$),其中h_i表示h的a^i次方;以及系统主私钥: MSK=(g, a).

2)用户注册.对身份基加密系统和身份基广播加密系统中的用户,可信第三方根据用户的唯一身份标识ID生成用户私钥:$SK_{ID}=g^{1/(a+ID)}$.

3)数据上传.数据所有者使用身份标识加密j明文M,并将密文$C=(C_0, C_1, C_2)$存储在云服务器中,其中:$C_0=Me(g,h)^s$,$C_1=h^{s(a+ID)}$,$C_2=u^{s(a+ID)}$.

4)转换密钥生成.数据所有者指定分享策略,并利用自身私钥以及新指定接收者身份标识集合生成转换密钥,并将该密钥发送给云服务器.简单起见,假设数据所有者想将所有密文分享给身份标识集$S=\{ID1,ID2,\cdots,IDn\}$中的用户,计算:

$d_1=(g^a)^{-t}$, $d_2=(h^{(a+ID1)}h^{(a+ID2)}\cdots h^{(a+IDn)})^t$

$d_3=H(e(g,h)^t)h^r$,$d_4=SK_{ID}u^{-r}$,

其中H表示从群G_T到G的哈希函数.数据所有者将转换密钥$TK=(d_1,d_2,d_3,d_4)$发给云服务器.

5)密文转换.云服务器将密文$C=(C_0, C_1, C_2)$转换成身份基广播加密密文$C'=(C'_1, C'_2, C'_3, C'_4, C'_5)$,其中$C'_1=d_1$, $C'_2=d_2$, $C'_3=d_3$, $C'_4=d_4$, $C'_5=C_0/e(C_1,d_4)$.

6)数据访问.新指定的数据使用者下载广播加密密文,并使用自身私钥解密.对于密文$C'=(C'_1, C'_2, C'_3, C'_4, C'_5)$,集合$S$中的用户ID$i$计算:$A_1=\prod_{j=1,j\neq i}IDj$, $A_2=\prod_{j=1,j\neq i}(a+IDj)$,以及$B=(e(C'_1, h^{\Delta})e(SK_{IDi}, C'_2))^{1/A1}$,其中$h^{\Delta}=1/a(A_2-A_1)$;最后计算$h^r=C'_3/H(B)$,恢复明文$M=C'_5/e(h^r, C'_4)$.

除了实现身份基密文到身份基广播密文的转换外,本研究团队还构造了属性基加密密文到身份基加密密文的转换方法.该方法主要适用于移动数据访问场合,针对移动设备资源受限问题,将复杂的属性基密文转换为简单的身份基密文,使移动设备无需进行属性基解密运算也可访问加密数据.同时,该方法也支持更大范围的密文分享,数据所有者可以将属性基加密数据分享给除最初指定接收者之外的更多用户.

3　差分隐私

3.1　云计算数据相关性隐私保护

云计算环境下数据的相关性可引发数据隐私泄露[57].现有的相关性隐私保护工作聚焦于自相关性引发的隐私泄露问题,主要分为两大类:一类是自相关性差分隐私保护方法;另一类是互相关性差分隐私保护方法.

一方面,专家学者运用具有严格数学定义的差分隐私框架,提出优秀的时序大数据中自相关性隐私保护方法.首先,在自相关性量化的基础上,Chen等人[58]运用长度可变的n-grams模型,构建时序数据的自相关性,实现差分隐私保护.吴云乘等人[59]采用马尔可夫链模拟用户真实位置间自相关性,分析真实数据的先验概率和后验概率间的关系,实现差分隐私保护.霍峥和孟小峰[60]则运用四分树和R树,在自由空间和路网空间上实现拉普拉斯机制.其次,在没有量化相关性的情况下,于东和康海燕[61]结合固定抽样法和Kalman过滤技术,实现基于抽样过滤技术的差分隐私保护.Wang和Xu[62]运用高斯白噪声,提出差分隐私保护的时序数据发布方法.Cao等人[63-64]提出时空相关性的差分隐私保护方法,以实现增强的差分隐私保护时序数据发布.Bassily等人[65]提出一个称为“耦合世界的隐私(coupled-worlds privacy)”的框架,要求一个实体的参与与否不会带来任何影响,并且数据分布被认为是满足特定分布.为提高隐私保护方法的数据可用性,本研究团队结合奇异谱分析、傅立叶变换以及拉格朗日乘数法,提出电力数据差分隐私保护方法[66]和轨迹数据差分隐私保护方法[67].最后,对于时序数据的聚集,研究人员提出了一些基于差分隐私保护框架的数据发布方法[68-69].

另一方面,数据收集中心可把所有数据发布给云服务提供商,以便实现不同的应用服务,如监控、决策等.半可信的云服务提供商可访问数据收集中心所发布的时序数据,并且可能会挖掘数据间互相关性,进而敌手可推断出社交关系等敏感信息.针对此类问题,本研究团队[70]结合傅立叶变换、约束优化和拉普拉斯机制等,提出可隐藏社交关系的时序数据隐私保护方法——互相关性差分隐私保护(Cross-correlated Differential Privacy,CDP),在实现隐私保护的同时,确保数据可用性最佳.CDP方法步骤描述如下所示.

1)执行CDP框架:假设D和δD_k分别表示单个个体的时间序列数据D的第k个原始傅立叶系数及其对应的噪声,那么CDP框架为:$D_k'=D_k+\delta D_k$,其中$k=0, 1, \cdots, N-1$;噪声同时包含实部和虚部,即$\delta D_k=\delta D_k^r+j\delta D_k^i$,j为虚数单位,上标r,i分别表示实部和虚部.

2)生成互相关的噪声:分别在两个个体u和v的

时间序列数据记录的傅立叶系数上所添加的噪声：

$\delta(D_{k+k'})^{\mathrm{corr}(u)}$和$\delta(D_{k'})^{\mathrm{corr}(v)}$，

满足：$E\{\delta(D_{k+k'})^{\mathrm{corr}(u)}(\delta(D_{k'})^{\mathrm{corr}(v)})^{*}\}=C_k$，其中$(\cdot)^{*}$表示共轭计算.

3.2 深度学习中数据隐私保护

深度学习中数据隐私保护问题引起了专家学者的广泛关注.2015年，Shokri等人[71]提出了具有隐私保护的分布式深度学习框架，在此框架中，各参与方分布式地独立地训练各自的模型，并且有选择地分享其模型参数的子集.2016年，Phan等人[72]运用拉普拉斯机制，在目标函数上添加噪声，发布最小化的添加噪声后的目标函数，输出差分隐私保护的模型.Abadi等人[73]提出一个差分隐私保护的随机梯度下降方法，以确保输出模型的隐私保护.然而，在随机梯度下降方法的迭代计算过程中，会造成累积的隐私损失.为解决此类问题，Yu等人[74]运用集中式差分隐私保护方法(Concentrated Differential Privacy，CDP)，分析各个数据批处理方法的隐私损失，研发隐私账目方法，并提出差分隐私保护的训练方法，以实现隐私预算的动态分配.Li等人[75]研究基于长短期记忆网络的股票价格预测中隐私泄露问题，在复合分数中添加高斯噪声，确保训练模型的隐私保护.

4 总结与展望

本文围绕云计算环境下数据安全与隐私保护问题，指出保证数据安全与隐私的重要方法是加密和差分隐私保护，并进一步从密文查询、密文分享和差分隐私三个方面阐述云计算数据安全与隐私保护的国内外研究现状；然后，重点介绍了本研究团队提出的空间关键字密文查询技术和跨密码系统的细粒度密文分享技术，并给出了主要研究思路.然而，目前云计算环境下数据安全与隐私保护还有一些问题尚待解决，例如，针对用户位置和关键字动态更新的空间多关键字搜索、前向安全与后向安全的多关键字可搜索加密、适应性安全的跨密码系统密文分享，以及高可用性的差分隐私保护技术等.本研究团队将在现有基础上，研究如何进一步解决上述问题.

参考文献

[1] 胡志刚，肖慧，李克勤.云计算中基于多目标优化的虚拟机整合算法[J].湖南大学学报(自然科学版)，2020，47(2)：116-124.
HU Z G，XIAO H，LI K Q. Virtual machine consolidation algorithm based on multi-objective optimization in cloud computing [J]. Journal of Hunan University (Natural Sciences)，2020，47(2)：116-124.(In Chinese)

[2] 张玉清，王晓菲，刘雪峰，等.云计算环境安全综述[J].软件学报，2016，27(6)：1328-1348.
ZHANG Y Q，WANG X F，LIU X F，*et al*. Survey on cloud computing security[J].Journal of Software，2016，27(6)：1328-1348.(In Chinese)

[3] SONG D X，WAGNER D，PERRIG A. Practical techniques for searches on encrypted data[C]//Proceeding 2000 IEEE Symposium on Security and Privacy. Berkeley，CA，USA：IEEE，2000：44-55.

[4] CHANG Y C，MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[C]//Applied Cryptography and Network Security. 2005：DOI：10.1007/11496137_30.

[5] CURTMOLA R，GARAY J，KAMARA S，*et al*. Searchable symmetric encryption：improved definitions and efficient constructions [C]//Proceedings of the 13th ACM conference on Computer and communications security-CCS′06. New York：ACM Press，2006：79-88.

[6] KAMARA S，PAPAMANTHOU C，ROEDER T. Dynamic searchable symmetric encryption[C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security-CCS ′12. New York：ACM Press，2012：965-976

[7] KAMARA S，PAPAMANTHOU C. Parallel and dynamic searchable symmetric encryption[C]//Financial Cryptography and Data Security. 2013：DOI：10.1007/978-3-642-39884-1_22.

[8] HAHN F，KERSCHBAUM F. Searchable encryption with secure and efficient updates[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York：ACM，2014：310 - 320.

[9] ZHANG Y P，KATZ J，PAPAMANTHOU C. All your queries are belong to us：the power of file-injection attacks on searchable encryption[C]//SEC′16：Proceedings of the 25th USENIX Conference on Security Symposium.2016：707-720.

[10] BOST R. $\sum o\varphi o\varsigma$：Forward secure searchable encryption[C]// Proceedings of the ACM Conference on Computer and Communications Security. 2016：1143-1154.

[11] KIM K S，KIM M，LEE D，*et al*. Forward secure dynamic searchable symmetric encryption with efficient updates[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York：ACM，2017：1449-1463.

[12] SONG X F，DONG C Y，YUAN D D，*et al*. Forward private searchable symmetric encryption with optimized I/O efficiency[J].IEEE Transactions on Dependable and Secure Computing，2020，17(5)：912-927.

[13] BONEH D，CRESCENZO G，OSTROVSKY R，*et al*. Public key encryption with keyword search [C]//Advances in Cryptology - EUROCRYPT 2004. 2004：DOI：10.1007/978-3-540-24676-3_30.

[14] XU P，JIN H，WU Q H，*et al*. Public-key encryption with fuzzy keyword search：a provably secure scheme under keyword guessing attack[J].IEEE Transactions on Computers，2013，62(11)：2266-2277.

[15] YIN H，QIN Z，ZHANG J X，*et al*. Secure conjunctive multi-keyword ranked search over encrypted cloud data for multiple data owners [J]. Future Generation Computer Systems，2019，100：689-700.

[16] LYU F, REN J, CHENG N, *et al*. LeaD: large-scale edge cache deployment based on spatio-temporal WiFi traffic statistics [J]. IEEE Transactions on Mobile Computing, 2021, 20(8): 2607-2623.

[17] CAO N, WANG C, LI M, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data [C]//IEEE Transactions on Parallel and Distributed Systems.IEEE, 2011: 222-233.

[18] CAO N, WANG C, LI M, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data [J].IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 222-233.

[19] XU Z Y, KANG W S, LI R X, *et al*. Efficient multi-keyword ranked query on encrypted data in the cloud [C]//2012 IEEE 18th International Conference on Parallel and Distributed Systems. Singapore: IEEE, 2012: 244-251.

[20] FU Z J, REN K, SHU J G, *et al*. Enabling personalized search over encrypted outsourced data with efficiency improvement [J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(9): 2546-2559.

[21] XIA Z H, WANG X H, SUN X M, *et al*. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data [J].IEEE Transactions on Parallel and Distributed Systems, 2016, 27(2): 340-352.

[22] HUANG H S, GARTNER G, KRISP J M, *et al*. Location based services: ongoing evolution and research agenda [J].Journal of Location Based Services, 2018, 12(2): 63-93.

[23] 杨柳,唐卓,朱敏,等.基于风险的云计算环境用户效用分析[J].湖南大学学报(自然科学版),2011,38(7):78-82.
YANG L, TANG Z, ZHU M, *et al*. Analysis of user utility in cloud computing environment based on risk [J]. Journal of Hunan University (Natural Sciences), 2011, 38(7): 78-82. (In Chinese)

[24] ZHANG S B, MAO X J, CHOO K K R, *et al*. A trajectory privacy-preserving scheme based on a dual-K mechanism for continuous location-based services [J]. Information Sciences, 2020, 527: 406-419.

[25] ZHENG Y D, LU R X, GUAN Y G, *et al*. Towards private similarity query based healthcare monitoring over digital twin cloud platform [C]//2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS). Tokyo: IEEE, 2021: 1-10.

[26] XIE J F, TANG H, HUANG T, *et al*. A survey of blockchain technology applied to smart cities: research issues and challenges [J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2794-2830.

[27] WONG W K, CHEUNG D W L, KAO B, *et al*. Secure kNN computation on encrypted databases [C]//Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2009: 139-152.

[28] WANG X Y, MA J F, LIU X M, *et al*. Search me in the dark: privacy-preserving Boolean range query over encrypted spatial data [C]//IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. Toronto: IEEE, 2020: 2253-2262.

[29] ZHENG Y D, LU R X, GUAN Y G, *et al*. Efficient and privacy-preserving similarity range query over encrypted time series data [J]. IEEE Transactions on Dependable and Secure Computing, 2021. DOI: 10.1109/TDSC.2021.3061611.

[30] SHU J G, JIA X H, YANG K, *et al*. Privacy-preserving task recommendation services for crowdsourcing [J] . IEEE Transactions on Services Computing, 2021, 14(1): 235-247.

[31] SONG F Y, QIN Z, LIU D X, *et al*. Privacy-preserving task matching with threshold similarity search via vehicular crowdsourcing [J]. IEEE Transactions on Vehicular Technology, 2021, 70(7): 7161-7175.

[32] SONG F Y, QIN Z, XUE L, *et al*. Privacy-preserving keyword similarity search over encrypted spatial data in cloud computing [J]. IEEE Internet of Things Journal, 2021. DOI: 10.1109/JIOT.2021.3110300.

[33] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]// Proceedings of the Annual International Cryptology Conference. 2001: 213-229.

[34] LANGREHR R, PAN J X. Tightly secure hierarchical identity-based encryption [J]. Journal of Cryptology, 2020, 33(4): 1787-1821.

[35] BRAKERSKI Z, LOMBARDI A, SEGEV G, *et al*. Anonymous IBE, leakage resilience and circular security from new assumptions [C]// Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2018: 535-564.

[36] KIM J, SUSILO W, AU M H, *et al*. Adaptively secure identity-based broadcast encryption with a constant-sized cipher text [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 679-693.

[37] BELLARE M, HOANG V T. Identity-based format-preserving encryption [C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 1515-153.

[38] WEI J, CHEN X, WANG J, *et al*. Forward-secure puncturable identity-based encryption for securing cloud emails [C]// Proceedings of the European Symposium on Research in Computer Security. 2019: 134-150.

[39] SAHAI A, WATERS B. Fuzzy identity-based encryption [C]// Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005: 457-473.

[40] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data [C]//Proceedings of the 13th ACM conference on Computer and communications security - CCS '06. New York: ACM Press, 2006: 89-98.

[41] ATTRAPADUNG N. Dual system framework in multilinear settings and applications to fully secure (compact) ABE for unbounded-size circuits [C]//Public-Key Cryptography - PKC 2017.DOI: 10.1007/978-3-662-54388-7_1.

[42] ATTRAPADUNG N. Dual system encryption framework in prime-order groups via computational pair encodings [M]//Advances in Cryptology - ASIACRYPT 2016.Berlin: Springer Berlin Heidelberg, 2016: 591-623.

[43] CHEN J, GONG J Q, KOWALCZYK L, *et al*. Unbounded ABE via bilinear entropy expansion, revisited [M]//Advances in Cryptology-EUROCRYPT 2018. Cham: Springer International Publishing, 2018: 503-534.

[44] DATTA P, KOMARGODSKI I, WATERS B. Decentralized multi-authority ABE for DNFs from LWE [M]//Lecture Notes in Computer Science. Cham: Springer International Publishing. 2021: 177-209.

[45] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography [M]//Lecture Notes in Computer Science. Berlin: Springer Berlin Heidelberg, 1998: 127-144.

[46] ATENIESE G, FU K, GREEN M, *et al*. Improved proxy re-

encryption schemes with applications to secure distributed storage [J]. ACM Transactions on Information and System Security, 2006, 9(1):1-30.

[47] LI Z P, MA C G, WANG D. Achieving multi-hop PRE via branching program [J]. IEEE Transactions on Cloud Computing, 2020, 8(1):45-58.

[48] CAO Z F, WANG H B, ZHAO Y L. AP-PRE: autonomous path proxy Re-encryption and its applications [J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(5):833-842.

[49] GE C P, LIU Z, XIA J Y, *et al*. Revocable identity-based broadcast proxy re-encryption for data sharing in clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1214-1226.

[50] FUCHSBAUER G, KAMATH C, KLEIN K, *et al*. Adaptively secure proxy re-encryption[C]// Proceedings of the IACR International Workshop on Public Key Cryptography. 2019: 317-346.

[51] XU P, JIAO T F, WU Q H, *et al*. Conditional identity-based broadcast proxy re-encryption and its application to cloud email [J]. IEEE Transactions on Computers, 2016, 65(1):66-79.

[52] GE C P, SUSILO W, WANG J D, *et al*. Identity-based conditional proxy re-encryption with fine grain policy[J]. Computer Standards & Interfaces, 2017, 52:1-9.

[53] LIANG X, WENG J, YANG A, *et al*. Attribute-based conditional proxy re-encryption in the standard model under LWE[C]// Proceedings of the European Symposium on Research in Computer Security. 2021: 147-168.

[54] JIANG P, NING J T, LIANG K T, *et al*. Encryption switching service: securely switch your encrypted data to another format [J]. IEEE Transactions on Services Computing, 2021, 14(5):1357-1369.

[55] DöTTLING N, NISHIMAKI R. Universal proxy re-encryption [C]// Proceedings of the IACR International Conference on Public-Key Cryptography. 2021: 512-542.

[56] DENG H, QIN Z, WU Q H, *et al*. Identity-based encryption transformation for flexible sharing of encrypted data in public cloud [J]. IEEE Transactions on Information Forensics and Security, 2020, 15:3168-3180.

[57] LI Y N, REN X B, YANG S S, *et al*. Impact of prior knowledge and data correlation on privacy leakage: a unified analysis[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(9): 2342-2357.

[58] CHEN R, ACS G, CASTELLUCCIA C. Differentially private sequential data publication via variable-length n-grams [C]//Proceedings of the 2012 ACM conference on Computer and Communications Security-CCS'12. New York: ACM Press, 2012:638-649.

[59] 吴云乘,陈红,赵素云,等.一种基于时空相关性的差分隐私轨迹保护机制[J].计算机学报,2018,41(2):309-322.
WU Y C, CHEN H, ZHAO S Y, *et al*. Differentially private trajectory protection based on spatial and temporal correlation[J]. Chinese Journal of Computers, 2018, 41(2):309-322.(In Chinese)

[60] 霍峥,孟小峰.一种满足差分隐私的轨迹数据发布方法[J].计算机学报,2018,41(2):400-412.
HUO Z, MENG X F. A trajectory data publication method under differential privacy [J]. Chinese Journal of Computers, 2018, 41(2):400-412. (In Chinese)

[61] 于东,康海燕.面向时序数据发布的隐私保护方法研究[J].通信学报,2015,36(S1):243-249.
YU D, KANG H Y. Privacy protection method on time-series data publication [J]. Journal on Communications, 2015, 36(S1):243-249. (In Chinese)

[62] WANG H, XU Z Q. CTS-DP: Publishing correlated time-series data via differential privacy [J]. Knowledge-Based Systems, 2017, 122:167-179.

[63] CAO Y, YOSHIKAWA M, XIAO Y, *et al*. Quantifying differential privacy in continuous data release under temporal correlations [J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 31(7):1281-1295.

[64] CAO Y, YOSHIKAWA M, XIAO Y H, *et al*. Quantifying differential privacy under temporal correlations[C]//2017 IEEE 33rd International Conference on Data Engineering (ICDE). San Diego: IEEE, 2017:821-832.

[65] BASSILY R, GROCE A, KATZ J, *et al*. Coupled-worlds privacy: exploiting adversarial uncertainty in statistical data privacy [C]// Proceedings of the 54th IEEE Annual Symposium on Foundations of Computer Science. Berkeley, 2013:439-448.

[66] OU L, QIN Z, LIAO S L, *et al*. Singular spectrum analysis for local differential privacy of classifications in the smart grid[J]. IEEE Internet of Things Journal, 2020, 7(6):5246-5255.

[67] OU L, QIN Z, LIAO S, *et al*. Releasing correlated trajectories: towards high utility and optimal differential privacy [J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(5): 1109-1123.

[68] YANG B, SATO I, NAKAGAWA H. Bayesian differential privacy on correlated data[C]// Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data. Melbourne, 2015: 747-762.

[69] NIU C Y, ZHENG Z Z, WU F, *et al*. Unlocking the value of privacy: trading aggregate statistics over private correlated data[C]// Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. New York: ACM, 2018: 2031-2040.

[70] OU L, QIN Z, LIAO S, *et al*. An optimal noise mechanism for cross-correlated IoT data releasing [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 1:1528-1540.

[71] SHOKRI R, SHMATIKOV V. Privacy-preserving deep learning [C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2015: 1310-1321.

[72] PHAN N, WANG Y, WU X T, *et al*. Differential privacy preservation for deep auto-encoders: an application of human behaviour prediction[C]//AAAI'16: Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence. 2016:1309-1316.

[73] ABADI M, CHU A, GOODFELLOW I, *et al*. Deep learning with differential privacy [C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016:308-318.

[74] YU L, LIU L, PU C, *et al*. Differentially private model publishing for deep learning[C]//2019 IEEE Symposium on Security and Privacy (SP). San Francisco: IEEE, 2019: 332-349.

[75] LI X, LI Y, YANG H, *et al*. DP-LSTM: differential privacy-inspired LSTM for stock prediction using financial news[C]// Proceedings of the 33rd Conference on Neural Information Processing Systems. Vancouver, Canada, 2019:1-9.