

基于属性加密的云存储隐私保护机制研究

冯涛, 殷潇雨

(兰州理工大学计算机与通信学院, 甘肃 兰州 730000)

摘要: 以典型的云存储体系结构为研究对象, 从数据拥有者、云服务器、授权机构、用户以及用户撤销机制5个方面对云存储系统的隐私保护机制进行了研究, 通过分析比较发现, 云存储系统中的隐私保护问题主要可以分为系统参与者的身份隐私问题、敏感属性信息泄露问题、云存储系统敏感内容信息泄露问题。针对上述问题, 研究了当前基于属性加密的云存储系统隐私保护机制, 并讨论了其中存在的不足、可能的解决方案以及未来可能的研究方向。

关键词: 云存储; 隐私保护; 属性加密; 访问结构; 撤销机制

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00070

Research on privacy preserving mechanism of attribute-based encryption cloud storage

FENG Tao, YIN Xiao-yu

(School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730000, China)

Abstract: The typical cloud storage architecture was presented as research objects and the privacy preserving mechanism of attribute-based encryption cloud storage including following aspects-data owner, cloud servers, authorized agency, data user and revocation of user was researched. By analyzing and comparing, it was discovered that the privacy preserving problems of cloud storage could be divided into privacy issues of users' identity, sensitive attribute information disclosure and leakage of privacy content in the system. Aiming at the above problems, the current privacy preserving mechanism of attribute-based encryption cloud storage was studied and shortages of the present schemes, possible solutions and the study trend in the future were discussed.

Key words: cloud storage, privacy preserving, attribute-based encryption, access structures, revocation mechanism

1 引言

云存储是云计算概念的延伸, 是一个以数据存储和管理为核心的云计算系统。随着数据共享的需求日益增加, 越来越多的人开始使用云存储技术, 大量的数据被存储到云平台, 云存储下的数据保密及使用者的隐私问题也随之出现。如何实现使用者身份和敏感数据的隐私保护成为云存

储中的关键问题。

属性加密作为一种适用于云存储的加密机制, 可以在数据分享过程中实现隐私保护机制。为了保护使用者的隐私、敏感数据不被泄露, 研究人员已经针对云存储系统中不同的参与实体提出了很多属性加密方案。例如, 文献[1, 2]中的方案强调了使用者的隐私保护问题; 文献[3]针对不完全可信的服务器采取隐私保护机制, 实现了内

收稿日期: 2016-06-02; 修回日期: 2016-06-27。通信作者: 冯涛, fengt@lut.cn

基金项目: 国家自然科学基金资助项目 (No.61462060, No.61562059)

Foundation Item: The National Natural Science Foundation of China (No.61462060, No.61562059)

容信息保密以及用户匿名访问;文献[4, 5]则实现了安全的用户权限撤销机制。

基于属性加密的云存储系统已经成为云存储系统研究领域的热点问题,并逐渐形成了以密文策略属性加密算法为核心的云存储体系结构。本文以典型的云存储体系结构模型为研究对象,从数据拥有者、数据使用者、多授权中心、云计算服务器以及用户访问权限撤销机制5个方面研究了云存储系统的隐私保护机制。本文研究了当前基于属性加密的云存储方案,通过分析比较发现,云存储系统中的隐私保护问题可以分为系统参与者的身份隐私问题、敏感属性信息泄露问题、云存储系统敏感内容信息泄露问题,针对研究人员对上述3类问题的解决思路,分析了当前基于属性加密的云存储系统隐私保护机制,讨论了方案中存在的不足、可能的解决方案以及未来可能的研究方向。

2 云存储与属性加密

2.1 属性加密

为了解决传统加密机制中需要真实公钥证书的难题,Shamir^[6]提出了基于身份的加密机制,以用户的身份作为公钥加密,Sahai和Waters^[7]在身份加密(IBE, identity-based encryption)技术的基础上提出了属性加密(ABE, attribute-based encryption)机制。属性加密是一种新兴的公钥加密机制,与传统的公钥机制不同,属性加密不再以个人身份作为公钥进行加密,而是引入属性的概念,以群属性作为群体的公钥,将原始的一对一加密机制变为一对多加密机制。属性加密机制以数据消费群体的群属性作为公钥加密,只有属性匹配的用户才能解密密文。但基本的属性加密方案很难实现对数据的细粒度访问控制,Goyal等^[8]提出基于密钥策略的属性加密(KP-ABE, key policy ABE)方案,由接收方制定访问结构,支持属性的与、或以及门限操作。Bethencourt等^[9]提出基于密文策略的属性加密(CP-ABE, ciphertext policy ABE)方案。密钥策略属性加密方案中密文与属性集合相关,密文策略的属性加密由数据拥有者制定访问结构,访问结构与密文相关,用

户私钥与属性集合相关。

上述属性加密方案都基于单一的授权机构,单一授权机构不可信且在受到攻击时会造成数据以及用户隐私的泄露。Chase^[10]最早提出多授权机构属性加密方案,将密钥管理、计算等分散给多个授权机构,这种机制解决了单一授权机构的缺陷,同时也带来了新的隐私安全问题,授权机构以及用户之间可能合谋,威胁数据、个人信息安全。Chase等^[10]第一次使用中心授权机构(CA, central authority)、用户唯一标识GID、伪随机函数解决了多授权中属性加密方案中的用户合谋问题;但是,可以解密任何密文的CA给系统增加了新的不安全因素,为避免CA带来的安全问题,Lin等^[11]基于DBDH假设提出无CA的多授权机构方案。

属性加密不仅可以实现云存储数据的加密,还可以实现数据的细粒度访问控制。属性加密有以下4个优点^[12]: 1) 数据拥有者只需根据属性进行加密,无需关注用户的数量和身份; 2) 只有符合属性要求的用户才能解密密文,实现数据保密; 3) 属性加密机制中的密钥与随机数相关,可以防止用户合谋攻击; 4) 支持灵活的访问结构,保证细粒度的访问控制。

2.2 基于属性加密的云存储系统

属性加密在云存储中的应用已经非常广泛,使用属性加密进行数据加密时不需要知道用户的具体身份,适用于用户身份不明确的云存储系统。但是,云存储中数据与所有者分离的模式仍然给属性加密方案的设计带来了极大挑战。近年来,研究人员已经提出了很多适用于云存储的属性加密方案^[13~18],基本实现了云存储中的安全数据分享,从最初的单一授权机构逐渐发展到多授权机构,云存储系统的效率及安全性得到了改善,大量的属性加密方案为以后的进一步研究奠定了坚实基础。

基于属性加密的云存储系统体系结构逐渐发展为如图1所示的体系结构模型。该体系结构一般有4种参与实体:数据拥有者、用户、云服务器(CS, cloud server)以及授权机构。在将数据上传到云服务器之前,数据拥有者制定访问结构并用访问结构对数据进行加密,然后

将加密数据上传到云服务器；云服务器主要负责密文的存储和分发，响应用户的密文请求；授权机构在早期方案中的具体名称不同，但都负责计算和分发密钥，授权机构又可分为中心授权机构和属性授权机构（AA, attribute authority），在多授权机构方案中，每个 AA 管理一个属性域；属性加密方案中用户负责发送密文请求以及密文请求，下载密文后满足访问结构的用户可以解密密文得到共享数据。

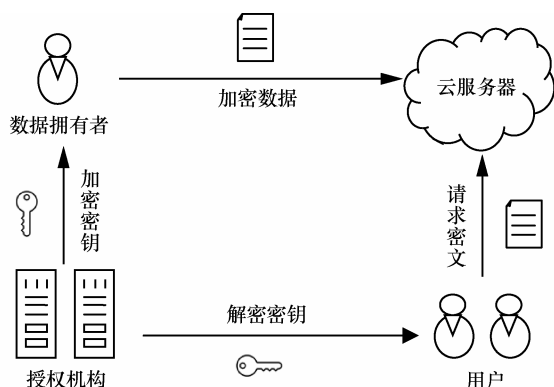


图1 基于属性加密的云存储系统体系结构模型

2.3 存在的隐私问题

目前，基于属性加密的云存储系统中仍然存在隐私泄露问题：1) 数据所有者制定的访问结构可能被不可信的云服务器窃取，造成身份、敏感信息泄露；2) 用户在请求密文或密钥时，需要提交的身份标识可能造成身份信息泄露；3) 系统中涉及到的服务器并不完全可信，存在合谋问题，用户的属性可能被合谋获取，威胁用户的隐私安全；4) 用户权限撤销作为实际应用中不可缺少的一部分，不安全的撤销机制可能严重威胁到系统安全，密钥泄露问题也需要妥善处理。

通过比较分析，本文将存在的隐私保护问题分为使用者的身份隐私问题、敏感数据泄露问题和撤销机制问题。云存储中涉及的隐私问题在一定程度上阻碍了云存储应用的推广，因此，完善系统中的隐私保护机制已经成为云存储研究中的热点问题。本文针对存在的问题从使用者、第三方服务器、撤销机制3个方面进行了归纳、比较，最后指出属性加密中隐私保护策略仍然存在的问题和未来研究的趋势。

3 使用者的隐私保护机制

随着云存储的应用越来越广泛，数据与数据拥有者分离的模式使数据拥有者不能控制已经外包的内容数据，数据和身份信息无法得到安全有效的保障。尽管属性加密可以在一定程度上保护外包数据，但属性加密中用户的身份由一系列属性决定，用户的身份信息很可能被恶意分析、窃取。

3.1 数据拥有者

云存储在发展的同时也延伸出了一些其他应用，例如，云医疗通过在云存储中建立病人完整的电子医疗档案，包括使用者的信息、病人病历数据等，实现了更加高效、快捷的医疗服务。但大量敏感信息存储在云端，如何实现完全的隐私保护成为研究的核心要点。

最早出现的隐私保护机制通过散列函数解决访问结构暴露的问题。例如，Li^[19]提出的方案将访问结构隐藏到密文中，方案中的每个属性可以有多个值，通过定义散列函数 H ，将第 i 个属性的第 k 个值映射为 0、1 这 2 部分，然后与 2 个不同的群生成器一起计算属性值的密文，实现隐藏策略。在解密阶段，定义一个二元关系判定用户属性列表是否满足访问结构，用户只能检查自己的属性列表是否匹配密文策略，不能知道访问结构中自己没有的属性。

在一般的云存储系统中，多数属性加密方案的访问结构都采用了属性名称与属性值分离机制。Ying^[20]在合数阶群上构造了半策略隐藏的属性加密方案。方案将属性分割成名称和属性 2 部分，属性值是始终被隐藏，即使更新属性值也不会造成隐私信息泄露，数据拥有者使用线性秘密共享方案（LSSS, linear secret sharing scheme）进行加密，属性值被隐藏不可见，但是访问结构是可见的，实现半策略隐藏。数据拥有者的信息改变时，云服务器负责密文访问结构的更新。数据加密者加密的密文分为密文部分和冗余部分，冗余部分匹配用户私钥中的属性，用户不能知道访问结构中的属性集合，实现隐私保护。Guan 等^[21]基于 CP-ABE 提出多授权机构访问控制方案，在方案中引入属性管理服务器（AMS）为用户属性分配属性授权机构。方案中数据拥有者将所有属

性按最小化原则分成 N 个不相交的组，每组有一个属性名称，组元素为属性名的值。访问树节点为属性名。这些分组由 AMS 分配给 N 个 AA 分别管理。云服务器上的属性以属性名形式存储，处理信息均使用属性名，用户请求密钥时，云服务器验证后向 AMS 申请密钥，AMS 将密钥计算任务交给响应 AA 计算密钥，密钥经由 AMS 和 CS 以密文的形式发送给用户，AMS 以及 CS 均不能获得密钥内容。方案防止了云服务器窃取数据以及属性信息，实现了隐私保护。

3.2 用户

用户在请求密钥时，需要提交属性信息以及身份标识，这种情况下很容易泄露隐私信息。Chase 等^[22]提出一种隐私保护的多授权机构 ABE 方案。方案中的匿名密钥分发协议（anonymous key issuing protocol）增强了对用户隐私的保护，用户与不同的 AA 交互时采用与绑定在同一私钥的多个别名，无需提交身份标识（GID），阻止了属性授权机构之间的合谋。用户请求私钥时，AA 通过不经意计算生成私钥，生成密钥不会暴露任何隐私信息。用户通过匿名密钥分发协议得到密钥对密文进行解密。

为了避免用户在密文请求时暴露身份信息，Xu 等^[23]提出基于 CP-ABE 的匿名云存储隐私保护方案，方案中拥有同一属性的所有用户以二叉树的形式构成一个群。方案引入注册机制，用户需要向云服务器请求注册并获得随机的身份标识 ID 序列；请求相同数据的用户将 k 个请求聚类计算，同态加密机制算法保证用户向云服务器提交请求时具有 k 匿名 l 多样性，系统中无需可信第三方，实现了用户访问匿名。

3.3 分析比较

从数据拥有者方面实现的隐私保护机制主要是对密文的访问结构进行隐藏，文献[19]通过散列函数对属性值进行加密，文献[20, 21]将属性分为属性名称和属性值 2 部分，实现了属性值隐藏，但是文献[20]为了实现动态的策略更新，访问结构是公开的，属于半隐藏策略。

文献[22]基于匿名证书的思想实现了用户密钥请求的隐私保护方案及用户 GID 隐藏；文献[23]引用了同态加密机制，不仅随机化了用户的 ID 且实现了密文请求匿名。多种加密机制的结合很好地实现了属性加密中的隐私保护策略。方案比较如表 1 所示。

4 第三方服务器的隐私保护机制

云存储在为用户带来便捷服务的同时也带来了相应的安全隐患，第三方服务器的恶意行为、黑客攻击、系统安全运维等都会导致用户数据的泄露。由于网络环境非常复杂且应用环境完全开放，云存储的安全性面临巨大的挑战^[24]。

4.1 云服务器

在复杂的网络环境中，盈利性的云服务器并不是完全可信的，数据拥有者不能完全依靠云服务器对数据进行访问控制，应该自己采取措施保护数据隐私，外包数据可能会因为服务器故障、内部工作人员非法窃取等问题被泄露，所以，在设计属性加密方案时，应该考虑云服务器对数据以及隐私造成的潜在威胁，保证方案的安全性。

Dong 等^[3]所提方案中的云服务器无需响应密文请求，只需根据用户列表分发密文，避免了用户的隐私泄露。方案基于密文策略的属性加密

表 1 使用者隐私保护方案比较

使用者	方案	隐私保护机制	解决的问题	访问结构	方案特点	困难问题	ABE 方案
数据拥有者	Li ^[19]	访问策略隐藏	敏感属性信息	树	用户可追责，访问结构隐藏	双线性群	CP-ABE
	Yin ^[20]	半隐藏	敏感属性信息	LSSS	动态访问策略更新，计算开销小	合数阶群	CP-ABE
	Guan ^[21]	访问结构隐藏	敏感属性信息	树	文件读写访问控制，密钥按需分配	素数阶群	CP-ABE
用户	Chase ^[22]	匿名密钥分发协议	身份隐私	树	无 CA，隐藏 GID	素数阶群	ABE
	Xu ^[23]	数据请求匿名	身份隐私	LSSS	同态加密机制，不可逆密钥更新	l -BDHE	CP-ABE

和身份加密,云服务器存储授权用户的ID列表,只负责存储、分配文件、分发密钥,不能知道任何的存储数据及隐私信息,实现完全隐私保护。数据拥有者为用户分配属性集合并为每个属性生成私钥,使用用户ID对私钥进行加密并通过云服务器分发,每个用户的私钥组合唯一且互不相同。方案中数据拥有者制定访问结构并且生成用户解密所需的私钥,其中,消费者的ID作为公钥对私钥进行加密,云服务器无法得到任何隐私信息,避免了云服务器造成的隐私泄露问题。

数据分割技术实现了云服务器对数据的分块存储。Shi等^[25]提出数据分割的CP-ABE机制,方案中数据加密者使用线性数据分割方法将上传数据进行分割,小数据块用CP-ABE加密,大数据块使用一般的加密方法加密,只有通过验证的用户才可以解密小数据块并进行数据拼合,方案中云服务器存储的是数据块,无法获取数据信息,云服务器只负责验证用户是否满足小的数据块,避免了数据泄露,保护了数据机密性。Xu^[26]的方案同样进行了数据分割,数据被分为大、小两块,小的数据块作为对称密钥加密大的数据块后上传,同样实现了云服务器的分块存储。

目前,属性加密方案已经可以实现解密操作外包功能,需要在云服务器中引入同态机制才能实现隐私保护机制。Li等^[27]提出云存储中解密外包的多授权机构属性加密方案MAACS。方案采用单一CA机制,CA不能解密任何密文,负责发布用户GID相关的密钥,不参与任何与属性相关的操作。在预解密阶段引入同态机制,且用户将私钥加密后才发送给云服务器进行计算,云服务器在整个过程中无法获取用户身份以及私钥信息,实现数据的保密以及身份的隐私保护。方案比较如表2所示。

4.2 授权机构隐私保护

云存储系统在实际数据安全共享的过程中引入了第三方授权机构对密钥进行管理发布。早期提出的属性加密方案都是基于单一授权机构,如文献[28~30]方案中,属性均是由单一授权机构管理的。但单一授权机构系统存在不可避免脆弱性,且在实际的云存储系统中,用户的属性由不同的授权机构管理更加安全可行。所以,研究人员提出了一些多授权机构的属性加密方案,文献[31~34]方案中都有多个授权机构。根据CA可以将多授权机构的属性加密方案分为采用CA方案以及无CA方案。

多授权机构虽然避免了单一授权机构带来脆弱性,但授权机构并不是完全可信的,可能合谋窃取用户的属性,造成身份隐私泄露问题,Lewko^[35]提出新的MA-CP-ABE机制,任何参与方都可以成为AA,成为AA的参与方需要生成公钥并给不同的用户发布属性相关的私钥,不同的AA之间没有任何联系,用户的私钥组件来自不同的AA,全局身份标识唯一且与用户属性相关,防止了合谋攻击。无CA机制避免了中心授权机构对系统造成的威胁。方案中定义的散列函数 H 将用户的身份标识散列成组合阶双线性群元素 $H(\text{GID})$,解密时,满足访问树的用户可以恢复出目标群元素,群元素包含的秘密共享可以恢复出明文。该方案实现了匿名密钥生成,实现了数据保密和身份隐私安全。

在多授权机构属性加密方案中,AA负责管理一个属性域,几个AA就有可能恢复出用户的属性,造成隐私泄露,Jung^[36]提出云存储数据的隐私保护机制,属性按类别分为 N 部分,由 N 个属性授权机构分别管理,如性别{男,女}、国籍{中国,韩国,美国}等。由于用户的身份识别ID识

表2 云服务器隐私保护方案比较

方案	隐私保护机制	解决的问题	访问结构	方案特点	困难问题	ABE方案
Dong ^[3]	避免响应密文请求	身份隐私	LSSS	IBE机制,撤销只需重加密部分密文	双线性群	CP-ABE
Shi ^[25]	CS分块存储	敏感内容信息	树	分块存储,系统开销低	—	CP-ABE
Xu ^[26]				分块存储,双重加密	DBDH	CP-ABE
Li ^[27]	CS同态预解密	敏感内容信息	LSSS	解密外包,高效的属性撤销机制	组合阶双线性群	CP-ABE

别包含一部分个人身份信息,所以,方案中的AA需要政府部门的监管。每个数据文件都有多种访问树决定操作权限。每个AA只管理一种属性,一方面用户不知道哪些AA管理对应的属性,需要向所有的AA提交私钥申请;另一方面,每个AA只管理一种用户的属性,AA不能在交互中推测出任何身份信息。AA响应私钥请求并将生成的私钥发送给用户,只有私钥满足访问结构的情况下才能解密密文,有效阻止了AA对用户信息的恶意窃取。

一些半匿名方案中,属性授权机构合谋就可以恢复出密钥申请者的属性,进而推测出用户的身份信息。密钥在请求传输过程中,虽然有安全协议,但仍然需要更加安全的保障机制。Jung等^[37]提出完全匿名的属性加密方案,在密钥生成算法中引入多选一不经意传输(1-out-of- n OT),发送者Bob有 n 条消息 $M_1, M_2, \dots, M_n$,接收者Alice可以得到想要的消息 M_i ,但是不会知道其他消息;Bob不会知道Alice选择了哪条消息。本文方案中每个AA管理同一类别的所有属性,同一类别的 k 种属性值中,密钥请求者至多有一种。发生密钥请求时,AA给每一个属性值随机选择一个数生成私钥。生成私钥后,AA和请求者之间采用多选一的不经意传输(1-out-of- k OT),用户从 k 个密钥中选择想要的密钥。密钥请求者可以在不泄露身份信息的前提下得到想要的属性密钥,实现完全匿名。方案比较如表3所示。

4.3 分析比较

第三方服务器具有强大的存储以及计算功能,给云存储用户之间的数据分享提供了便捷高效的服务,但是第三方服务器并不是完全可信的,用户的数据以及身份隐私可能遭到窃取、泄露。

针对云服务器的隐私保护方案主要采用保护机制使云服务器不能获得任何有用信息。文献[3]中数据拥有者使用用户的身份ID加密私钥,云服

务器只是存储分发数据,避免了用户向云服务器请求数据造成的隐私泄露;文献[25,26]云服务器中的数据以分块形式存储,保护了数据的隐私;文献[27]中的云服务器同样只是负责存储数据,预解密的同态机制也保护了用户的属性以及身份信息。

对于负责密钥生成和分发的授权机构,在密钥请求阶段,授权机构有可能进行合谋,造成用户隐私泄露。文献[35]方案实现了匿名密钥生成,任何参与方都可能成为AA,AA之间互不相关,不能进行合谋攻击。文献[36]在密钥请求阶段,用户和AA之间进行盲交互,由于AA只有一种用户的属性,因此,不能获得用户信息,实现半匿名。本文在文献[37]方案上进行改进,引入多选一不经意传输,AA不能知道用户从生成的 n 个属性密钥选择了哪一个密钥,即使合谋也不能得到任何有用信息,实现了完全匿名。

5 用户撤销机制中的隐私保护

云存储中的用户不仅数量巨大且是动态改变的,因此,属性加密在实际应用于云存储系统时必须要有撤销机制。属性加密中的撤销机制可以分为间接撤销和直接撤销2种方式,文献[38,39]主要采用了间接撤销机制,密钥需要周期性地更新,实时性较差;文献[40]采用的直接撤销机制无需定期更新密钥,只需要通过撤销列表就可以实现撤销机制;文献[41]实现了2种方式的结合。考虑到实际应用,细粒度的撤销机制可以使属性加密更好地应用于在云存储系统,文献[42~44]中的撤销机制就存在粒度过粗问题。考虑到密钥泄露以及数据隐私问题,撤销机制不仅需要确保数据的保密性,还需要保证在密钥泄露时系统不会受到安全威胁。

5.1 间接撤销

在属性加密中,如果密钥泄露密文被未授权

表3 授权机构隐私保护方案比较

方案	隐私保护机制	解决的问题	访问结构	方案特点	困难问题	ABE方案
Lewko ^[35]	匿名密钥生成	敏感属性信息	LSSS	任何参与方都可以成为授权机构,抗合谋攻击	组合阶双线性群	CP-ABE
Jung ^[36]	匿名数据访问	敏感属性信息	树	AA与用户盲交互细粒度的文件权限控制	DBDH	CP-ABE
Jung ^[37]	完全匿名	敏感属性信息	树	多选一不经意传输	DBDH	CP-ABE

的用户解密,那么没有权限的用户也可以访问数据,引入时间周期的间接撤销可以在一定程度上防止密钥泄露造成的危害,Pirretti等^[45]最早提出了间接撤销机制,根据属性周期更新密钥。Wei等^[46]提出前向安全的属性加密方案,方案利用完全二叉树结构管理用户私钥的生命周期,时间间隔与二叉树的叶子节点对应,加密密文时需要输入当前的时间周期标记,同时私钥更新时需要使用下一周期的周期标记,通过时间标记实现安全撤销。Hong等^[47]提出密钥隔离的属性加密机制,这种机制不仅可以实现前向和后向安全,而且可以在密钥泄露的情况下为系统提供安全保护,方案中系统的生命周期被离散化,不同的时间间隔内只有私钥需要更新而系统的公共参数不会改变,私钥每隔一个固定周期进行一次更新,用户在密钥协助器的帮助下得到最新版本的私钥,已经撤销的用户使用旧的私钥不能进行解密操作。

Yu等^[48]将代理重加密机制引入CP-ABE方案中,并将撤销方法扩展到KP-ABE,主要采用版本号进行标记,AA生成代理重加密密钥,密文和密钥随之更新,撤销用户的私钥版本不满足新的密文,防止密钥泄露对系统造成威胁。Xu等^[26]采用CA的多授权机构方案同样使用了代理重加密机制,云服务器为需要更新的属性生成代理重加密密钥,属性授权机构对比密文以及代理重加密密钥的版本号,重加密密文,并更新未撤销用户的密钥组件。即使密钥泄露,旧版本号的密钥也无法解密新密文,实现了数据的隐私保护。

5.2 直接撤销

虽然间接撤销可以解决密钥泄露问题,但是密钥更新开销很大,直接撤销模式通过撤销列表就可以实现撤销,实用性更强。Shi等^[49]提出基于属性加密的直接密钥撤销机制,发生撤销时,只需要更新撤销列表,非撤销用户的私钥不需要更新,不受撤销机制影响。方案中的私钥被分为2部分,一部分与访问控制相关,一部分与用户的身份相关;密文同样被分为2部分,一部分与属性相关,一部分与撤销列表相关。撤销列表更新时,密文进行更新,由第三方审计核实更新是否正确。旧的密钥无法解密更新后的密文,实现

撤销机制的前向安全。Li等^[27]方案中的撤销机制针对用户属性,每种属性由单一的属性授权机构管理,AA属性域中的每一种属性都有对应的用户群,用双线性树表示。发生撤销时,AA只需重新定义属性消费者群,选择新的属性群密钥,然后加密私钥并发送给未撤销的用户,不需要为每个未撤销的用户更新私钥。方案可以同时实现前向和后向安全。直接撤销可在实现隐私保护的同时保证高效细粒度的撤销机制。

5.3 分析比较

属性撤销方案中的间接撤销机制大多引入了时间周期的概念,没有更新的用户私钥无法进行解密操作。文献[46]方案中密文和密钥均采用时间标记,密钥使用时间标记更新;文献[47]中的密钥隔离机制在不同的周期内更新不同的密钥,实现安全撤销。直接撤销机制采用直接撤销用户属性以及用户的方式,文献[26,48]均采用代理重加密机制实现安全撤销;文献[49]中的撤销列表更新后,密文也随之更新,旧的密钥无法解密密文,文献[27]中的撤销机制主要通过更新属性用户群来实现,同时可以保证前向和后向安全。撤销方案比较如表4所示。

6 分析与工作展望

基于属性加密的云存储方案中的保护机制日趋成熟,各种方案中的隐私保护措施分别考虑了对使用者身份以及敏感内容信息的隐私保护。本文从系统参与者的身份隐私问题、敏感属性信息泄露问题、云存储系统敏感内容信息泄露问题3个方面对现存的基于属性加密的云存储隐私保护机制进行总结。

从系统参与者的身份隐私问题方面看,文献[3,23]主要是解决了用户在请求密文时提交身份标识造成的身份隐私泄露问题;文献[22]方案实现了用户请求密钥时的身份隐藏。这些方案基本解决了用户在访问加密内容时的身份泄露问题,但是对于数据拥有者的身份保护机制研究还不够完善,数据访问前的交互过程也可能造成使用者的身份信息泄露。

从敏感属性信息泄露问题方面看,文献[19~21]实现了访问结构隐藏,针对访问结构中的

表 4 撤销机制分析

分类	方案	撤销机制	解决的问题	安全性	方案特点	困难问题	撤销粒度	ABE 方案
间接撤销	Wei ^[46]	私钥密文均有时间标记	敏感内容信息	前向	私钥生命周期离散化	1-BDHE	用户	CP-ABE
	Hong ^[47]	密钥隔离	敏感内容信息	前向 后向	无双线性对操作, 解决密钥泄露问题	CDH	用户	ABE
	Yu ^[48]	代理重加密	敏感内容信息	前向	数据双重加密, 代理重加密	DBDH	用户	ABE
	Xu ^[26]	代理重加密	敏感内容信息	前向	数据分割, 代理重加密机制	DBDH	用户	CP-ABE
直接撤销	Shi ^[49]	非撤销用户无需更新密钥	敏感内容信息	前向	授权密文验证, 未撤销用户不更新密钥	$(d+3)$ -MDDH	用户	KP-ABE
	Li ^[27]	属性用户群	敏感内容信息	前向 后向	解密外包, 高效撤销	组合阶双线性群	用户属性	CP-ABE

属性进行了保护；文献[36, 37]中方案主要是对用户个人的属性采取保护机制，防止 AA 合谋造成的属性信息泄露问题。虽然上述方案实现了对敏感属性的保护机制，但不可避免地造成了用户解密开销、系统计算开销过大的问题。

从云存储敏感内容信息泄露问题方面来看，文献[25, 26]主要是在数据加密的基础上进一步对内容数据进行分割，实现安全的分块存储；文献[27]中的同态机制有效地防止了敏感内容信息被云服务器窃取；文献[26, 27, 46~49]中的撤销方案基本满足了云存储用户动态改变的需求，文献[27, 47]中的方案可以同时实现系统的前向和后向安全，安全性较高。但目前属性加密云存储方案中的撤销机制普遍存在粒度过粗、开销过大的问题，需要进一步的优化和改进。

通过上述比较和总结发现，目前基于属性加密的云存储系统隐私保护机制仍然存在一些待解决的问题，隐私保护机制未来研究的方向可能有以下几个方面。

1) 为了建立完善云存储系统的隐私保护机制，数据拥有者在与系统参与方交互时的身份保护机制可能成为未来的研究方向，此外，可以实现用户身份匿名的匿名证书系统非常具有研究价值。

2) 属性加密中涉及到的敏感属性泄露，可能造成用户的敏感信息被窃取。当前属性值隐藏以及密钥盲交互的方案增加了用户解密以及密钥的生成和分发的计算开销，存在开销过大问题，需要研究更加高效的隐私保护机制。

3) 云存储中的内容可能涉及到使用者敏感的个人信息，一旦被窃取，将给用户的隐私安全

造成严重威胁。数据分割技术增强了对敏感内容信息的保护，相关研究还相对较少；云存储中用户权限的撤销机制可以保护隐私内容不被未授权用户访问，但是要想实现前向、后向、高效、细粒度的撤销机制，仍然需要更加深入的研究。

4) 属性加密与其他加密机制的结合可以很好地解决云存储涉及到的隐私问题，同态加密机制可以实现在密文上的计算，保护外包的隐私内容；属性加密与对称加密的结合可以实现低开销的内容隐私保护机制；可搜索加密对云存储内容的匿名搜索与访问机制也是未来研究中可以借鉴的^[50]，所以，多种加密机制的结合是未来研究的热点问题。

7 结束语

云存储作为一种新型的数据存储、分享技术，已经成为互联网应用热点，不仅实现了海量数据的存储和共享，还在此技术上延伸出了很多应用。但由于网络环境的复杂性，大多数的用户一般只在云存储中存放一些无关紧要的数据内容，隐私信息、企业数据等重要数据很少存放在云平台，信任危机成为制约云存储发展的重要因素，建立云存储中完善的隐私保护机制成为云存储中的研究热点。云存储服务中，将数据拥有者和数据分离的模式，加大了隐私和数据被非法窃取的风险，黑客攻击、软件漏洞、服务器故障等都可能造成严重的安全问题。目前，研究人员已经建立了一定的技术基础但仍然缺乏关键的安全保障技术。数据安全和隐私保护是云存储中无法回避的核心问题，从长远角度看，仅从技术方面保障是远远不够的，解决云存储中的安全问题仍然需要政府以及

相关部门制定针对安全问题合理的法律法规。

参考文献:

- [1] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//ACM Conference on Computer and Communications Security. c2009:121-130.
- [2] PRASAD P S, AHAMMED G F, et al. Attribute-based encryption for scalable and secure sharing of personal health records in cloud computing[J]. International Journal of Computer Science and Information Technologies, 2014,5(4):5038-5040.
- [3] DONG X, YU J, LUO Y, et al. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing[J]. Computers & Security, 2013, 42(5):151-164.
- [4] LIANG K, MAN H A, LIU J K, et al. A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing[J]. Future Generation Computer Systems, 2014,52(C): 95-108.
- [5] WANG G, LIU Q, WU J, et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security, 2011, 30(5):320-331.
- [6] SHAMIR A. Identity-based cryptosystems and signature schemes[M]//Advances in Cryptology. Berlin Heidelberg: Springer, 1984:47-53.
- [7] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques. c2005:457-473.
- [8] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//ACM Conference on Computer and Communications Security(CCS). c2006:89-98.
- [9] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// 2007 IEEE Symposium on Security and Privacy. c2007:321-334.
- [10] CHASE M. Multi-authority attribute based encryption[C]// Theory of Cryptography Conference. c2007:515-534.
- [11] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute based encryption without a central authority[C]// International Conference on Cryptology. c2008:2618-2632.
- [12] 苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6):1299-1315.
SU J S, CAO D, WANG X F, et al. Attribute-based encryption schemes[J]. Journal of Software, 2011, 22(6):1299-1315.
- [13] YU S, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//Conference on Information Communications.c2010:1-9.
- [14] ZHANG L, HU Y. New constructions of hierarchical attribute-based encryption for fine-grained access control in cloud computing[J]. Ksii Transactions on Internet & Information Systems, 2013, 7(5):1343-1356.
- [15] LI F, RAHULAMATHAVAN Y, RAJARAJAN M, et al. Low complexity multi-authority attribute based encryption scheme for mobile cloud computing[C]//IEEE International Symposium on Service Oriented System Engineering. c2013:573-577.
- [16] KUMAR N S, LAKSHMI G V R, BALAMURUGAN B. Enhanced attribute based encryption for cloud computing[J]. Procedia Computer Science, 2014,46:689-696.
- [17] TAN Y L, GOI B, KOMIYA R, et al. Design and implementation of key-policy attribute-based encryption in body sensor network[J]. International Journal of Cryptology. Research, 2013, 4(1): 84-101.
- [18] NING J, DONG X, CAO Z, et al. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud[M]//Computer Security — ESORICS 2015. Berlin: Springer, 2015: 270-289.
- [19] LI J, REN K, ZHU B, et al. Privacy-aware attribute-based encryption with user accountability[C]//International Conference on Information Security. c2009:347-362.
- [20] 应作斌, 马建峰, 崔江涛. 支持动态策略更新的半策略隐藏属性加密方案[J]. 通信学报, 2015, 36(12):178-189.
YING Z B, MA J F, CUI J T. Partially policy hidden CP-ABE supporting dynamic policy updating[J]. Journal on Communications, 2015, 36(12):178-189.
- [21] 关志涛, 杨亭亭, 徐茹枝, 等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报, 2015, 36(6):116-126.
GUAN Z T, YANG T T, XU R Z, WANG Z X. Multi-authority attribute-based encryption access control model for cloud storage[J]. Journal on Communications, 2015, 36(6):116-126.
- [22] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//ACM Conference on Computer and Communications Security. c2009:121-130.
- [23] 徐潜, 谭成翔. 基于密文策略属性加密体制的匿名云存储隐私保护方案[J]. 计算机应用, 2015, 35(6):1573-1579.
XU Q, TAN C. Anonymous privacy-perserving scheme for cloud storage based on CP-ABE[J]. Journal of Computer Applications, 2015, 35(6):1573-1579.
- [24] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1):71-83.
FENG D G, ZHANG M, ZHANG Y, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.
- [25] 施荣华, 刘鑫, 董健, 等. 云环境下一种基于数据分割的CP-ABE隐私保护方案[J]. 计算机应用研究, 2015(2):521-523.
SHI R H, LIU X, DONG J. Private protection scheme in cloud computing using CP-ABE based on data partition[J]. Application Research of Computers, 2015(2):521-523.
- [26] XU X L, ZHOU J L, et al. Multi-authority proxy re-encryption based on CPABE for cloud storage systems[J]. Journal of Systems Engineering & Electronics, 2016, 27(1):211-223.
- [27] LI Q, MA J, LI R, et al. Secure, efficient and revocable multi-authority access control system in cloud storage[J]. Computers & Security, 2016, 59(C):45-59.
- [28] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy. c2007: 321-334.
- [29] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//ACM Conference on Computer and Communications Security(CCS). c2006:89-98.
- [30] HUR J. Improving security and efficiency in attribute-based data sharing[J]. IEEE Transactions on Knowledge & Data Engineering, 2013, 25(10):2271-2282.
- [31] MUMÜ, LLER S, KATZENBEISSER S, et al. On multi-authority ciphertext-policy attribute-based encryption[J]. Bulletin of the Ko-

- rean Mathematical Society, 2009, 46(4):803-819.
- [32] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute based encryption without a central authority[C]// International Conference on Cryptology. c2008:2618-2632.
- [33] LIU Z, CAO Z, HUANG Q, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles[M]//Computer Security—ESDRICS 2011, Berlin: Springer, 2011:278-297.
- [34] GUO Z, LI M, CUI Y, et al. Dynamic multi-attribute based encryption[J]. International Journal of Digital Content Technology & Its Applications, 2011, 5(9):281-289.
- [35] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. c2011:568-588.
- [36] JUNG T, LI X Y, WAN Z, et al. Privacy preserving cloud data access with multi-authorities[J]. IEEE Infocom, 2013, 12(11): 2625-2633.
- [37] JUNG T, LI X, WAN Z, et al. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(1):190-199.
- [38] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//ACM Conference on Computer and Communications Security (CCS). c2008:417-426.
- [39] LUAN I, PETKOVIC M, NIKOVA S, et al. Mediated ciphertext-policy attribute-based encryption and its application[C]//International Workshop on Information Security Applications. c2009: 309-323.
- [40] ATTRAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based encryption[C]//The 3rd International Conference on Pairing-Based Cryptography. c2009:248-265.
- [41] ATTRAPADUNG N, IMAI H. Attribute-based encryption supporting direct/indirect revocation modes[C]//International Conference on Cryptography and Coding. c2009:278-300.
- [42] YU S, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//IEEE Conference on Information Communications. c2010:1-9.
- [43] HUR J, NOH D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2011, 22(7):1214-1221.
- [44] ATTRAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based encryption[C]//The 3rd International Conference on Pairing-Based Cryptography. c2009:248-265.
- [45] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure attribute-based systems[C]//ACM Conference on Computer and Communications Security(CCS). c2006:799-837.
- [46] 魏江宏, 刘文芬, 胡学先. 前向安全的密文策略基于属性加密方案[J]. 通信学报, 2014, 35(7):38-45.
- WEI J H, LIU W F, HU X X. Forward-secure cipher text-policy attribute-based encryption scheme[J]. Journal on Communication, 2014, 35(7):38-45.
- [47] HONG H, SUN Z. High efficient key-insulated attribute based encryption scheme without bilinear pairing operations[J]. Springer-plus, 2015, 5(1):1-12.
- [48] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]// ACM Symposium on Information, Computer and Communications Security(ASIACCS 2010). c010:261-270.
- [49] SHI Y, ZHENG Q, LIU J, et al. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation[J]. Information Sciences, 2015, 295:221-231.
- [50] 李尚, 周志刚, 张宏莉, 等. 大数据安全高效搜索与隐私保护机制展望[J]. 网络与信息安全学报, 2016, 2(4): 21-32.
- LI S, ZHOU Z G, ZHANG H L, et al. Prospect of secure-efficient search and privacy-preserving mechanism on big data[J]. Chinese Journal of Network and Information Security, 2016, 2(4): 21-32.

作者简介:



冯涛(1970-), 男, 甘肃临洮人, 博士, 兰州理工大学研究员、博士生导师, 主要研究方向为网络与信息安全。



殷潇雨(1991-), 女, 山西太原人, 兰州理工大学硕士生, 主要研究方向为网络与信息安全。