doi:10.11959/j.issn.1000-436x.2015292

云环境下的数据多副本安全共享与关联删除方案

熊金波，沈薇薇，黄阳群，姚志强
（福建师范大学 软件学院，福建 福州 350108）

摘 要：针对共享在公共云环境的用户数据因所有权与管理权分离而导致的用户隐私泄露问题，结合对称加密算法、属性加密算法和副本定位技术，提出一种云环境下的数据多副本安全共享与关联删除方案，对用户数据进行加密等处理封装成副本关联对象(RAO, replication associated object)，随后将 RAO 共享到云服务商，建立副本关联模型对 RAO 所产生副本进行管理并实现关联删除。分析表明方案是安全与有效的，能够对用户共享的数据及其副本进行安全共享与关联删除，有效保障了数据多副本的隐私安全。
关键词：云环境；用户隐私；数据多副本；安全共享；关联删除
中图分类号：TP309 **文献标识码**：A

Security sharing and associated deleting scheme for multi-replica in cloud

XIONG Jin-bo, SHEN Wei-wei, HUANG Yang-qun, YAO Zhi-qiang
(Faculty of Software, Fujian Normal University, Fuzhou 350108, China)

Abstract: In order to protect the privacy of data stored in public cloud environment, a security sharing and associated deleting scheme for multi-replica was proposed, which was based on symmetric encryption algorithm, attribute encryption algorithm and replica location technology. In this security scheme, the user's data was first encrypted and encapsulated into the replication associated objects (RAO), then the RAO was shared in cloud service provider and managed by the replica correlation model. The comprehensive analyses show that the scheme is security and effective, and is able to support the data security sharing and associated deleting for multi-replica to protect the data privacy.
Key words: cloud environment; user privacy; multiple-replicas; security sharing; related deletion

1 引言

云计算的飞速发展促使人类社会逐步信息化，每天都有数以亿计用户的私密邮件、文件等隐私数据存储到云环境中。由于用户数据被分享到云环境中，授权用户或云服务提供商的再次分享、下载或转存到其他云服务提供商中等操作不可避免地会产生多个数据副本文件，使被广泛传播的用户数据不再受到数据拥有者的约束与管控，如访问时间段等不受控制。当用户数据到达其存储期限需要被删除时，如果缺乏有效的数据多副本关联删除机制，则该用户数据的其他副本得不到有效删除，这不仅造成存储空间的极大浪费，而且导致用户数据滥用和隐私泄露等问题，严重影响社会稳定，甚至危害国家安全。因此如何对这些涉及隐私信息的用户数据及其产生的数据副本实施安全有效的保护和关联删除是迫切需要解决的问题。

本文针对云环境下数据多副本的安全共享与关联问题，提出一种能够有效解决因授权用户或服务提供商分享、下载、转存等操作所产生的数据多副本关联删除问题的方案，保障用户数据的隐私安全并实现数据多副本的关联删除。

收稿日期：2015-10-25
基金项目：国家自然科学基金资助项目（61402109, 61370078）；福建省自然科学基金资助项目（2015J05120）
Foundation Items: The National Natural Science Foundation of China (61402109, 61370078) ; The Natural Science Foundation of Fujian Province(2015J05120)

2　目标、模型与假设

本方案的设计目标在于设定一种封装有用户数据和访问权限属性的数据结构—副本关联对象(RAO, replication associated object)，使 RAO 在其存储期限内能够遵循访问权限约束，并实现访问期限过期后的用户数据多副本的自动关联删除，有效保护用户隐私安全。

本方案设计的系统模型如图 1 所示，数据拥有者首先通过客户端将待分享数据进行加密等操作封装成 RAO 后共享到 CSP，随后 RAO 副本可能通过 CSP 以数据备份或用户转存等方式存储到其他 CSP 中；授权用户通过 CSP 下载到 RAO 副本后再进行解析解密等操作，最终获取用户数据明文。

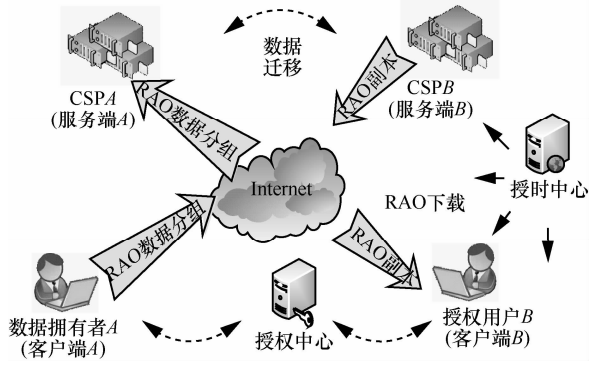

图 1　系统模型

为实现方案设计目标，现做如下安全假设[1,2]。

1) 数据拥有者、授权用户、授时中心和密钥授权中心可信。数据拥有者是 RAO 的创建者，是可信的；授权用户不会主动泄露自己的私钥信息或传播已解析出的用户数据明文；授时中心作为提供可信时间戳的第三方服务器，不会提供虚假时间参考；密钥授权中心负责验证用户身份并提供授权用户的私钥，不会主动泄露用户的私钥信息。

2) 云服务商(CSP, cloud service provider)之间、CSP 与客户端之间存在安全通信协议。CSP 之间、CSP 与客户端之间预先设定安全通信协议，能够识别处理双方发送的消息指令并做出相应操作，如客户端能够正确识别并执行 CSP 所发送的删除目标 RAO 指令。

3　方案构造

本方案将对称加密算法、基于属性的加密算法和副本定位技术相结合，提出一种云环境下的数据多副本安全共享与关联删除方案，能够有效保护用户的隐私安全，并实现副本的关联删除。具体地，数据拥有者首先通过客户端将待分享数据进行加密等操作封装成 RAO 后上传到 CSP 进行存储，随后 RAO 副本可能通过数据备份或用户转存等方式存储到其他 CSP 并在其副本目录中做相应信息记录；授权用户下载到 RAO 副本后再进行解析解密等操作，最终获取用户数据明文。

为实现数据多副本关联删除，本文在文献[3]的基础上设计出如下副本关联模型。

通过副本目录[3]记录云存储系统中所有副本的相关信息，即每个存储服务器中都存储有副本目录，记录有用户分享的 RAO 所产生的所有副本相关信息，包括 RAO 副本的逻辑文件名[3]、物理文件名[3]和存储期限 T'。本方案中使用 RAO 副本的散列摘要值[4]作为逻辑文件名，确保存储在服务器上的所有相同 RAO 副本拥有全局的唯一标识符；使用 RAO 副本存储在 CSP 或客户端中的物理路径和 CSP 编号或客户端编号作为 RAO 的物理文件名。

同时每个服务器设定有副本目录的同步机制和监测机制：同步机制用于时刻记录 RAO 产生或删除副本的操作行为，一旦产生新的 RAO 副本，则副本目录同时更新，记录该 RAO 副本的物理文件名等相关信息；监测机制用于监测副本目录中记录的存储期限，一旦存储期限过期则对该 RAO 副本进行删除。

本方案的基本工作原理如图 2 所示，主要分为 3 个阶段。

第 1 个阶段为 RAO 的封装及存储阶段，该阶段具体工作原理可由 6 个算法描述。

1) $Encrypt(Data, key)\rightarrow C$，通过使用对称密钥 *key* 加密数据拥有者待分享的原始数据 *Data*，得到数据密文 *C*，本文使用对称加密算法 AES 进行实验分析。

2) $ABEEncrypt(key, k_{\text{pub}})\rightarrow C_k$，通过公钥 k_{pub} 对对称密钥 *key* 进行属性加密，得到密钥密文 C_k，本文使用 ABE 基于属性加密算法进行实验分析。

3) $Encapsulate(C, C_k, T)\rightarrow RAO$，数据拥有者指定数据访问期限 *T*，结合前面步骤所获得的数据密文 *C* 和密钥密文 C_k 使用算法 *Encapsulate* 将其封装成副本关联对象 RAO 并上传到 CSP 中进行存储，同时设置 RAO 在 CSP 中的存储期限 T'。

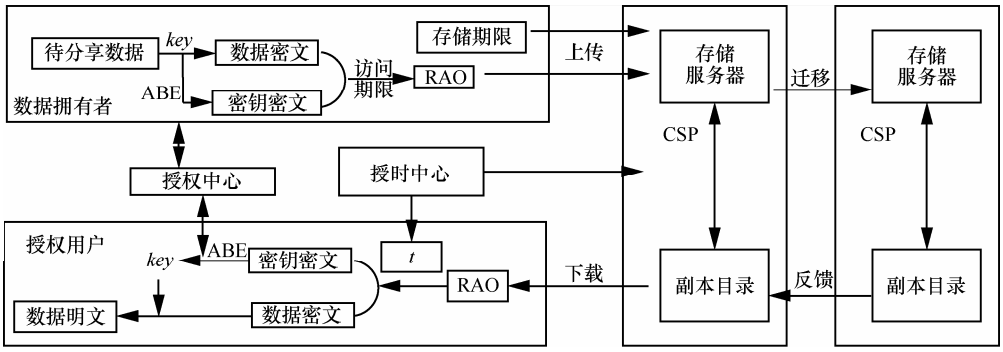

图 2 方案基本工作原理

4) *Hash*(*RAO*)→*LFN*，CSP 接收到 RAO 后，通过使用散列算法计算出 RAO 副本的摘要值作为 RAO 的逻辑文件名 *LFN*，确保存储在 CSP 上的所有相同 RAO 副本拥有全局唯一标识符。

5) *AddRecord*(*LFN*, *PFN*, *Deadline*)，使用副本目录记录算法在 CSP 存储的副本目录上记录数据拥有者上传的 RAO 副本的相关信息：逻辑文件名、物理文件名、存储期限，其中物理文件名由 RAO 存储的物理路径和其 CSP 编号构成。

6) *Feedback*(*LFN*, *PFN*)，当授权用户或 CSP 对 RAO 副本进行备份或转存到下级 CSP 时，下级 CSP 将该 RAO 副本的相关信息存储到自身的副本目录，并将物理文件名反馈给上级 CSP 进行记录，实现数据多副本的关联。

第 2 个阶段为解封装阶段，该阶段具体工作原理可由 4 个算法描述。

1) *Verify*(*RAO*, T_{now})，当授权用户对 RAO 副本进行访问时，算法 *Verify* 首先对 RAO 副本进行解析获得访问期限，随后使用从授时中心处获取到的可信时间 T_{now} 对 RAO 的访问期限进行验证，若当前可信时间处于 RAO 访问期限之前，则停止 RAO 的解析；若当前可信时间处于 RAO 访问期限之后，则进入删除阶段，对该 RAO 副本进行删除；若当前可信时间处于 RAO 访问期限之间，则继续对 RAO 进行解析获取数据密文 *C* 和密钥密文 C_k。

2) *Decapsulate*(*RAO*)→*C*, C_k，当 RAO 的访问期限通过验证后，算法 *Decapsulate* 对 RAO 进行进一步解析获取数据密文 *C* 和密钥密文 C_k。

3) *ABEDecrypt*(C_k, k_{pri})→*key*，授权用户从密钥授权中心处获取私钥 k_{pri} 后，对密钥密文 C_k 进行解密获得对称密钥 *key*。

4) *Decrypt*(*C*, *key*)→*Data*，算法 *Decrypt* 使用对称密钥 *key* 对数据密文 *C* 进行解密，最终获得用户数据明文 *Data*。

第 3 个阶段为删除阶段，该阶段具体工作原理可由 4 个算法描述。

1) *CSPDelete*(*t*)，CSP 中，算法 *CSPDelete* 以当前可信时间作为输入，时刻对其存储的副本目录进行检索，若存储 RAO 副本的存储期限已过期，即当前时间 *t* 晚于存储期限时，则算法获取该 RAO 在该 CSP 中的物理文件名并对 RAO 进行删除。

2) *Instruct*(*LFN*)算法，根据 RAO 副本的逻辑文件名对副本目录进行检索，查找存储有该 RAO 副本的下级 CSP 并向其发送删除指令。

3) *DeleteFeedback*(*PFN*)，下级 CSP 接收到上级 CSP 发送的删除指令，并对 RAO 副本进行删除后，通过算法 *DeleteFeedback* 将所删除的 RAO 副本的物理文件名反馈给上级 CSP，上级 CSP 接收到反馈后将调用算法 *DeleteRecord* 进行相关操作。

4) *DeleteRecord*(*PFN*)，当 CSP 成功删除 RAO 副本后，算法 *DeleteRecord* 对副本目录进行修改，即删除本次 RAO 副本存储在 CSP 中的相关记录信息。

4 综合评价与安全性分析

4.1 综合评价

与已有的云环境下用户数据在其全生命周期[5]内隐私安全保护与安全删除方案相比，文献[6~8]采用密钥集中管理方式，依赖加密算法的安全性和密钥安全管理来保障用户数据的隐私不被侵犯，文献[1,2,9~13]采用密钥分散管理方式，利用 DHT 网络节点周期性更新的特性实现用户数据自动删除，以此来保障用户隐私安全，但存在用户不能自定义共享数据的访问期限的局限性，而且其大部分密文并没有被真正删除，造成空间资源浪费的同时也依旧存在密文被非法获取并强力破解的隐患。针对以

上方案的局限性，文献[14]所提方案能够使用户自定义控制数据访问期限，并且在访问期限到期时直接删除密文数据，释放存储空间，但以上所提方案的访问或存储期限控制仅作用于单一数据副本，并不能对数据所产生的其他副本产生作用，即这些方案并未涉及数据多副本关联删除。而本文所提方案则能够较好地解决这些问题，通过对用户数据进行加密处理保障用户隐私安全，通过数据拥有者自定义设置访问期限和存储期限使用户数据在超过访问期限后被删除，通过副本关联机制对数据副本进行关联管理，结合副本定位技术[15]和副本删除技术[16]，实现在源数据被删除后，其产生的副本数据能够被关联删除的设计目标。

4.2　安全性分析

在本文的安全假设中，假设数据拥有者、授权用户和密钥授权中心可信，不会主动泄露用户私钥信息或传播用户数据明文，而 CSP 作为非可信第三方服务器，可能遭到敌手非法攻击泄露 RAO 副本，即攻击者非法持有 RAO 副本并企图通过强力攻击的方法获取数据明文，因此本方案的安全性依赖于所采用的数据加密算法(即对称加密算法 AES 和基于属性加密算法 ABE)的安全性。

本方案在封装 RAO 前首先对用户待分享数据进行对称加密获得数据密文，所使用的对称密钥通过 ABE 加密算法进行加密获得密钥密文，随后将数据密文与密钥密文和访问期限进行组合封装最终获得 RAO。因此假设攻击者获得 RAO 副本，首先需要对 RAO 进行解析，成功分离出数据密文后才能进行强力攻击或密码分析攻击。而 ABE 算法是可证明安全的[17]，在多项式时间内无法破解密钥密文获得对称密钥信息并对数据密文进行解密，而 AES 算法的攻击复杂度依赖于分组长度和密钥长度，假设 AES 算法采用的密钥长度为 1 024 bit，则对其密文进行强力攻击也需要耗费成千上万年，因此理论上攻击者无法获取原始密文，本方案是安全的，能够有效保护用户的隐私安全。

5　结束语

本文设计了一种云环境下的数据多副本安全共享与关联删除方案，能够实现云环境下的数据多副本的安全存储与共享，并实现副本关联删除，使在数据拥有者删除存储在云服务端上的原始数据后，其他存储有该数据副本的云服务端能够自动删除该数据副本。同时该方案能够实现控制数据副本的访问期限和存储期限，有效保障用户数据的隐私安全。

进一步研究工作的重点主要为：结合 Hadoop[18] 开发出一个云环境下数据多副本安全共享与关联系统，对本方案进行更全面的仿真实验测试，对本方案中的副本关联模型进行完善，制定最优副本管理策略并提高副本定位与选择效率，最终对本方案进行优化并尝试推广使用。

参考文献：

[1] WANG G J , YUE F S, LIU Q. A secure self-destructing scheme for electronic data[J]. Journal of Computer and System Sciences, 2013, 79(2): 279-290.

[2] 熊金波, 姚志强, 马建峰, 等.面向网络内容隐私的基于身份加密的安全自毁方案[J].计算机学报，2014，37(1)：139-150.
XIONG J B,YAO Z Q,MA J F, *et al*. A secure self-destruction scheme with IBE for the internet content privacy[J]. Chinese Journal of Computers, 2014, 37(1): 139-150.

[3] 田荣阳. 数据网格中的副本定位及选择服务[D]. 重庆:重庆大学, 2006.
TIAN R Y. Replica Location in the Grid Location and Selection Service[D]. Chongqing: Chongqing University, 2006.

[4] MERKLE R C. One way hash functions and DES[J]. Lecture Notes in Computer Science, 1990, 435:428-446.

[5] XIONG J B, LI F H, MA J F, *et al*. A full lifecycle privacy protection scheme for sensitive data in cloud computing[J]. Peer-to-Peer Networking and Applications,2015, 8(6): 1025-1037.

[6] TANG Y, LEE P P C, LUI J C S, *et al*. FADE: secure overlay cloud storage with file assured deletion[A]. Security and Privacy in Communication Networks[C]. 2010. 380-397.

[7] PERLMAN R. File system design with assured delete[A]. IEEE International Security in Storage Workshop[C]. 2005. 88.

[8] TANG Y, LEE P P C, LUI J C S, *et al*. Secure overlay cloud storage with access control and assured deletion[J]. IEEE Transactions on, Dependable and Secure Computing, 2012, 9(6): 903 -916.

[9] GEAMBASU R, KOHNO T, LEVY A A, *et al*. Vanish: increasing data privacy with self-destructing data[A]. USENIX Security Symposium[C]. 2009. 299-316.

[10] 熊金波, 姚志强, 马建峰, 等.基于属性加密的组合文档安全自毁方案[J].电子学报, 2013, 42(2): 366-376.
XIONG J B, YAO Z Q, MA J F, *et al*. A secure self-destruction scheme for composite documents with attribute based encryption [J]. Acta Electronica Sinica, 2013, 42 (2) : 366-376.

[11] 姚志强, 熊金波, 马建峰, 等.云计算中一种安全的电子文档自毁方案[J]. 计算机研究与发展, 2014, 51(7): 1417-1423.
XIONG J B,YAO Z Q,MA J F, *et al*. A secure electronic document

self-destructing scheme in cloud computing[J]. Journal of Computer Research and Development, 2014, 51(7):1417-1423.

[12] XIONG J B,YAO Z Q, MA J F, *et al*. A secure document self-destruction scheme with identity based encryption[A]. Proc of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems[C]. 2013. 239-243.

[13] 王丽娜，任正伟，余荣威，等.一种适于云存储的数据确定性删除方法[J].电子学报, 2012, 40(2): 266-272.
WANG L N,REN Z W,YU R Z, *et al*. A data assured deletion approach adapted for cloud storage[J]. Acta Electronica Sinica. 2012, 40(2): 266-272 .

[14] XIONG J B, LIU X M, YAO Z Q, *et al*. A secure data self-destructing scheme in cloud computing[J]. IEEE Transactions on Cloud Computing, 2014, 2(4):448-458.

[15] 李东升, 李春江, 肖侬,等. 数据网格环境下一种动态自适应的副本定位方法[J]. 计算机研究与发展, 2003, 40(12):1775-1780.
LI D S,LI C J,XIAO N, *et al*. Dynamic self-adaptive replica location method in data grids[J]. Journal of Computer Research and Development, 2003, 40(12):1775-1780.

[16] 刘田甜, 李超, 胡庆成,等. 云环境下多副本管理综述[J]. 计算机研究与发展, 2011, S3: 254-260.
LIU T T ,LI C,HU Q C, *et al*. Multiple-replicas management in the cloud environment[J]. Journal of Computer Research and Development, 2011, S3: 254-260.

[17] 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.

[18] WHITE T. Hadoop: the definitive guide[J]. O'reilly Media Inc Gravenstein Highway North, 2010, 215(11):1 - 4.

作者简介：

熊金波[通信作者]（1981-），男，湖南益阳人，福建师范大学讲师，主要研究方向为云数据安全与隐私保护技术。E-mail:jinbo810@163.com。

沈薇薇（1991-），女，福建诏安人，福建师范大学硕士生，主要研究方向为云数据安全与隐私保护技术。

黄阳群（1991-），女，福建永泰人，福建师范大学硕士生，主要研究方向为信息安全。

姚志强（1967-），男，福建莆田人，福建师范大学教授，主要研究方向为信息安全。