云数据安全研究进展

鲁金钿[①] 肖睿智[①] 金舒原*[①②]

[①](中山大学数据科学与计算机学院 广州 510006)

[②](鹏城实验室网络空间安全研究中心 深圳 518000)

摘 要：云数据安全问题是制约云计算发展的重要因素之一。该文综述了云数据安全方面的研究进展，将云数据安全所涉及的云身份认证、云访问控制、云数据安全计算、虚拟化安全技术、云数据存储安全、云数据安全删除、云信息流控制、云数据安全审计、云数据隐私保护及云业务可持续性保障10方面相关研究工作纳入到物理资源层、虚拟组件层及云服务层所构成的云架构中进行总结和分析；并给出了相关技术的未来发展趋势。

关键词：云数据安全；云数据隐私保护；云数据安全删除；云信息流控制；云数据安全审计

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2021)04-0881-11

DOI: 10.11999/JEIT200158

A Survey for Cloud Data Security

LU Jintian[①] XIAO Ruizhi[①] JIN Shuyuan[①②]

[①](*School of Data and Computer Science*, *Sun Yat-sen University*, *Guangzhou* 510006, *China*)

[②](*Cyberspace Security Research Center*, *Peng Cheng Laboratory*, *Shenzhen* 518000, *China*)

Abstract: The security of cloud data is one of the most important factors to obstruct the development of cloud computing. Therefore, on the basis of proposed three-tiers cloud architecture that consists of physical resources layer, virtual component layer, and cloud service layer, this paper makes a detail survey on existing works that focus on the security of cloud data, which involves in cloud identify authentication, cloud access control, cloud data secure computing, virtualization, cloud data security storage, cloud data secure deletion, information flow control, cloud data secure auditing, cloud data privacy preserving, and cloud business continuity, respectively. Finally, research trends in the field of cloud data security are presented.

Key words: Cloud data security; Cloud data privacy preserving; Cloud data secure deletion; Information flow control; Cloud data secure auditing

1 引言

云计算自提出以来，得到了IBM, Google, Amazon及微软等大型企业的推进，并迅速拓展到产业界和学术界。近十年来，云数据安全问题一直是制约云技术及产业发展的重要因素，如2010年Hotmail邮箱数据丢失、2018年万豪集团5亿用户数据泄露等均造成了严重的经济损失。当云租户将其数据存储到云计算平台时，就将其数据的控制权交给了云服务商，这种数据使用权和控制权的分离是导致云数据不安全的根本原因。

收稿日期：2020-03-10；改回日期：2020-08-05；网络出版：2020-08-12

*通信作者： 金舒原 jinshuyuan@mail.sysu.edu.cn

基金项目：国家重点研发项目(2018YFB1800705)，国家自然科学基金(61672494)

Foundation Items: The National Key Research and Development Program of China (2018YFB1800705), The National Natural Science Foundation of China (61672494)

在国内，武汉大学王骞教授团队、中国科学院李凤华教授团队等均致力于研究云数据安全和隐私保护，其主要通过可搜索加密方法、以及访问控制模型等实现对云数据的安全保护；暨南大学的翁建教授在保护云数据、隐私数据存储安全等方面也做了深入工作，提出了代理重加密、基于身份加密等方法。国外研究团队如布里托斯大学Thomas Pasquier教授与剑桥大学Barbara Liskov教授等通过分布式信息流控制技术保障云数据在系统流动过程中的保密性和完整性，并在此基础上建立了全系统溯源跟踪系统以增强系统安全。国内外还有很多对云计算安全和云数据安全研究成果突出的团队，如国内启明星辰公司，国外墨尔本大学Buyya教授团队等。

为清晰地讨论云的数据安全问题，本文基于云虚拟化、多租户和服务弹性化等特点，将云的体系结构分为3层：物理资源层、虚拟组件层及云服务层。其中，物理资源层主要包含硬件基础设施及资

源；虚拟组件层主要包含虚拟化组件，如虚拟机管理器、虚拟机及容器等组件；云服务层由具体的云服务构成，主要包括资源管理、安全管理及弹性计费管理等云服务。其架构如图1所示。云的数据安全主要涉及以下7个关键环节：

(1) 云数据存储安全。云租户将数据上传到云服务提供商(Cloud Service Provider, CSP)存储，CSP因系统故障、恶意攻击等原因令数据面临高安全风险。使用加密存储机制，如基于代理和广播的重加密以及基于可搜索加密的云数据安全存储等可有效地保证云数据存储的安全性。

(2) 云数据管理安全。如何保障云数据资源高效管理、海量数据的精确定位是云数据安全管理面临的主要问题。云资源的动态更新会造成云数据多副本等问题，影响云数据管理的效率和数据定位的准确度，令云数据安全管理和调度复杂化、存储资源开销增加。使用虚拟化安全等技术可有效降低管理开销，实现监管的合规性，防止因虚拟层穿透或资源耗尽引起的隐私泄露问题。

(3) 云数据访问安全。为应对云数据被恶意用户或攻击者访问、修改等风险，通常采用身份认证、访问控制、云数据安全计算、云信息流控制等技术来保障访问过程中的数据完整性和安全性。

(4) 云数据安全删除。当删除云数据资源时，需要确保数据确定性删除且不可恢复，同时也要确保与目标数据相关联的副本数据的删除，以防攻击者对数据进行恶意修复而导致隐私数据泄露。

(5) 云数据安全审计。对存储于并被CSP管理的云数据的完整性及持有性等特性进行高效的审计，以保障云数据的使用规范性和对违规操作的追责。此外，云数据审计过程中的隐私保护也是安全审计的重要方面。

(6) 云数据隐私保护。云数据隐私保护是云数据安全研究的重要方面，包括存储安全以及云数据访问模式、查询索引、限门链接及身份隐私的保护等。

(7) 云业务可持续性保障。云服务层业务的可持续性保障是衡量云计算系统或服务的重要指标之一。通常通过云数据备份及恢复等方法实现云服务的持续性供给。

基于以上云数据安全保护的7个关键环节，本文将云数据安全所涉及的云身份认证、云访问控制、云数据安全计算、虚拟化安全技术、云数据的存储安全、云数据的安全删除、云信息流控制、云数据安全审计、云数据隐私保护及云业务可持续性保障10方面的相关研究工作纳入到物理资源层、虚

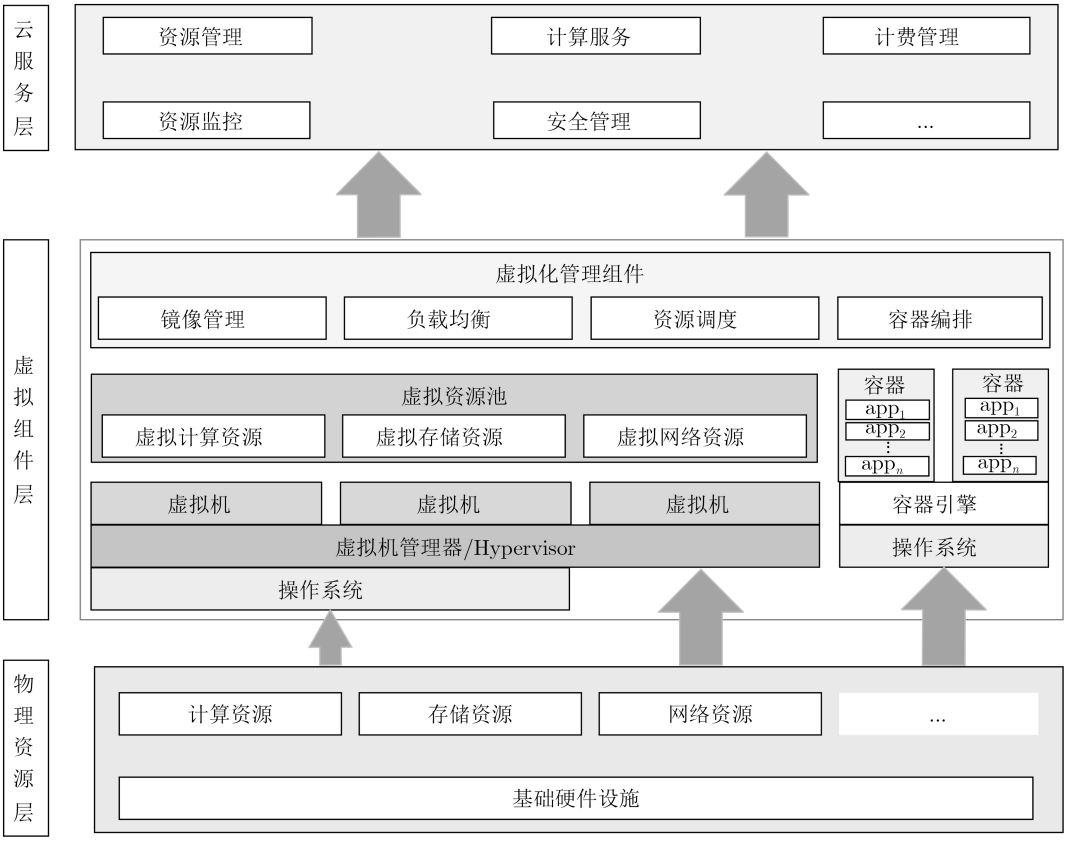

图 1 云计算架构

拟组件层及云服务层所构成的3层云架构中进行总结和分析，如图2所示。

2　云身份认证

云身份的合法认证可有效防止云数据被非法用户访问或非法提权而导致的数据泄露或破坏。

2.1　基于安全凭证的云身份认证

基于安全凭证的身份认证包括基于用户秘密、硬件凭证及多因子认证。云计算环境中有多种基于安全凭证的认证技术，如Google使用的ACCESS Key凭证认证、X.509证书认证以及将传统的登录证书及授权用户持有的硬件设备码相结合的多因子认证技术等。

2.2　基于单点登录的联合云身份认证

云的联合身份认证一般基于单点登录实现，目前主要包括基于安全协议和安全断言标记语言(Security Assertion Markup Language, SAML)的云身份认证。其中，包括OpenID协议[1]和OpenID Connect[2]在内的基于安全协议的单点登录通常是使用如OpenID身份认证来访问相应云服务，或者是通过提供授权允许授权第三方网站访问存储在云端的信息(如OAuth协议)；基于SAML的单点登录云身份认证主要以安全断言标记语言为基础，以较好地支持多安全站点或安全域同一用户的单点登录。

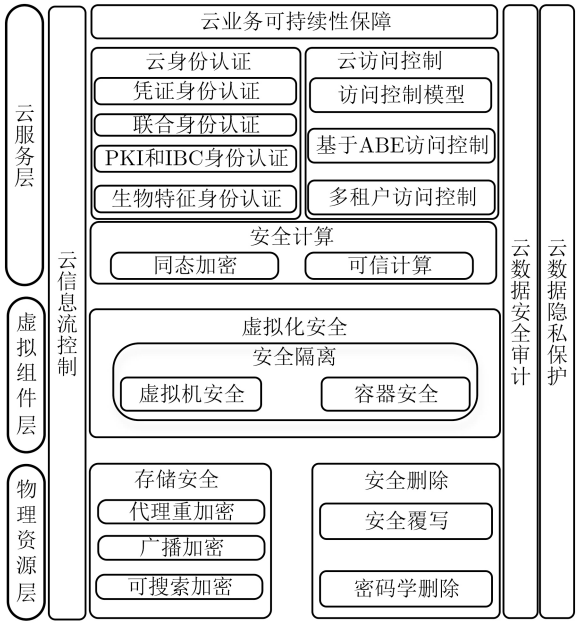

图 2 云数据安全技术

2.3　基于PKI和IBC的云身份认证

公钥基础设施(Public Key Infrastructure, PKI)及基于身份的密码技术(Identity-Based Cryptography, IBC)也是云身份认证的重要方法之一。前者可实现跨云的服务访问，包括数据加密、数字签名、身份识别以及密钥和证书管理等，其在效率和证书撤销复杂度等方面存在不足；后者主要用于云内部的认证。为了降低基于证书的PKI实现的复杂度和减少证书的使用，通常采用PKI和IBC结合的方式，即在云内采用IBC、在云间采用PKI认证。

2.4　基于生物特征的云身份认证

基于如手指静脉、掌纹静脉、虹膜等生物特征的云身份认证具有高效率、高安全性、高灵活性及难伪造性等特性，但在复杂的云环境下容易受到服务提供者的模拟攻击[3]，如误用生物识别技术或指纹登录等。

云身份认证所使用的不同协议和方法之间的优缺点比较如表1所示。

3　云访问控制

与传统的访问控制模型相比，云访问控制主要面对的挑战在于：(1)用户失去了对其数据的掌控权；(2)访问主体、被访问对象的边界模糊，侧信道等攻击成为可能；(3)用户和云平台之间缺乏信任。鉴于此，云访问控制的研究主要集中在云访问控制模型、基于属性加密(Attribute-Based Encryption, ABE)的密码机制及多租户访问控制3个方面。

3.1　云访问控制模型

云访问控制模型的研究主要集中于基于角色和基于属性两大类。在基于角色的访问控制模型(Role-Based Access Control, RBAC)方面，基于任

表 1　云身份认证各类方法比较

技术	机制/方法	优点	缺点	适用场景
ACCESS Key	安全凭证	可靠	灵活性较差	安全需求高场景
OpenID	单点登录	方便	安全性较低	减轻租户负担
OpenID Connect	单点登录	互操作	安全性较低	减轻租户负担
OAuth	单点登录	方便	安全性较低	统一授权场景
基于SAML	单点登录	互操作	安全性较低	统一身份证认证
基于PKI&IBC	PKI&IBC	跨云	复杂性较高	跨云的服务访问
基于生物特征	虹膜/静脉等	灵活	易攻击/复杂性高	小规模高效认证

务与RBAC结合模型(Task-Role-Based Access Control, T-RBAC)可实现同一安全分类中不可信用户之间的安全资源共享。在基于属性的访问控制(Attribute-Based Access Control, ABAC)[4]模型方面，结合RBAC的授权机制和ABAC模型可较好解决细粒度访问控制和大规模用户动态扩展问题。

3.2 基于ABE机制的云访问控制

ABE密码算法因其机制本身支持不同的解密算法，非常适用云计算这种解密方不固定的分布式环境下的访问控制。基于ABE的访问控制主要包括密钥策略的属性加密(Key-Policy ABE, KP-ABE)和密文策略的属性加密(Cipher-Policy ABE, CP-ABE)两种：前者基于密钥访问控制策略，后者基于密文访问控制策略。使用基于ABE的访问控制方法目前还不能很好解决效率和可扩展性等问题，在用户属性撤销方面也会产生高额的计算开销[5]。

3.3 多租户访问控制

在多租户访问控制方面，文献[6]制定了不同租户间的资源共享机制，并通过形式化方法证明了不同租户间权限激活和委托机制的正确性。文献[7]提出的云环境下多租户风险感知虚拟资源分配机制可将数据泄露的风险降到最低。

不同的云访问控制技术的优缺点对比如表2所示。

4 云数据安全计算

本文中云数据安全计算是指保证云数据在动态计算过程中的安全。目前该领域的研究主要集中在同态加密和可信计算技术。

4.1 基于同态加密的云数据安全计算

同态加密[8]实现了无需解密的情形下的密文数据计算，是云安全计算领域广泛采用的技术之一。Gentry等人[9]提出了基于理想格的第1个全同态加密方法，通过构造加密算法、解密“打散”及“引导程序”实现了“隐私同态”，但该方法存在复杂度较高和效率低的不足。其后，文献[10]在加密数据的计算隐私性、完整性及可信性等方面进行了较大的改进。

4.2 基于可信计算的云数据安全计算

2017年，中国工程院院士沈昌祥[11]在《用可信计算构筑云计算安全》报告中指出“要用可信计算构建云计算安全，在云的基础上解决数据安全”。可信云计算的一般模型是利用可信平台模块在云环境下对用户或资源实施监控，以保证虚拟环境、客户和服务方的可信性。Contractor等人[12]利用可信计算组提供的信任链基本功能，构建了可问责的云计算系统。

云数据安全计算的不同方法的优缺点对比如表3所示。

5 虚拟化安全技术

目前虚拟化技术主要有基于虚拟机和基于容器的虚拟化，如何保障虚拟化安全并进行有效的虚拟机数据隔离是保障云数据安全的重要方面。

5.1 虚拟机安全

目前虚拟机安全的研究可划分为两类：虚拟机管理及虚拟机使用，这两个方面安全需求、面临的安全威胁及解决方法如图3所示，图3中所列主要威胁和解决方法来自于文献[13,14]。

表 2 云访问控制技术方法比较

方法/模型	机制			技术	优点	缺陷	适用场景
	拓展的传统方案	基于ABE	多租户技术				
ABAC	●			RBAC	动态性	拓展性差	自适应访问控制
T-RBAC	●			Task-RBAC	安全性	拓展性差	资源共享频繁
ABAC	●			ABAC	细粒度	效率问题	大规模信息系统
Li等人[5]		●		用户组	有效性	高额计算外包	用户属性撤销
文献[6]			●	共享机制	有效性	复杂性高	资源共享频繁
文献[7]			●	基于敏感度	安全性	拓展性差	虚拟资源分配

表 3 云数据安全计算方法比较

方法	方法		技术	优点	缺陷	适用场景
	同态加密	可信计算				
文献[9]	●		理想格	全同态	复杂低效	对效率要求不高
文献[10]	●		DynamoDB	全同态	密文复杂	简单高效的环境
基于TPM		●	TPM	可信性	复杂性	规模较小
文献[12]		●	TCG	可问责	拓展性	需要追责的场景

5.2 容器安全

与基于虚拟机的虚拟化技术相比，容器虚拟化在内存、CPU和存储资源等方面具备更高使用效率和快速部署优势，容器即服务(Container as a Service, CaaS)已作为一种交付模型被提出。基于CaaS，文献[15]提出了解决容器的管理效率和开销问题的方法，随后提出的基于容器的CQSTR系统[16]在效率方面有了大幅度提升，但在保障云数据安全方面略显不足。

5.3 云数据安全隔离

云数据安全隔离研究主要集中在虚拟机、容器、信息流控制技术、通信加密及多租户技术等方面。通常，虚拟机数据隔离是将应用程序放在虚拟机而非宿主机中执行，或者是在虚拟机中实现分布式服务来实现；容器与虚拟机相结合的方式也是实现云数据隔离的措施之一；基于标记的信息流控制技术可实现细粒度数据隔离；多租户技术可较好地保证不同租户的运行环境和服务的安全隔离。

6 云数据存储安全

6.1 基于代理重加密的云数据存储安全

代理重加密(Proxy Re-encryption, PRE)允许可信第三方将用户加密的密文转化为可用另一方私钥解密的密文，其主要包括基于身份、属性和区块链等方法的代理重加密方法。其中前两个方案较为普遍，现有代表性方法的比较如表4所示。其中，可重复性指代理执行再次加密操作时对随机因子的密文进行与之前同样的操作即可实现多次重加密；非交互性指重加密密钥的计算均可以由客户端独立完成，无需其他第三方参与；单向性指代理转换访问结构时若缺少随机因子与访问结构相关联的密文便无法转换访问结构；可验证性指加密结果及是否按照要求进行加解密均可验证。

6.2 基于广播加密的云数据存储安全

在云计算模式下广播加密机制主要包含基于属性的广播加密(Attribution-Based Broadcast Encrypt, ABBE)和基于身份的广播加密(Identity-Based Broadcast Encrypt, IBBE)。已有的ABBE方法大多关注于明文隐私，忽略了策略和广播列表隐私导致攻击者可通过密文和公共参数来确定访问策略和广播集。使用部分隐藏策略来实现访问策略中隐私信息的保护[21]并减少计算开销。目前的IBBE方法不需要任何额外身份验证，但私钥或公钥等参数随着系统中用户数的增加而呈线性增长。

6.3 基于可搜索加密的云数据存储安全

通常，加密是保障云数据安全的有效办法之一，但存在查询索引难以建立导致的加密数据查询低效问题。可搜索加密技术(Searchable Encryption, SE)[22,23]可较好地解决这个问题。检索效率、检索安全性及可验证性是SE研究主要关注的3个方面。其中检索效率主要体现在索引生成和检索算法或检索结构的计算复杂性方面；检索安全性指在检索过程中不泄露索引模式、索引信息及访问模式

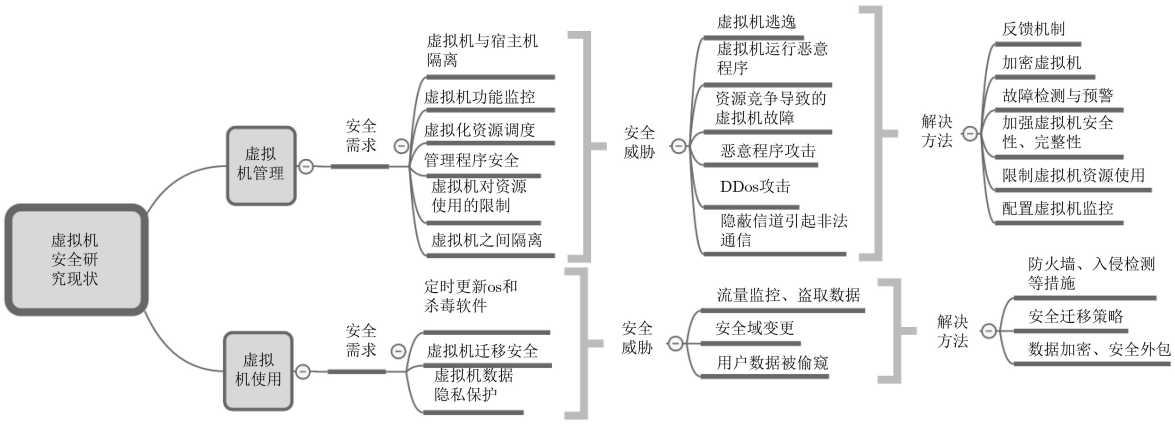

图 3 虚拟机面临主要威胁及解决方法

表 4 基于代理重加密方法比较

方法	可重复性	非交互性	单向性	可控性	可验证性	安全性
Liang[17]	√	√	√	×	×	防CCA
Luo[18]	√	√	√	√	×	防CPA
冯朝胜等人[19]	√	√	√	√	√	防CPA和合谋
PRE-MFAC[20]	√	×	√	√	√	防CPA

等，主要包含前后向检索安全性2方面；检索可验证主要体现在验证检索数据的准确性和完整性等方面。在该领域的代表性研究工作的比较如表5所示。

表 5 可搜索加密相关方法比较

方法	查询类型	前向安全性	后向安全性	可验证性
Bost[24]	单关键字	√	√	×
Chamani[25]	单关键字	×	√	×
Janus++[26]	单关键字	√	√	×
MB-FB-DSSE[27]	单关键字	√	√	×
VDRSE[28]	多关键字	√	√	√

7 云数据安全删除

7.1 基于安全覆写的云数据安全删除

安全覆写主要思想为首先对数据进行破坏，然后使用新数据对原有数据进行覆写。Paul等人[29]提出了数据擦除时将数据最高有效位和最低有效位反转的方法，实现了数据的不可恢复销毁，但该方法需要云服务商参与。随后，Luo等人[30]结合沙漏函数提出了基于覆写的云数据确定性删除方法，可从云服务器的驱动器中删除数据，实现了云数据的安全删除。

7.2 基于密码学的云数据安全删除

基于密码学的云数据安全删除是通过删除数据的同时也删除云端的密文数据和密钥管理者持有的解密密钥的方式实现即使云端保留了数据副本也无法解密的数据安全删除。其主要包括基于可信第三方、分散式哈希表和密钥调制函数3类方法。基于可信第三方的方法，如FADE协议[31]是通过撤销策略来实现数据删除的不可恢复性；基于分散式哈希表的方法，如SelfDoc[32]是通过原始密文和访问密钥在数据删除后无法恢复来实现数据的安全删除；基于密钥调制函数的方法，如Xue等人[33]提出的方法是通过改变主密钥来实现数据的安全删除。基于密码学的数据安全删除方法的不足主要在于包括额外存储在内的系统开销较高。

8 云信息流控制

云环境下的信息流控制技术主要通过控制数据信息在云中的流动来保障云数据安全，其核心是控制策略的制定和描述、标签的生成、管理和传播。这里，以CloudFence[34]为例来说明信息流跟踪即服务(DFTaaS)的模式结构，其主要包括：(1)用户API 在DFTaaS上注册，同时获取用户统一身份标识证书；(2)云服务器为用户提供服务；(3)云基础设施对用户隐私数据进行标记及跟踪，并记录审计信息；(4)用户获取自身数据审计记录。其后，Camflow[35]系统实现了PaaS模型下的细粒度信息流转控制，CloudSafetyNet[36]不仅实现了细粒度信息流控制，还可以追踪网络环境中的隐私数据。

9 云数据安全审计

云数据安全审计主要解决数据持有性和完整性两个问题，通常的解决思路是：仅取回少量数据，通过使用特定知识证明协议或概率分析，以高可信概率判断云端数据是否完整或为某租户所有。

9.1 云数据持有审计

为保证文件在不可信存储系统上的存储安全，基于RSA同态令牌，Ateniese等人[37]构建了可证的数据持有(Provable Data Possession, PDP)模型，实现了对云数据进行公开可验证审计，但该模型不支持动态存储。其后提出的支持动态存储的Dynamic PDP[38]以及OOPDP模型[39]等改进了PDP的缺陷，实现了审计的轻量级计算。在持有审计的可证明性方面，Wang等人[40]针对外包数据传输提出了可证明的持有的DT-PDP方法，其后提出的IAID-PDP[41]等方法都在可证明性和减少管理开销方面做了大量的工作。

9.2 云数据完整性审计

数据可检索证据模型(Proofs of Retrievability, POR)[42] 可保证云数据的完整性，但其在数据的动态更新、第三方审计和验证方面略显不足。Shacham等人[43]基于双线性签名方法，改进了POR模型。其后，Wang等人[44] 基于同态令牌和纠删码实现了对云存储完整性的审计，Jiang等人[45]提出了一种基于向量承诺和验证本地撤销组签名的安全组用户撤销的高效公共完整性审计方法。为优化数据完整性审计协议涉及的复杂密钥管理，Li等人[46]分别提出了基于属性的云数据完整性审计机制和基于生物特征作为模糊身份的模糊身份审计协议。

9.3 云数据审计的隐私保护

云数据审计的隐私保护主要实现审计云数据持有性或完整性前的提下对数据所有者身份和位置信息等数据进行隐私保护，该领域主要机制和方法包括表6中所列的4种方法。

10 云数据隐私保护

云数据隐私保护主要包括存储的隐私数据、所查询的数据及所使用的访问模式的隐私保护，其中隐私数据的存储可使用密码学方法(见第6节中的加密方法)实现，本节主要关注云数据访问过程中的查询和访问模式隐私保护。

10.1 查询隐私保护

目前针对查询隐私保护的研究主要集中在索引隐私、关键字隐私和限门不可链接性方面[47]。其中索引隐私要求原敏感数据的索引信息不被泄露，其主要思想是通过安全索引函数隐藏原数据和索引之间的关系来防止隐私泄露；关键字隐私[48]指任何查询关键字不能使用通过对限门分析推导得出，主要思想是通过将查询关键字转化为特殊的限门来实现关键字隐私保护；限门不可链接性指限门间关系不能通过对多个查询限门的推导得出。另外，环签名和群签名方法也常用于隐藏租户身份信息进而实现身份信息的隐私保护。但当群中租户频繁更改或者租户数量变化很大时，环签名和群签名方法在效率上存在不足。

10.2 访问模式隐私保护

访问模式[49]是一个访问序列，攻击者通过对其观察分析可以推断出如访问权限、访问频率及访问习惯等隐私信息。常见的访问模式隐藏方法有隐私信息检索(Private Information Retrieval, PIR)协议[50]和不经意随机访问(Oblivious RAM, ORAM)[51]。PIR协议的主要思想是通过存储在分布式服务器中的数据副本(每个副本之间不能进行通信)、令每个PIR协议执行参与方均不能获取访问的相关信息来保护隐私。ORAM的主要思想是通过数据和物理块之间的分层独立性来实现访问模式的隐私保护，包括局部清洗ORAM、多轮ORAM、单轮ORAM及并行ORAM等。其代表性方法优缺点比较如表7所示。

11 云数据可持续性保障

通常数据备份与恢复技术是云服务可持续性的主要保障手段之一。目前，常见的云数据备份机制主要有热备份、冷备份及暖备份等，它们的比较如表8所示。还有一些云服务商直接采用面向快速备份和恢复的操作系统来实现服务的可持续性，如HSDRT[52], Linux box[53], ERGOT[54], SBBR[55]等，这些系统的优缺点比较如表9所示。

12 总结与展望

本文讨论了云的数据安全所涉及的7方面的关键环节，并从10个方面总结和分析了已有的云数据安全保护的方法和技术。以下给出每个方面可进一步探索的研究问题：

(1) 云身份认证：

(a) 云计算环境下跨域身份认证。随着云计算环境的复杂化，跨域数据交换普遍存在，如何有效且安全地实现跨域身份认证是未来云应用的重要方面；

(b) 认证协议实施的安全性保障。在认证协议安全性理论证明的同时，在安全协议实施[56]过程中，由于实施人员的参差不齐和工程实践的差异所造成的协议实施与定义的不一致将引起云数据隐私泄露等问题。

(2) 云访问控制技术：

(a) 策略描述和属性撤销。通过基于属性加密的策略描述和属性撤销，以增强策略的表达能力和可用性；

表 6　云数据审计隐私保护方法比较

技术	应用场景	可拓展性
同态线性认证器&随机伪装	第三方审计，分批的远程数据审计	较好
同态消息验证码	共享数据的审计	一般
线性映射	分块数据集跨云数据审计	较好
同态可验证群/环签名	共享数据分块第三方审计	较差

表 7　云数据隐私保护方法比较

隐私对象	方法		优点	缺点
访问模式	PIR	信息论PIR	通信开销低	计算开销高
		可计算PIR	节省带宽，防止合谋	计算开销高
	ORAM	局部ORAM	系统开销较高	清洗部分遗漏
		多轮ORAM	系统开销可承受	效率较低
		并行ORAM	系统开销低	系统性能要求高
		单轮ORAM	系统开销较高	效率低
查询隐私	索引隐私		–	–
	关键字隐私和限门不可链接	非确定性限门	隐私性强	计算开销较高
用户身份隐私	环/群签名	环/群签名	攻击难度大/强隐私	可拓展性差

表 8 常见备份技术之间区别

技术模型	同步时间	恢复时间	备份特点	容错支持
热备份	几秒	几秒或几分钟	物理镜像	很高
改进的热备份	几分钟	约1 h	虚拟镜像	高
暖备份	几小时内	1～24 h	限制的物理镜像	一般
冷备份	几天内	超过24 h	从站点备份	低

表 9 云数据备份和恢复系统比较

方法/系统	主要技术	优点	缺点	适用场景
HSDRT[52]	超广泛分布的数据传输和高速加密技术	隐私保护、可靠性	需要调整web应用文件副本增加时，性能下降	云文件备份
Linux box[53]	Simple Linux box硬件盒	隐私保护、开销较小，灾难影响较小，成本低	浪费带宽	CSP之间服务迁移
ERGOT[54]	DHT协议、语义覆盖网络	检索准确、网络流量小	不能与语义相似性模型混合	基础设施下基于语义匹配场景
SBBR[55]	关注IP逻辑连接	开销小	逻辑和物理配置不一致	低开销和路由故障场景

(b) 结合多属性的访问控制。在基于属性的访问控制模型中，使用单一的属性实现访问控制面临较高安全风险，可以尝试将云计算中的新属性纳入云的访问控制机制，如位置属性、风险属性、访问目的和隐私需求等，建立基于多属性的访问控制机制；

(c) 软硬件协同。访问控制的软硬件协同设计，将软件实现的细粒度访问控制与硬件实现的控制机制相结合。

(3) 云数据安全计算：

云中多方安全计算[57]。将云计算所涉及的隐私数据计算、抽象为安全多方计算，以保护多云应用的隐私。

(4) 虚拟化安全技术：

基于信息流控制的云容器数据安全。当云容器中运行多种应用服务，由于云计算分布式协同合作的本质，各个应用服务之间的信息共享必然面临安全性问题，信息流控制技术可用来增强容器内的数据安全性。

(5) 云数据安全存储：

(a) 代理重加密。现有的代理重加密在效率方面有一定缺陷，可考虑将基于身份的代理重加密方法、区块链和后量子密码相结合，研究更高效的代理重加密方法；

(b) 前后向安全可验证的可搜索加密。SE的前向和后向安全分别防止注入攻击和在删除的数据上执行查询操作，而已有研究工作极少有同时保证前向安全和后向安全及其可验证性。

(6) 云数据安全删除：

(a) 移动云隐私数据的安全删除。已有研究工作很少关注移动云隐私数据的安全删除，尤其是移动云及移动终端产生的如支付信息、敏感私密消息等的安全删除且不可恢复；

(b) 海量数据的细粒度安全删除。在各种云和大数据应用中，对海量数据进行按需的细粒度删除可大大减少云存储实际投入的同时，实现对用户隐私数据的保护；

(c) 关联数据确定性删除。在跨云应用场景下，云应用可能跨越多个不同的云，云服务提供商通过备份及动态共享等机制对用户数据进行迁移，这将引起数据的多副本问题。建立多副本数据之间的关联规则，能较好解决跨云的数据确定性删除且不可恢复问题。

(7) 云信息流控制技术：

(a) 信息流控制模型的标准化。建立统一的标签描述和相互转化标准及标签管理框架及规则，形成统一的信息流控制方法和框架；

(b) 语言级别的信息流控制。在云计算、大数据、物联网和机器学习等新领域背景下，设计适合多核并行下信息流控制的新型程序设计语言，并对信息流控制安全性进行无干扰验证与分析。

(8) 云数据安全审计：

高效的密钥管理机制和审计方法。近年来很多研究工作使用ABE和IBE技术相结合实现了数据的完整性审计，令审计机制中密钥管理的复杂性得以优化。更高效的密钥管理仍然是云数据审计机制中重要的关注点。使用基于身份和基于区块链PDP方法代替证书验证，也可提升审计效率。

(9) 云数据隐私保护：

(a)隐私保护下的问责机制。在某种程度上，隐私和问责是两个对立问题，同时实现这两个目标并不容易。目前大部分研究工作只关注于隐私保护，探索隐私保护下的问责机制是非常必要的；

(b)隐私保护下的数据访问效率。目前的研究工作基本采用PIR和ORAM等方法防止数据访问过

程中的隐私数据泄露，但这些方法的数据访问效率较低；而通过密文搜索的查询准确率也不高。如何在隐私保护前提下提高数据访问效率和查询准确率是难点问题。

(10) 云服务层业务的可持续提供：

可信任评估及成本优化。研究如何评估值得信任的服务提供者以及有效降低数据恢复成本的实现机制和方法，以降低用户自身数据的丢失风险，推动云服务的广泛应用。

云的数据安全问题一直是学术界和产业界共同关注的热点之一。随着技术的不断发展，该领域必将有更多实用化的方法和技术涌现。

参 考 文 献

[1] SAKIMURA N, NRI, BRADLEY J, *et al*. OpenID Authentication 2.0[OL]. https://openid.net/specs/openid-authentication-2_0-11.html, 2007.

[2] SAKIMURA N, NRI, BRADLEY J, *et al*. OpenID Connect Core 1.0[OL]. https://openid.net/specs/openid-connect-core-1_0.html#toc. 2014, 2014.

[3] JIANG Qi, MA Jianfeng, and WEI Fushan. On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services[J]. *IEEE Systems Journal*, 2018, 12(2): 2039–2042. doi: 10.1109/JSYST.2016.2574719.

[4] SERVOS D and OSBORN S L. Current research and open problems in attribute-based access control[J]. *ACM Computing Surveys*, 2017, 49(4): 65. doi: 10.1145/3007204.

[5] LI Jiguo, YAO Wei, ZHANG Yichen, *et al*. Flexible and fine-grained attribute-based data storage in cloud computing[J]. *IEEE Transactions on Services Computing*, 2017, 10(5): 785–796. doi: 10.1109/TSC.2016.2520932.

[6] ALAM Q, MALIK S U R, AKHUNZADA A, *et al*. A Cross Tenant Access Control (CTAC) model for cloud computing: Formal specification and verification[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(6): 1259–1268. doi: 10.1109/TIFS.2016.2646639.

[7] ALMUTAIRI A, SARFRAZ M I, and GHAFOOR A. Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters[J]. *IEEE Transactions on Cloud Computing*, 2018, 6(1): 168–181. doi: 10.1109/TCC.2015.2453981.

[8] ACAR A, AKSU H, ULUAGAC A S, *et al*. A survey on homomorphic encryption schemes: Theory and Implementation[J]. *ACM Computing Surveys*, 2018, 51(4): 79. doi: 10.1145/3214303.

[9] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. The 41st Annual ACM Symposium on Theory of Computing, Bethesda, USA, 2009: 169–178. doi: 10.1145/1536414.1536440.

[10] POTEY M M, DHOTE C A, and SHARMA D H. Homomorphic encryption for security of cloud data[J]. *Procedia Computer Science*, 2016, 79: 175–181. doi: 10.1016/j.procs.2016.03.023.

[11] SHEN Changxiang. Constructing cloud security with trusted computing[J]. China Economic & Trade Herald, 2017(16): 56–57.

[12] CONTRACTOR D and PATEL D. Accountability in cloud computing by means of chain of trust[J]. *International Journal of Network Security*, 2017, 19(2): 251–259. doi: 10.6633/IJNS.201703.19(2).10.

[13] 拱长青, 肖芸, 李梦飞, 等. 云计算安全研究综述[J]. 沈阳航空航天大学学报, 2017, 34(4): 1–17. doi: 10.3969/j.issn.2095-1248.2017.04.001.

GONG Changqing, XIAO Yun, LI Mengfei, *et al*. Summary of cloud computing security research[J]. *Journal of Shenyang Aerospace University*, 2017, 34(4): 1–17. doi: 10.3969/j.issn.2095-1248.2017.04.001.

[14] SIERRA-ARRIAGA F, BRANCO R, and LEE B. Security issues and challenges for virtualization technologies[J]. *ACM Computing Surveys*, 2020, 53(2): 45. doi: 10.1145/3382190.

[15] KUMAR N, AUJLA G S, GARG S, *et al*. Renewable energy-based multi-indexed job classification and container management scheme for sustainability of cloud data centers[J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(5): 2947–2957. doi: 10.1109/TII.2018.2800693.

[16] AIKAT J, AKELLA A, CHASE J S, *et al*. Rethinking security in the era of cloud computing[J]. *IEEE Security & Privacy*, 2017, 15(3): 60–69. doi: 10.1109/MSP.2017.80.

[17] LIANG Xiaohui, CAO Zhenfu, LIN Huang, *et al*. Attribute based proxy re-encryption with delegating capabilities[C]. The 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 2009: 276–286. doi: 10.1145/1533057.1533094.

[18] LUO Song, HU Jianbin, and CHEN Zhong. Ciphertext policy attribute-based proxy re-encryption[C]. The 12th International Conference on Information and Communications Security, Barcelona, Spain, 2010: 401–415. doi: 10.1007/978-3-642-17650-0_28.

[19] 冯朝胜, 罗王平, 秦志光, 等. 支持多种特性的基于属性代理重加密方案[J]. 通信学报, 2019, 40(6): 177–189. doi: 10.11959/j.issn.1000-436x.2019127.

FENG Chaosheng, LUO Wangping, QIN Zhiguang, *et al*. Attribute-based proxy re-encryption scheme with multiple features[J]. *Journal on Communications*, 2019, 40(6): 177–189. doi: 10.11959/j.issn.1000-436x.2019127.

[20] 苏铓, 史国振, 付安民, 等. 基于代理重加密的云端多要素访问控制方案[J]. 通信学报, 2018, 39(2): 96–104. doi: 10.11959/j.issn.1000-436x.2018028.

SU Mang, SHI Guozhen, FU Anmin, *et al*. Proxy re-encryption based multi-factor access control scheme in cloud[J]. *Journal on Communications*, 2018, 39(2): 96–104. doi: 10.11959/j.issn.1000-436x.2018028.

[21] XIONG Hu, ZHAO Yanan, PENG Li, *et al*. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing[J]. *Future Generation Computer Systems*, 2019, 97: 453–461. doi: 10.1016/j.future.2019.03.008.

[22] 张玉磊, 文龙, 王浩浩, 等. 多用户环境下无证书认证可搜索加密方案[J]. 电子与信息学报, 2020, 42(5): 1094–1101. doi: 10.11999/JEIT190437.

ZHANG Yulei, WEN Long, WANG Haohao, *et al*. Certificateless authentication searchable encryption scheme for multi-user[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1094–1101. doi: 10.11999/JEIT190437.

[23] 牛淑芬, 谢亚亚, 杨平平, 等. 加密邮件系统中基于身份的可搜索加密方案[J]. 电子与信息学报, 2020, 42(7): 1803–1810. doi: 10.11999/JEIT190578.

NIU Shufen, XIE Yaya, YANG Pingping, *et al*. Identity-based searchable encryption scheme for encrypted email system[J]. *Journal of Electronics & Information Technology*, 2020, 42(7): 1803–1810. doi: 10.11999/JEIT190578.

[24] BOST R, MINAUD B, and OHRIMENKO O. Forward and backward private searchable encryption from constrained cryptographic primitives[C]. 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1465–1482. doi: 10.1145/3133956.3133980.

[25] CHAMANI J G, PAPADOPOULOS D, PAPAMANTHOU C, *et al*. New constructions for forward and backward private symmetric searchable encryption[C]. 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018: 1038–1055. doi: 10.1145/3243734.3243833.

[26] SUN Shifeng, YUAN Xingliang, LIU J K, *et al*. Practical backward-secure searchable encryption from symmetric puncturable encryption[C]. 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018: 763–780. doi: 10.1145/3243734.3243782.

[27] ZUO C, SUN Shifeng, LIU J K, *et al*. Dynamic searchable symmetric encryption with forward and stronger backward privacy[C]. The 24th European Symposium on Research in Computer Security, Luxembourg, 2019: 283–303. doi: 10.1007/978-3-030-29962-0_14.

[28] NAJAFI A, JAVADI H H S, and BAYAT M. Verifiable ranked search over encrypted data with forward and backward privacy[J]. *Future Generation Computer Systems*, 2019, 101: 410–419. doi: 10.1016/j.future.2019.06.018.

[29] PAUL M and SAXENA A. Proof of erasability for ensuring comprehensive data deletion in cloud computing[C]. The 3rd International Conference on Recent Trends in Network Security and Applications, Chennai, India, 2010: 340–348. doi: 10.1007/978-3-642-14478-3_35.

[30] LUO Yuchuan, XU Ming, FU Shaojing, *et al*. Enabling assured deletion in the cloud storage by overwriting[C]. The 4th ACM International Workshop on Security in Cloud Computing, Xi'an, China, 2016: 17–23. doi: 10.1145/2898445.2898447.

[31] TANG Yang, 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. doi: 10.1109/TDSC.2012.49.

[32] 杜瑞忠, 石朋亮, 何欣枫. 基于覆写验证的云数据确定性删除方案[J]. 通信学报, 2018, 40(1): 130–140. doi: 10.11959/j.issn.1000-436x.2019012.

DU Ruizhong, SHI Pengliang, and HE Xinfeng. Cloud data assured deletion scheme based on overwrite verification[J]. *Journal on Communications*, 2018, 40(1): 130–140. doi: 10.11959/j.issn.1000-436x.2019012.

[33] XUE Liang, YU Yong, LI Yannan, *et al*. Efficient attribute-based encryption with attribute revocation for assured data deletion[J]. *Information Sciences*, 2019, 479: 640–650. doi: 10.1016/j.ins.2018.02.015.

[34] PAPPAS V, KEMERLIS V P, ZAVOU A, *et al*. CloudFence: Data flow tracking as a cloud service[C]. The 16th International Symposium on Research in Attacks, Intrusions, and Defenses, Rodney Bay, USA, 2013: 411–431. doi: 10.1007/978-3-642-41284-4_21.

[35] PASQUIER T F J M, SINGH J, EYERS D, *et al*. Camflow: Managed data-sharing for cloud services[J]. *IEEE Transactions on Cloud Computing*, 2017, 5(3): 472–484. doi: 10.1109/tcc.2015.2489211.

[36] PRIEBE C, MUTHUKUMARAN D, KEEFFE D O, *et al*. CloudSafetyNet: Detecting data leakage between cloud tenants[C]. The 6th edition of the ACM Workshop on Cloud Computing Security, Scottsdale, USA, 2014: 117–128. doi: 10.1145/2664168.2664174.

[37] ATENIESE G, BURNS R, CURTMOLA R, *et al*. Provable data possession at untrusted stores[C]. The 14th ACM Conference on Computer and Communications Security, Alexandria, USA, 2007: 598–609. doi: 10.1145/1315245.1315318.

[38] ERWAY C C, KÜPÇÜ A, PAPAMANTHOU C, *et al*. Dynamic provable data possession[J]. *ACM Transactions on Information and System Security*, 2015, 17(4): 15. doi: 10.1145/2699909.

[39] WANG Yujue, WU Qianhong, QIN Bo, *et al*. Online/offline provable data possession[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(5): 1182–1194. doi: 10.1109/TIFS.2017.2656461.

[40] WANG Huaqun, HE Debiao, FU Anmin, *et al*. Provable data possession with outsourced data transfer[J]. *IEEE Transactions on Services Computing*, To be published. doi: 10.1109/TSC.2019.2892095.

[41] WANG Huaqun, HE Debiao, YU Jia, *et al*. Incentive and unconditionally anonymous identity-based public provable data possession[J]. *IEEE Transactions on Services Computing*, 2019, 12(5): 824–835. doi: 10.1109/TSC.2016.2633260.

[42] JUELS A and KALISKI B S. Pors: Proofs of retrievability for large files[C]. The 14th ACM conference on Computer and communications security, Alexandria, USA, 2007: 584–597. doi: 10.1145/1315245.1315317.

[43] SHACHAM H and WATERS B. Compact proofs of retrievability[J]. *Journal of Cryptology*, 2013, 26(3): 442–483. doi: 10.1007/s00145-012-9129-2.

[44] WANG Cong, WANG Qian, REN Kui, *et al*. Toward secure and dependable storage services in cloud computing[J]. *IEEE Transactions on Services Computing*, 2012, 5(2): 220–232. doi: 10.1109/TSC.2011.24.

[45] JIANG Tao, CHEN Xiaofeng, and MA Jianfeng. Public integrity auditing for shared dynamic cloud data with group user revocation[J]. *IEEE Transactions on Computers*, 2016, 65(8): 2363–2373. doi: 10.1109/TC.2015.2389955.

[46] LI Yannan, YU Yong, MIN Geyong, *et al*. Fuzzy identity-based data integrity auditing for reliable cloud storage systems[J]. *IEEE Transactions on Dependable and Secure Computing*, 2019, 16(1): 72–83. doi: 10.1109/TDSC.2017.2662216.

[47] DU Minxin, WANG Qian, HE Meiqi, *et al*. Privacy-preserving indexing and query processing for secure dynamic cloud storage[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(9): 2320–2332. doi: 10.1109/TIFS.2018.2818651.

[48] SUN Jianfei, HU Shengnan, NIE Xuyun, *et al*. Efficient ranked multi-keyword retrieval with privacy protection for multiple data owners in cloud computing[J]. *IEEE Systems Journal*, 2020, 14(2): 1728–1739. doi: 10.1109/JSYST.2019.2933346.

[49] PINKAS B and REINMAN T. Oblivious RAM revisited[C]. The 30th Annual Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2010: 502–519. doi: 10.1007/978-3-642-14623-7_27.

[50] TANG Jun, CUI Yong, LI Qi, *et al*. Ensuring security and privacy preservation for cloud data services[J]. *ACM Computing Surveys*, 2016, 49(1): 13. doi: 10.1145/2906153.

[51] WILLIAMS P, SION R, and CARBUNAR B. Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage[C]. The 15th ACM Conference on Computer and Communications Security, Alexandria, USA, 2008: 139–148. doi: 10.1145/1455770.1455790.

[52] UENO Y, MIYAHO N, SUZUKI S, *et al*. Performance evaluation of a disaster recovery system and practical network system applications[C]. 2010 5th International Conference on Systems and Networks Communications, Nice, France, 2010: 195–200. doi: 10.1109/ICSNC.2010.37.

[53] JAVARAIAH V. Backup for cloud and disaster recovery for consumers and SMBs[C]. 2011 5th IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, India, 2011: 1–3. doi: 10.1109/ANTS.2011.6163671.

[54] UENO Y, MIYAHO N, and SUZUKI S. Disaster recovery mechanism using widely distributed networking and secure metadata handling technology[C]. The 4th Edition of the UPGRADE-CN Workshop on Use of P2P, GRID and Agents for the Development of Content Networks, New York, USA, 2009: 45–48. doi: 10.1145/1552486.1552514.

[55] PALKOPOULOU E, SCHUPKE D A, and BAUSCHERT T. Recovery time analysis for the Shared Backup Router Resources (SBRR) architecture[C]. 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 2011: 1–6. doi: 10.1109/icc.2011.5963411.

[56] LU Jintian, YAO Lili, HE Xudong, *et al*. A security analysis method for security protocol implementations based on message construction[J]. *Applied Sciences*, 2018, 8(12): 2543. doi: 10.3390/app8122543.

[57] ZHAO Chuan, ZHAO Shengnan, ZHAO Minghao, *et al*. Secure multi-party computation: Theory, practice and applications[J]. *Information Sciences*, 2019, 476: 357–372. doi: 10.1016/j.ins.2018.10.024.

鲁金钿：男，1991年生，博士生，研究方向为网络安全、云数据安全及信息流控制等.

肖睿智：女，1997年生，博士生，研究方向为网络安全、云审计及隐私保护等.

金舒原：女，1974年生，教授，博士生导师，研究方向为云安全、网络攻击与防御等.

责任编辑：余　蓉