云计算数据安全

陈 龙 肖 敏 罗文俊 等 著

科学出版社

云计算数据安全

陈 龙 肖 敏 罗文俊 等 著

科学出版社
北京

内 容 简 介

云计算数据安全是学术界和产业界都非常关注的核心问题。当大量用户采用云存储模式后，用户数据不仅面临数据保密与数据共享的挑战，还面临可信数据安全问题。本书总结云计算环境下的数据安全威胁与需求，重点讨论基于属性加密的云数据访问控制、云计算环境下可搜索的数据加密、可证明数据安全与数据完整性验证，以及电子证据存储应用等侧面的最新技术与解决方案。

本书适合对云存储、云数据安全服务感兴趣的读者。对从事云计算数据安全、云存储安全研究的相关人员，从事云存储管理、服务的技术人员，以及云安全服务研发的相关人员有重要的参考作用。本书内容主要为云计算数据安全方面的最新研究成果，也可作为高年级本科生和研究生的教材或参考书。

图书在版编目(CIP)数据

云计算数据安全/陈龙等著. —北京：科学出版社，2016

ISBN 978-7-03-046911-3

Ⅰ. 云… Ⅱ. 陈… Ⅲ. 计算机网络-安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2015)第 318687 号

责任编辑：魏英杰 纪四稳 / 责任校对：桂伟利

责任印制：张 倩 / 封面设计：陈 敬

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2016 年 3 月第 一 版 开本：720×1000 1/16

2016 年 3 月第一次印刷 印张：13 3/4

字数：275 000

定价：90.00 元

(如有印装质量问题，我社负责调换)

前　言

云计算代表IT领域向集约化、规模化与专业化道路发展的趋势，是IT领域正在发生的深刻变革。云计算已进入稳步发展阶段，云计算的安全越来越受到重视。

云计算安全成为云计算领域亟待突破的重要问题。云计算环境的安全问题主要包括数据安全、网络安全以及计算安全三个方面，其中最为核心的是数据安全问题。当大量用户采用云存储模式后，很多用户数据既需要保密又需要共享，同时用户数据还可能遭到其他用户意外的修改及损坏，甚至云计算服务商的非诚信对待。研究人员将数据解密、密钥分配和数据访问控制结合起来，为加密数据共享提供灵活的访问控制方式；同时，支持处于加密状态的用户数据搜索利用也有了进展。对于数据安全存储及应用，可证明数据安全或安全审计为云存储提供了额外的安全保障及信用机制。服务方需要提供一种证明来表明数据安全性——保证用户数据的完整性、可用性、容错性或可靠性。电子数据在我国新的法律体系中也已作为新的证据类型独立存在，预先采取技术手段预防纠纷或提供电子数据证据成为广泛的实际需求。可证明数据安全的第三方证明、验证的结果可为解决纠纷提供有力的电子数据证据。

现有国内可见的云计算安全相关著作(译著)较多关注宏观层面的云计算环境下的安全问题，以及云计算部署、应用等方面的安全问题及风险，对云计算环境的安全技术与传统安全技术的差异关注不足。现有工作未能专门系统地讨论云计算数据安全问题。与同类书相比，本书具有以下特点：针对性、系统性地分析云计算环境、云存储面临的数据安全威胁，归纳、提炼具有可行性、实用性的前沿研究成果，重点讨论基于属性加密的云数据访问控制、可搜索的数据加密、可证明数据安全与数据完整性验证，以及电子证据存储应用等侧面的最新技术与解决方案。

本书是近年来国内外相关研究的简要总结，主要是项目组几年来研究成果的归纳与系统化。本书的第1、4、5、6章由陈龙负责编写，第2章由肖敏负责编写，第3章由罗文俊负责编写。全书由陈龙负责协调、统稿。参与项目组的研究工作或者参加本书的资料整理、协助编写的有曾经或正在重庆邮电大学就读的研究生王明昕、王春蕾、孙志蔚、郭函、陈亚琼、方新蕾、娄晓会、刘邦岚、宋巍、陈宏波、李俊中、甘慧、罗玉柱、王也、张涵等。

本书的出版得到重庆邮电大学出版基金的资助，也得到科学出版社的大力帮助，特此致谢！相关的研究工作得到国家社会科学基金项目(No. 14BFX156)、重庆

市自然科学基金项目(No. cstc2011jjA40031、No. cstc2011jjA0042)的支持。感谢导师王国胤教授对我们研究工作的指导！感谢计算智能重庆市重点实验室、计算机网络与通信重庆市重点实验室、网络与信息安全重庆市工程实验室、重庆邮电大学计算机科学与技术学院对我们研究工作的支持！也在此感谢为本书撰写付出辛苦努力的作者和参与者。

由于作者学术水平所限，书中难免会有不妥之处。恳请读者理解和批评指正，在此先致感谢！

陈　龙

2015 年 12 月

目　录

前言
第 1 章　云计算与数据安全 …… 1
1.1　云计算 …… 1
1.2　云计算安全 …… 3
1.3　云计算环境的数据安全威胁 …… 3
1.3.1　数据安全属性 …… 3
1.3.2　数据安全威胁 …… 4
1.4　本书组织结构 …… 6
参考文献 …… 6
第 2 章　云数据访问控制 …… 8
2.1　云数据访问控制需求 …… 8
2.2　属性加密机制 …… 8
2.2.1　属性加密基础 …… 9
2.2.2　KP-ABE …… 11
2.2.3　CP-ABE …… 12
2.2.4　用户属性撤销 …… 15
2.2.5　ABE 机制面临的主要攻击 …… 16
2.3　基于属性加密的云数据访问控制 …… 17
2.3.1　基本系统模型 …… 17
2.3.2　基于 KP-ABE 的方案 …… 18
2.3.3　基于 CP-ABE 的方案 …… 20
2.3.4　隐私问题 …… 23
2.4　多权威的基于属性加密的访问控制 …… 25
2.4.1　基本系统模型 …… 25
2.4.2　多权威云存储数据访问控制方案 …… 25
2.4.3　用户隐私保护 …… 33
2.4.4　多权威属性加密在个人医疗记录中的应用 …… 39
2.5　本章小结 …… 41
参考文献 …… 41

第 3 章 云计算环境的可搜索数据加密 …… 44
3.1 可搜索数据加密介绍 …… 44
3.1.1 对称可搜索加密的研究进展 …… 44
3.1.2 公钥可搜索加密的研究进展 …… 46
3.1.3 多关键字可搜索加密的研究进展 …… 48
3.1.4 多用户可搜索加密的研究进展 …… 48
3.1.5 结构化可搜索加密的研究进展 …… 50
3.2 对称可搜索加密 …… 52
3.2.1 基于为随机数的可搜索加密方案 …… 52
3.2.2 基于布隆过滤器的可搜索加密方案 …… 54
3.2.3 基于字典的可搜索加密方案 …… 55
3.2.4 多关键字可搜索加密方案 …… 56
3.2.5 Curtmola 的两个可搜索加密安全方案 …… 58
3.2.6 支持动态更新的 Kamara 方案 …… 59
3.2.7 基于 *k*NN 计算的可搜索加密方案 …… 60
3.2.8 top-*k* 问题讨论 …… 61
3.3 公钥可搜索加密 …… 62
3.3.1 公钥可搜索加密简介 …… 62
3.3.2 基于双线性对的可搜索加密方案 …… 63
3.3.3 基于关键词更新的公钥可搜索加密方案 …… 64
3.3.4 基于身份的公钥可搜索加密方案 …… 66
3.3.5 基于 SDH 假设的公钥加密搜索方案 …… 67
3.3.6 一种基于强 RSA 的多用户可搜索加密方案 …… 68
3.3.7 一种基于大数分解困难问题的可搜索加密方案 …… 70
3.3.8 一种基于布隆过滤器的多用户可搜索加密方案 …… 71
3.4 支持模糊处理的可搜索加密 …… 73
3.4.1 模糊处理问题分析 …… 74
3.4.2 基础概念 …… 74
3.4.3 基于通配符的密文模糊搜索方案 …… 76
3.4.4 基于 LSH 的密文模糊搜索方案 …… 77
3.4.5 基于安全 *k*NN 计算的密文模糊搜索方案 …… 79
3.4.6 支持同义词的密文模糊搜索方案 …… 81
3.4.7 其他方案简介 …… 87
3.4.8 研究方向 …… 88
3.5 本章小结 …… 88
参考文献 …… 88

第 4 章　云计算环境的可证明数据安全 …… 92
4.1　可证明数据安全概论 …… 92
4.1.1　可证明数据安全需求 …… 92
4.1.2　数据安全证明模型 …… 93
4.1.3　可证明数据安全研究发展 …… 95
4.1.4　可证明数据安全验证方案分类 …… 97
4.1.5　数据安全威胁与安全需求 …… 98
4.2　数据安全证明机制 …… 100
4.2.1　数据安全证明通用框架 …… 100
4.2.2　选择性验证方法 …… 102
4.2.3　一个数据完整性私有验证方案实例 …… 103
4.3　可公开验证的证明方法 …… 105
4.3.1　三方安全模型 …… 105
4.3.2　基于双线性对的公开验证方法 …… 107
4.3.3　具有完全隐私保护能力的方案 …… 111
4.3.4　签名的数据粒度方案 …… 112
4.3.5　防欺诈的验证方案 …… 115
4.4　数据容错性安全验证方案 …… 116
4.4.1　备份数据容错 …… 116
4.4.2　纠删码数据容错 …… 121
4.4.3　基于网络编码的数据容错 …… 121
4.5　移动云计算环境的数据安全 …… 122
4.5.1　威胁模型 …… 122
4.5.2　完整性验证方案 …… 123
4.5.3　安全性分析 …… 125
4.5.4　性能分析 …… 129
4.6　本章小结 …… 131
参考文献 …… 131
第 5 章　云计算环境的可证明动态数据安全 …… 133
5.1　动态数据认证结构 …… 133
5.1.1　动态默克尔哈希树 …… 133
5.1.2　带相对序号的动态默克尔哈希树 …… 135
5.1.3　跳表 …… 136
5.2　动态数据完整性验证方案 …… 136
5.2.1　系统模型与需求 …… 136
5.2.2　数据完整性验证方案 …… 137

5.2.3 数据动态操作 …… 142
5.2.4 多用户数据的批处理验证 …… 145
5.2.5 安全性分析 …… 147
5.2.6 性能分析 …… 147
5.3 多粒度动态数据安全 …… 149
5.3.1 多粒度需求及设计目标 …… 149
5.3.2 多粒度数据完整性验证方案 …… 150
5.3.3 多粒度方案动态操作 …… 152
5.3.4 安全分析 …… 153
5.3.5 性能分析 …… 154
5.4 多副本动态数据安全方案 …… 156
5.4.1 方案思路 …… 156
5.4.2 符号定义 …… 156
5.4.3 主要算法 …… 157
5.4.4 算法安全及性能分析 …… 161
5.5 用户签名协同计算方案 …… 162
5.5.1 协同计算方案 …… 162
5.5.2 安全及性能分析 …… 163
5.6 本章小结 …… 165
参考文献 …… 166
第 6 章 云计算环境的电子证据存储应用 …… 167
6.1 引言 …… 167
6.1.1 电子数据证据存储的安全需求 …… 167
6.1.2 电子法定专业特权数据处理方法 …… 168
6.1.3 大数据量的细粒度证据固定 …… 169
6.1.4 云计算环境的电子证据固定与存储 …… 171
6.2 细粒度数据完整性原理 …… 171
6.2.1 哈希可压缩性 …… 171
6.2.2 组合编码原理 …… 171
6.2.3 基于组合编码原理的完整性检验 …… 172
6.2.4 细粒度的完整性检验方法 …… 173
6.3 具有单错指示能力的细粒度数据完整性检验方法 …… 179
6.3.1 单错指示问题 …… 179
6.3.2 组合单错完整性指示码 …… 180
6.3.3 超方体单错完整性指示码 …… 182
6.3.4 单错完整性指示码设计实例分析 …… 185

6.4　具有多错指示能力的细粒度数据完整性检验方法 …… 186
6.4.1　多错指示问题 …… 186
6.4.2　有限域划分方法 …… 187
6.4.3　有限域多错完整性指示码 …… 191
6.4.4　有限域多错指示码设计实例分析 …… 199
6.5　电子数据证据存储应用 …… 201
6.5.1　存储模型及处理流程 …… 201
6.5.2　电子数据安全存储方案 …… 202
6.6　本章小结 …… 207
参考文献 …… 207

第 1 章　云计算与数据安全

1.1　云　计　算

1. 云计算

云计算体现为一种商业计算模型，通过网络以按需、易扩展的方式提供各种应用系统所需的硬件、平台、软件资源或者用户需要的基于信息化手段的服务。从使用者的角度，这些资源或服务如同水、电等资源的供给方式，可以按需获取和使用，并按使用付费。云计算最终表现为一种服务，一般称为云服务。云计算表明信息技术领域向集约化、规模化与专业化道路发展的趋势，它改变了对信息技术的供给和使用方式。与传统的方式相比，云服务最大的优势在于供给弹性和低成本，云计算的发展也是信息化进一步深化的必然需求，从而得到世界范围内的广泛关注、研究与建设实施。

2. 云计算特性

云计算作为新的计算模式，具有新的重要特性。

(1) 超大规模。构成云的设施具有相当大的规模，云计算能为用户提供前所未有的计算能力，无规模无法实现其优势[1]。谷歌、亚马逊、微软等公司的云计算已拥有几十万、几百万台服务器。

(2) 虚拟化[1]。云计算拥有庞大的计算、存储各类资源的资源池，支持用户不分地点、时间、终端特性、接入形式来获取服务。所请求的资源、服务由“云”提供，不依赖于具体的某个部分的实体。

(3) 按需服务。基于云计算的庞大资源池，用户按需购买，服务实现时可自动获取计算资源或服务。

(4) 高可伸缩性。云计算具有弹性架构，资源或服务能力可以快速、弹性地供应，满足应用和用户规模变化的需要。用户可以根据需求随时获得和调用基础设施资源，也可随时撤销和缩减这些资源，避免了资源不足或资源浪费。

(5) 高可靠性与通用性[1]。云计算整体上需要采用多种措施来提高、保障可靠性；同时，云计算不针对特定的场景或应用，在云计算平台可以实现千变万化的应用，可以同时支撑不同的应用运行。

(6) 廉价特性。云计算的廉价基础设施、弹性架构、自动管理，以及云的规模效应保证其具有优越的性能价格比优势。

3. 云计算的部署

依据云计算的部署方式，可区分为以下不同类型。

(1) 公有云。由云服务提供商拥有或间接使用，并负责对云中的软件资源进行管理和维护，向用户开放。而用户只需要支付相应的资源费用，就可以使用公有云中的所有业务。用户本身并不需要做相关的投资和建设。其优势在于开放性，用户使用方便。由于是公共服务产品，所以对于云计算的物理安全以及逻辑安全的监管程度是比较低的。同时，公有云要求把用户或公司的数据从内部网络转移到外部网络中，业务运行需要宽带的支持；除了需要一定的成本，响应时间、数据量也需要匹配。公有云中的数据安全成为普遍担心的问题。

(2) 私有云。由云服务提供商拥有，其所有服务均不提供给外部用户使用，仅为某个特定的组织服务。由该组织机构自身负责对服务的配置、管理等任务。与私有云有关的网络、存储等基础设施都由该组织机构单独所有，并不与其他机构分享。私有云的部署比较适合有许多分支的大型企业。私有云的缺点是持续运营成本比较高，可能会超出使用公有云的成本。

(3) 混合云。两个或多个保持各自实体独立性的不同云基础设施(私有的或公共的)形成的一个组合，该组合可实现数据和应用程序的可移植性。实际上，混合云是公共云和私有云的混合。它结合了公有云和私有云各自的特点，可提供各种组合的优化特性。

4. 云存储

云存储属于提供数据存储的一种云服务。该服务主要为用户提供数据存储和必要的数据管理服务。用户在有网络连接的地方，可以随时随地存放或获取云上的数据。云存储可以采用上述不同的部署方式，从而可分为公有云存储、私有云存储和混合云存储。基于虚拟化的效果，用户数据往往存储在多个虚拟服务器上。

和云计算整体的特点类似，云存储服务具有如下一些明显的优势。

(1) 容量的可扩展性。云存储的备份容量是没有限制的，用户可以根据自己的需求随时扩展和获取。用户基于云存储服务商的扩展能力，而不需关心存储容量问题。当用户的需求扩大时，云存储服务将可以很方便地在原有基础上扩展存储空间，满足需求。

(2) 统一管理并提升工作效率。当组织、公司的数据量很大，或者涉及的管理面较多时，分散的管理往往不能保证数据的一致性，员工或用户自己管理自己的存储，效率较低，同时也很难实现对信息的有效控制。数据备份、数据压缩等多方面的用户需求均由服务方自动实现。

(3) 成本、费用的节省。使用云存储服务，用户不必担心设备升级、数据迁移

或者设备淘汰等问题，云服务提供商将承担存储基础设施的建设与维护。边使用边付费的模式减少了备份设备的采购、实施、维护等方面的成本，相对而言，将因此节省大量经费。

1.2　云计算安全

云计算具有分布式计算及存储、无边界、虚拟化、多租户、数据所有权与管理权分离等特性，也更加具有开放性。由于云中包含了大量的软件与服务，数据量十分巨大，系统非常复杂，所以传统的安全技术和管理方案难以奏效，需要在传统技术的基础上研究新的技术与方案。云计算系统中存放的信息比传统信息系统数据更多，若是云计算系统遭到攻击，遭受的损失比传统服务更加严重。

冯登国等总结了关于云计算与安全之间关系的两种对立的说法[2]：持有乐观看法的人认为，采用云计算会增强安全性，因为通过部署集中的云计算中心，可以组织安全专家以及专业化安全服务队伍实现整个系统的安全管理，避免了现在由个人维护安全，由于不专业导致安全漏洞频出而被黑客利用的情况；另一种观点认为，集中管理的云计算中心将成为黑客攻击的重点目标，并且由于系统的巨大规模以及前所未有的开放性与复杂性，其安全性面临着比以往更为严峻的考验。所以，对于普通用户，其安全风险不是减少而是增多。

总之，云计算面临的安全问题已经严重阻碍了云计算系统和业务的进一步发展，成为迫切需要应对的重要问题，学术界和产业界都十分关注。

云计算技术在不断演进，云计算在努力提高整体使用效率的同时，为实现用户信息资产安全与隐私保护带来极大的冲击与挑战[2-5]。IDC的调查、研究人员的看法都显示云计算的安全问题是人们接受云服务所担心的首要问题，人们对云计算还缺乏足够的信任[2,3,5]。云计算安全成为云计算领域亟待突破的重要问题[6-9]。文献[9]将云计算环境涉及的安全问题分为数据安全、计算安全和网络安全三个方面。下面针对其中的数据安全展开讨论。

1.3　云计算环境的数据安全威胁

1.3.1　数据安全属性

1. 数据机密性

数据机密性指未经授权的个人和实体不能得知数据的内容。通常结合数据加密技术和数据访问控制的手段来实现。

2. 数据完整性

数据完整性指特定的数据在存储状态或传输过程中保持完全不变。数据完整性在任何系统中均是关键的要素之一。保证数据完整性一方面是要确保访问控制实施得当，只授权给适当的人进行访问；另一方面是对数据完整性进行检查。由前面的讨论可知，云计算环境下数据完整性在数据传输、数据迁移等情形下都有受到影响的可能。云计算环境下，数据存储不受用户的直接控制，用户一般不知道他们的数据存储在哪个物理机器上，或者哪些系统安放在何处。而且数据集可能是动态的、频繁变化的，这些频繁变化使得传统完整性的技术无法发挥效果。数据完整性除了从数据安全的角度考虑，还需要结合特定情形的计算安全性。

3. 数据可用性

数据可用性指具有访问权限的用户在需要数据时可以及时得到该数据。

4. 数据容错性

数据容错性是数据可用性的扩展，只有在数据存在的条件下才能保证数据可用。数据容错性保障在自然条件下抵抗数据出现差错的能力，在数据出现一定程度的错误时可以恢复出原数据。现有的备份技术、纠错码技术为云计算服务提供了实现条件。

5. 数据安全可证明性

数据安全可证明性指存在一种安全证明机制，数据的安全不仅客观得到实现，还可以向用户提供证明。理想的情况是这种机制既约束服务方提供承诺的服务质量，也约束用户方诚实地交付数据。数据的完整性与可用性以及数据容错性都可以基于该机制间接实现，为数据的真实性、安全性提供额外的信用安全保障。

1.3.2 数据安全威胁

云计算环境下数据的安全威胁有以下几个方面。

1. 数据泄露

数据泄露是对数据机密性的破坏，是云计算安全中的一个重大威胁，数据的泄露将对企业和用户造成重大损失[10]。

云计算环境有很多场景会造成对数据机密性的损害，相应地存在技术性的若干挑战。

(1) 数据加密。首先,若数据以明文形式存在,其在传输、存储、处理的过程中都有可能被非授权获取,并直接得知数据内容。基于密码学上安全的算法实现数据加密、保证数据的机密性是普遍的办法。同时,在云计算环境下,采用数据加密的方式来确保数据的机密性和隐私性,也存在不少的困难。一方面是数据加密的方式,若由用户自行加密,用户方需要加密、解密计算任务,而且数据被加密后在云中进行查找,加工处理变得十分困难[6]。若是由服务方加密、解密,也存在攻击者攻击服务方,或者管理方通过虚拟机监控器获取内存快照从而获得密钥、私钥甚至篡改相关数据的可能等问题[11]。另一方面是密钥的传递与分发管理,涉及大量用户共享的情形则问题十分复杂。

(2) 数据隔离。多租户技术是云计算中用到的关键技术。多个租户或用户的数据会存放在同一个存储介质上、同一个数据表里,在同一个服务器上由程序运行时使用,存在用户之间交叉访问数据的可能性[6,12]。

(3) 数据起源。数据不断地传递、加工、处理,数据的来源确定往往也会成为困难问题。

(4) 数据迁移。云计算模式下,提供服务的进程可能在服务器上不断地迁移,进程迁移过程中需要对内存数据、机器状态以及相应的磁盘数据进行迁移,数据在迁移过程中存在被泄露、被篡改的可能[6,11,12]。

(5) 数据清洗。数据在删除后可能没有彻底清除,在物理上可能有残留。数据残留可能被有心者有意收集,从而透露用户的敏感信息。基于云计算的模式,数据在传输、存储、处理过程中很难保证其被彻底删除。数据清洗则定位于考虑各种可能的情况,彻底删除特定的敏感数据[12]。

(6) 数据位置。云计算的分布式处理方式及动态迁移特性导致数据在处理的过程中位置十分不确定,数据位置的确定也是一大困难任务。数据穿越国界(境)之后还存在不同国家的法律约束不同的问题[12]。

2. 数据丢失、篡改

数据丢失、篡改是对数据完整性的破坏,是云计算环境数据安全面临的主要威胁。攻击者可能由于各种原因将攻击对象的数据删除,云服务提供商对数据存储采取的防护措施不当,可能会导致数据丢失。数据的保密性需要大量的密钥,若用户对密钥管理不当,甚至丢失密钥,将很有可能使数据丢失[10]。若服务方不可信,也存在数据删除、有损压缩的情况。

3. 拒绝服务/数据劫持

拒绝服务/数据劫持是对数据可用性的破坏,拒绝服务、用户身份或服务流量被劫持也是云计算的一个安全威胁[10]。典型的情况包括:网络上的拒绝服务攻击

导致服务方不能提供数据访问，使数据不能正常使用；云计算服务商因故障出现停机情况；云计算中存储的数据出现丢失现象，无法访问到用户数据；云计算服务商因特殊原因而倒闭，不提供数据存储、访问服务。

如果攻击者获取到用户的账号、口令信息，既可以修改用户口令，造成拒绝服务，也可以窃取到用户的数据和个人信息。攻击者还可能通过这些用户账号信息发起新的攻击。

4. 数据隐私

除了用户数据泄露造成数据机密性被破坏，还可能对用户隐私构成威胁[10]。用户身份、个人私密信息等方面的内容可能来源于数据泄露，还可能缘于长期的行为监视、数据之间的关联等，数据隐私需要匿名机制的支持。

1.4 本书组织结构

数据安全涉及的问题十分广泛，研究者也相应地有不少研究成果。本书主要针对云计算环境中的几个关键问题，总结、阐述研究组的研究成果。

第 2 章讨论云计算环境下的数据访问控制。数据加密是普遍采用的安全措施，访问控制是实现数据安全的最主要手段。数据拥有者必须通过加密数据并控制用户的解密能力以实现访问控制。基于属性的密文数据访问控制十分受关注。属性加密机制将密文与私钥分别与一组属性相关联，当用户的私钥属性与密文属性相互匹配达到一个门限值时，可以给用户解密密文。属性加密机制可以有效地解决大量用户共享数据的问题。

第 3 章讨论云计算环境下可搜索数据加密技术。数据加密后密文的处理十分困难，可搜索的加密技术对密文处理支持十分重要。

第 4～6 章讨论可证明数据安全及应用。基于数据安全可证明性，针对数据完整性并结合其可用性、容错性，分别讨论可证明静态数据安全、可证明动态数据安全以及可证明数据安全的一种应用场景——电子数据的固定与存储。

参 考 文 献

[1] 刘鹏. 云计算. 3 版. 北京：电子工业出版社，2015：3-4.

[2] 冯登国，张敏，张妍，等. 云计算安全研究. 软件学报，2011，22(1)：71-83.

[3] Kaufman L M，Harauz J，Potter B. Data security in the world of cloud computing. IEEE Security & Privacy，2009，7(4)：61-64.

[4] Mather T，Kumaraswamy S，Latif S. 云计算安全与隐私：企业风险处理之道. 刘戈舟，等，译. 北京：机械工业出版社，2011.

[5] CSA. Security Guidance for Critical Areas of Focus in Cloud Computing V2. 1. http://www.cloudsecurityalliance.org/guidance/[2015-6-20].

[6] 冯朝胜，秦志光，袁丁. 云数据安全存储技术. 计算机学报，2015，38(1)：150-163.

[7] 俞能海，郝卓，徐甲甲，等. 云安全研究进展综述. 电子学报，2013，41(2)：371-381.

[8] 林闯，苏文博，孟坤，等. 云计算安全：架构、机制与模型评价. 计算机学报，2013，36(9)：1765-1784.

[9] 邹德清，金海，羌卫中，等. 云计算安全挑战与实践. 中国计算机学会通讯，2011，7(12)：55-61.

[10] 张尼，刘镝，张云勇，等. 云计算安全技术与应用. 北京：人民邮电出版社，2014：36-40.

[11] Rocha F，Correia M. Lucy in the sky without diamonds：stealing confidential data in the cloud. Proceedings of the International Conference on Dependable Systems and Networks Workshops，2011：129-134.

[12] Jansen W A. Cloud hooks：security and privacy issues in cloud computing. Proceedings of the 44th Hawaii International Conference on System Sciences，2011：1-10.