Journal of Security and Safety Technology 安防技术, 2017, 5(3), 36-41
Published Online September 2017 in Hans. http://www.hanspub.org/journal/jsst
https://doi.org/10.12677/jsst.2017.53006

Hans汉斯

Cloud Data Lifecycle Security Issues and Encryption Technology Research

Nengneng Li[1,2], Yongsheng Zhang[1,2]

[1]School of Information Science & Engineering, Shandong Normal University, Jinan Shandong
[2]Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan Shandong
Email: linengneng1992@163.com

Received: Aug. 15th, 2017; accepted: Aug. 30th, 2017; published: Sep. 5th, 2017

Abstract

With the development of cloud computing, more and more enterprises and individuals are using the cloud platform to store data and deal with the relevant data. The data is uploaded to the cloud server and stord and managed by the cloud server. However, with the increase in users and cloud service providers, more and more cloud service providers appear the situation data leakage; cloud computing security issues have become increasingly prominent. The data is uploaded to the cloud server until the data is definitely deleted. In the process of data storage, data transmission and data destruction, the data is easily stolen and illegally used, and it can not be deleted; the data generated a great threat. This paper will study the security of data in cloud computing, discuss the data transmission security in cloud environment on the basis of analyzing the current situation of cloud computing and the main technology of cloud computing, and put forward the corresponding measures to ensure the data transmission security in cloud computing.

Keywords

Cloud Computing, Cloud Security, Data Security, Encryption, Erase Technology

云数据生命周期安全性问题及加密技术研究

李能能[1,2]，张永胜[1,2]

[1]山东师范大学，信息科学与工程学院，山东 济南
[2]山东师范大学，山东省分布式计算机软件新技术重点实验室，山东 济南
Email: linengneng1992@163.com

收稿日期：2017年8月15日；录用日期：2017年8月30日；发布日期：2017年9月5日

文章引用：李能能，张永胜．云数据生命周期安全性问题及加密技术研究[J]．安防技术, 2017, 5(3): 36-41.
DOI: 10.12677/jsst.2017.53006

摘　要

随着云计算的深入发展，越来越多的企业和个人都利用云平台来存储数据以及进行相关数据的处理，将数据上传到云服务器，由云服务器进行储存和管理。然而，随着用户以及云服务商的增多，越来越多的云服务商出现数据泄露的情况，云计算的安全问题也日渐突出。在数据存储、数据传输和数据销毁的过程中，数据极易出现被盗取后非法使用及无法删除数据的情况，对数据产生极大的威胁。本文将针对云计算中数据的安全性进行研究，在分析云计算发展现状及云计算主要技术的基础上对云环境下的数据传输安全进行讨论，并提出相应的解决措施，以保证云计算中数据传输的安全性。

关键词

云计算，云安全，数据传输安全，加密技术，擦除技术

1. 引言

云计算作为一种新的运行模式或者说是一种信息服务的新概念，其发展已逐步趋于成熟。尽管如此，很多企业对这种模式的商业应用仍然持观望态度，主要原因在于云计算较低的安全性。云计算用户的多样性、结构的复杂性和数据的动态性都可能使在云环境下的数据存在很多的不确定性，甚至还会造成巨大的损失[1]。本文将分析云计算数据传输的安全性的相关问题，并给出相应的解决措施。

2. 云计算发展现状

2.1. 云计算概念

云计算是按使用量进行付费的一种模式，这种模式可以提供便捷的、可用的、按需的网络访问，进入可配置的计算资源共享池(包括网络资源，服务器资源，存储资源，应用软件资源和服务资源等)，这些资源能够被快速地提供，只需要投入很少的管理工作，或与服务商进行很少的交互。

2.2. 国内外研究现状

云计算作为一个新的概念在 2006 年 8 月 9 日由 Google 首席执行官埃里克·施密特(Eric Schmidt)在搜索引擎大会(SES San Jose 2006)首次被提出，依次经历了电厂模式、效用计算、网络计算和云计算四个阶段逐步发展到现在这样比较成熟的水平。当前，包括国际电信联盟[2]、云计算安全联盟[3]和结构化信息标准[4]等的越来越多的组织和结构已经加入到了云计算标准的研究和制定行列中[5]，以及 Amazon、IBM、Sales force、微软和 Google 等 IT 巨头企业投入了大量的人力、物力和财力来研究云计算，并相继推出了各自的云计算平台[6]。

3. 数据生命周期

云计算中，数据从产生到销毁共经历六个过程，简称为云数据的生命周期，这六个阶段包括：数据创建、数据存储、数据传输、数据使用、数据归档及数据销毁。具体过程如下图 1 所示：

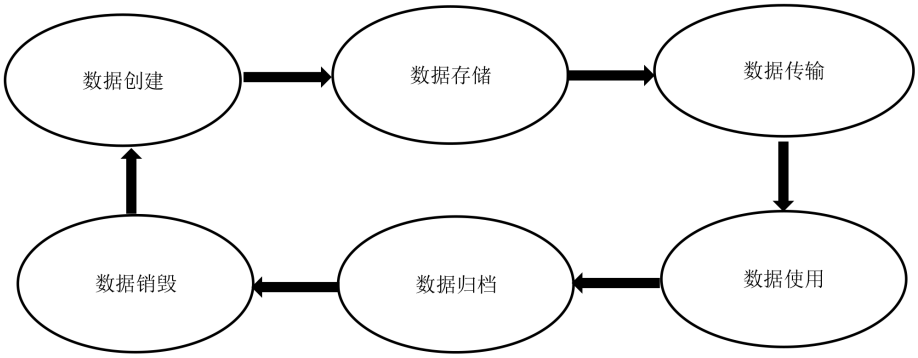

Figure 1. Data life cycle
图 1. 数据生命周期

在云计算中数据生命周期的各个阶段都存在着安全性问题，所以，要想减少云数据的安全隐患，就要在数据发展的各个阶段做好安全问题处理工作。

1) 数据的创建

数据的创建过程是由个人完成的，个人或企业通过自己的设备进行数据的采集、输入、查询、整编等创建出自己所需的数据。在这一过程中可能会出现数据的泄露和外来人员访问的安全性问题，为了保障整个过程中数据的安全与可信，需要对对数据进行访问权限、加密和安全等级等方面的控制。

2) 数据的存储

数据产生后被存储在存储空间中，如内存、硬盘等，但是这些存储空间必须是在合同、服务水平协议和法规允许的地理位置，存储的数据必须要保证包括所有的副本和备份，以防止数据丢失而造成损失。例如，使用由欧盟的“法规遵从存储条例”管理的电子健康记录，可能对数据拥有者和云服务提供商都是一种挑战[7]。将数据存放在云端后要考虑其可靠性、保密性以及完整性，考虑供应商的安全权限管理措施是否完善，对存储的数据是否进行了安全管理，以及数据的存放格式是否合理[8]。所以，要保证在这一过程中数据的安全，需要对数据进行完整性保证、数据加密以及数据隔离等措施。

3) 数据的传输

数据的最大的特性就是其共享性，数据通过传输来为其他客户提供数据，实现数据的共享性。云数据通过网络、进程通信等方式传输给其他的客户和虚拟服务所使用，由于网络的开放性，数据不能在没有安全控制的情况下进行传输。数据的创建者要考虑是否要对数据进行管理权限的设置，所以要保证传输数据的安全，就要使用数据加密技术同时维护数据传输过程中的保密性及传输后的完整性。

4) 数据的使用

数据的使用是云计算数据生命周期中数据建立的最终的目的，用户在使用数据前要先检查数据的来源，确定安全后对数据进行解密，然后再对数据进行操作。在使用数据前要先对数据进行备份，不能随便假定云环境下的数据都有备份并可恢复，为防止在使用过程中数据的丢失、覆盖或是损坏，必须对数据进行有效的备份和制定有效的数据恢复计划。

5) 数据的归档

数据归档就是将已经使用完的旧数据遵从一定的规则进行保存，这些旧数据在后面的是过程中具有一定的参考价值且是很重要的数据。数据存档具有索引和搜索功能，以便数据在以后的使用过程中很容易找到。但是这些数据要求很高的安全性和访问控制，在云环境下，在没有仔细检查第三方服务的情况下，将合规数据通过云存档的方式存放可能会带来风险。所以，在数据归档的过程中，要对数据进行加密，如磁盘备份和其他长期储存介质。

6) 数据的销毁

云端中的数据在被外部存储空间存储后，如果该数据已经使用完毕，就必须对该数据进行清除，即方便存储其他服务数据，更重要的是保证该数据的安全性。在原有的销毁工作中，最常用的方法就是删除，但这种方法知识销毁了文件的指针，没有将文件彻底销毁。对于企业用户的核心文件和保密数据，云服务系统有必要为其设定一种擦除服务，或者提供一种更为直接的介质删除方法类来对敏感数据进行相应的保护。

4. 数据安全技术

在云计算中，数据的安全问题贯穿了整个云终端的使用过程，数据流动到的地方都需要建立安全防护机制。在上述的数据生命周期过程中，为保证数据的机密性和完整性，数据加密技术、数据备份技术、数据隔离技术和数据擦除技术是必不可少的。

4.1. 数据加密技术

数据加密是数据生命周期过程中保证数据安全核心内容，在数据的创建、存储、传输、使用和归档过程中云计算的服务商和商户都需要采用数据的加密技术来保证数据的安全保密和完整传输。现在，云计算服务提供商对数据的加密环境进行了改进和提升，但是用户仍然需要对自己的数据进行加密，也可以使用第三方技术对服务过程中的数据进行加密处理[9] [10] [11]。

加密技术由算法和密钥两个部分组成，算法指的是如何将数据与密钥相结合产出密文和将密文解密成原始数据的操作过程，密钥则是数据加密和解密所对应的算法。密码机制可分为对称加密技术和非对称加密技术，经典的对称加密技术是 DES 算法，经典的非对称加密技术为 RAS 算法。

4.1.1. 对称加密技术 DES

对称加密技术是指在数据的加密和解密过程中使用相同的加密密钥和解密密钥，以此来保证数据的安全性，对称技术有着使用简单方便的优点，能够满足基本的数据加密的要求，是使用最普遍的数据加密技术。图 2 是对称加密算法的流程图。

对称加密算法包括两种类型：分组密码算法和流密码算法。分组密码算法是以数据块为单位对明文进行处理，它将输入的明文分组作为一个整体，输出一个等长的密文分组。分组密码大多数情况下采用 Feistel 结构，并通过多轮的相同的操作来提高加密算法的安全性。在每一轮中仅仅只对分组的一半进行代换，等交换后，下一轮再对另一半进行代换，每一轮操作使用的密钥都是不同的。流密码算法又可称为序列密码算法，是对明文进行连续不断的处理，通常以比特或字节作为操作对象。典型的流密码结构包括一个伪随机数发生器，在不知道密钥的时候，可以产生一个不能够预知的伟随机流，输入的明文依次与该伪随机流进行异或操作，加密数据。下面介绍典型的对称加密技术 DES。

DES [12]的设计核心思想是让所有的秘密寓于密钥之中。DES 在加密之前先以 64 比特为分组单位，对整个明文进行分组；然后对每个分组进行加密，生成一组密文，每组密文的信息还是 64 比特；最后连接每一组密文得出加密后的信息。图 3 是 DES 加密的原理图。

DES 算法主要分三个阶段对明文进行处理。

阶段一：置换 IP，在这个过程中对每个 64 bit 分组明文按照比特进行重新编排，不需要使用密钥。初始置换只是简单的移位操作，把明文的 64 bit 中的 0 和 1 bit 串按 8 × 8 矩阵进行排列并编号，然后打乱重排，按照将原来分组明文的第 58 位和第 50 位置换成第 1 位和第 2 位的规则来打乱顺序。

阶段二：置换和代替，进行 16 次与密钥相关的循环加密运算。已经进行初始置换的 64 位将进行 16 次于密钥相关的循环加密运算。

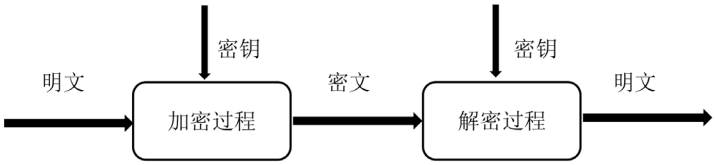

Figure 2. Encryption algorithm flow chart
图 2. 加密算法流程图

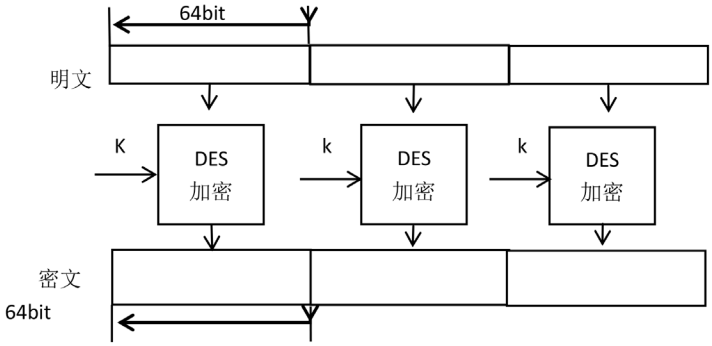

Figure 3. DES encryption schematic
图 3. DES 加密原理图

阶段三：IP^{-1}，即逆初始置换，这一过程是置换过程的逆运算，所以也不会使用密钥。

在这过程中的初始置换的功能就是把输入的 64 位数据块进行重新组合，并分别输出 L1 和 R1 两部分，每部分长度都为 32 位，其置换的规则是将输入的第 58 位换到第 1 位，第 50 位换到第 2 位……以此类推，最后一位是原来的第 7 位。L1、R1 是换位后输出的两部分，L1 是左 32 位，R1 是右 32 位。例如置换前输入的数值是 N1N2N3……N64，那么经过初始置换后输出的是：L1 = N58N50……N8；R1 = N57N49……N7。置换规则为：

58，50，42，34，26，18，10，2，60，52，44，36，28，20，12，4，
62，54，46，38，30，22，14，6，64，56，48，40，32，24，16，8，
57，49，41，33，25，17，9，1，59，51，43，35，27，19，11，3，
61，53，45，37，29，21，13，5，63，55，47，39，31，23，15，7。

4.1.2. 非对称加密技术 RAS

非对称加密算法也可称为公钥加密算法。非对称加密算法主要包括六个要素：加密算法、解密算法、明文、密文、公钥和私钥，其中公钥和密钥是密钥的两个组成部分。公钥被登记在一个可信的公共数据库中，它是公开形式的，所有人都能够访问的。私钥由用户自己负责保存，是私密的，非对外公开的。数据发送者采用加密算法使用公钥对明文进行加密，形成密文，然后将密文发送给数据接收者，接收者使用自己的密钥对密文进行解密，读取数据。非对称加密算法过程如图 4 所示。

RAS 公钥密码算法作为非对称密码算法的典型代表，主要分为两部分：密钥生成方法和加密(解密)算法。RSA 的算法涉及三个参数，n、e1、e2。其中，n 是两个大质数 p、q 的积，n 的二进制表示时所占用的位数，就是所谓的密钥长度。e1 和 e2 是一对相关的值，e1 可以任意取，但要求 e1 与(p-1)*(q-1)互质；再选择 e2，要求(e2*e1)mod((p-1)*(q-1)) = 1。(n，e1)，(n，e2)就是密钥对。其中(n，e1)为公钥，(n，e2)为私钥。

RSA 加解密的算法完全相同，设 A 为明文，B 为密文，则：A = B^e2 mod n；B = A^e1 mod n；(公钥加密体制中，一般用公钥加密，私钥解密)e1 和 e2 可以互换使用，即：A = B^e1 mod n；B = A^e2 mod n。

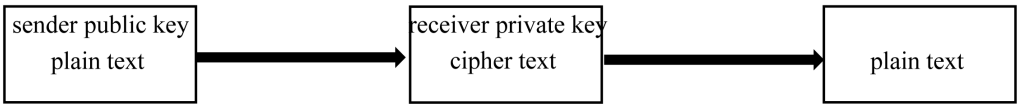

Figure 4. The process of asymmetric encryption algorithm
图 4. 非对称加密算法过程

RSA 的公钥和私钥一般都是由两个大于 100 位的十进制素数进行构造，因此破解起来比较困难，具有较高的安全性。但是缺点在于它的计算量非常大，导致其运算速度缓慢，相比 DES 慢了将近 100 倍。因为速度的限制，RSA 一般只用于少量数据加密[10] [13] [14]。

4.2. 数据擦除技术

在数据使用完后，系统中会存在大量的数据操作的痕迹，这些记录包括很多个人隐私信息，极其容易对个人信息安全造成威胁。极大多数的用户都是在使用完之后将数据进行删除，活着清楚使用记录，但是很多数据恢复类软件能够对这些信息进行恢复。所以，在数据被使用完后，要对数据进行擦除，销毁用户使用记录。

在云计算中数据擦除技术主要是按照用户的信息消除需求，定位到这些数据并切对这些数据进行不可逆地消除。数据擦出技术的主要目的在于对抗数据恢复技术，在真正意义上实现数据消除。目前主流的信息消除技术都是利用无意义的数据将有意义的数据存储区域进行覆盖，通过多次反复写入后达到无法恢复的目的。

5. 总结

本文对云计算数据的生命周期进行了简要的说明，介绍了数据在产生、传输、分享以及使用等过程中遇到的安全问题，并给出了相关的解决方案。文章阐明了保证数据安全性的两种技术，数据加密技术和数据擦除技术，但是这种数据安全技术的使用只局限于企业和有较高安全意识的用户，并没有普及到普通的用户中，普通用户对云计算中的数据还是缺乏安全意识，没有体会到使用数据安全技术的重要性，所以，将云计算数据安全与人们日常生活更加密切地联系起来也变得十分重要。

参考文献 (References)

[1] 程风刚. 基于云计算的数据安全风险及防范策略[J]. 图书馆学研究, 2014(2): 15-17.
[2] International Telecommunications Union. http://www.itu.int/en/pages/default.asp
[3] Cloud Security Alliance. http://www.cloudsecurityalliance.org/
[4] Organization for the Advancement of Structured Information Standards. http://www.oasia-open.org/
[5] 韩帅. 基于云计算的数据安全关键技术研究[D]: [硕士学位论文]. 成都: 电子科技大学, 2012.
[6] 段春乐. 云计算的安全性及数据安全传输的研究[D]: [硕士学位论文]. 成都: 成都理工大学, 2012.
[7] 王新磊. 云计算数据安全技术研究[D]: [硕士学位论文]. 郑州: 河南工业大学, 2012.
[8] 刘邵星. 云计算中数据安全关键技术的研究[D]: [硕士学位论文]. 青岛: 青岛科技大学, 2014.
[9] 王庆波, 何乐, 赵阳, 等. 云计算宝典技术与实践[M]. 北京: 电子工业出版社, 2012: 3-110.
[10] 云计算发展现状与前景[DB/OL]. http://news.sina.com.cn/m/2010-12-13/155621632626.shtml, 2010-12-13.
[11] 陈俊健. 面向对象存储系统安全技术研究[D]: [博士学位论文]. 武汉: 华中科技大学, 2011.
[12] W. Stallings, 著. 密码编码学与网络安全——原理与实践(第四版) (M). 孟庆树, 等, 译. 电子工程出版社, 2006.
[13] 苏弘逸. 云计算数据隐私保护方法的研究[D]: [硕士学位论文]. 南京: 南京邮电大学, 2012.
[14] John W. Rittinghouse, James F. Ransome. 云计算实现、管理与安全[M]. 田思源, 赵学锋, 译. 北京: 机械工业出版社, 2010.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2330-4677，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：jsst@hanspub.org