浅析云计算安全技术

李　婷

（山西财经大学，山西 太原 030006）

摘　要：随着云计算技术的飞速发展，云计算使用率也在不断的提高，云计算安全问题已经成为制约云计算发展的一个瓶颈，其重要性及急切性不断飙升。解析认识云计算领域的安全问题，在带来机遇的同时也充满着挑战，现对云计算安全技术做一简单分析与介绍。

关键词：云计算；云计算安全；同态加密；Hadoop

1　云计算安全发展现状

当前，云计算技术在飞速发展，云模式包括了基础设施即服务（Infrastructure as a Service，IaaS）、平台即服务（Platform as a Service，PaaS）以及软件即服务（Software as a Service，SaaS）三种，分别从不同的服务深度设计了廉价租用信息系统计算资源及存储资源问题的解决方案。同时，在网络环境越来越好的情形下，云计算的模式能够推广到越来越广泛的应用领域。遗憾的是，在这项技术快速发展的同时，新的计算、存储方式带来了安全上新的挑战。这些问题的解决，有助于推进云计算向前发展。

目前，云计算安全问题集中体现在以下几个方面：

（1）数据安全性、隐私性的矛盾。对于IaaS，用户完全控制虚拟资源，可以通过公钥基础设施PKI实现，而PaaS/SaaS，平台/软件由云服务商提供，用户的数据文件和平台、软件的交互使用就会出现新的安全问题，常见的诸如文件检索引擎等就不能够在数据加密的情形下运行。这样，应用功能正常运行和安全就存在对立的矛盾。

（2）数据隔离。多用户共享存储器资源，存在用户恶意访问其他用户存储器数据的可能，不能依赖软件的访问控制机制来防范，应该依靠信息安全技术从根本上解决问题。与之相似的还有服务器集群工作状态下单个机器故障还原数据的问题，针对当前的集群工作故障还原策略，设计符合工作实际的安全方案，是确保数据完整性、机密性的关键。

（3）数据安全审计。这要求数据外包存储时，能让第三方通过在客户端进行安全审计判断数据是否完整，所有权属于用户。在当前网络传输速度远小于本地访问速度的情形下，减少网络传输要求，通过少量数据实现安全审计，是实现云模式下数据安全审计的思路之一。

2　开展课题研究的基础

在云计算安全问题研究过程中，拟通过一个具体的平台

监视、控制中心，以屏幕、键盘及鼠标为主要监控手段，仅在操作台上设置紧急事故停炉按钮、少量仪表盘及后备操作站，保证DCS出现全局故障时锅炉安全停机。

3.6　尾部烟气处理

本工程锅炉排烟要求控制NO_x排放浓度≤50 mg/Nm³，烟尘排放浓度≤5 mg/Nm³，SO_2排放浓度≤35 mg/Nm³，各指标都按干基6%氧的基准条件折算。采用“基于流态重构的悬浮流化水煤浆锅炉+炉内喷钙脱硫+炉内SNCR脱硝（备用）+半干法脱硫布袋除尘一体化装置”的技术路线。

4　经济分析

4.1　总投资及资金来源

本工程总投资约为3.2亿元，资金来源包括自有资金和银行贷款，其中自有资金约0.64亿元，占总投资的20%，剩余资金约2.56亿元通过银行贷款解决。

4.2　营业收入

本工程建成后将形成年产蒸汽25.9万t、供热320万m²的生产能力。根据现行销售单价——蒸汽单价约200元/t，供热单价约5元/（m²·月），结合当地供暖期测算，正常运营年份营业收入约14 000万元。

4.3　营业成本

根据现有集中供热营业成本，测算本工程正常运营年份营业成本约9 200万元，主要包括外购原材料费用、外购燃料及动力费、工资及福利费、修理费、制造费用、管理费用、销售费用等。

4.4　财务指标

根据《建设项目经济评价方法与参数》（第三版）中的财务测算方法，本工程所得税后项目投资财务内部收益率约10.5%，所得税后投资回收期约7.2年（含建设期）。集中供热行业所得税后基准内部收益率为8%，经测算，本工程项目投资财务净现值约3 300万元，财务指标大于0，表示本工程在财务上是可行的。

5　结语

基于流态重构的悬浮流化水煤浆锅炉技术已被广泛运用，技术运用成熟且高效，本工程在技术和财务上都是可行的，对北方集中供暖地区的热力设施建设具有一定的借鉴意义。

[参考文献]

[1] 郝玉平，李雅辰. 一种新型水煤浆循环流化高效洁净燃烧锅炉技术与应用[J]. 工业锅炉，2018(4)：23-26.

[2] 朱国桢，徐洋. 循环流化床锅炉设计与计算[M]. 北京：清华大学出版社，2004.

收稿日期：2019-10-24

作者简介：刘永华（1987—），男，山东潍坊人，工程师，主要从事工程前期咨询工作。

作为实际操作的研究对象，发现实践中存在的需求，从而使安全方案的设计更加贴近实际。将某具体云计算应用和安全技术结合起来研究，从而发现应用存在的安全环境设计以及具体的语言、技术特性，使安全方案更加细化和贴合实际。

Hadoop平台是当前广泛应用的平台，该平台开源的特点，使得研究过程中，我们能够深入理解平台内部结构，并结合安全功能应用改进扩展某些组件部分。将Hadoop平台作为实现对象，能够更加方便地确定云计算的实际应用情形，结合已有的安全方案，进一步拉近两者的距离。

3 安全方案设计相关技术

在云模式下解决服务功能和安全的矛盾时，应从如下几个方面分析体制在各种攻击方式下的安全性：

选择明文攻击（CPA），攻击者能够获得加密服务，可以选择任意的明文消息并得到与之对应的密文，攻击者能够通过明-密文对来攻击安全方案。

选择密文攻击（CCA），攻击者能够获得解密服务，可以选择任意的密文消息并得到对应的明文。在这种前提下，得到目标密文进行分析，如果能够得到相应明文信息，就说明攻击安全方案成功。

适用性选择密文攻击（CCA2），不同于分析目标密文时解密服务立即停止，它总是能够获得解密服务。

可以通过越来越宽松的条件设定，赋予敌手较强的攻击能力，从而为所设计安全方案的实用性提供可靠的保障。从对称加密体制、公钥密码体制到后来的代理重加密、关键字搜索和属性基加密，都是为了适应复杂的应用需要设计的加密方案。安全机制的设立更多的是结合实际应用情形来完善自身的构造方式，对应的安全攻击定义、安全模型定义也体现了这一点。云计算在实际应用当中，对安全提出了更多新的要求。

云数据的存储，是云计算的应用情形之一，它要能够支持数据的分布式存储，这就要求信息冗余以及故障恢复。对于密文状态下的文件，实现文件管理需要安全机制能够对应有所创新。

同态加密定义如下：S、S'为明文空间和密文空间，$a,b\in S$，E为加密函数，那么在+、×运算上，满足$E(a+b)=E(a)+E(b)$，$E(a\times b)=E(a)\times E(b)$。当前该方案的不足之处在于效率太低，复杂度较高，不能满足实际运算需求。但其数学性质良好，在实际应用中非常理想。

虚拟监控机制VMM，是在云端以虚拟监控器来自动管理文件的传输存储过程，并在中间环节实现对文件的加解密，对使用人员透明。该机制虽然对用户而言是安全的，但对于云服务提供商而言，还是能够在虚拟监控器上获取到安全信息，从而对文件的安全构成威胁。这个机制的缺点在于，过分依赖于虚拟监控器，它的不足和崩溃，都会对安全机制造成致命的影响，实际的虚拟监控器不总是可靠的，可靠性仍然需要建立在机制本身上。

代理重加密技术，为数据的存储和已有对称加密、公钥加解密技术的结合提供了支持，这里需要解决服务器和某用户的合谋威胁，以及系统运算的规模复杂度问题。运算的规模n扩大，系统的运算复杂度就将非线性增加，难以扩展，需要改进运算的效率。

查询检索云数据技术，关键字搜索是服务器对云端文件进行维护的应用情形，文件能在密文状态下进行有效的搜索，对于文件查找，方便用户和管理员做某些日常应用非常有必要。当前主要问题在于，关键字搜索只能精确匹配，不能关联搜索，还有关键字的撤销问题，而且搜索效率也存在规模增加而计算复杂度急剧增加的问题，不能在云计算情形下有效使用。该方向需要更多的结合实际的检索算法来实现对应的设计方案，例如预先建立快速检索目录，建立关键字检索密文之间的关联性等，以有效提升算法的效率。

除此之外，协调客户端和服务器之间的加密运算负载，也是需要考虑的问题之一。考虑到客户端运算能力有限，更多地将加解密运算移交到服务器端进行，也是方案改进优化的内容。服务器集群之间的信息安全沟通，也是类似的问题，它们之间的安全性识别，数据安全高效的交流转换，是需要考虑的重要方面。这些也要能够提供安全机制，确保云计算的安全有效运行。

除了数据的安全存储，和它息息相关的另一个问题就是密文的访问控制，文件需要存储到某一位置，在处理的过程中，会加载到其他位置，对这之间的环节进行安全设计就会使得密文状态的文件处理起来非常困难。而且这里还有密文的数据粒度问题，文件夹级别、文件级别以及其他的要求，都会使得处理过程较为复杂。密钥的访问控制策略，采用了密钥分发的思想，结合整个控制结构，实现密文的对应特征密钥解密，而控制结构控制在云端，因此，来自云服务提供商的攻击将不能避免。基于密文的属性加密，将密文结合访问控制结构来加密密文，能够使得云服务器不能随意改动访问控制结构。但两者的问题在于，当访问控制策略是动态的访问控制策略时，需要随时随着策略的改变而重新加解密密文，运算代价较大，如能够实现类似于代理重加密的机制，能够随着可联想的访问控制结构进行对应的密文转换，从而有效降低复杂度，就能够一定程度上缓解这个矛盾。

4 结语

现如今，越来越多的企业高校将OA办公平台及业务管理系统等集成到云平台上，云计算在我们生活与工作的方方面面都有着非常广泛的应用，因此，学习、了解云计算安全非常重要。未来，在云计算安全方面，我们还有很长的路要走。

［参考文献］

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

[2] SUN云计算架构介绍白皮书[Z]，2009.

[3] 路万里. 云计算下网络安全技术的现状与对策研究[J]. 网络安全技术与应用，2019(4)：59-60.

收稿日期：2019-10-24

作者简介：李婷（1990—），女，山西曲沃人，硕士研究生，研究方向：网络安全。