

基于自认证密钥的安全云计算

刘 立, 尹召芳, 王 建

(天津大学 电子信息工程学院, 天津 300072)

摘 要: 介绍了一种安全的云计算框架, 论述了自认证密钥机制的特点和在云计算中的主要实现, 包括标识密钥的分发、身份认证、数据交换等. 在基本操作的基础上, 密云计算还可以实现网络数据的分类提取等延伸服务, 满足大数据应用的需求.

关键词: 云计算; 网络安全; 自认证密钥; 大数据

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)04-0071-04

Secure Cloud Computing Based on Self-authenticated Cryptography

LIU Li, YIN Zhao-fang, WANG Jian

(College of Electronic Information Engineering, Tianjin University, Tianjin 300072, China)

Abstract: In this article, a crypto cloud computing framework is introduced for cloud security. The paper introduced the self-authenticated cryptography, and discussed its primary operations in crypto-cloud computing, including key distribution, user authentication and data exchange. Other advance operation such as data tracing can also be realized under the introduced crypto cloud framework, which is essential for big data analysis.

Key words: cloud computing; network security; self-authenticated cryptography; big data

1 引言

云计算(Cloud Computing)通过互联网和虚拟化技术将分散的信息、软硬件平台等资源和服务集中共享, 并根据需求以动态伸缩的方式向用户提供服务, 而用户通过终端特别是移动终端向服务商获取资源^[1].

云计算在硬件和操作系统的基础设施之上, 形成包括管理软件、虚拟化组件和云计算管理系统等系统和管理平台, 并在此基础上提供各种虚拟机, 开展具体的云计算使用服务, 同时实现对计算资源的动态分配^[2]. 根据其资源所在的层次, 云计算服务相应地分为三类, 即: 基础设施即服务(Infrastructure as a Service, IaaS), 平台即服务(Platform as a Service, PaaS), 软件即服务(Software as a Service, SaaS). 其中, IaaS 提供计算资源的服务, 主要表现为存储与计算, 如亚马逊的 EC2; PaaS 提供实施开

发的平台环境 and 能力, 如 Google 的 APP Engine; SaaS 提供云计算基础之上的各种应用, 如 Facebook、网页游戏等.

在享受云计算提供便利服务的同时, 云计算带来的安全隐患也不容忽视^[3-5].

当前在信息系统的各个环节均有一些保护方案, 比如针对软件应用的 360 安全卫士等. 但是云计算安全指云环境下数据与应用的安全保护, 需要关注云计算环境中各个环节的信息与运作的保护, 是一个范围较广的概念, 孤立的研究单个环节如终端、平台等的保护并不能实现系统的信息与操作的安全保护.

常见的基于浏览器的电脑杀毒软件可看作是一种云计算安全服务的雏形. 除了对操作系统与应用的操作保护, 在网络环境中对数据、信息与应用的加密分发、共享和存储等也需要以云计算服务的方式提供. 此外, 云计算时代, 大数据中有效信息的分解

收稿日期: 2013-05-28; 修回日期: 2013-07-20

基金项目: 国家自然科学基金面上项目(NSFC61002030)

跟踪也可以加密服务的形式实现. 以上与网络与信息安全相关的服务在目前的云计算框架下很难实现, 需要重新定义内嵌加密功能的网络架构来实现云计算的安全服务, 即密云计算.

2 密云计算

密云计算是一种新型的安全云计算架构, 它首先需从系统层次上提供对信息安全保护, 同时也能够让用户方便准确地获得计算资源与服务. 在密云计算环境下, 任何的交互均在保密的环境下实现, 数据的处理与传输也都通过加密解密方式进行的. 加密技术是实现数据安全与保护的重要手段, 因此, 可靠的密钥体系对实现数据的认证与保护发挥着不可或缺的作用.

2.1 密即服务

在密云计算环境下, 加密解密天然地集成于密云环境, 作为一种服务提供给用户, 实现可伸缩的数据与信息交流的安全. 比如, 在用户访问云端的邮件服务时, 用户终端的密钥与服务端的密钥进行交互认证, 云服务器自动提供加密的通道与数据加密服务给请求者. 另一方面, 在云端的邮件信息则是通过服务器对用户的密钥进行加/解密. 服务器本身提供的是加/解密服务, 在用户或其他实体密钥缺失的情况下, 不能对相应的数据进行处理和保存. 这种服务不仅仅是软件平台和架构服务, 也是将认证与加/解密有机结合, 形成密云系统中的“密服务”(Crypto Service)提供给用户. 密云服务可根据客户需求由云端提供, 它可以包括对数据的加密、对用户操作的加密, 甚至是对用户自身存在的加密, 从而形成了密云环境下的“密即服务”(Crypto as a Service, CaaS).

2.2 密云服务的特点

网络环境下的基本密服务包括用户认证与信息加解密. 用户认证是在数据交互时, 用户对参与方身份真实性的确定和对自身身份真实性的保证. 密云体系中, 可以非对称密码方法实现这一功能. 密云中所有的实体均以分配的私钥作为身份认证的标识, 从构建云计算基础架构的各单元到形成云平台的各个环节, 以及实现具体云服务的虚拟化硬件功能, 都有各自的密钥标识. 不但如此, 在云计算的结构基础设施上所产生的各种事件也分配唯一的密钥, 可以实现对事件本身的签名认证. 在密服务中, 参与操作的各方以自己的私钥来对自身操作与处理数据的可靠性提供保障, 通过公私钥配合实现数信息的保密

传递加密. 此外还可以进一步衍生出信息溯源、数据归集等多种密服务. 结合上述服务, 密云体系可以从结构上保证信息及交互的安全性及可信性.

为实现这样的服务, 密云计算采用的密钥技术需要满足如下要求. 首先, 这种密钥技术应该能够对云计算设计的各个单元要素进行认证. 其次它能够实现对各个要素的加解密, 不仅可以在数据层次上加/解密, 还应该可以在云计算的各个要素, 包括: 基础架构、平台和软件上进行加解密. 尤其重要的是, 体系中的公钥获取应该是不依赖于第三方的自认证密钥. 当前的非对称体系如 PKI 等并不完全适用^[6-7]. 在自认证的密钥体系下, 用户与云端可以以内在的方式建立互信, 而不用担心非认证用户的入侵或第三方的劫持, 从而减少了云计算安全的隐患.

3 自认证密钥及其在密云计算的实现

3.1 非对称密钥体系

在网络环境中, 非对称的加密方式被证明是一种有效的信息保护手段. 在非对称密钥体系下, 用户采用公私钥对的形式进行数据的认证和加密: 发送方可通过私钥对发送数据进行加密, 而接收方可利用发送方的公钥进行解密, 从而达到数据认证传送的目的; 在认证的基础上, 发送方可用接收方的公钥对传送数据进行加密, 而接收方可用其自身的私钥对接收数据进行解密, 从而达到数据加密传输的目的.

目前主流的非对称密钥应用基于 PKI 体系, 而 PKI 体系中的公钥获取与认证均借助第三方认证中心和在线数据库的支持, 公钥的传递同样也会占用大量的网络资源^[6]. 在云计算的应用中, 存在着海量的数据交换和认证事件, 从而对 CA (Certificate Authority) 即认证中心的响应也提出了更高的要求. 另一方面, PKI 体系将密钥集中保存, 但认证中心一旦被破坏, 将影响整个系统的安全. 随着云计算应用规模的扩大, 基于 PKI 的密钥体系, 在实际应用中将会受到很大的限制.

3.2 自认证密钥体系及基本操作

自认证密钥是一类特殊的非对称密钥体系, 其公钥获取与认证完全在本地进行, 不依赖于第三方, 如认证中心 (Certificate Authority, CA) 这样的机构. 在信息交互时, 发送方与接收方均可以根据对方提供的公开标识来自行确定相应的公钥, 并对对方的私钥签名进行验证; 另外, 用户可根据任意其他用户的公开标识确定其公钥, 利用该用户的公钥对数

据进行加密和传输,从而实现了与特定用户之间的数据交互与共享.这些过程中,公钥的获得由参与操作各方独自实现,减少了网络资源消耗,提高了数据加密与认证的安全性.

3.2.1 自认证密钥分发

自认证密钥体系最重要一环是密钥的产生与发放,其实现具有多种形式,两种常用的形式如下:在小规模的应用情况下,可以将公钥数据库打包分发给每一个用户,这样用户与其他用户进行加密操作时,可以自行地通过本地的数据库来查询对应用户的公钥,完成其操作;而在应用规模较大的情况下,可以采用密钥生成函数的形式来实现,即输入用户公开标识通过本地函数即时产生公钥,如组合公钥方法^[4].

以组合公钥方法为例,自认证密钥体系密钥分发如图1所示.申请密钥的实体将其唯一标识ID传递给密钥产生中心(Key Generation Center, KGC),KGC对其ID信息进行某种变换,即图1中对应的私钥矩阵可产生用户的私钥.密钥产生中心在向实体传递其私钥的同时,还将体系的公钥矩阵传递给实体.这样用户在已知其他用户唯一标识信息的情况下,就可以通过公钥矩阵生成其公钥,即公钥的获取不依赖于第三方,实现了自认证的过程.

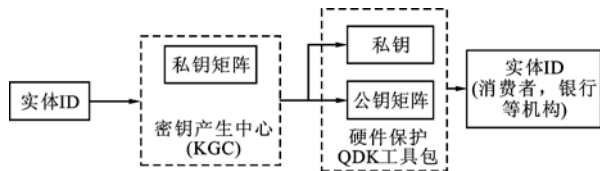


图1 自认证密钥体系结构图

3.2.2 身份认证

自认证体系的身份认证不需要第三方参与,仅在交互双方进行.具体实现过程如下:

(1)用户 Alice 利用其私钥及标识 ID 对信息进行加密,形成具有用户 Alice 签名的信息,即签名码;

(2)通过网络环境,将 Alice 的签名码传递给用户 Bob,Bob 根据 Alice 公开标识唯一 ID 查询其公钥,利用公钥完成签名码的认证过程;

(3)认证器若能恢复出信息 m,则认证成功;否则认证失败.

图2中给出了一种实现的流程图.注意其过程在认证参与双方进行,无第三方参与.

3.2.3 数据加密与交换

由于对称加密方法数据处理速度快,自认证密

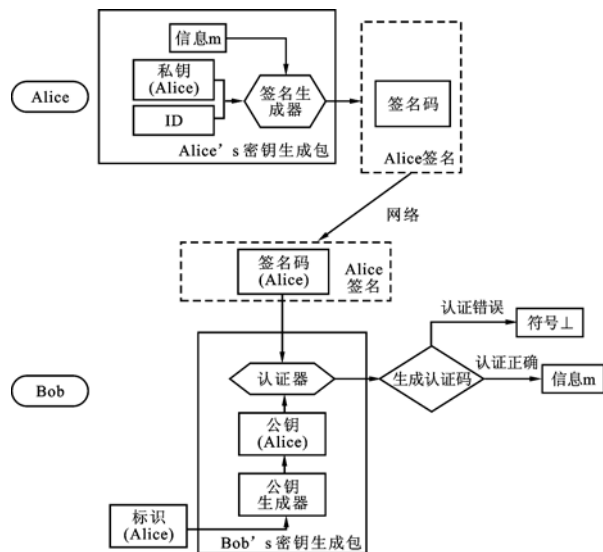


图2 基于自认证非对称密钥体系的数据认证过程
钥体系下的大数据加密可采用非对称与对称方法结合的形式,与传统实现类似.具体的流程如图3所示.

(1)加密过程:①用户 Alice 利用对称密码将数据 Data,通过对称加密器将数据进行加密,形成加密的数据;②用户 Alice 根据用户 Bob 的唯一标识 ID 利用 KMC 分发的公钥生成器产生用户 Bob 的公钥;③利用 Bob 的公钥,通过非对称加密器将对称密码进行加密,形成加密的密码;④发送加密的密码与加密的数据

(2)解密过程:①用户 Bob 接收到加密数据集; Bob 利用自身的私钥通过密码解密器对接收到的加密密码进行解密,得到解密的密码;②Bob 利用解密后的密码通过数据解密器对加密的数据进行解密,获得明文数据.

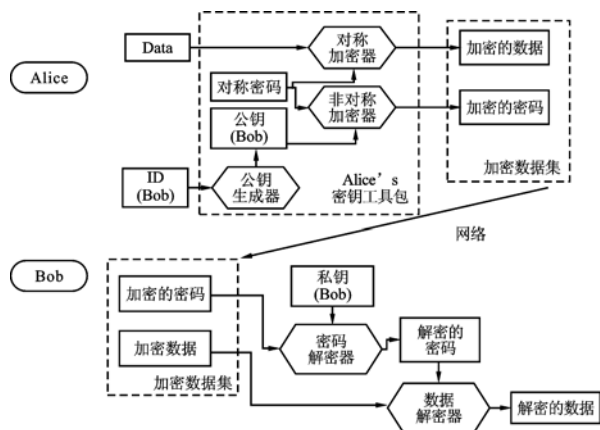


图3 数据加密传输过程

3.3 密云计算中的扩展服务

在上述基本操作的基础上,可进一步衍生出用

于密云计算更加完备的服务,如信道保护、信息溯源、大数据中信息的归集等.在密云计算环境中,传输信道自身也被授予唯一的密钥标识,可根据需求用自身私钥对当前传输数据签名,实现对数据真实性的认证,避免了信道劫持等不安全因素.对于重要信息,发送者和经手者均需要签名.通过对传输数据签名的分析,可实现对信息的溯源.此外,网络中任意的信息都可以密钥为依据连接起来,用户可在复杂的网络大数据中方便地找到与自己相关的数据,即以密钥实现信息的归集.另一方面由于有标识密钥的保护,需要保护的信息不会被外界所破解.这一特性在网络大数据时代尤为重要.

4 结束语

文中介绍了一种新型的安全云计算框架,即为基于自认证密钥的密云计算.这一框架可实现原生的云计算环境中数据的安全服务,即“密即服务”,为云计算数据安全共享传输提供了有力地保证.本文的密云计算构建于自认证非对称密钥技术.这样密服务的实现,包括用户与服务器云端、用户与用户间的操作可真正以点对点的方式建立互信.这一过程中,公钥的获取不需要类似 CA 认证中心这样的机构,而是通过本地数据库查询或者自动生成等方式获得,从而在提高网络资源应用效率的同时,更是降低了非认证用户的入侵或第三方劫持的可能性.基于自认证的密云计算除了网络安全的优势,其基于标识密钥的数据标定方式还可以实现在大数据中准

确的获取有效信息,方便实现信息归集和溯源,实现网络大数据的高效处理.

参考文献:

- [1] 张建勋,古志民,郑超.云计算研究进展综述[J]. 计算机应用研究,2010,27(2):429-433.
- [2] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing[J]. Communications of the ACM, 2010, 53(4):50-58.
- [3] Brodtkin J. Gartner: Seven cloud- computing security risks[N]. Net world, 2008-6-2.
- [4] 张健. 全球云计算安全研究综述[J]. 电信网技术, 2010,9:15-18.
- [5] Carlin S, Curran K. Cloud Computing Security[J]. International Journal of Ambient Computing and Intelligence, 2011, 3(1):14-19.
- [6] 李勇,吴作顺,刘秋彩. 基于 CPK 的融合网络密钥建立与认证[J]. 计算机应用, 2009,29(S2):72-75.
- [7] Tan WZ, Yang WS, Yang MJ, et al. A modification on public key infrastructure application[C]//E-Business and Information System Security. Wuhan,2009.

作者简介:

刘立男,(1975—),男,博士,副教授,硕士生导师.研究方向为信息安全、物联网技术、计算机视觉.

尹召芳女,(1988—),硕士研究生.研究方向为物联网技术、信息安全.

王建男,(1976—),博士,讲师.研究方向为彩色图像处理、计算机视觉.

(上接第 70 页)

- [2] 洪志令,姜青山,董槐林,等.模糊聚类中判别聚类有效性的新指标[J]. 计算机科学,2004, 31(10): 121-125.
- [3] 孔攀.模糊聚类分析及其有效性研究[D]. 重庆:西南大学,2009.
- [4] Krista Rizman Žalik, Borut Žalik. Validity index for clusters of different sizes and densities[J]. Pattern Recognition Letters,2011, 32(2): 221-234.
- [5] Witold Pedrycz. A dynamic data granulation through

adjustable fuzzy clustering [J]. Pattern Recognition Letters, 2008, 29(16): 2059-2066.

- [6] Zhang Yunjie, Wang Weina, Zhang Xiaona, et al. A cluster validity index for fuzzy clustering [J]. Information Sciences,2008, 178(4): 1205-1218.

作者简介:

王丽娜女,(1979—),博士研究生,讲师.研究方向有数据挖掘、机器学习、人工智能.