云服务环境下的密钥管理问题和挑战

杨 璐 叶晓俊

(清华大学软件学院 北京 100084)

摘 要 为了在云环境下安全地交互各种云数据服务,存储这些服务生成或处理的敏感性数据,云服务提供商应提供多种类型的安全加密机制。相比于传统IT环境,由于云用户和云服务供应商之间的所有权不同,各种云计算服务模式(基础设施即服务、平台即服务、软件即服务)在加密服务中产生了大量密钥,使得密钥的管理和使用变得更为复杂。明确了云环境中的密钥类型、可能的状态、基本的管理功能及通用安全要求,讨论了3种典型云服务模式中密钥管理安全功能的架构方案,并从密钥管理服务互操作性需求方面给出了密钥管理互操作相关应用系统的架构和功能设想。

关键词 云服务,安全功能,密钥管理,密钥管理互操作

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.03.002

Key Management Issues and Challenges in Cloud

YANG Lu YE Xiao-jun

(School of Software, Tsinghua University, Beijing 100084, China)

Abstract In order to securely interact with cloud data services and store sensitive data which generated or processed by these services in the cloud environment, cloud suppliers need to provide different kinds of security encryption mechanisms. Compared with traditional IT systems, due to different ownerships among customers, suppliers and owners, cryptographic services will generate large scales of keys in different cloud service modes (Infrastructure as a Service, Platform as a Service, Software as a Service) which leads to much more complex issues of key management. This paper identified some key types, kinds of possible key states, essential key management functions and common security requirements, discussed key management's security capabilities in the context of architectural solutions by taking three common cloud services modes as examples, and proposed some suggestions about related application system architecture of key management interoperability and possible system features of key management interoperability in the respect of interoperability requirements.

Keywords Cloud service, Security capability, Key management, Key management interoperability

1 引言

在云计算环境中,由于加密数据类型和处理过程相对复杂,数据的物理分布性和处理并行性使密钥及密码资源数据变得极为可观。此外,云服务中数据资源的物理和逻辑控制权又被各种云服务角色分开管理[1],密钥及其元数据的安全性直接关系到云数据服务安全。只有未来的密钥管理系统满足密码服务互操作性等规范[2],才能真正保障有效的云数据加密安全服务能力[3]。

为确保云服务加密机制达到期望的安全程度,数据加密算法、协议等加密核心组成部件及其实现框架需要满足各种密码标准与规范,在算法和协议的实现方面必须满足相关的测试规范,如美国国家信息技术研究所(NIST)的加密算法验证程序(CAVP)和加密模块验证程序(CMVP)[4,12]。另一方面,密钥安全共享和使用是云数据加密和安全服务的核心,密钥必须集中管理,并满足各种云服务互操作性要求[32-33]。

针对云环境中的密钥服务,本文主要讨论3个方面的内容:1)针对不同云服务模式及用户角色,明确云环境中的密钥类型、状态、管理功能及安全要求;2)根据云服务特性和密钥服务产生、存储、处理的数据类型总结3种典型云服务模式(IaaS,PaaS和SaaS)中执行密钥管理的安全功能、可行的架构解决方案等;3)从互操作性需求方面分析目前密码管理服务产品的核心功能,设想云环境下密码服务互操作性的应用需求及发展趋势[13,34]。

2 密钥管理服务

2.1 密钥类型

在密码学中,按用途将密钥分为对称密钥(秘密密钥)和非对称密钥(公/私密钥对)。秘密密钥用于对称加密算法,使用消息认证码或某种加密操作模式来保证数据的完整性。公/私密钥对用于非对称加密中的身份认证、数字签名或证书。公/私密钥对的所有者拥有私钥并对外界保密,但可以发

到稿日期:2016-01-08 返修日期:2016-07-09 本文受国家科技支撑计划项目(2015BAH14F02)资助。

杨 璐(1992—),女,硕士生,主要研究方向为数据库安全,E-mail:yang-l14@mails.tsinghua.edu.cn;叶晓俊(1964—),男,博士,教授,主要研究方向为数据库安全、数据库技术。

布公钥被受信任的第三方使用。在面向密码设备的接口规范 PKCS#11 中，密钥类型对象就是按照这种用途进行分类的[5]。在最新的面向分布式加密的密码集中服务规范 OASIS KMIP 中，除上述 3 种密钥外又添加了拆分密钥(Split Key)、导出密钥(Derived Key)[2]。文献[4]也总结了公/私认证密钥对、公/私签名密钥对、公/私密钥生成密钥对、对称加/解密密钥、对称消息认证码(MAC)密钥、对称密钥以及包装密钥这几种云数据服务中可能用到的密钥类型[4]。

2.2 密钥状态

表 1 列出了 NIST 密钥管理指南(SP800-57)第 4 版[6]，KMIP 版本 1.2[2]、IEEE 密钥管理基础架构 (P1619.3)[7]和 ISO/IEC 11770[8]密钥管理规范了密钥管理系统(KMS)的密钥状态对应关系。其中 KMIP(v1.2)已获得工业界的广泛认可，它完全引用了 SP800-57 第 3 版的密钥状态，而 2015 年的 SP800-57 第 4 版去掉了销毁破解(Destroyed-Compromised)状态，增加了挂起(Suspended)状态。挂起的密钥可以转换到除预激活(Pre-Activation)以外的所有状态。IEEE P1619.3 将激活(Active)状态细分为保护与处理(Protect-and-Process)和仅处理(Process-Only)状态，失活(Deactivated)状态被过期(Expired)和禁用(Disabled)两种状态取代，增加了清除(Terminal/Purged)状态。

表 1 现有密码服务规范中的密钥状态对照表

SP800-57(r4)	KMIP(v1.2)	IEEE P1619.3	ISO/IEC 11770
预激活	预激活	预激活	等待激活
激活	激活	保护和处理	激活
挂起	—	仅处理	—
—	—	过期	—
失活	失活	禁用	后激活
破解	破解	破解	—
—	—	禁用破解	—
销毁	销毁	销毁	销毁
—	销毁破解	销毁破解	—
—	—	清除	—

这并不意味着在真实的 KMS 实现过程中没有其他附加状态出现。事实上，这些规范中的状态子集可能出现在不同商业化密钥管理系统的实现过程中。根据面向云数据服务密钥状态及其转换关系，还应包括归档、撤回等前面 4 个规范中未包括的状态[4]。

2.3 密钥管理功能

密钥管理功能应涵盖从密钥产生到最终销毁的过程，包括密钥的生成、分配和协商、存储、托管、使用、备份/恢复、更新、撤销和销毁等。具体包括：密钥生成、域参数生成、密钥和元数据绑定、密钥与个体绑定、密钥激活、密钥失活、密钥备份(密钥托管)、密钥恢复、元数据管理、密钥更新、密钥挂起、密钥还原、密钥撤回、密钥归档、密钥销毁、信任锚点管理等[35]。

为简化分布式环境下的 KMS 应用，结构化信息标准促进组织(OASIS)于 2009 年联合惠普、IBM 以及 RSA 等业界厂商制定了密钥管理互操作协议(KMIP)，旨在为企业级密钥管理服务和密钥应用系统间的通讯提供一个单一的、全面的协议。KMIP 服务器存储并控制管理密钥的相关对象。客户端在服务器端实现的安全模式下访问这些管理对象，操作包括创建密钥，在 KMS 中注册对象，从系统中获取、销毁或查询密钥对象，增删改密钥对象属性值等近 40 个管理操作。KMIP 支持如 IEEE 1619.3(用于存储)和 OASIS EKMI(用于 XML)等 KMS 行业标准，并且将与 PKCS#11 结合来作为未来密钥管理云服务标准项目的补充。但目前的 KMIP 版本还没有涵盖密钥备份、密钥挂起等状态管理功能，而这两个功能对云环境下的密钥恢复和撤销使用方面又起着十分重要的作用，相信 KMIP 的未来版本会考虑添加这些密钥管理云服务安全功能要求。

2.4 密钥管理安全要求

云数据服务中不同密码模块的密码算法及其实现机制可以参照 FIPS-142 规范进行安全评估。但云服务安全能力并不仅依赖于密码算法的安全性，密钥的机密性和完整性也决定了整个密码体制的安全性。NIST 在不断更新密钥管理建议书(SP800-57A)的同时又推出了 KMS 设计框架(SP800-130)、替换 FIPS 140-2 的密码算法使用转换及密钥长度建议书(SP800-131A)等[10]。SP800-131A 增强了加密算法并增加了密钥长度以提高分布式环境下密钥的安全性，同时提供了转换方式和严格方式。为保证联邦政府密码管理规范，2015 年 NIST 又颁布了密码管理保护轮廓(如 SP800-152)。综合这些密码管理建议、框架、使用建议等，密钥管理安全要求应包括：用户身份验证、防欺骗操作要求、可追溯性要求、密钥机密性要求、不可否认性要求、密码资源数据保护、密钥强度要求。

若通过不安全的公共网络实现这些密钥管理的安全要求必然会遇到问题[14]。不同的云服务模式应根据它们提供的核心功能特性提供可行的数据加密安全功能的架构解决方案及相应的密钥管理安全功能。

3 云环境下的密钥管理服务

本节从传统 IT 环境和云环境下的密钥管理问题的对比出发[36]，明确了 3 种服务模式的安全功能的架构解决方案，并介绍了它们分别存在的密钥管理的相关挑战[4,27]。

3.1 传统 IT 环境与云环境下的密钥管理问题

在传统的 IT 环境下，密钥管理功能及工具全部由同一内部运营团队开发并维护，而在云数据服务中，密钥管理可能采取的是共享模式或完全由供应商负责和维护[15,37]。

由于 KMS 与受保护资源基础设施的控制和所有权不同，支持云数据加密操作的 KMS 将面临诸多挑战[16]。例如，云服务中的数据归云用户所有，但是数据物理驻留的存储资源受云供应商的控制。另外 KMS 一般也运行在云供应商提供的计算资源上。这样，能否从那些加密操作上寻求到必要的安全保证是云环境下的密钥管理用户不得不面对的问题[17]。

3.2 IaaS 中的加密操作和密钥管理

IaaS 为用户提供计算、存储、网络和其他基础计算资源。用户无需管理底层基础设施，但要控制操作系统，存储、部署应用程序和网络组件[18]。一般来讲，云用户在云供应商的基础设施中启动并运行虚拟机(VM)实例以部署计算资源[38]。IaaS 云用户分为服务级管理员、应用级管理员和应用程序用户，它们分别执行不同的任务，且相应的安全要求也不同。服务级管理员通过虚拟机管理程序接口执行 VM 认证和授权

检查以及生命周期内的 VM 启动、终止、暂停、重启等运维管理操作[19,39]。因此 IaaS 云服务应提供 3 种基本安全服务能力(SC)。

(1)VM 镜像模板的认证和授权(SC-1)。租赁之前需要对云供应商的预置 VM 镜像进行身份认证,确保它们来自授权源而未被篡改过[22]。目前的方法包括:对 VM 模板进行数字签名(见图 1)、使用消息认证码 MAC 认证 VM 模板(见图 2)、使用密码哈希函数认证 VM 模板(见图 3)、基于云供应商的自主访问控制认证 VM 模板等[40]。

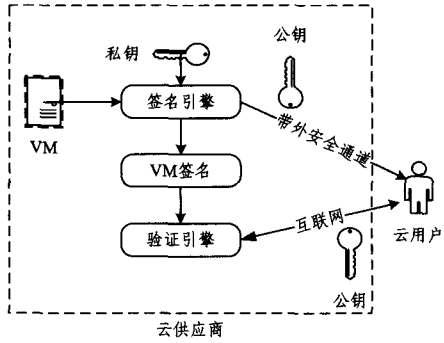

图 1　数字签名认证 VM 模板

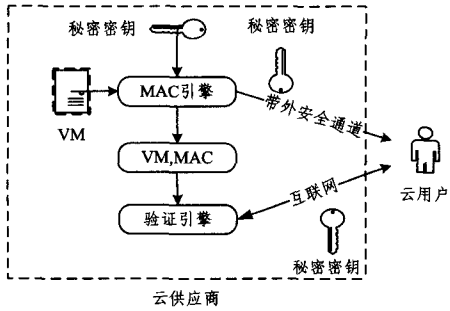

图 2　MAC 认证 VM 模板

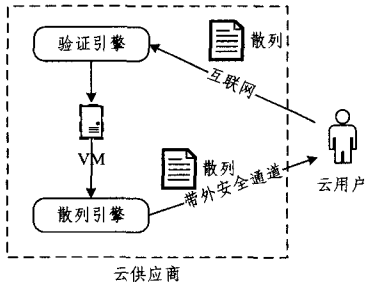

图 3　密码散列认证 VM 模板

在密钥管理方面,前 3 种方法共同的安全问题在于云用户在利用密钥与验证引擎通信获取验证结果时是否建立了安全会话以及运行在云供应商环境中的验证引擎是否真实可信。此外,在图 3 所示方法中,除非每个云用户的秘密密钥是唯一的,否则某些用户很可能会通过修改 VM 模板来破坏其他云用户的使用环境,而唯一密钥的做法无疑会加重云供应商密钥管理的负担[41]。图 3 所示方法有两方面的局限性:每次修改 VM 模板都需要利用安全的带外方式公布新的散列值;每个 VM 模板散列值都需要以安全的带外方式公布,而云环境下的 VM 模板数量又十分庞大,处理起来难免复杂繁琐。

(2)虚拟机程序接口(API)安全(SC-2)。目前的虚拟化有两种解决方案:虚拟机管理程序(如 Xen 和 KVM)和容器。它们都存在操作系统、设备模拟、I/O 和设备驱动等接口安全性问题。因此 VM 管理接口应只接受和执行已被验证的 API 调用。可信的权威机构将绑定云用户身份的公钥签名成公钥证书,VM 管理接口通过它验证云用户发送给 VM 实例的 API 调用签名。云用户可以通过安全隧道(SSH 或 SSl/TLS)或 VPN 与 VM 管理接口建立安全会话。在密钥管理方面,无论系统处于休眠还是使用状态,云用户都需要保护系统中用于签名 VM 管理命令的私钥。

(3)VM 实例管理操作的安全通信(SC-3)。目前一般的解决方案是使用 SSH 提供非对称密钥对或基于密码的客户端认证技术[42]。云用户生成密钥对,公钥关联 VM 实例中的帐户,为了确认对应私钥拥有者的身份,VM 将公钥添加到协议(ftp,scp)或控制台命令支持的 SSH 登录实例授权密钥文件中。这种加密认证机制防止了对 VM 实例的匿名连接及猜测口令的认证攻击。在密钥管理方面,云用户需要保护认证其身份的非对称密钥对中的私钥[23]。

云服务级管理员通过 SC-1 认证并检查 IaaS 服务商的预定义 VM 镜像,利用 SC-2 安全配置 VM 实例的 API 接口,以保证 VM 实例的启动和运行安全,再通过 SC-3 与 VM 实例的安全交互执行 VM 的配置管理。这样,云应用级管理员就可以在 VM 实例上安装并配置 Web 服务器、数据库管理服务器等平台软件、云应用程序执行环境(Java VM,Java 运行时的模块等)、云应用程序执行文件等。应用程序运行在 VM 上以后,应用程序用户与这些应用安全交互(通过设置的安全会话)并且执行不同的应用功能。IaaS 服务级管理员、应用级管理员和应用程序用户都需要数据存储服务。数据存储服务涵盖不同类型的数据:静态数据、应用程序产生的结构化或非结构化数据等。因此面向应用的 IaaS 云服务安全能力还应包括以下安全能力。

(1)IaaS 服务中的 VM 实例上应用程序的安全通信(SC-4)。应用程序用户通过与应用程序实例建立保证完整性和机密性的安全会话。传输层安全协议(TLS)能够使服务实例和客户端通过加密方式进行相互认证,也可以配置用于加解密和生成消息认证码的安全会话密钥[43]。在密钥管理方面,安全会话需要服务实例的非对称密钥对和客户端的可选密钥对。客户端的私钥可以被企业级 KMS 管理,而服务器端的私钥则不得不被云供应商 KMS 管理。

(2)IaaS 服务能够安全存储静态应用程序支持的数据(SC-5)。为了保证应用程序在 VM 实例中的运行,云应用用户需要安全存储服务来存储静态数据(如应用程序的源代码与配置参数数据、归档数据和运行日志等)。在密钥管理方面,云用户加密的数据应上传到云供应商的存储设备中,相关密钥应受到管理控制[24]。

(3)IaaS 服务使用数据库安全存储结构化的应用程序数据(SC-6)。云用户可以通过订阅数据库服务来存储 VM 实例中应用程序运行产生的结构化数据。云供应商包装数据库管理系统(DBMS)实例提供这些云数据服务[44]。DBMS 实例提供数据库级加密和用户级加密机制,本文第 4 部分将详细介绍 DBMS 云服务相关的密钥管理问题。

(4)IaaS 服务能够安全存储非结构化应用程序数据(SC-7)。

NoSQL云数据服务也需要存储级加密[45]，类似于结构化数据库管理系统中的透明加密，因此具有相似的密钥管理挑战问题[9]。

3.3 PaaS 中的加密操作和密钥管理

PaaS 的目标是为用户开发或部署应用程序提供计算平台和必要的应用程序开发环境及工具套件[46]。尽管托管开发工具的底层操作系统平台对用户已知，但是用户不能控制它的配置功能及平台运行环境[25]。用户可能需要存储基础设施来存储支持数据和用于测试应用程序功能的数据[20,47]。PaaS 云服务安全功能包括 4 个方面：

1)能够与 PaaS 中部署的应用程序和开发工具实例建立安全的交互；

2)能够安全地存储和加密不由应用程序直接处理的 PaaS 支持数据；

3)利用结构化数据库管理系统安全地存储应用程序的结构化数据[48]；

4)利用非结构化数据管理系统(NoSQL 系统)能够安全存储应用程序的非结构化数据[49]。

这些操作与 IaaS 服务的 SC-4－SC-7 的 4 条安全功能完全相同，因此 PaaS 应提供类似的数据加解密解决方案和密钥安全管理能力[26]。

3.4 SaaS 中的加密操作和密钥管理

SaaS 提供了访问云供应商托管的应用程序的服务。SaaS 云用户与这些应用程序实例安全交互并执行不同的应用程序功能[50-51]。SaaS 云供应商提供与应用程序安全交互的功能，SaaS 云用户则负责以加密的形式存储应用程序产生或处理的数据[21]。SaaS 的典型安全功能包括两个方面。

(1)与应用程序安全交互。该安全功能与 IaaS 的 SC-4 相同，相关的密钥管理挑战也类似。

(2)加密存储应用程序数据。该安全功能与 IaaS 的 SC-6 和 SC-7 相同，主要有两种使用场景：1)加密 SaaS 中的所有数据；2)对于结构化数据，云用户希望选择性地加密部分字段集。前者操作规模较大，因此加密功能可由云供应商提供；后者由于每个用户选择的字段集不同，因此有关加密策略及其相关的加解密操作可能发生在客户端。

对于云服务端的数据加密，为了高效地加密和存储应用程序数据，SaaS 云供应商一般将物理存储资源分成逻辑存储块(磁盘存储卷)，并在磁盘存储卷集合上分配不同的加密密钥。

在密钥管理方面，SaaS 云供应商控制所有的加密密钥，如果没有额外的安全措施，这种解决方案没有为用户提供抵御内部威胁的安全保障[27]。其次，属于不同用户的数据很可能位于单独的磁盘存储卷但被同一个加密密钥保护，导致无法对属于不同云用户的数据进行隔离加密。另外，大型 SaaS 云平台为存储海量数据供了大量密钥，大量密钥的管理可能还会用到多个密钥管理服务器。如果密钥管理功能由硬件存储模块(HSM)实现，那么同样需要创建和维护多个 HSM 分区[52]。

对于选择性加密数据库字段，如果用户选择加密字段，使用的加密网关通常为云用户的企业内部网络。在架构上，网关位于 SaaS 客户应用程序和 SaaS 云应用程序(SaaS 云供应商托管)之间，扮演者反向代理服务器的角色监督所有传入和传出应用流量(例如 HTTP，SMTP，SOAP 和 REST)。在此上下文中的传出有效载荷通常是发送给 SaaS 云应用程序进行存储的数据。根据规则配置的网关用于加密不同数据项，加密或标记实时数据并将修改的数据转发到 SaaS 云应用程序中。同样，SaaS 云应用程序检索并返回已加密或已标记的数据，在被 SaaS 客户应用程序显示出来以前实时转换成明文[28]。这种加密模式不需要改变 SaaS 云供应商的应用程序或 SaaS 云用户的客户应用程序。加密网关的解决方案的适用场景为：SaaS 云用户需要选择性地加密某些字段，因此包括加密字段在内的所有过程都发生在用户方，就那些字段而言，云平台中的 DBMS 实例仅用于存储加密数据；在云平台中，标记为加密的字段值在应用程序处理和存储期间都是以加密形式存在的[30]；明文数据仅对通过加密网关使用 SaaS 客户应用程序与 SaaS 云应用程序进行交互的已被授权的客户端可见。

在密钥管理方面，加密网关可能使用单一或不同密钥加解密应用程序的不同所选字段。不论使用的密钥数量如何，由于加密网驻留在企业网络边界内，所有密钥完全受控于 SaaS 云用户，因此可应用企业内部密钥管理策略和实践来保护密钥。

可见，不论数据库级/文件级加密还是字段级加密，面向多租户的云数据管理都会产生大量的密钥，需要集成 IaaS，PaaS 和 SaaS 中的硬件存储模块，通过集中的方式高效地对密钥及其密码资源数据进行管理，才能保证云数据的安全服务能力。

4 云数据服务中密钥服务的互操作性

4.1 云环境下密钥服务互操性的应用及挑战

密钥控制着云数据服务中敏感数据的加解密，前文安全服务能力 SC-6 和 SC-7 提到了数据库级 I/O 层面的透明加密(TDE)[29]和用户级加密服务，密钥集中管理对这两者都尤为重要。因此工业界推出了 AMS Key Management Service，Azure Key Vault，Oracle Key Vault 等商业化密钥管理服务产品。而云数据服务的 TDE[31]使用这些第三方工具或 DBMS 引擎本身提供的加密机制对敏感数据进行加密保存。

TDE 类似于存储级加密，加密引擎操作于 I/O 层面，并在写入磁盘之前对数据进行加密。数据加密密钥(DEK)可保护云端某个数据库、数据文件或数据库表，因此 DEK 的保护方式更为复杂，可能会使用到 HSM。由于 TDE 在 I/O 层面执行了所有的加密操作，不需要修改应用程序逻辑或数据库模式，因此现在的 DBMS 和 NoSQL 系统都开始支持该功能。在密钥管理方面，云用户管理 DBMS 实例及 DEK。由于加密发生在 I/O 层，存储 DEK 的位置需要接近数据库数据的存储资源，因此云用户存储 DEK 的云平台就是 DBMS 实例的运行平台[53]。尽管 TDE 实现了列和表级加密，但最常用的还是存储级别的加密(尤其在 NoSQL 系统中)，因此无法为拥有不同权限或角色的用户提供不同的密钥子集。

对于用户级加密服务，用户可以选择加密列、表或对应多个表、索引的数据文件集合。在密钥管理方面，由于需要利用不同的加密密钥对不同的数据库对象进行加密，安全服务器

需要额外地将用户会话权限集合和密钥集合进行映射，然后向 KMS 发起调用，从密钥存储器中检索需要的密钥集合。为保证安全性，安全服务器、KMS 和密钥存储器应该运行在被云用户内部部署的云平台中或与 DBMS 运行在不同的云平台中。基于 DBMS 用户的认证证书，安全服务器和 KMS 分别执行角色-密钥映射和密钥检索功能。然而，用户会话期间使用的密钥会保留在与 DBMS 实例相同的云平台的存储空间缓存中。安全地将 KMS 中检索的密钥传送给运行在云供应商平台的应用程序同样存在安全问题：表面上看，与 DBMS 应用的安全会话一旦建立，云用户就可以在 DBMS 应用程序所在的云平台中运行安全服务器和 KMS。但如果没有额外的安全措施，该方法遗留的敏感数据易受到云供应商管理员的访问攻击。

4.2　云环境下密钥服务互操作性的发展

如上所述，由于云数据密码服务中的所有权问题，随之而来的密钥管理互操作也会变得更为复杂。这种互操作涉及到两方面内容：1）与 HSM 等加密设备的密钥服务互操作，典型的安全标准是 PKCS＃11；2）在密钥集中管理的互操作管理，典型的安全标准是 KMIP。KMIP 通过集中式密钥管理服务实现系统和设备之间的密钥共享，使来自不同用户的应用程序可以共享加密数据[11]。PKCS＃11 实现的应用程序接口可以在多租户环境中交互不同的加密设备，解决了安全性应用程序和服务的集成要求。

结合 KMIP 管理密钥生命周期，PKCS＃11 交互硬件安全模块，可以将云平台的密钥服务互操作分为几个主要部分。

1）管理用户及认证：授权用户信息，进行用户访问控制，记录用户操作日志等。

2）密钥相关管理对象：云平台中的数据隐私、安全可用数据以及对它们的相关操作。

3）密钥管理接口：由云平台中 PKCS＃11 标准定义的设备之间的对话和 KMIP 标准定义的各种执行请求组成。由于加密设备的存在，密钥管理操作可以在平台内执行。KMIP 确保安全访问加密函数，PKCS＃11 利用安全认证控制台提供加密设备。

4）安全通信（消息）：KMIP 定义密钥管理服务器上密钥操作的消息格式以及可在服务器上执行加密相关操作的消息。

结束语　密钥管理系统整合了密钥创建、维护、保护、使用等管理的全部操作，云平台的分布式环境使得密钥管理变得更为复杂。本文从 3 种典型云服务环境的核心功能出发，总结分析了它们各自的安全功能及可能存在的密钥管理方面的问题。结合 KMIP 和 PKCS＃11 两个标准，提出未来云数据服务中密钥服务互操作的可能的安全功能要求。

参 考 文 献

[1] LIU F, TONG J, MAO J, et al. NIST Cloud Computing Reference Architecture: NIST SP 500-292[S]. National Institute of Standards and Technology, 2011.

[2] THOTA K, BURGIN K. Key Management Interoperability Protocol Specification v1. 2[S]. OASIS, 2015.

[3] 陈兴蜀，左晓栋，闵京华，等. 信息安全技术云计算服务安全指南：GB/T 31167-2014[S]. 北京：中国标准出版社，2014.

[4] CHANDRAMOULI R, IORGA M, CHOKHANI S. Secure Cloud Computing [M]. Springer New York, 2014: 1-30.

[5] GLEESON S, ZIMMAN C. PKCS＃11 Cryptographic Token Interface Base Specification v2. 40[S]. OASIS, 2015.

[6] BARKER E. Recommendation for Key Management-Part 1: General (Revision 4): SP800-57[S]. National Institute of Standards and Technology, 2015.

[7] BALL M V, HIBBARD E. Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data: IEEE P1619. 3[S]. 2009.

[8] Information technology-Security techniques-Key management-Part 1: Framework: ISO/IEC11770[S]. Tampa, Florida (USA): ISO/IEC JTC 1/SC 27, 2010.

[9] WONG M S. Current Data Security Issues of NoSQL Databases [DB/OL]. [2014]. https://www.fidelissecurity.com/files/NDFInsightsWhitePaper.pdf.

[10] BARKER E, BRANSTAD D, CHOKHANI S, et al. Cryptographic Key Management Workshop Summary[DB/OL]. http://csrc.nist.gov/publications/nistir/ir7609/nistir-7609.pdf.

[11] BARROSO J M D, AGUILAR L J, GUNDÍN P G, et al. Digital Enterprise and Information Systems[M]. Springer Berlin Heidelberg, 2011: 691-702.

[12] MELL P, GRANCE T. The NIST definition of cloud computing [J]. Communications of the ACM, 2011, 53(6): 50.

[13] FERNADES D A B, SOARES L F B, GOMES J V, et al. Security issues in cloud environments: a survey[J]. International Journal of Information Security, 2014, 13(2): 113-170.

[14] JANSEN W A. Cloud hooks: Security and privacy issues in cloud computing[C]// 2011 44th Hawaii International Conference on System Sciences (HICSS). IEEE, 2011: 1-10.

[15] LEI S, DAI Z S, GUO J D. Research on key management infrastructure in cloud computing environment[C]// 2010 9th International Conference on Grid and Cooperative Computing (GCC). IEEE, 2010: 404-407.

[16] RAMGOVIND, SUMANT, ELOFF M M, et al. The management of security in cloud computing[C]// Information Security for South Africa (ISSA), 2010. IEEE, 2010: 1-7.

[17] SO, KUYORO. Cloud computing security issues and challenges [J]. International Journal of Computer Networks, 2011, 3(5): 247-255.

[18] HASHIZUME K, ROSADO D G, FEMANDEZ E B, et al. An analysis of security issues for cloud computing[J]. Journal of Internet Services and Applications, 2013, 4(1): 1-13.

[19] BHARDWAJ S, JAIN L, JAIN S. Cloud computing: A study of infrastructure as a service (IAAS)[J]. International Journal of engineering and information Technology, 2010, 2(1): 60-63.

[20] BONIFACE M, NASSER B, PAPAY J, et al. Platform-as-a-service architecture for real-time quality of service management in clouds[C]// 2010 Fifth International Conference on Internet and Web Applications and Services (ICIW). IEEE, 2010: 155-160.

[21] SOARES L F B, FERNANDES D A B, GOMES J V, et al. Cloud security: state of the art[M]// Security, Privacy and Trust in

Cloud Systems. Springer Berlin Heidelberg, 2014: 3-44.

[22] VAQUERO, LUIS M, LUIS R M, et al. Locking the sky: a survey on IaaS cloud security[J]. Computing, 2011, 91(1): 93-118.

[23] JANSEN, WAYNE, GRANCE T. Guidelines on security and privacy in public cloud computing[J]. NIST special publication, 2011, 800(144): 10-11.

[24] MELL, PETER, GRANCE T. Effectively and securely using the cloud computing paradigm[J]. NIST, Information Technology Laboratory, 2009: 304-311.

[25] BERNSTEIN, DAVID, VIDOVIC N, et al. Cloud PAAS for high scale, function, and velocity mobile applications-with reference application as the fully connected car[C]// 2010 Fifth International Conference on Systems and Networks Communications (ICSNC). IEEE, 2010: 117-123.

[26] TAKABI, HASSAN, JOSHI J B D. Security and privacy challenges in cloud computing environments[J]. IEEE Security & Privacy, 2011, 8(6): 24-31.

[27] KRUTZ, RONALD L, VINES R D. Cloud security: A comprehensive guide to secure cloud computing[M]. Wiley Publishing, 2010.

[28] JU J, WANG Y, FU J, et al. Research on key technology in SaaS [C]// 2010 International Conference on Intelligent Computing and Cognitive Informatics. IEEE, 2010: 384-387.

[29] DESHMOKH A P, QVRESHI R. Transparent Data Encryption-Solution for Security of Database Contents[J]. International Journal of Advanced Computer Science & Applications, 2011, 2(3).

[30] LUO J Z, JIN J H, SONG A B, et al. Cloud computing: architecture and key technologies[J]. Journal of China Institute of Communications, 2011, 32(7): 3-21.

[31] HU J, KLEIN A. A benchmark of transparent data encryption for migration of Web applications in the cloud[C]// Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009(DASC'09). IEEE, 2009: 735-740.

[32] BRENDER, NATHALIE, MARKOV I. Risk perception and risk management in cloud computing: Results from a case study of Swiss companies[J]. International Journal of Information Management, 2013, 33(5): 726-733.

[33] ASHKTORAB, VAHID, TAGHIZADEH S R. Security threats and countermeasures in cloud computing[J]. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2012, 1(2): 234-245.

[34] ADAMSON, GÖRAN, WANG L H, et al. The state of the art of cloud manufacturing and future trends[C]// ASME 2013 international manufacturing science and engineering conference collocated with the 41st North American manufacturing research conference. American Society of Mechanical Engineers, 2013: V002T02A004-V002T02A004.

[35] LUO W J, X M. Attribute-based encryption and re-encryption key management in cloud computing[J]. Journal of Computer Applications, 2013, 33(10): 2832-2834. (in Chinese)
罗文俊, 徐敏. 云环境下的基于属性和重加密的密钥管理[J]. 计算机应用, 2013, 33(10): 2832-2834.

[36] KULKARNI, GAURAV, et al. A security aspects in cloud computing[C]// 2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS). IEEE, 2012: 547-550.

[37] BAMIAH, MERVAT, et al. Cloud implementation security challenges[C]// 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM). IEEE, 2012: 174-178.

[38] VAQUERO, LUIS M, LUIS R M, et al. Locking the sky: a survey on IaaS cloud security[J]. Computing, 2011, 91(1): 93-118.

[39] IBRAHIM, AMANI S, HAMLYN-HARRIS J H, et al. Emerging security challenges of cloud virtual infrastructure[C]// APSEC 2010 Cloud Workshop. Sydney, Australia, 2010.

[40] COSTANZO, ALEXANDRE D, et al. Harnessing cloud technologies for a virtualized distributed computing infrastructure[J]. Internet Computing, IEEE, 2009, 13(5): 24-33.

[41] DOMINIK B, WEGENER C. Technical issues of forensic investigations in cloud computing environments[C]// 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE). IEEE, 2011: 1-10.

[42] JAYASINGHE, DEEPAL, et al. Expertus: A generator approach to automate performance testing in IaaS clouds[C]// 2012 IEEE 5th International Conference on Cloud Computing (CLOUD). IEEE, 2012: 115-122.

[43] ASTROVA, IRINA, KOSCHEL A, et al. IaaS Platforms: How Secure are They[C]// 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2016: 843-848.

[44] BHATNAGAR, YATHARTH, SARWESH S, et al. DBMS as a Cloud Service[J]. (IJCSIT) International Journal of Computer Science and Information Technologies, 2014, 5(3): 3052-3054.

[45] KONSTANTINOU, IOANNIS, et al. On the elasticity of nosql databases over cloud management platforms[C]// Proceedings of the 20th ACM International Conference on Information and Knowledge Management. ACM, 2011: 2385-2388.

[46] GIESSMANN A, STANOEVSKA-SLABEVA K. Business models of platform as a service (PaaS) providers: current state and future directions[J]. JITTA: Journal of Information Technology Theory and Application, 2012, 13(4).

[47] RODERO-MERINO L, VAQUERO L M, CARON E, et al. Building safe PaaS clouds: A survey on security in multitenant software platforms[J]. Computers & Security, 2012, 31(1): 96-108.

[48] VAQUERO, LUSI M, LUIS R M, et al. Dynamically scaling applications in the cloud[J]. ACM SIGCOMM Computer Communication Review, 2011, 41(1): 45-52.

[49] LIU Z H, WANG Y H, LIN R H. A novel development and analysis solution to PaaS log by using CouchDB[C]// 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC). IEEE, 2012: 251-255.

[50] AHMED M. Trust enhanced security in SaaS cloud computing [R]. Deakin University, 2013.

[51] ZHONG C, ZHANG J, XIA Y, et al. Construction of a trusted SaaS platform [C]// 2010 Fifth IEEE International Symposium on Service Oriented System Engineering (SOSE). IEEE, 2010: 244-251.

[52] FABIO B, CORRADI A, FOSCHINI L. Database security management for healthcare SaaS in the Amazon AWS Cloud[C]// 2012 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2012: 000812-000819.

[53] PARK N. Secure data access control scheme using type-based re-encryption in cloud environment[M]// Semantic Methods for Knowledge Management and Communication. Springer Berlin Heidelberg, 2011: 319-327.

（上接第 2 页）

从图 2 可以看到，其生理年龄分布明显偏向右方，即整个群体的健康风险要比日历年龄 30 岁大一些。如果以各群体测算的生理年龄对应百分比作为权重，测算保费的均值为 0.1302，也明显要比日历年龄 30 岁的纯保费更大。

如果考虑日历年龄为 21～47 岁的群体，计算每个日历年龄所对应的群体在生理年龄下测算的终身寿险纯保费（1 元保额），并计算其均值，得到该均值随日历年龄变化的关系，如图 3 所示。

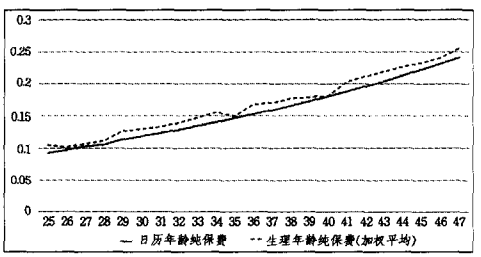

图 3　日历年龄定价结果与生理年龄定价结果的比较[1)]

从图 3 可以看出，整体上，生理年龄定价结果要普遍高于日历年龄定价结果，这反映了整个群体面临的风险要超过传统模式测算的保费，从另外一个角度说明利用生理年龄定价更加公平合理，让保险公司避免“死差风险”，也减小了投保人逆向选择的可能。

考虑到深度学习技术的特征，生理年龄应用于保险领域并不仅局限于测算保费。事实上，保险公司里的许多业务可以直接引入深度学习，例如核保核赔、保单审核、过程管理等。希望通过此研究让保险公司意识到深度学习的作用，真正建立起自己的“智能大脑”。此外，因为保险公司自身拥有更多数据，这会进一步发挥深度学习技术的潜力。

2　研究背景

众所周知，金融和保险行业积累了大量数据，但是在与大数据及人工智能技术结合上的发展动力还不足，这一方面是因为金融和互联网存在一定的跨界性，复合的人才较少，创新思维缺乏；另外，金融业自身的既有模式也起到了一定的阻碍作用。

这种阻碍在许多细分领域得到了体现。本文以寿险定价为突破口来展示深度学习对传统模式的挑战，后续还将就此进行大量试验和研究，力图从多角度变革金融模式。具体来说，传统模式的寿险定价的核心在于获得寿命的分布函数（或者是生存函数），然后通过计算精算现值获得精算纯保费。从保险诞生之初持续到现在[2)]，该模式一直未曾改变。但是常说的年龄真的反映了个体的死亡风险或者健康风险了吗？答案是否定的，它恰好和保险人所要承保的“风险”相关性不大，正因如此，保险公司必须承保大量个体来实现风险的分担，这反映了当前保险业的一个现实，即保险人不能更好地“把握”投保的个体所面临的风险。

限于多方因素，该矛盾在过去不可能得到实质性解决，但是在基因、互联网、医疗技术、穿戴设备、人体量化、大数据等技术高速发展的背景下，我们认为解决的时机已经显现。本文就是沿着该思路，将这种可能归结为生理年龄（Biological Age），从而引入将深度学习作为代表的人工智能技术，基于大数据样本的积累，重新变革定价模式以反映个性化的风险程度。

参 考 文 献

[1] GLEI D A, GOLDMAN N, RISQUES R A, et al. Predicting Survival from Telomere Length versus Conventional Predictors: A Multinational Population-Based Cohort Study[J]. Plos One, 2016, 11(4): e0152486.

[2] LEVINE M E. Modeling the rate of senescence: can estimated biological age predict mortality more accurately than chronological age? [J]. The journals of gerontology. Series A, Biological sciences and medical sciences, 2013, 68(6): 667-674.

[3] HILTON G E, SALAKHUTDINOV R R. Reducing the Dimensionality of Data with Neural Network[J]. Science, 2006, 313: 504-507.

[4] LECUN Y, BENGIO Y, HILTON G. Deep Learning [J]. Nature, 2015, 521: 436-444.

[5] KRIZHEVSKY A, SUTSKEVER I, HINTON G. ImageNet classification with deep convolutional neural networks[C]// Proc. Advances in Neural Information Processing Systems. 2012, 25: 1090-1098.

[6] TOMPSON J, JAIN A, LECUN Y, et al. Joint training of a convolutional network and a graphical model for human pose estimation[C]// Proc. Advances in Neural Information Processing Systems. 2014, 27: 1799-1807.

[7] MIKOLOV T, DEORAS A, POVEY D, et al. Strategies for training large scale neural network language models[C]// Proc. Automatic Speech Recognition and Understanding. 2011: 196-201.

[8] MA J, SHERIDAN R P, LIAW A, et al. Deep neural nets as a method for quantitative structure-activity relationships[J]. Journal of Chemical Information & Modeling, 2015, 55(2): 263-274.

[9] WESTON J, BORDES A, CHOPRA S, et al. Towards AI-complete question answering: a set of prerequisite toy tasks[OL]. http://arxiv.org/abs/1502.05698.

[10] MNIH V, et al. Human-level control through deep reinforcement learning[J]. Nature, 2015, 518: 529-533.

1) 其样本数据截至 2016 年 10 月 1 日，后期我们将进一步引入新数据以调整模型和提升结果。

2) 最早在 1693 年，哈雷就编制了德国布勒斯劳市的生命表。