



专题:云计算技术与应用

云环境下的敏感数据保护技术研究^{*}

刘明辉¹, 张 尼¹, 张云勇¹, 胡 坤², 宫 雪¹, 曲大林¹

(1. 中国联合网络通信有限公司研究院 北京 100032;

2. 中国联合网络通信集团有限公司客户服务部 北京 100032)

摘 要:针对在云计算服务领域中,用户最关心存储在云端的敏感数据的安全这一问题,研究了云环境下敏感数据所面临的安全风险,分析了云环境下的敏感数据安全需求,在敏感数据分类分级的基础上,给出了云环境下的敏感数据保护技术方案。

关键词:云计算安全;敏感数据;数据脱敏

doi: 10.3969/j.issn.1000-0801.2014.11.001

Research on Sensitive Data Protection Technology on Cloud Computing

Liu Minghui¹, Zhang Ni¹, Zhang Yunyong¹, Hu Kun², Gong Xue¹, Qu Dalin¹

(1. China Unicom Research Institute, Beijing 100032, China;

2. Customer Service Department, China United Network Communications Group Company Limited, Beijing 100032, China)

Abstract: In the field of cloud computing services, one of the most important problems concerned by the users is the security of their sensitive data stored in the cloud. The security risks when sensitive data is in a cloud environment were studied, and the sensitive data protection requirements in cloud environments were analyzed. On the basis of sensitive data classification and grading, technical solutions were given to protect sensitive data in cloud environments.

Key words: security of cloud computing, sensitive data, data masking

1 引言

对电信运营商而言,敏感数据可以分为两大类:第一类是企业自身敏感信息,如企业战略规划、财务信息、投融资决策、产购销策略、大客户资料、经营分析报告等,这些信息不为公众所知悉,能为企业带来经济利益,具有实用性,包括经营信息和技术信息;第二类是用户的个人信息,随着电信运营商业务的快速发展,业务生产系统积累了大量包含用户姓名、身份证件号码、住址、电话号码、账

号等敏感信息的数据,如果这些数据发生泄露、损坏,不仅会给电信运营商带来经济上的损失,而且会给电信运营商的声誉带来负面影响。

随着云计算技术的广泛采用,大量企业及用户敏感数据集中在云中存储,如果缺乏安全保障,敏感数据可能会被泄露或篡改,尤其是企业的敏感数据可能包含很多商业机密,如果泄露出去,将给企业及用户造成重大损失,也必将影响运营商的信誉,不利于云计算的发展和应用。

^{*} “新一代宽带无线移动通信网”国家科技重大基金资助项目专项(No.2012ZX03002001-002, No.2013ZX03002004-002, No.2013ZX03002003-005)

目前,电信运营商在业务开展、开发测试、审计监管等使用过程中如何保证敏感数据安全已经成为一个重要的问题。因此急需建设敏感数据保护系统,对数据存储、使用的管理流程进行规范化管理,通过技术措施提高使用敏感数据的安全保障^[1]。本文提出建立从使用前的敏感数据治理,到使用中的敏感数据保护,再到使用后的敏感数据审计和泄露追溯的整体保护体系,从而达到降低数据使用的风险,扩大数据的使用范围的目的。

随着云计算应用的广泛开展,有关云数据安全的研究和实践也已逐步展开,参考文献[2]以图书馆行业为例分析了云环境下的风险,参考文献[3]分析云环境下的数据安全风险,并建立了数据安全和隐私保护模型,基于加解密算法的解决方案^[4]可以实现数据的加密存储;参考文献[5]是以标签技术为基础,提出了一种具体的文件扩散分析和追溯技术;参考文献[6, 7]研究了同态加密技术在云数据保护中的应用。同态加密等技术还处于理论探索阶段,目前还无法应用于实际环境中。本文从工程实施的角度,建立云环境下的敏感数据保护实施方案,其中的关键技术也是目前较成熟的。

2 云环境下的敏感数据安全问题

在云环境下,敏感数据在存储和传输过程中被非法获取或篡改的风险依然存在,同时,云计算动态虚拟化的服务模式也带来了一系列新的安全问题。

首先,敏感数据的防护边界发生了变化。采用云计算技术就意味着一个企业的数据和应用会分布到多个数据中心,这就为企业创建了新的安全边界,企业需要在更多的地方实施防护,防护边界的变化增加了敏感数据安全防护的复杂度。

其次,资源共享机制带来了新的安全风险。由于云计算多租户共享资源的特点,其资源以虚拟、租用的方式供应,多个用户使用的虚拟资源很可能会绑定到同一个物理资源上。如果云平台中的虚拟化软件中存在安全漏洞,用户的数据就存在泄露的风险^[8]。

再次,数据存储模式发生了变化。云环境下,数据的存储是碎片化的^[4],很难知道敏感数据存储的物理位置,基于物理机的数据防护手段就变得无能为力了。

最后,数据存储结构发生了变化。云化的数据中心网络向扁平化架构过渡,数据中心内部之间的流量将会大大增加,云化的数据中心和高速的 Internet 出口带宽可能被黑客

利用作为攻击跳板,从而带来敏感数据泄露的风险。

上述安全问题,可以总结为:系统中的敏感数据有哪些?关键的敏感数据在云环境下的逻辑位置如何?静态的敏感数据如何保护?动态的数据如何监管?发生数据泄露问题后如何补救?

3 敏感数据安全需求

为解决云环境下的敏感数据保护安全问题,本文从敏感数据使用前的治理、使用中的保护和使用后的审计溯源 3 个方面入手,分析敏感数据的安全需求,使用前的治理应做到避免安全事件的发生或降低安全事件发生的概率,使用中的保护措施应做到减少安全事件造成的影响,使用后的审计应做到在安全事件发生后可追溯。

使用前的治理:按照敏感数据所处的位置、形式等进行分类,按照敏感数据的重要性进行分级,掌握云环境下敏感数据资产的分类分级、所处的位置、状态等信息,这是采取后续保护措施的前提条件。对敏感的静态数据进行规范存储和管理,防止静态数据的滥用。

使用中的保护:包括脱敏、监控、防泄露等内容。数据脱敏是指对敏感数据进行的变形,隐藏敏感属性,不仅可以避免云环境下的重要敏感数据直接暴露给黑客的风险,还可以防止内部员工滥用敏感数据。掌握了敏感数据的静态属性还不能满足数据动态流转过程中的保护需求,因此,需要对数据的流转、操作、异常状况以及敏感文件的打开、复制和转移等关键操作进行实时或准实时的监控,部署智能阻断模块,对违规操作进行封堵。为保护敏感数据不被泄露,需要监控潜在的数据泄露途径,实现敏感数据泄露预警、封堵等功能。

使用后的审计与溯源:一旦发生敏感数据泄露事件,需要及时找到泄露的源头,从而进行查缺补漏。

4 云环境下的敏感数据保护方案

4.1 总体逻辑架构

如图 1 所示,云环境下的敏感数据保护总体逻辑架构自下而上分别为敏感数据发现层、敏感数据集中管理层和敏感数据治理和保护层。

- 敏感数据发现层包括敏感数据发现算法和保护代理模块,在系统中的主机、服务器、数据库等部署敏感数据安全代理,实现基于内容识别技术的敏感数据发现,敏感数据安全保护策略的接收和执行。

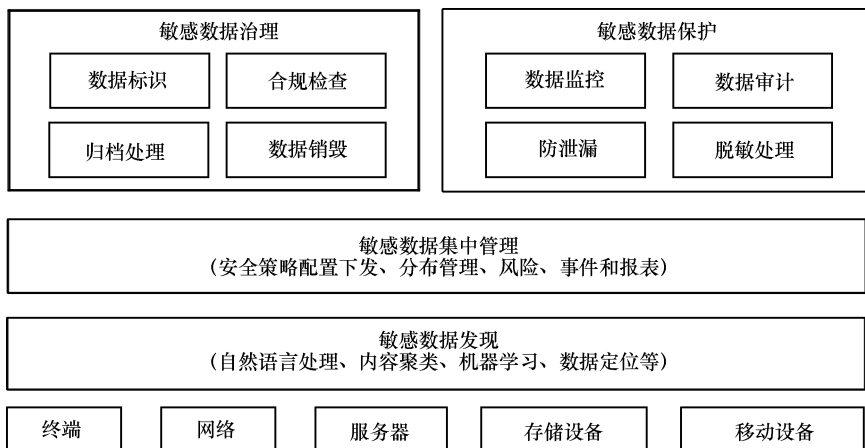


图1 敏感数据保护总体逻辑架构

- 敏感数据集中管理层是在敏感数据发现的基础上，建立起云环境下敏感数据总体分布视图，进行统一的敏感数据保护策略的管理和下发，通过安全策略配置，实现差异化的敏感数据治理和保护机制。
- 敏感数据治理和保护层是下层安全策略的执行层。敏感数据治理是指敏感数据的安全管理，主要包括数据标识、合规检查、数据归档和数据销毁等数据安全要求；敏感数据保护是指敏感数据的安全技术保护手段，主要包括数据脱敏、敏感数据使用监控、敏感数据防泄露和敏感数据审计与追溯等安全措施。

4.2 敏感数据分类分级

云环境往往承载着海量数据，其中一部分是敏感数据，另一部分是普通数据。对所有数据不加区别地保护，需要投入大量资源，存在大量浪费，经济上抵消了云平台的优势，十分不可取^[9]。如何识别敏感数据并实施有针对性的保护，是进行数据保护的重要基础工作。

FFIEC(美国联邦金融机构研究委员会)的合规指南要求数据分类必须是企业风险评估流程中的一个组成部分。不同的数据可以有很多不同的分类，而更为敏感和高价值的的数据显然需要更严格的保护机制。数据分类是把数据分为从低价值到高价值的各种类型并且与部门和用户的权限要求相对应从而达到强制对一种特定类型的信息进行正确安全控制的目标，如客户的身份信息类、设计方案类、销售记录类、合同类等。敏感数据的分级是指敏感数据项的泄露可能会直接对客户或机构造成损失的高低，如某设计公司的设计图纸，对机构来说就是最高安全级别，而员工的通讯录就属于一般安全级别；敏感数据的分级又需要

考虑组合敏感数据的情况，即单个数据项泄露不会造成损失，但是若干个数据项集中泄露可能会造成客户或机构的损失^[10]。

4.3 敏感数据发现

敏感数据的发现是指对目标系统的全量数据进行梳理，从中抽取出敏感数据，并记录敏感数据所在的物理位置、逻辑位置、存储格式、状态、数据量等信息，对云环境下海量的数据进行梳理，需要自动化手段来完成^[11]。

最常见的自动处理方式是通过检索指定文件或数据中是否包含预先定义的关键词来判定文档是否敏感，并对敏感文档进行管理和授权。由于关键词比对仅仅是对于设定的关键词进行“有”或“无”的判断，因而这种分类方式较为粗糙，对分类的判断不够准确。如含有“合同”这一关键词的并不一定是法律合同而含有“协议”但无“合同”关键词的，也有可能是法律合同。而且，依靠简单关键词也不能将文档具体细化为何种分类，即不能判断是财务类、人事类、销售类或技术类等，导致文件安全管理存在较大缺陷。若想提高敏感数据分类的准确性，可以应用自然语言处理和文档分类算法。

自然语言识别是语言信息处理的一个重要组成部分，采用人工智能的理论和将设定的自然语言机理用计算机程序表达处理，从而构造出能够理解和识别自然语言的机器智能软件。文档分类是在预定义的分类体系下，根据文档的特征，将给定的文档与一个或多个类别相关联的过程。因此，文档分类是自然语言理解与模式识别密切结合的系统，其核心技术是构建一个具有高准确度和较高速度的分类器。

敏感数据发现的一般流程如下。

(1)数据获取:抓取终端、服务器、数据库、云存储、网络等云环境中的不同数据。

(2)格式解析:对抓取的数据格式和字符集进行分析,包括文档、数据库、网络协议,获取文本内容、图片信息等。

(3)内容分类:采用自然语言处理和数据分类等技术对内容进行分析,也对格式进行匹配,完成数据的分类,从而完成敏感数据的发现。

4.4 敏感数据集中管理

敏感数据集中管理层汇集数据发现层上传的数据分布情况,根据分类分级、用户、设备、账户等维度,对不同等级的敏感数据设置有区别的安全保护策略,并发送到上层的敏感数据治理和保护层进行策略的实际执行。

4.5 敏感数据治理

数据标识,是指根据敏感数据泄露追溯要求,对敏感数据添加特殊的标识,如添加水印或其他特殊字符等,在发生敏感数据泄露的情况下,可以根据事先添加的数据标识,定位数据泄露的源头。数据标识的添加,原则上不能影响数据的正常使用,而且不能将被添加者之外的实体去除。

敏感数据内容合规性检查,是指对敏感数据内容进行合规性扫描,如标题、格式、大小限制、敏感内容等,需要实现梳理出敏感数据的合规扫描规则,在规则中指定检查依据,合规检查过程完成后生成合规报表。

敏感数据归档处理,是指将不再经常使用的数据移到一个单独的存储设备进行长期保存。数据归档必须遵从规则来保存,具有索引和搜索功能,使得文件可以很容易地找到。数据归档应满足如下要求:对完整的数据条目进行归档;可从现有应用程序界面访问归档数据,以及恢复完整的归档数据或归档快照;建立完整的归档过程追踪和管理制度;对归档数据的所有访问、保留、清除和保留活动进行记录^[12]。

敏感数据销毁,是指数据删除后保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。常见的数据销毁方法有覆写法(需专业设备)、消磁法(需专业设备)、捣碎法、焚毁法和化学腐蚀法等。

4.6 敏感数据保护

4.6.1 数据脱敏

数据脱敏是指根据数据保护规范和脱敏策略,对业务数据中的敏感信息实施自动变形,实现对敏感信息的隐藏。数据脱敏的内涵是:借助数据脱敏技术,屏蔽敏感信

息,并使屏蔽的信息保留其原始数据格式和属性,以确保应用程序可在使用脱敏数据的开发与测试过程中正常运行。脱敏算法的设计与数据应用的场景紧密相关,在设计脱敏算法时要考虑的因素主要包括如下几个方面。

- 脱敏后保持数据业务属性,取值范围合理,脱敏后保留数据业务属性和商业价值,仍可作为生产数据使用。业务数据中的人名、地名、日期等在脱敏后需要保持可读性。脱敏后数据要能正确通过有效性验证,如身份证号的校验码和生日区间,取值范围要合理,如信用卡号变换后仍属于发卡行号码区间等。
- 脱敏后保持数据完整性,保留数据字段原格式、长度不变,如对手机号码进行脱敏,脱敏完成后仍为11位手机号码,并且已经不是真实的电话号码。
- 脱敏可逆性,脱敏后可以恢复成原始业务数据。随着大数据分析应用的逐步开展,业务部门经常需要将脱敏后的数据还原成原始业务数据,以开展下一步工作,例如,电信运营商将脱敏后的海量用户上网行为详单交给第三方大数据分析厂商,归纳用户行为;在得到分析结果后,运营商需要将虚构身份信息还原为真实用户身份,以获得真实用户偏好数据,才可以进行精准营销。
- 脱敏可重复性,不同轮次的脱敏结果相同;例如,某企业正在内部测试一套分析预测系统,为了更好地再现真实场景,需要连续从业务系统每周抽取客户购买数据,要求每次抽取脱敏过程对同一身份证号的变换结果必须相同,才可以保证同一客户的行为模式被正确理解分析,否则就会影响测试效果。在另外的场景中,出于保密考虑,对同一字段每次进行脱敏的结果都要求具有一定差异性,以避免黑客或内部员工收集大量脱敏前后数据,通过逆向工程还原真实数据。
- 脱敏完备性,防止使用非敏感数据重建敏感数据;如果某些非敏感数据的组合可以用来重建敏感数据,那么这些非敏感数据也需要进行脱敏处理。例如,即使将病案号进行了脱敏,但使用病人年龄等个人信息、治疗方式代码和药物名称等,就能追溯回这个特定的病案号甚至病人,那么需要将年龄、治疗方式代码和药物名称等也进行一定程度的脱敏处理,防止病人隐私泄露。黑客经常实施这种含有推理分析的攻击,脱敏算法设计时需要考虑防范此种情况。



表 1 脱敏算法对比分析

技术类别	主要优点	主要缺点	代表技术	典型应用场景
基于公开加密算法的技术	数据真实、无缺损； 高隐私保护度、可逆、可重复	计算开销大； 部署简单	公开对称加密算法如 3DES、AES、SM1、SM4 等	在分布式环境下的通信加密； 机密性要求高； 不需要关联性； 不需要保持业务属性
基于数据失真的技术	计算开销小；实现简单 适用于各类数据、众多应用，算法通用性高； 能保证发布数据的真实性，实现简单	数据失真，不可逆 存在一定程度的数据缺损； 存在一定程度的隐私泄露； 不可逆； 算法成熟度低，目前应用范围不广	随机干扰； 阻塞、凝聚； 不可逆乱序； 散列如 MD5/SHA1 匿名化模型： • k-匿名； • l-diversity； • m-invariance 匿名化算法： • Mondrian； • Incognito； • r-cellular	群体信息统计； 需要关联性； 需要保持业务属性 群体信息统计
基于可逆的置换算法	数据真实、无缺损； 算法效率高； 可逆，可重复	算法规则或映射表泄露对隐私数据威胁较大	位置变换； 表映射变换； 基于算法的映射	需要保持业务关联性； 需要可逆的厂商； 需要保持业务属性

目前常用的数据脱敏算法可以分为基于公开加密算法、基于数据失真和基于可逆置换算法三大类^[3]。表 1 对 3 类算法的主要优缺点、代表技术和典型应用场景进行了分析和总结。

云计算环境中需要保持业务属性的存储数据可以分为两类：静态数据和动态数据。静态数据是指用户的文档、报表、资料等不参与计算的用户数据；动态数据是指需要动态验证或参与计算的用户数据。静态数据脱敏通过创建可在内部和外部安全共享的真实但无法识别归属的数据，防止敏感数据意外泄露。静态数据脱敏应具备以下主要功能：可以为任意格式的敏感数据创建数据脱敏算法，能够保留数据字段格式，同时脱敏原始数据值，维护脱敏数据的完整性；能够创建可在整个系统中重复使用的数据脱敏规则和标准，通过定制数据隐私策略以满足每种业务需求。动态数据脱敏能够实时防止未授权用户访问敏感信息，阻止、审计和提醒访问敏感数据的最终用户、IT 人员和外包团队。动态数据脱敏应具备以下主要功能：能够实时地应用大量安全措施，对未授权访问进行动态数据脱敏、加密、阻止、审计和提醒；通过一次性定义数据脱敏策略并多次使用，实现跨工具、应用程序和环境的迅速、一致的访问限制；能够保证脱敏数据的完整性并满足业务系统的数据需要^[1]。

4.6.2 敏感数据使用监控

敏感数据的使用监控是指针对应用系统运行、开发测试、对外数据传输和前后台操作等使用环节，根据定义的

敏感数据使用规则对数据的流转、存储与使用进行监控，及时发现违规行为并进行下一步处理^[3]。敏感数据的访问规则包括主机链接规则、数据库访问操作规则、应用访问操作规则以及终端数据访问规则。

主机链接规则监控是指通过梳理敏感数据所在主机的合法网络链接情况，将合法访问链接定义为白名单，并制定主机链接监控策略，根据策略对所有主机网络链接进行监控分析，对不在白名单范围内的网络链接进行告警。

应用访问操作规则监控是指通过梳理应用流量与业务操作、敏感数据之间的关联关系，制定的访问监控策略，采用流量采集的方式对所有的应用流量进行分析，从而发现与敏感数据相关的违规操作行为。

数据库监控是指对数据库的访问操作行为进行监控，及时发现对敏感数据所在表的非法访问和操作，对于后台的数据库访问和操作可以基于堡垒主机实现，数据库监控模块能够采集堡垒主机的日志，根据监控策略对用户的行为进行分析，监控策略能够基于命令（如 select、update、insert、delete 等）和表名的黑白名单配置。对于前台的数据库访问和操作，可以在数据库前端部署流量采集设备，对访问数据库的流量进行协议分析和还原，并根据监控策略对用户的行为进行分析。监控策略能够基于命令（如 select、update、insert、delete 等）和表名的黑白名单配置。

终端使用监控是指对存储敏感数据的终端进行安全管理和监控。可以根据组织、部门、用户等设计设备的从属

关系,定义设备和所存储数据的对应权限规则(允许/监督/禁止等)。如果发生敏感数据违规操作的情况,如敏感数据出现在不安全的位置,非法打印含有敏感信息的文件,非法复制或转移含有敏感数据的文件或使用即时通信、邮件等工具进行数据外发等,即可发现并报告风险。如果终端用户试图在非授权的情况下操作敏感数据,会触发报警提示,对严重违反安全策略的操作可以直接进行操作阻断。

4.6.3 敏感数据防泄露

敏感数据被从系统外发到安全不可控区域、第三方设备、个人终端设备等不可信域时,需要采取输出数据的合规审计和出口敏感数据防泄露措施。

针对需要通过外网传输或者通过专用接口外发到合作伙伴以及第三方机构的敏感数据,对其输出数据的安全状态进行统一审计,包括数据内容安全审计、数据格式合规性审计、数据输出行为合法性审计。

在网络出口上可以使用镜像流量的方式对旁路流量进行标识扫描以发现敏感数据,或通过内容扫描发现预定的敏感数据,发现异常后,即触发告警信息或阻断操作,及时对敏感数据的泄露进行封堵。

4.6.4 敏感数据的审计与防扩散

敏感数据的审计和防扩散是数据使用后的敏感数据保护措施,审计是指对泄露点的发现,防扩散是指在发生

数据泄露的情况下,找到泄露的源头进行追责,并防止进一步的敏感数据扩散。

敏感数据的审计指对敏感数据进行访问的各种行为进行日志收集和审计分析,是一种事后的查询取证功能,前提是相关的系统需要对用户的数据访问行为进行日志记录,包括敏感数据的治理、数据脱敏、敏感数据使用监控和敏感数据防泄露的日志记录。

对于从系统外发的敏感数据,需要提供必要的防扩散安全技术防护措施,通过对敏感数据进行防扩散跟踪和防扩散管控,达到尽可能的安全防护效果。常用的技术手段是数据标识和数字水印^[14]。

4.7 系统部署方案

云环境下的敏感数据保护系统部署方案如图 2 所示,其中,敏感数据中央管理服务器是整个敏感数据保护系统的核心服务器,负责下发敏感数据治理和敏感数据保护策略,采集系统日志,建立洞察云环境全局的敏感数据及相关安全事件视图,生成报表。敏感数据发现服务器,完成敏感数据的分类分级设置和扫描发现。数据脱敏服务器负责按照预定的安全策略,对敏感数据实施脱敏计算。互联网出口泄露监控使用旁路方式实现,通过在互联网出口交换机上设置镜像,将互联网出口流量复制到核心数据泄露监控设备进行流量监测,以发现核心数据通过互联网出口发

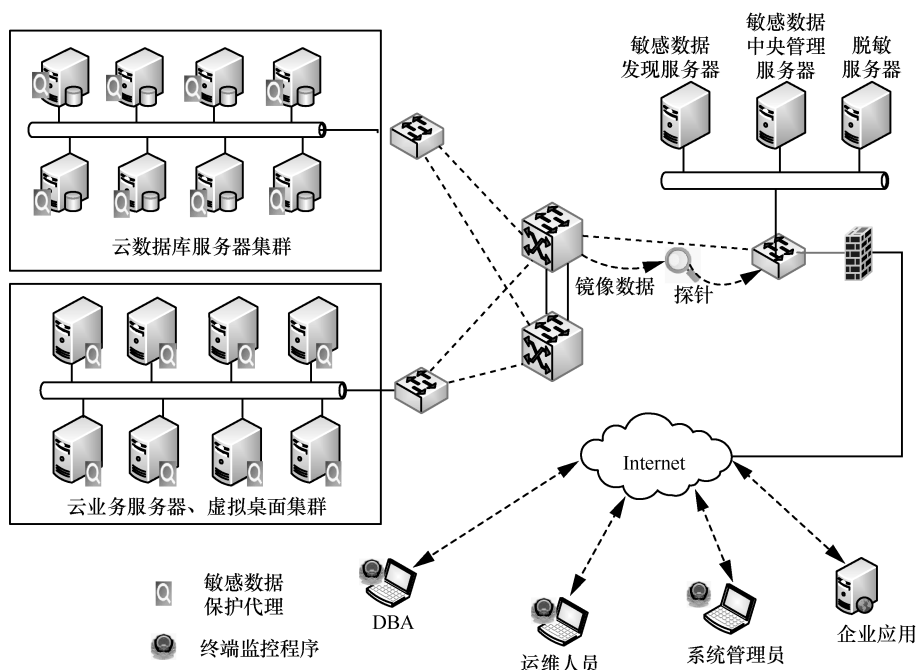


图 2 云环境下的敏感数据保护系统部署方案



生的泄露事件。在云数据库、主机和虚拟桌面上部署敏感数据保护代理软件,负责进行敏感数据的扫描和发现,并将扫描结果上传至敏感数据发现服务器;在运维终端上部署终端监控程序,对运维终端上发生的数据泄露事件进行采集并上传到敏感数据中央管理服务器。

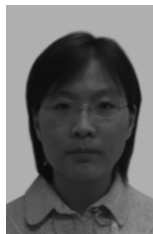
5 结束语

本文分析了云环境下敏感数据安全问题的新特点,在此基础上总结出敏感数据保护的安全需求,包括敏感数据使用前的分类分级管理,使用中的脱敏、监控、防泄露以及使用后的审计与追溯。为满足以上安全需求,提出了完整的云环境下的敏感数据保护方案:首先对敏感数据进行梳理,在此基础上进行集中安全策略制定、管理和下发,由执行层的敏感数据治理和保护措施模块来完成安全策略的执行,从而实现敏感数据的保护。

参考文献

- 1 姜日敏. 电信运营商数据脱敏系统建设方案探讨. 中国科技信息, 2014(8):132~133
- 2 程风刚. 基于云计算的数据安全风险及防范策略. 图书馆学研究, 2014(2): 15~36
- 3 张文科, 刘桂芬. 云计算数据安全和隐私保护研究. 信息安全与通信保密, 2012(11): 38~40
- 4 胡光永. 基于云计算的数据安全存储策略研究. 计算机测量与控制, 2011, 19(10): 2539~2541
- 5 王志文, 王强. 云计算敏感数据防泄露技术研究. 信息安全与通信保密, 2013(8): 85~87
- 6 李清玉. 云计算数据安全研究. 信息安全与通信保密, 2012(11):62~65
- 7 任福乐, 朱志祥, 王雄. 基于全同态加密的云计算数据安全方案. 西安邮电大学学报, 2013, 18(3): 92~95
- 8 尹彬彬. 云计算中统一身份认证和数据标记方案研究. 华中科技大学硕士学位论文, 2012
- 9 韩建民, 于娟, 虞慧群等. 面向数值型敏感属性的分级1-多样性模型. 计算机研究与发展, 2011, 48(1): 147~158
- 10 郭健, 沈杰. 电信运营商安全审计系统小概率关联分析技术探讨. 电信科学, 2013, 29(4): 137~140
- 11 王衍锋, 陈典友, 姜帆等. 商业银行敏感数据识别与风险分析. 计算机安全, 2011(10): 26~30
- 12 张逢喆, 陈进, 陈海波等. 云计算中的数据隐私性保护与自我销毁. 计算机研究与发展, 2011, 48(7): 1155~1167
- 13 周水庚, 李丰, 陶宇飞等. 面向数据库应用的隐私保护研究综述. 计算机学报, 2009(5): 847~861
- 14 明华, 张勇, 符小辉. 数据溯源技术综述. 小型微型计算机系统, 2012(9): 1917~1923

[作者简介]



刘明辉,女,博士,中国联合网络通信有限公司研究院云计算实验室高级工程师,主要研究方向为智能卡、版权保护、物联网安全技术、大数据安全等。



张尼,男,博士后,中国联合网络通信有限公司研究院云计算实验室高级工程师,主要从事移动互联网安全、云计算安全、信息安全等领域研发工作。



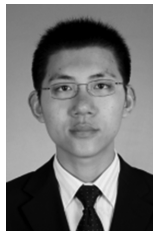
张云勇,男,博士后,中国联合网络通信有限公司研究院副院长、高级工程师,主要研究方向为下一代开放网络、固定移动通信核心网、移动互联网及业务、云计算。



胡坤,男,博士,中国联合网络通信集团有限公司客户服务部高级工程师,主要研究方向为云计算、大数据应用、机器学习等。



宫雪,女,中国联合网络通信有限公司研究院云计算实验室工程师,主要从事业务与支撑系统、近场通信、信息安全等领域的研究咨询工作。



曲大林,男,中国联合网络通信有限公司研究院云计算实验室工程师,主要研究方向为网络与信息安全规划、数据安全等。

(收稿日期:2014-10-16)