



一种细粒度的移动数据安全保护模型

杨育斌,程丽明

(蓝盾信息安全技术股份有限公司 广州 510665)

摘要: 提出一种细粒度的移动数据安全保护模型,通过在智能终端和移动接入网关/服务器处针对移动数据、移动应用进行标记,对移动数据的操作进行控制,达到移动数据安全隔离的目的,进而实现对移动数据细粒度的安全管理功能。模型由移动数据管理模块和标签控制管理模块组成。移动数据管理模块根据标签识别用户权限和数据保密级别,对移动数据的移动应用进行操作控制;标签控制管理模块对数据标签和应用标签的生成、修改、存储和传输进行控制管理。对模型的移动智能终端侧进行了实验,证明模型能对移动数据进行细粒度的保护。

关键词: 细粒度;移动数据;标签;数据安全

doi: 10.3969/j.issn.1000-0801.2014.01.003

A Fine-Grained Mobile Data Security Model

Yang Yubin, Cheng Liming

(Bluedon Information Security Technology Co., Ltd., Guangzhou 510665, China)

Abstract: A kind of fine-grained security model for mobile data was proposed, tagged the mobile data and mobile applications in the intelligent terminal and the mobile access gateway/server, to control the operation of mobile data, and achieve the purpose of mobile data security isolation. Thus fine-grained security for mobile data management capabilities were achieved. The model was consisted of mobile data management module and the label control management module. The mobile data management module identified the user permissions and level of data privacy through the label to control the operation of mobile application of mobile data. The creating, modifying, storing and transmitting of the data label and application label were controlled and managed by the label control management module. Experiments on the Android device were carried out, and the security of the model was confirmed.

Key words: fine-grained, mobile data, tag, data security

1 引言

近年来随着智能手机、平板电脑等移动设备的飞速发展,移动计算的应用范围不断扩大,提供的服务也愈加广泛。BYOD(bring your own device,自带设备)就是移动计算服务重要的领域之一,BYOD是指携带自己的设备办公,这些设备包括个人电脑、手机、平板电脑等,在公司办公场所之外登录公司邮箱、在线办公系统,不受时间、地点、设

备、人员、网络环境的限制。2013年3月,IT168对企业移动安全应用状况进行了一份调查,结果显示300人以下使用移动办公的企业占到48%、300~500人使用移动办公的企业占22%、500~1000人使用移动办公的企业占24%、1000~2000人使用移动办公的企业占3%、2000人以上使用移动办公的企业占3%。BYOD已得到了相当广泛的应用。

BYOD利用移动智能设备使用灵活的特点,为员工在



办公室外工作提供了极大的方便,大大提升了企业或组织的办公效率,但同时也带来了严峻的安全问题,主要集中在用户访问、追踪移动设备、保护移动数据等,其中最重要的就是企业数据的安全保护。Cisco 公司在“BYOD and Virtualization”中提到,BYOD 中最关心的就是企业数据安全威胁问题。Accellion 公司在“10 Mobile Security Requirements for the BYOD Enterprise”中也强调,BYOD 移动安全控制就是对企业数据存储、处理中基于权限的安全控制。SAP 公司计划在 3~6 个月后推出自行研制的一款软件,帮助用户在他们的智能手机或平板电脑上把商业数据从个人信息中分离出来,以此保障信息安全,但大多国际和国内的 MDM (mobile device management) 或 MAM (mobile application management) 产品都没有基于用户权限对企业数据进行细粒度操作控制管理的功能。

2 国内外相关研究

国内外学术研究者针对移动办公中的数据安全问题进行了相当深入的研究。杨卫军和秦海权^[1]提到攻击者的目的可以划分为收集用户隐私数据、使用移动设备计算资源以及破坏设备正常运行 3 种类型;针对移动设备的攻击方式可以分为四大类:利用移动网络服务接入、利用互联网接入、利用蓝牙接入、利用 USB 及其他外围设备接入。陆宏亮^[2]提出移动云环境下基于终端上下文信息的数据保护架构,利用 ASFC 在数据决策模块中应用层次分析的方法对数据安全保护策略进行决策,实现在对用户终端进行保护的同时,减少终端资源的消耗并提升事务处理性能,进而改善移动用户的事务处理体验。石莎^[3]利用散列加密原理提出了一种通过设计全新的内容安全分权分域解决方案来满足云计算环境下的内容分配和内容管理中的相关安全和授权问题的方法,以保护移动互联网中的内容和文档的安全。杜久升和陈宜金^[4]通过 5 种方式提高数据传输的安全性,分别为:在客户端进行身份验证,确保用户合法性;针对使用者,采用授权与访问控制的方式明确权限范围;通过网络防护手段保证内外网的安全性;通过特定技术手段提高数据传输的可靠性;通过多种方式确保数据在公网传递的保密性。Butter T 和 Aleksy M^[5]展示了在移动和上下文感知应用环境中,基于运行在 Java 虚拟机内部的虚拟机执行不可信代码进行数据隔离和服务隔离的方法。Nkosi M 和 Mekuria F^[6]使用云计算协议管理模型(提供多媒体感应信号处理),向移动设备提供安全存储即服务。

Wonjoo P、Sun J K 和 Kee S C^[7]提出了一个管理复杂移动终端的安全管理框架,向同步接收多种服务和系统管理的复杂终端提供安全保护功能。Wu J J、Zhou J 和 Ma J 等^[8]提出了一种主动防止数据泄漏的模型,利用可信存储与虚拟隔离技术,并结合数据对象保护要求,防止内部威胁。但以上研究均未对移动数据进行单独的、细粒度的保护。

本文提出一种细粒度的移动数据安全保护模型,通过在智能终端和接入网关/服务器处对移动数据、移动应用进行标记,以控制对移动数据的访问、处理操作,实现移动终端数据的安全隔离(含企业/个人数据隔离功能),进而实现对移动数据保密性的细粒度安全管理功能。

3 模型的系统结构

本文提出了一种细粒度的移动数据安全保护模型,根据标签识别用户权限和数据保密级别,对移动数据的移动应用进行操作控制,以实现移动数据细粒度的保密安全防护。模型包含标签控制管理模块和移动数据管理模块。标签控制管理模块主要对数据标签 (data-tag) 和应用标签 (App-tag) 进行管理,有效记录数据的保密级别和应用操作的权限及其生成数据的保密级别,进而在移动数据的创建、存储和传输环境中进行安全保护,确保数据的存储安全、操作安全和传输安全,包括标签生成器、标签存储管理和标签传输控制 3 个子模块;移动数据管理模块主要根据移动数据标签和移动应用标签来保护数据的安全,进行细粒度的管理,是数据处理过程的安全隔离控制、数据传输过程的安全控制和数据存储中的安全隔离控制的具体功能实现部分。系统模型如图 1 所示。

系统将标签(数据标签和应用标签)作为基础的安全控制的信息载体,对移动数据进行细粒度的安全保护。本模型针对每个移动应用和移动数据创建标签。标签分为移动数据标签和移动应用标签,其中移动数据标签仅在移动智能终端上保存,移动应用标签需在移动接入网关/服务器和移动智能终端上同时保存。

(1) 数据标签保密级别、数据存放地址

保密级别的值为大于或等于 0 的整数,不同级别的数字用于指明该移动数据是否需加/解密,确保安全传输;数据存放地址是该数据在移动智能终端上的保存路径。

(2) 移动应用标签应用 ID、操作权限、生成数据的保密级别

应用 ID 是该应用进行特定操作的唯一标识,由应用

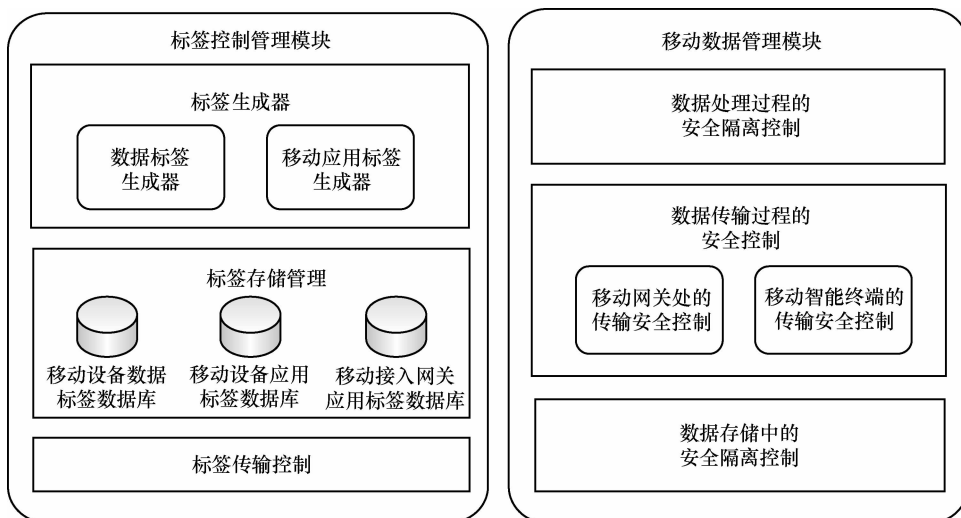


图 1 一种细粒度的移动数据安全保护系统模型

的唯一标识和操作的唯一标识组成。操作权限是该应用进行此操作有权处理的数据保密级别（当应用 a 对数据 b 进行操作 c 时，若应用 a 进行操作 c 的应用标签的操作权限大于或等于数据 b 的保密级别，则可对数据 b 进行操作）。此外，该标签在移动接入网关/服务器处保存时，按照用户保存（同一用户智能设备上的所有应用对应的应用标签放入同一张表中）。

管理员在移动接入网关/服务器端赋值，指定某用户使用应用 X 进行操作 Z 的移动应用标签的操作权限。

模型的系统流程主要包括数据从移动网关进入移动

智能终端的处理流程、应用从移动网关进入移动智能终端的处理流程和应用 X 企图对移动数据 Y 进行操作时的处理流程。在这些流程中，系统能在办公环境中监控每个应用对数据的操作活动，对单个数据进行用户指定保密级别的安全守护，有力保证了移动数据的安全，具体如图 2 所示。

3.1 数据从移动网关进入移动智能终端的处理流程

当移动数据从内网或移动接入网关准备推送到移动智能终端时（序号 1），首先通知标签生成器生成数据标签（序号 2），标签生成器通知标签传输控制功能模块（序号 3）对移动数据标签加密，随后根据数据的保密级别与数据一

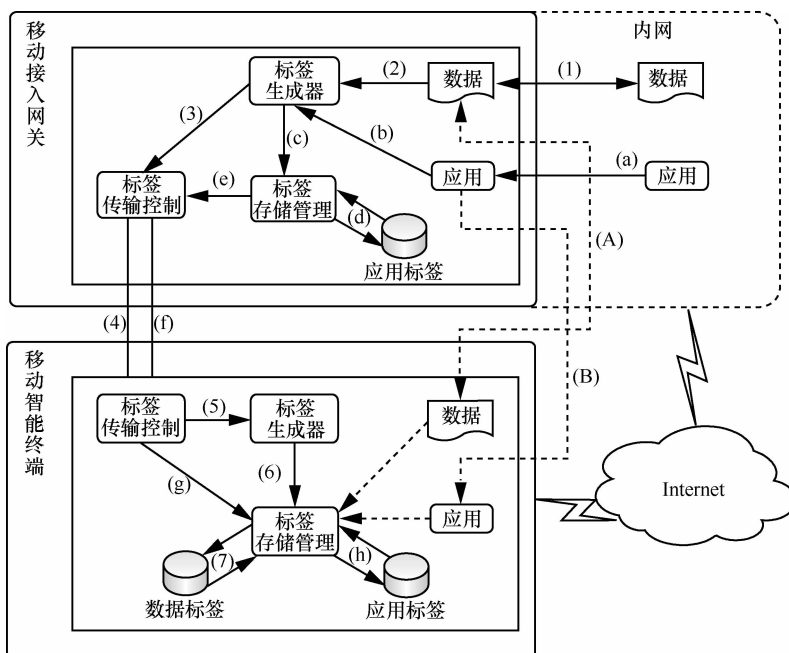


图 2 一种细粒度的移动数据安全保护模型系统流程



起加密并以合适的方式发送到移动智能终端(序号4、序号A)。移动智能终端接收到加密的数据标签和按照保密级别加密的数据后,将数据解密后再进行加密存储,并且通知移动智能终端处的标签生成器(序号5),标签生成器重新生成该数据对应的数据标签,并将此数据标签发送到标签存储管理功能(序号6),标签存储管理功能将之保存至移动数据标签数据库(序号7)。

3.2 应用从移动网关进入移动智能终端的处理流程

当移动应用从内网或移动接入网关准备推送到移动智能终端时(序号a),首先通知标签生成器生成移动应用标签(序号b),标签生成器生成该应用所有相关操作所对应的移动应用标签,并将这些移动应用标签发送到标签存储管理模块(序号c),标签存储管理模块将它们保存至移动应用标签数据库(序号d),然后通知标签传输控制功能模块(序号e)将这些移动应用标签加密,然后与应用一起,以合适的方式发送到移动智能终端(序号f、序号B)。移动智能终端接收到加密的移动应用标签后,解密并将它们发送到标签存储管理模块(序号g),标签存储管理模块将之保存至移动应用标签数据库(序号h)。

3.3 应用X企图对移动数据Y进行操作时的处理流程

数据存储中的安全隔离控制功能对移动终端上存储的数据进行隔离。当应用X企图对移动数据Y进行操作Z时,立即通知数据处理过程的安全隔离控制模块。若收到数据传送消息通知,则立即通知数据传输过程的安全控制模块。安全控制模块判断应用X进行操作Z的权限,以确认是否有权对移动数据Y进行操作。若有权处理,则解密数据后交由应用X进行操作Z,否则拒绝操作。

若应用X有权对移动数据Y进行操作Z,则标签生成器对处理后修改或生成的数据重新生成对应的数据标签,并通过标签存储功能对数据标签数据库进行更新。

4 模型子系统及算法

4.1 标签控制管理子模块

4.1.1 标签生成器

标签生成器包括数据标签生成器和移动应用标签生成器。数据标签生成器在移动智能终端和移动接入网关/服务器处,根据需要对移动数据创建或修改(移动接入网关/服务器处不修改)数据标签,并在移动智能终端维护数据标签数据库,此模块主要的算法为移动数据标签生成算法。移动应用标签生成器负责生成移动应用的标签,在移

动接入网关/服务器处对移动应用生成标签(存入对应使用者的数据表),并推送到相应使用者的移动智能终端(存入移动智能终端的移动应用标签数据库),此模块主要的算法为移动应用标签生成算法。

4.1.1.1 移动应用标签生成算法

移动应用标签生成器仅工作在移动接入网关/服务器处,当有新的应用需要推送到某一用户的移动智能终端或某一用户使用该应用的权限发生变化时,生成相应的移动应用标签,按用户存入移动接入网关/服务器处的移动应用标签数据库,将其推送至相应的移动智能终端,同时更新移动接入网关/服务器处和用户所使用的移动智能终端处的移动应用标签数据库。需注意的是,在移动智能终端侧不对标签进行任何修改。移动应用标签生成算法确保移动设备上的应用同步最新的权限操作信息,能细粒度地监控用户对移动数据的操作。具体流程如图3所示。

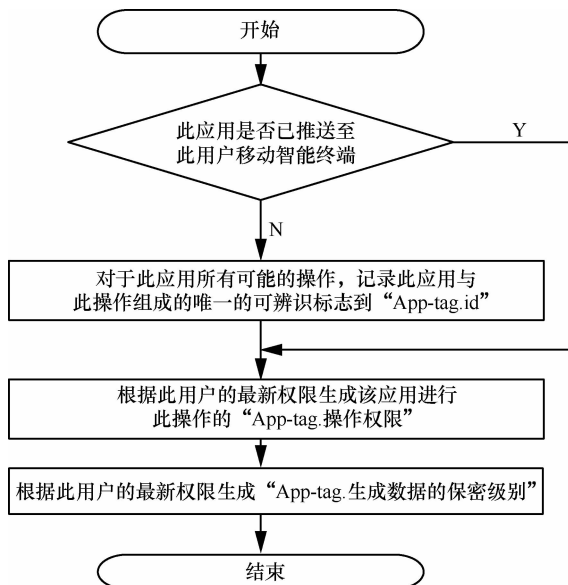


图3 移动应用标签生成算法具体流程

4.1.1.2 移动数据标签生成算法

移动数据标签生成器工作在移动接入网关/服务器处和移动智能终端。在移动接入网关/服务器处根据数据的机密程度等信息,针对每个移动数据标签的保密级别进行初始赋值操作,具体算法流程如图4所示。

赋值“data-tag.保密级别”:“data-tag.保密级别”等于对该数据进行处理的应用操作对应的“App-tag.生成数据保密级别”与该数据的“data-tag.保密级别”这两个数值中的较大者。

赋值“tag.用户权限”:“data-tag.保密级别”等于对数据

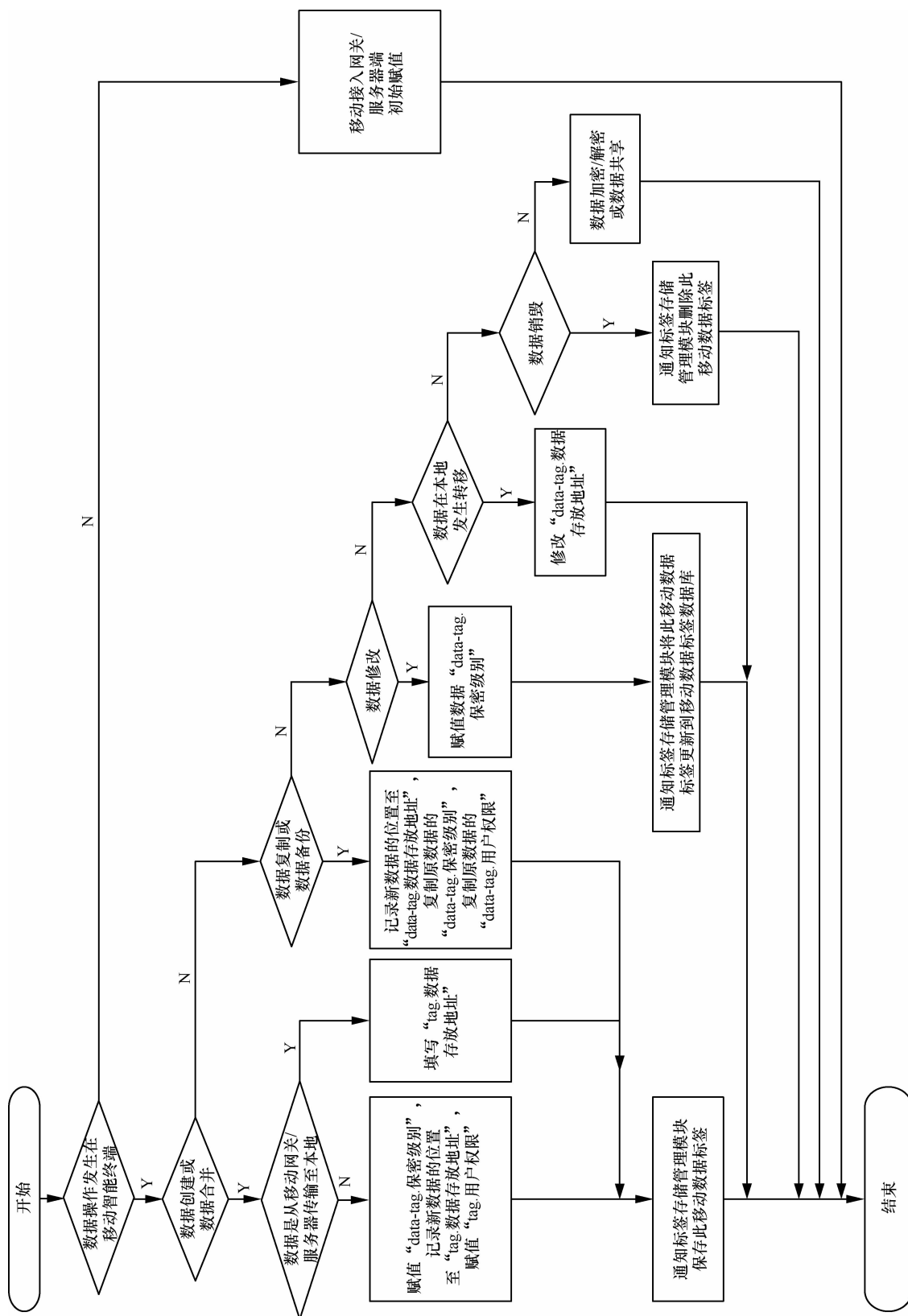


图 4 移动数据标签生成算法具体流程



进行处理的应用操作对应的“App-tag.生成数据保密级别”与被处理数据的“data-tag.保密级别”这两个数值中的较大者。

移动接入网关/服务器端初始赋值:由管理员指定该数据的保密级别,“用户权限”项留空。

4.1.2 标签存储管理功能和标签传输控制功能

标签存储管理模块负责移动数据标签和移动应用标签的存储管理以及移动终端上的移动数据标签数据库、移动终端处的移动应用标签数据库和移动接入网关/服务器处的移动应用标签数据库这3个数据库的运行维护。根据标签生成器生成、修改、删除标签的情况,标签存储管理功能对相应的数据库分别进行存储、更新和删除工作。

标签从移动接入网关/服务器向移动智能终端做单向的传输;在移动接入网关/服务器处加密以安全的方式传输至移动智能终端;在移动智能模块终端处对标签进行解密,传递给标签生成器。

4.2 移动数据管理模块

移动数据管理模块根据标签识别用户权限和数据保密级别,对移动数据进行处理的应用操作进行控制,以实现移动数据细粒度的保密安全防护。移动数据管理模块分为数据处理过程的安全隔离控制、数据传输过程的安全控制和数据存储的安全隔离控制。移动数据管理模块最关键的是权限确认算法。当该数据的情况发生变化(生成新数据、加/解密、共享、整体复制、多个数据合并、修改、备份、转移、销毁)时,权限确认算法判断用户是否有权对某一数据进行此操作。

权限确认算法具体介绍如下。

输入:移动应用标签、移动数据标签。

输出:Y或N。

具体流程如下。

- 查看“App-tag.操作权限”,读取用户使用该应用进行此操作的数据保密级别。
- 查看所有的“data-tag.保密级别”,读取最高的保密级别。
- 比较“App-tag.操作权限”与最高“data-tag.保密级别”的大小;若为大于或等于关系,则返回Y;若为小于关系,则返回N。

4.2.1 数据处理过程的安全隔离控制

数据处理过程的安全隔离控制主要是对移动智能终端上的指定数据情况进行监控,当有应用对该移动数据进

行操作时,利用权限确认算法判断用户是否有权操作,如果允许操作则调用移动数据标签生成算法处理。模型禁止用户复制数据内容中的一部分。具体流程如图5所示。

4.2.2 数据传输过程和数据存储过程的安全隔离控制

数据传输过程的安全控制包括对数据从移动接入网关/服务器传输到移动智能终端的过程和数据从移动智能终端传输到外部的过程进行数据安全控制(如图2所示)。当移动数据的位置发生改变或某一应用对其进行操作时,针对特定用户进行细粒度的权限判断,选择合适的加密和传输方式进行,在数据进入移动设备的情况下更新数据标签。

5 仿真实验及分析

5.1 实验设计与实验环境

5.1.1 实验设计

细粒度的移动数据安全保护模型的功能模块主要分为移动设备对数据安全的细粒度管理功能、移动接入网关/服务器与移动设备的标志加密通信功能和移动数据传输的通信功能。由于后两种功能比较普通,并且学术上已进行了深入的研究,商业上也相当成熟,所以重点验证移动设备上的系统对数据安全的细粒度管理能力。

移动智能平台主要有Android、iOS、Windows Phone和黑莓等。其中,Android的市场份额最大,也较为灵活;iOS的封闭性强、安全保障比其他平台稍好;剩下的其他平台的份额远不如前两大平台。实验选择在Android平台上完成,需要根据Android平台的特点对模型的算法进行一些调整:数据文件加密保存在外部存储,并采用双重密钥以增强安全性,密钥由监控程序保管;给每个应用程序和需要保护的数据文件分发标签,标签里存放应用程序或数据文件的保密级别,通过权限校验算法,细化应用程序对数据文件的操作权限;为了防止其他第三方应用伪装,对每个申请访问数据的应用程序进行签名验证以确定其身份;最后,通过签名验证和权限校验的应用程序可以获得所申请访问的数据文件的密钥,以进行数据访问。

在Android平台上实现了对指定路径下的数据文件的保护,根据Android平台对数据的操作原理,对数据标签增加一项“加密密钥”以记录移动数据解密密钥,进而控制对加密移动数据的任何操作,起到安全保护的作用。在监控程序中开启一个业务常驻后台,用FileObserver监视指定路径下文件的创建和删除,以增加/删除移动数据标签的项。一旦有新文件创建,则产生一个新的随机的移动数据

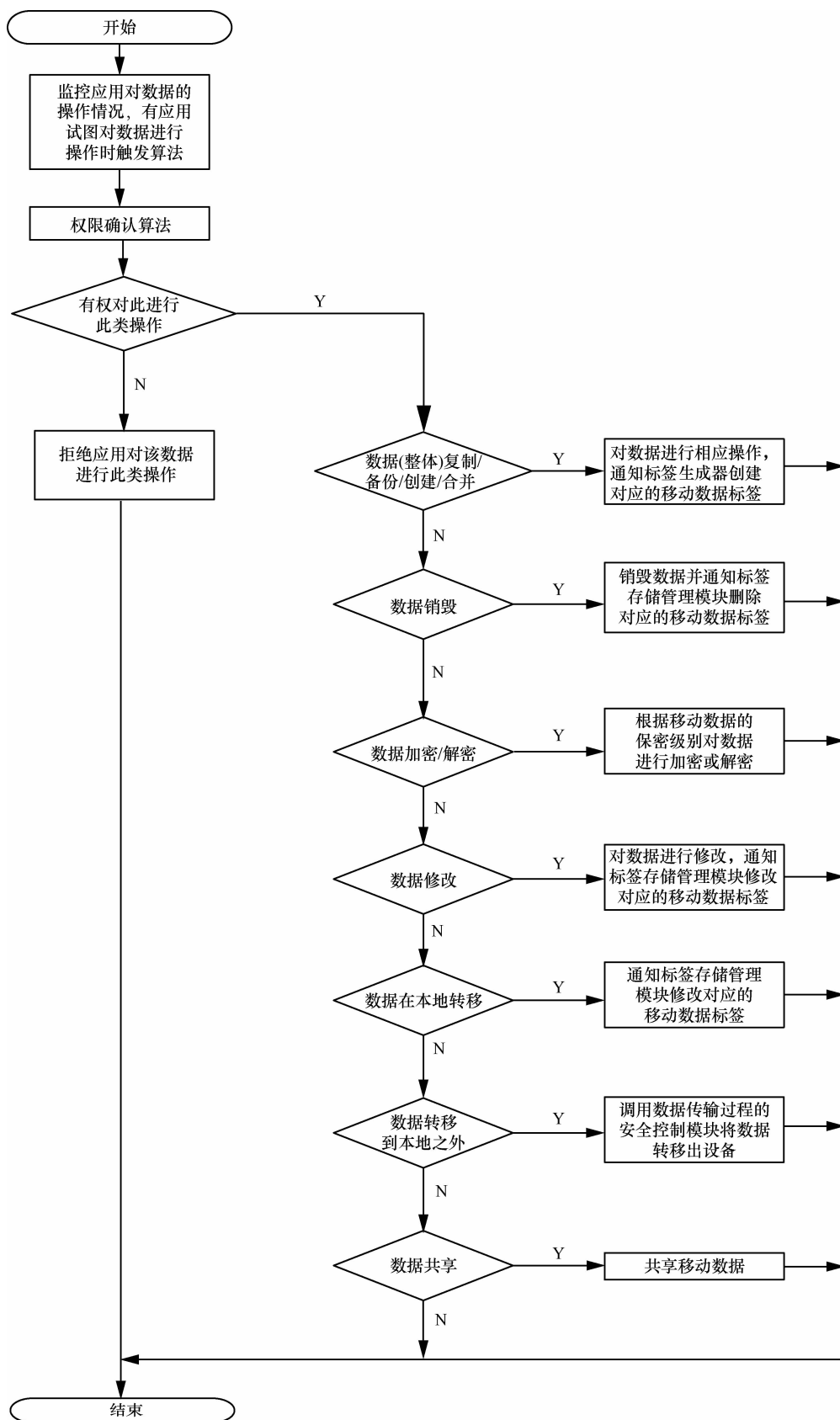
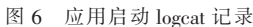


图 5 数据处理过程的安全隔离控制流程

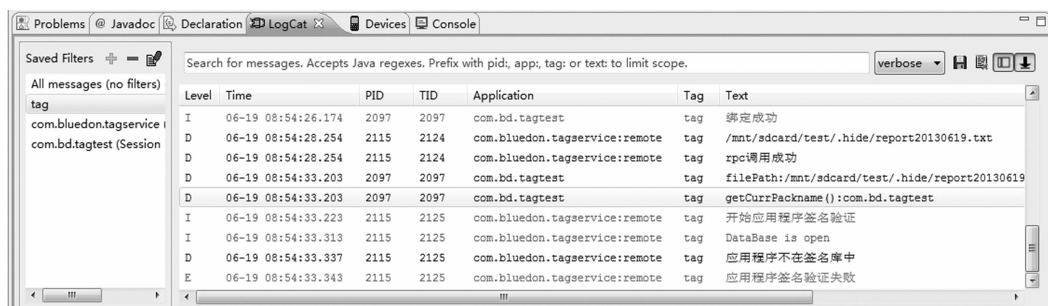


无线路由器。计算机与 2 台智能移动设备通过路由器连接组成一个移动局域网。

使用工具 Eclipse Java EE IDE for Web Developers 完成

首先,使用应用 TagTest 访问 report20130619 文件。此智能终端的使用用户有权使用应用 TagTest 对文件 report20130619 进行读操作。结果显示如图 7 所示,应用





(a)



(b)

图 8 未授权应用无权对文件 report20130619 进行相应操作

返回密钥（真实场景中直接将利用该密钥对文件进行操作）。

然后，使用另一未授权应用对文件 report20130619 进行读操作，系统拒绝操作，同时若用工具强行打开该文件，所显示的也为乱码。结果如图 8 所示。

由以上结果可见，本模型在 Android 环境下能根据应用的操作权限进行判断，以实现对移动数据细粒度的保护。

6 结束语

随着移动办公的兴起，移动计算的安全问题备受关注。BYOD 的安全问题主要集中在用户访问、追踪移动设备、保护移动数据等方面，其中最重要的就是企业移动数据的安全保护。但是国内外相关的学术研究均未把重点放在对移动数据进行单独的、细粒度的保护上，同时大多数国内外的 MDM 或 MAM 产品也都没有基于用户个体对企业数据进行细粒度的访问修改等操作的控制管理功能。

本文提出了一种细粒度的移动数据安全保护模型，与传统的无区分保护统一移动数据相比，该模型使用了移动数据标签和移动应用标签，并根据不同用户执行不同操作的权限控制管理，能针对每个单独用户对指定的每个数据的操作权限进行细粒度的控制，如允许某用户仅能使用移动应用 A 对数据 B 进行读取操作，但不能进行修改或共享等其他操作。通过在 Android 移动终端上进行实验，验证了模型在移动智能终端对移动数据控制的有效性和安全性。目前用户对应的移动应用操作权限、生成数据机密级别和移动数据机密级别参数仍需由管理员在移动接入网关/服务器处单独赋值，有一定的局限性，通过在移动接入网关/服务器根据已有策略自动对这 3 种参数赋值进行改进，是下一步研究工作的重点。

参考文献

- 1 杨卫军, 秦海权. 智能移动平台安全威胁分析. 警察技术, 2013(1):45~47
- 2 陆宏亮. 移动云环境下基于终端上下文信息的数据保护研究. 国防科学技术大学硕士学位论文, 1998

(下转第 30 页)



特点,降低了代码二次开发的难度;与 Zabbix 等第三方监控软件相比,由于采用了模块化设计,体现了高扩展性、二次开发简单的优点。系统所采用的采集模块未针对任何特定的云计算平台架构,经测试表明,系统具有网络适应性强、安全性及可靠性高的特点。

参考文献

- 1 沈青,董波,肖德宝. 基于服务器集群的云监控系统设计与实现. 计算机工程与科学, 2012,34(10):73~77
- 2 Mikyung K, Dong-In K, Stephen P. *et al.* Design and development of a run-time monitor for multi-core architectures in cloud computing. *Sensors*, 2011, 11(4):3595~3610
- 3 Shao J, Wei H, Wang Q X, *et al.* A runtime model based monitoring approach for cloud. *Proceedings of IEEE 3rd International Conference on Cloud Computing, Florida*, 2010: 313~320
- 4 赵海川,吴江,王鹏等. 面向电信业务的基础设施云监控系统. 西北大学学报(自然科学版), 2012, 42(5):729~734
- 5 Ruan L, Peng J B, Xiao L M, *et al.* Distributed virtual machine monitor for distributed cloud computing nodes integration. *Lecture Notes in Computer Science*, 2013(7861): 23~31
- 6 DeChaves S A, Uriarte R B, Westphall C B. Toward an architecture for monitoring private clouds. *Communications Magazine, IEEE*, 2011 (49):103~137
- 7 Eventlet. <http://eventlet.net/>, 2012
- 8 Rick C. *Essential SQL Alchemy*. O'Reilly Media Inc, 2008
- 9 Stacklab:documentation:OpenStack-hacker. <http://wiki.stacklab.org/doku.php?id=stacklab:documentation:OpenStack-hacker>, 2013
- 10 Thamarai S, Somasundaram, Kannan G. Cloud monitoring and discovery service (CMDS) for IaaS resources. *Proceedings of the*

Third International Conference on Advanced, India, 2011:340~345

- 11 董波,沈青,肖德宝. 云计算集群服务器系统监控方法的研究. 计算机工程与科学, 2010,34(10):69~72
- 12 Get CPU usage with get system times. <http://www.codeproject.com/Articles/9113/Get-CPU-Usage-with-GetSystemTimes>, 2011
- 13 Paste Deployment. <http://pythonpaste.org/deploy/>, 2012
- 14 Zhao W B, Melliar-Smith P M, Moser L E. Fault tolerance middleware for cloud computing. *Proceedings of IEEE the 3rd International Conference on Cloud Computing, Florida*, 2010:67~74
- 15 Curl. <http://baike.baidu.com/view/1326315.htm>, 2011

[作者简介]



李磊,男,华南理工大学工程师,主要研究方向为云计算。

金连文,男,华南理工大学教授、博士生导师,主要研究方向为移动互联网、云计算、图像处理、机器学习。

黎德生,男,华南理工大学硕士研究生,主要研究方向为云计算、移动互联网终端技术、图像处理。

唐万万,男,香港云龙科技有限公司工程师,主要研究方向为云计算技术、网络集群化服务、公有云服务技术。

(收稿日期:2013-07-30)

(上接第 23 页)

- 3 石莎. 移动互联网网络安全认证及安全应用中若干关键技术研究. 北京邮电大学硕士学位论文, 2012
- 4 杜久升,陈宜金. 计算机工程与应用. 移动数据传输安全性研究, 2011, 47(34):11~14
- 5 Butter T, Aleksy M. MixVM-An approach to service isolation and data protection in mobile context-sensitive applications. *Proceedings of 2009 International Conference on Availability, Reliability and Security, ARES 09, Fribourg, Switzerland*, 2009:322~328
- 6 Nkosi M, Mekuria F. Improving the capacity, reliability & life of mobile devices with cloud computing. *Proceedings of IST-Africa Conference, South Africa*, 2011:1~9
- 7 Wonjoo P, Sun J K, Kee S. Framework for security management of mobile devices. *Proceedings of Communications and Information Technology, ISCIT 2009, Korea*, 2009:1219~1222
- 8 Wu J J, Zhou J, Ma J, *et al.* An active data leakage prevention

model for insider threat. *Intelligence Information Processing and Trusted Computing (IPTC)*, 2011(2):39~42

[作者简介]



杨育斌,男,蓝盾信息安全技术股份有限公司高级工程师、副总经理,主要研究方向为云计算。

程丽明,女,蓝盾信息安全技术股份有限公司高级工程师、高级研究员,主要研究方向为云计算。

(收稿日期:2013-07-01)