基于 Web 的手机信息管理平台的设计与实现 *

祝衍军,李建新,柯 钢,杨怀德
(东莞职业技术学院 计算机工程系,广东 东莞 523808)

摘 要:提出了一种通过 Web 方式来管理个人手机信息的管理平台解决方案,该平台采用了一种融合 MD5 和对称加密算法的混合加密技术实现单方加密多方解密的安全应用模型,保证了手机备份信息的安全存放。用户通过该平台不但可以轻松地实现个人手机信息的备份、恢复和整合,还可以随时随地获取自己备份的信息。

关键词:个人手机信息管理;手机数据安全备份;移动终端;信息安全;数据交换
中图分类号:TP311.1 **文献标识码**:A **文章编号**:1674-7720(2013)13-0013-04

Design and implement of mobile information management platform based on Web

Zhu Yanjun, Li Jianxin, Ke Gang, Yang Huaide
(Department of Computer Engineering, Dongguan Polytechnic, Dongguan 523808, China)

Abstract: The paper presents a solution of managing personal mobile phone information based on Internet, which solve the safety storage of personal mobile phone information by using a security model of one-encryption and multi-decryption, the model use a hybrid encryption technology which is composed of MD5 and symmetric encryption algorithm. On the platform users not only can backup, recovery and integrated their personal mobile phone information, but also can acquire their own backup information at any time and in any place.

Key words: personal mobile information management; mobile data security backup; mobile terminal; information security; data exchange

随着技术的发展和智能手机的推广,越来越多的人使用手机处理各种各样的事情,如用手机拍摄图片或视频记录生活的点滴、编辑私人的信息以便随时查看(如电话薄、工作记录、日志等)和处理办公邮件等。但如果使用的手机发生故障或者丢失,则损失的往往不仅是一部手机,更为重要的是将丢失手机中所存储的各种信息,因此如何安全地保存这些个人手机信息已成为人们迫切需要解决的问题。另外随着手机价格的下降,很多人拥有多部手机,且这些手机终端可能也不一样,如何更好地统一维护自己的手机个人信息以及实现不同手机终端之间的数据交换也成为人们希望解决的一个问题。

随着国内 3G 技术的普及推广,使得手机与互联网上的数据交换变得越来越容易,因此本文根据当前存在的问题提出了一种基于 Web 的个人手机信息管理平台,用户可以在平台上实现手机个人信息的统一管理,不但可以轻松实现手机信息的安全备份与恢复,还可以将其作为信息整合的工具来实现不同手机终端之间的数据交换。

* 基金项目:东莞职业技术学院院级科研基金项目(2012c13)

1 总体设计

1.1 总体架构设计

当前市场上存在各种各样的手机终端,这些终端有基于 Andriod 操作系统的,也有基于 iOS 或者其他操作系统的,由于不同终端获取手机信息的方式和接口不尽相同,因此采用了 B/S 与 C/S 混合架构的整体方案来实现各种手机终端的信息备份与恢复,针对不同的手机终端分别写一个对应的手机终端程序来读取和恢复手机信息,然后通过调用 Web 服务器上的统一接口实现信息的安全存储和备份,另外用户也可以通过浏览器管理自己的备份信息,可以对信息进行整合、导出和查看等

操作，总体架构如图 1 所示。

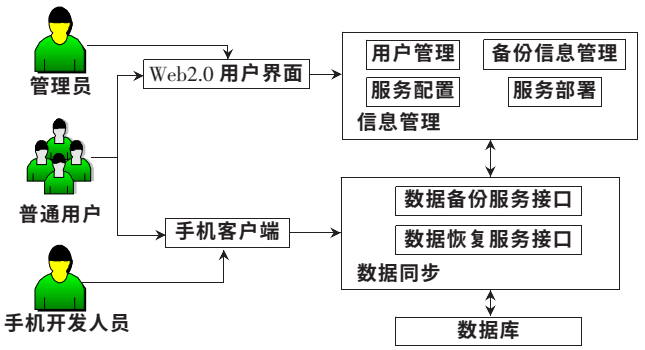


图 1 基于 Web 的个人手机信息管理平台总体架构

平台用户总共分为三类：系统管理员、普通用户和手机开发人员，系统管理员通过浏览器管理用户信息和数据接口配置信息；普通用户通过浏览器管理自己的手机备份信息，包括查看、整合和导出备份信息等操作，通过手机客户端轻松实现手机信息的远程备份与恢复；手机开发人员则根据信息管理平台的开发手册和开发 API 定制开发对应的手机备份与恢复功能，平台以 Web Service 接口的方式对外提供服务，具体分为数据备份和数据恢复两类接口。用户备份的个人手机信息中，除电子文档信息外，其他信息都保存在数据库中，而电子文档则将配置信息保存在数据库中，真实信息保存在文件系统中。

1.2 功能架构设计

用户通过信息管理平台来统一管理个人手机信息，不但可以实现手机信息的安全备份与恢复，还可以将其作为信息整合的工具来实现不同手机终端之间的数据交换。整个功能架构总体上可分为用户管理、备份信息管理、开放接口管理、系统运营分析 4 个大功能，具体如图 2 所示。

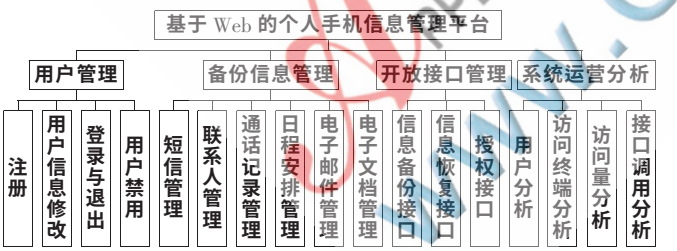


图 2 基于 Web 的个人手机信息管理平台功能架构

用户管理负责平台用户信息的管理，如用户名、密码、密钥等重要信息的管理，具有用户注册、用户信息修改、登录与退出和用户禁用等功能。

备份信息管理为用户通过浏览器统一管理备份信息提供各种操作功能，用户在该平台上可以对自己的备份信息进行查找、查看、删除、合并和导出等功能，具体包括短信管理、联系人管理、日期安排管理、电子邮件管理和电子文档管理等功能。

开放接口管理借鉴各种云平台的“开放平台”和“OpenAPI”思想[1]，为各种终端提供统一的备份和恢复信息接口，手机客户端只需要按照格式要求调用相应的接口就可以通过互联网实现手机信息的安全备份与恢复功能，所有接口采用开放的形式供手机终端开发人员随意调用，通过这种方式来丰富平台支撑的手机客户端和个性化应用，具体功能包括接口发布、接口鉴权、接口描述、调用队列管理和各种调用接口等功能。

系统运营分析则通过各种报表的方式分析和监控整个平台的运营情况，具体包括系统用户分析、用户手机终端分析、访问量分析、接口调用分析等功能。

2 关键技术实现

2.1 平台与手机客户端间的数据交换

个人信息管理平台为手机客户端提供 HTTP 实时交换接口，接口采用 RESTful Web Service[2]的方式对外提供，数据组织形式采用 JSON（Java Script Object Notation）[3]数据格式。REST 是一种充分利用 Web 特性的分布式软件架构风格，它可以降低系统开发的复杂性，为系统提供可伸缩性。RESTful Web Service 是遵循 REST 设计原则的面向资源的轻量级 Web 服务。它利用统一资源标识符（URI）定位和识别资源，并通过 HTTP 协议中定义的方法（PUT，GET，POST，DELETE）对资源进行 CRUD 操作[4-5]。数据交换采用的 JSON 作为一种轻量级的数据传输格式，可以在多种语言之间进行数据交换。JSON 易于阅读和编码，且它是 JavaScript 规范的子集，能被支持 JavaScript 的浏览器所解析，相比 XML，减少了解析时带来的性能和兼容性问题[6]。

采用这种数据交换方式降低了服务器和手机客户端的编程难度，服务器 Spirng 的 MVC 架构则只需要在视图层对应的方法上加上 @Response Body 注解就可以将对应的数据以对象的形式打包成 JSON 格式[7]，手机客户端也只需要通过 HttpClient 对象访问服务器的接口即可获取 JSON 数据格式的备份信息来实现信息的本地恢复，或者将需要备份的信息封装成 JSON 格式再调用服务器的接口来实现信息的远程备份。

2.2 单方加密多方解密的安全应用模型

手机信息作为个人的隐私，不希望被任何的第三个人查看或者浏览，因此如何安全存放备份信息则直接关系到用户是否会使用该平台和软件。手机信息的安全备份包括两个方面：一是数据的安全传输，备份信息在传输的过程中如何保证不被窃取和黑客窃取到信息后防止其查看真正的信息内容；二是备份信息的安全存储，信息一般都存储在数据库中，这就需要防止系统管理员利用职务的便利查看每个人的备份信息内容。由于信息管理平台和手机客户端都需要显示用户备份信息明文，所以本文采用了一种融合 MD5[8]和对称加密算法的混合加密技术来实现单方加密多方解密的安全应用模型[9-10]，从而实现手机信息的安全备份。安全应用模型由手机客

户端一方对备份信息进行加密，再由个人信息管理平台和手机客户端两方对备份信息进行解密和展示明文信息，加密密钥由用户在信息管理平台上设置的登录密码和信息加密密钥组成，其中登录密码以 MD5 存储在数据库中，信息加密密钥则以明文存储在数据库中。由于备份信息是由手机客户端根据每个用户设置的系统登录密码和加密密钥组合而成的密钥进行加密，其中系统登录密码存储在手机客户端，加密密钥存储在服务器端，以及信息发送过程不将加密密钥发送给服务器，因此有效地防止了黑客截获到密文信息然后对其进行解密，也防止了系统管理员通过职位的便利偷窥手机备份信息。

手机客户端在服务器进行备份时，需要先将手机客户端事先保存好的登录用户名和密码发送给管理平台进行验证，其中该用户名和密码与用户通过浏览器登录时的用户名密码保持一致，且密码是以明文方式存放在手机客户端中，管理平台通过验证后返回备份信息加密密钥，手机客户端然后根据用户操作读取对应的手机信息并根据服务器返回的加密密钥和手机客户端保存的登录密码对其进行加密，再将加密后的密文发给管理服务器，详细的手机客户端备份信息时序图如图 3 所示。

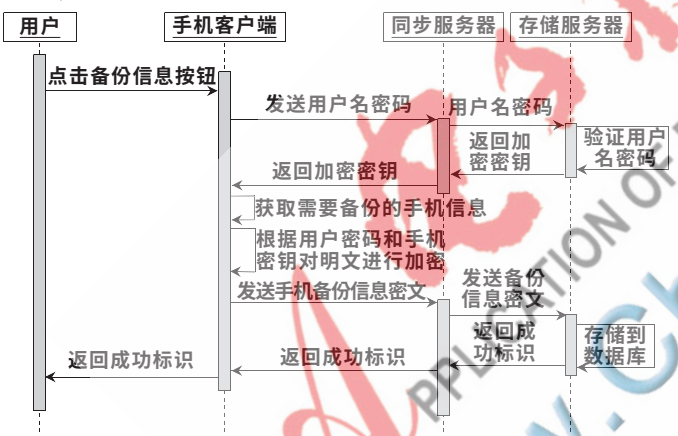


图 3 个人手机信息备份时序图

用户登录到个人信息管理平台对备份信息进行管理时需要向用户展示备份信息明文，由于备份信息都是以用户登录密码明文和加密密钥明文加密后的密文方式存在数据库中，而管理平台的登录密码也是经过 MD5 算法加密后的密文方式存放在数据库中，因此管理平台在用户登录成功后先将用户输入的明文密码保存到 session 中，在读取数据库里面的备份信息后再结合以明文形式存放的加密密钥对备份信息密文进行解密并展示给用户，详细的管理平台展现明文信息时序图如图 4 所示。

2.3 数据结构设计

以用户为中心，针对短信、通话记录和电子文档备份信息分别对应一张相应的存储表，由于一个联系人拥有多个电话号码，因此针对联系人备份信息则对应一个

图 4 管理服务器展示备份信息明文时序图

一对多的两张存储表。数据库里面存储的备份信息都是以经过加密后的密文形式进行存储，其中电子文档存储表只记录备份信息的一些基本信息，实际备份内容则存放在文件系统中，具体的数据逻辑模型如图 5 所示。

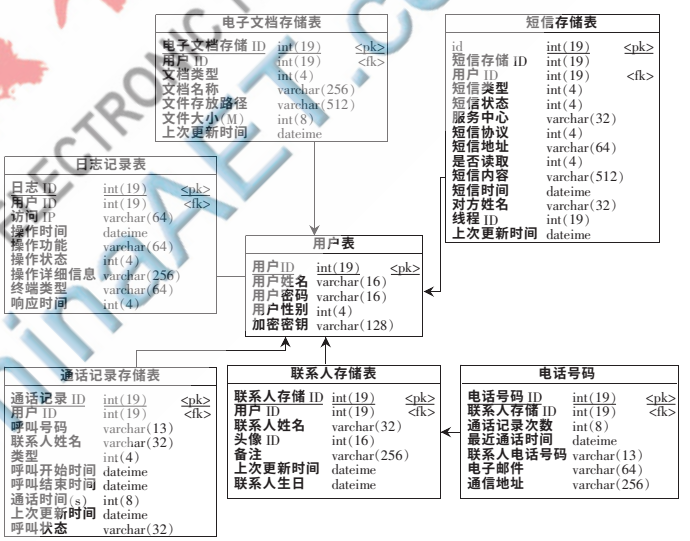
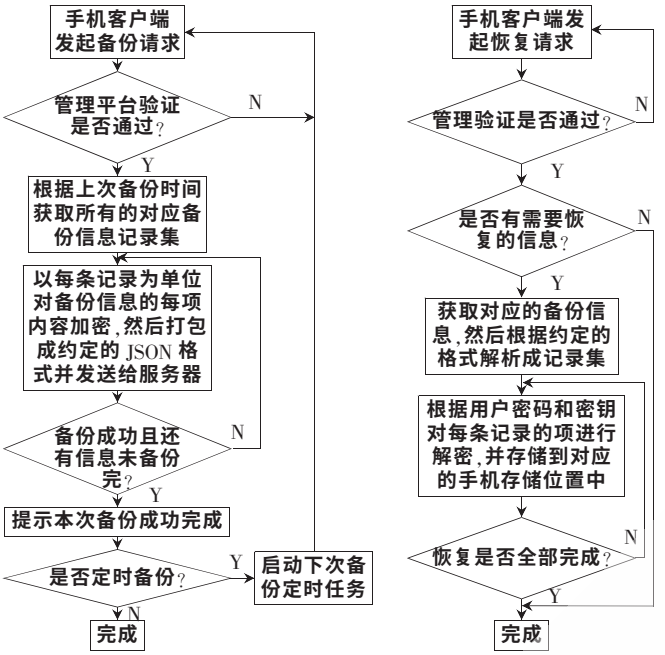


图 5 个人手机管理平台数据逻辑模型

2.4 手机客户端实现

手机客户端在手机终端层面通过调用手机操作系统的 API 接口完成手机个人信息的备份和恢复操作，具体包括短信备份与恢复、联系人备份与恢复、通话记录备份与恢复、各种电子文档备份与恢复等功能。对于各种手机终端，手机信息的备份都需要经过读取、加密和发送等几个基本流程以及手机信息的恢复需要经过发起备份请求、从管理平台接收备份信息、解密和往手机存储对应位置写入相应信息等几个基本流程，详细的手机客户端信息备份和恢复流程图如图 6 所示。

由于市场上的手机终端操作系统较多，主要有 Android、iOS、Symbian、Windows mobile 等，本文在当前流程的 Android 和 iOS 手机操作系统终端上开发了对应的



(a)手机客户端备份流程图　　(b)手机客户端恢复流程图

图6　手机客户端的信息备份与恢复流程

手机终端程序进行测试和验证,并将服务器部署到互联网上,手机客户端放到校园网上供校内师生免费使用,目前运行良好。另外管理平台也提供了一整套完整的客户端开发手册和开发API给校内师生,鼓励学生针对个人的使用习惯和手机终端开发对应的手机终端程序。

借鉴"开放平台"和"OpenAPI"思想,采用B/S与C/S混合架构的设计方案,本文设计并实现了一种基于Web的个人手机信息管理平台,普通用户通过手机客户端可以备份各种手机终端的手机信息到管理平台并在需要的时候将备份信息恢复到手机中,还可以通过浏览器浏览和整合先前备份的手机信息。平台采用了一种融合MD5和对称加密算法的混合加密技术来实现单方加密多方解密的安全应用模型,保证了手机备份信息的安全存放。平台通过给手机开发者提供开放的开发API和开发手册来丰富平台支撑的手机终端和增加手机终端的个性应用,提升了平台的活力和生命力。由于现有系统还只部署到校园网内试运行,目标客户也只针对学校内的师生,虽然目前运行稳定,但客户群一旦扩大,扩大到互联网上的客户,则还需要进一步考虑互联网上的恶意攻击和超大用户量(上千万)的使用等问题,因此下一步的研究重点就是研究超大用户量的并发处理和海量数据的存储问题。

参考文献

[1] 张京,刘甫迎.基于Android云计算消息框架(C2DM)的FoxNews_MID手持移动系统的研究[J].计算机科学,2011,38(10A):461-463.

[2] ALSHAHWAN F, MOESSNER K. Providing SOAP Web Services and RESTful Web Services from Mobile Hosts[C]. 2010 Fifth International Conference on Internet and Web Applications and Services. IEEE, 2010, 174-179.

[3] WANG G. Improving data transmission in web applications via the translation between XML and JSON[C]. Communications and Mobile Computing (CMC), 2011, 182-185.

[4] 冯新扬,沈建京.REST和RPC:两种Web服务架构风格比较分析[J].小型微型计算机系统,2010,31(7):1393-1395.

[5] 王建斌,胡小生.REST风格和基于SOAP的Web Services的比较与结合[J].计算机应用与软件,2010,27(9):297-300.

[6] 高静,段会川.JSON数据传输效率研究[J].计算机工程与设计,2011(32):2267-2270.

[7] 薛峰,梁峰,徐书勋,等.基于Spring MVC框架的Web研究与应用[J].合肥工业大学学报(自然科学版),2012,35(3):337-340.

[8] 王金柱,李元诚.MD5算法在J2EE平台下用户管理系统中的应用[J].计算机工程与设计,2008,29(18):4728-4730,4761.

[9] 庞辽军,李慧贤.一个单方加密—多方解密的公钥加密方案[J].计算机科学,2012,35(5):1059-1065.

[10] 魏海新,张超英.一种灵活的SOAP签名加密方案[J].计算机工程,2010,36(13):151-153.

(收稿日期:2013-04-14)

作者简介:

祝衍军,男,1982年生,硕士研究生,工程师,主要研究方向:企业信息化、商业智能。

李建新,男,1984年生,硕士研究生,助教,主要研究方向:智能软计算。

柯钢,男,1983年生,硕士研究生,讲师,主要研究方向:计算机网络与信息安全技术。