

面向移动云的基于时间的增量备份方案

慈云飞¹, 史国振¹, 谢绒娜¹, 潘耀明¹, 杨凤¹, 叶思水²

(1. 北京电子科技学院信息安全系, 北京 100070;

2. 瑞庭网络技术(上海)有限公司房产技术部, 上海 200127)

摘要: 提出一种面向移动云计算的基于时间的数据安全增量备份方案, 该方案针对移动设备的重要数据信息, 将时间作为参数引入到数据加密中, 依据时间阶段对用户上传的数据进行增量备份, 既解决了对最新的敏感数据及时备份问题, 又解决了由于备份密钥丢失造成的全部密文泄露问题。

关键词: 移动云; 时间粒度; 增量备份; 数据安全; 加密

中图分类号: TP393.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00079

Time based incremental backup scheme for mobile cloud computing

CI Yun-fei¹, SHI Guo-zhen¹, XIE Rong-na¹, PAN Yao-ming¹, YANG Feng¹, YE Si-shui²

(1. School of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China;

2. Department of House Technology, Ruiting Networking Technology (Shanghai) Co., Ltd., Shanghai 200127, China)

Abstract: A time-based data secure backup mechanism for moving the cloud was presented. Time was considered as a parameter into the data encryption for the important information in mobile device and backups the users' data according to the time period. It had not only solved the issue of the latest timely backup sensitive data, but also solved the entire ciphertext leak caused by missing the backup key.

Key words: mobile cloud, time granularity, incremental backup, data security, encryption

1 引言

移动设备的智能化使越来越多的用户选择使用移动设备来满足其信息获取和使用的需求, 据CNNIC第37次《中国互联网络发展状况统计报告》显示^[1], 截至2015年12月, 中国网民规模

达6.88亿, 互联网普及率为50.3%; 手机网民规模达6.2亿, 占比提升至90.1%; 无线网络覆盖明显提升, 网民Wi-Fi使用率达到91.8%。随着计算机、网络通信技术的进步, 移动终端设备的功能已经不再局限于简单的电话和文字信息传输, 而是开始面向复杂、多样的用户需求, 出现

收稿日期: 2016-04-08; 修回日期: 2016-06-25。通信作者: 史国振, sgz1974@163.com

基金项目: 新闻出版重大科技工程基金资助项目(No.1681300000119); 国家自然科学基金资助项目(No.61170251); 教育部重点基金资助项目(No.209156); 北京市自然科学基金资助项目(No.4152048); 江苏省自然科学基金资助项目(No. BK20150787); 北京电子科技学院2016年春蕾计划基金资助项目(No.2016CL04)

Foundation Items: The Major Science and Technology Project of Press and Publication(No.1681300000119), The National Natural Science Foundation of China(No.61170251), The Key Program of Scientific and Technology Research of Ministry of Education(No.209156), The Natural Science Foundation of Beijing(No.4152048), The Natural Science Foundation of Jiangsu Province(No. BK20150787), 2016 Spring Project of Beijing Electronic Science & Technology Institute(No.2016CL04)

了多媒体数据传输、云端数据共享、移动办公等多种服务模式。移动设备研究与开发也在硬件架构、软件体系、操作系统、智能应用等多个方面取得了诸多成果。现今的移动设备无论是硬件配置、软件性能,还是用户友好性等均取得了飞跃性的进步。

移动云服务具有便捷云端数据存储、大量的开放软件服务、无所不在的强大云计算支撑、终端配置要求低、移动互联、实时在线、便捷灵活实现传统云服务在移动互联网中的扩展和应用等特点^[2]。移动云计算集成了云计算技术和移动终端设备,充分体现了云计算数据集群、聚合、共享的能力和移动终端设备快捷、方便的优点。实现了通过移动终端设备就可以在云端进行数据创建、共享和存储管理的需求。然而,移动终端设备在性能和空间等方面与现有的PC系统无法比拟,无法满足大量数据的运算和存储需求。

2 相关工作

数据备份是为数据安全提供的一种有效的方式,数据备份有多种实现形式,从不同的角度可以对备份进行不同的分类,从备份策略的角度来分类,将备份的方式分为完全备份、增量备份、差量备份^[3]。随着云计算的发展,将网络中大量不同类型的存储设备通过应用软件集合起来协同工作,共同对外提供数据存储和业务访问功能,产生云存储技术^[4]。文献[5]提出一种云环境下海量数据组织与资源共享的存储模型,该模型包括结构化、半结构化及其非结构化数据与资源的对应存储方法,能兼顾海量大小数据文件处理的分布式文件系统。文献[6]设计了一种新的基于门限属性加密的安全分布式云存储模型。该模型由加密、存储、解密3个阶段组成且均具有分布式特点,该模型能抵抗共谋攻击。移动设备的使用越来越频繁,将移动终端设备的数据备份到云端,在用户需要的时候,再由云端将数据进行下载使用,这样既保证了移动设备的空间,也满足了用户随时随地使用数据的需求。但是由于云环境下数据的管理权与所有权分析,数据脱离用户的管理后便无法保证其完整性和机密性,针对移动云计算环境下数据的安全性问题,提出了面向用户

单独验证的数据可检索性证明(POR)方法^[7]、公开可验证的数据持有证明(PDP)方法^[8,9]。

数据重加密技术通常采用特定的算法,将现有密文进行再次加密处理,使生成的密文可被另一组公私钥对解密,主要用于数据的共享和分发中,如电子邮件安全转发^[10]、垃圾邮件的过滤^[11]、分布式文件系统管理^[12]、知识产权保护^[13]等许多领域。但是在云端数据备份中,可通过数据重加密方案,有效地利用云服务器的运算能力对数据进行分类管理,同时保证用户数据的安全性。

目前,微信、百度等移动应用都推荐用户进行通信录、短信等数据的备份,但这些都是敏感数据,存储在云端会对用户隐私带来很大威胁。数据是整块进行加密,然后上传,而查看需要将数据全部下载并解密,同时数据备份的密钥往往一成不变,如果用户的密钥泄露,将会威胁全部备份数据的安全性。本文针对上述问题,设计了一种面向移动云计算的基于时间粒度的数据安全增量备份方案,用于备份的时间粒度是可以根据用户自身的情况进行设置的,用户可以根据时间粒度对备份数据进行加密和访问。

3 安全备份方案

3.1 需求应用场景分析

依据云计算及移动计算的特点,在移动云环境下,数据面临移动终端设备的运算和存储能力有限、数据流通和处理量巨大、数据种类繁多和使用环境复杂等特点。

移动云计算环境下数据的备份能够有效地解决移动终端存储受限的问题,同时满足用户对数据随时随地的访问需求。但是,云计算和移动设备的特点使移动云环境下数据的安全备份面临的如下的安全需求。

1) 数据只在移动智能终端中才可以以明文形式存在,在通信过程中和在移动云的计算过程中均需以密文的形式出现。

2) 用户对数据的备份可在任意时间分散进行处理;云服务器则需对数据进行统一和定期的管理、归类。

3) 数据的加密需避免统一的备份密钥,防止密钥泄露造成的全部数据丢失问题;用户可以根据

据需要自行设置备份相关的参数信息,满足个性化的定制需求。

4) 需具有完备的用户密钥管理与保护方案。

根据上述需求,基于移动用户使用数据的特点和上述安全分析,将时间因素引入到云端数据的备份中,可以保证数据在备份和下载查看过程中的数据安全,也保证了用户备份数据的灵活性。如备份的初始阶段,服务器依据用户的需求定义时间片的大小,然后用户可以在需要的时候进行数据的备份,若用户所处的时间阶段为 T_1 时间段,则服务器将用户上传的数据归类到该阶段,以此类推对数据进行处理。

3.2 系统模型

本文方案的系统模型如图1所示,包含移动终端设备和云服务器两大部分。其中,移动终端设备指用户所持有的智能手机、平板电脑等,可以实现对数据的备份、访问和远程管理等功能。云服务器则包含内容备份服务器、数据中心、数据加解密服务器和时间服务器。各个服务器的功能说明如下。

- 1) 内容备份服务器:用于复杂用户请求的解析、数据的接收和分发处理等工作。
- 2) 数据中心:用于存储用户最终的备份数据。
- 3) 数据加解密服务器:用于对用户上传的数据进行加解密处理和密钥管理工作。
- 4) 时间服务器:用于反馈用户备份数据所处时间段信息。

当用户进行数据备份时,首先将敏感数据进行公钥加密,上传到云端;内容备份服务器解析用户请求,同时在时间服务器获取时间,确定用户所处时间阶段,并将该阶段作为数据重加密参数连同接收到的密文传递给数据加解密服务器,加解密服务器对数据进行重加密处理后反馈给内容服务器,内容服务器将其备份到数据中心。当用户访问数据时,首先向内容备份服务器提出请求,请求中包含数据的ID、数据所处时间阶段。内容备份服务器依据用户时间阶段和数据ID为用户在数据中心进行数据查询和反馈。

3.3 基于时间的云端数据加解密算法

基于时间的云端数据加解密算法是基于椭圆曲线的双线性配对的密码体制,该算法分为6个部分,具体过程如下。

1) 系统建立

$Setup(1^k)$: 输入参数 k , 输出结果 (q, g, G_1, G_T, e) , 其中, e 为双线性映射 $e(g^a, g_1^b) = e(g, g_1)^{ab}$, 选择摘要函数 H 满足 $H = \{0, 1\}^* \rightarrow \{0, 1\}^k$, g_1 为 G_1 不同于 g 的生成元, 输出参数 $param = (q, g, G_1, G_T, e, g_1, H)$ 。

2) 通用密钥提取

$KeyGen(param) \rightarrow (sk, pk)$: 输入系统参数 $param$, 随机选择 $sk \in Z_q^*$ 及其对应的公钥 $pk = g^{sk}$ 。

3) 时间密钥提取

$TransformKey(param, sk_{t_i}, pk_{t_j}) \rightarrow Tk_{t_i \rightarrow t_j}$: 根

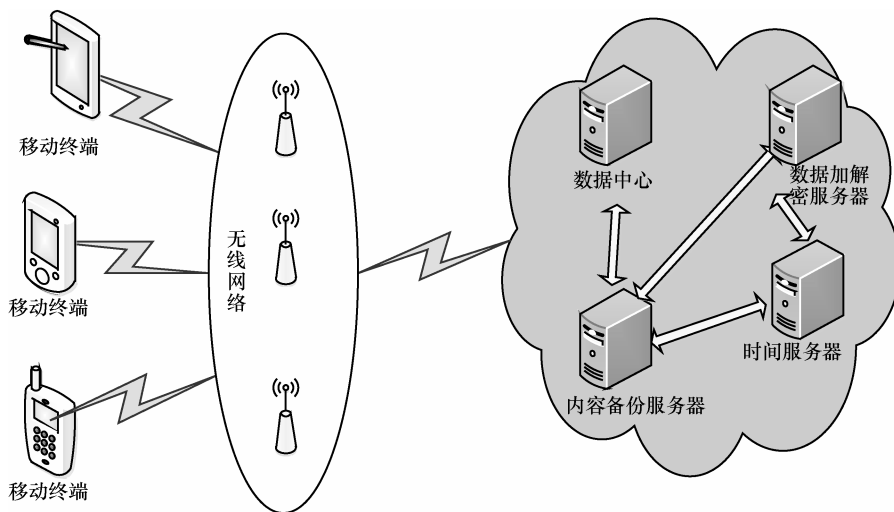


图1 安全备份方案系统模型

据 t_i 的私钥 sk_{t_i} 和 t_j 的公钥 pk_{t_j} 生成从时间粒度 t_i 到时间粒度 t_j 的转换密钥 $Tk_{t_i \rightarrow t_j} = (Tk_1, Tk_2, Tk_3)$ 。随机选择 $r_1 \in Z_q^*$ 使 $Tk_1 = g^{r_1}$, $Tk_2 = g^{r_1} pk_{t_j}^{r_1}$, $Tk_3 = H(Tk_1 \parallel H(Tk_1 \parallel Tk_2))$ 。

4) 加密

$Encrypt(param, pk, M) \rightarrow C$: 通过输入的公共参数 $param$ 、公钥 pk 以及明文 M , 加密得到密文 $C = (C_1, C_2, C_3)$ 。随机选择 $r_2 \in Z_q^*$, $C_1 = g^{r_2}$, $C_2 = Me(g_1, pk)^{r_2}$, $C_3 = H(C_1 \parallel H(C_1 \parallel C_2))$ 。

5) 代理重加密

$TransformEncrypt(param, C_i, Tk, Tk_{t_i \rightarrow t_j}) \rightarrow C_{t_j}$: 使用转换密钥对密文 C_{t_i} 进行转换, 得到 $C_{t_j} = (C_1, C_2, C_3)$ 。这里假设 $C_{t_i} = (C_1, C_2, C_3)$ 为 $C_{t_i} = (C'_1, C'_2, C'_3)$ 。首先使用 Tk_1 、 C'_1 和时间粒度 t_j 请求终端用户生成密钥 $Tk = (Tk_a, Tk_b)$, 其生成过程如下。

随机选择 $r_z \in Z_q^*$, $Tk_a = g^{r_z}$, $Tk_b = e(g_1^{r_z}, pk_{t_j})e(Tk_1, C_1)^{-sk_{t_j}}$ 。

随机选择 $r_{i \rightarrow j} \in Z_q^*$, 使 $C_1 = Tk_a$, $C_2 = Me(g_1, pk_{t_j})^{r_z} e(C'_1, Tk_2)Tk_b = Me(g_1, pk_{t_j})^{r_z}$, $C_3 = H(C_1 \parallel H(C_1 \parallel C_2))$ 。

6) 解密

$Decrypt(Tk_b, C_{t_i}, sk) \rightarrow M$: 使用时间参数和私钥 sk 将密文 C_{t_i} 解密得到明文 M 。首先验证密文的完整性 $C_3 = H(C_1 \parallel H(C_1 \parallel C_2))$, 如果等式成立, 则做如下计算。

$$C_2 e(C_1, g_1)^{-sk_{t_i}} = e(C_1, pk_{t_i})^{r_z} e(C_1, g_1)^{-sk_{t_j}} = M$$

从而得到明文 M ; 否则输出 $\perp$ 。

3.4 安全备份方案具体实施方法

安全备份方案大致可分为密钥初始化、加密上传备份、云端服务器定期进行数据整合以及用户进行数据访问等过程。

1) 密钥初始化

如图 2 所示, 包括生成公共参数、生成设定密文整合时间粒度和相应粒度的公私钥以及生成粒度间密文整合的转换密钥, 它们分别对应算法中的 $Setup$ 、 $KeyGen$ 及 $TransformKey$ 过程。 $Setup$ 主要通过接收一个安全的密钥长度来生成接下来运算需要的公共参数, $KeyGen$ 设定时间粒度并产生相应时间粒度的公私钥。

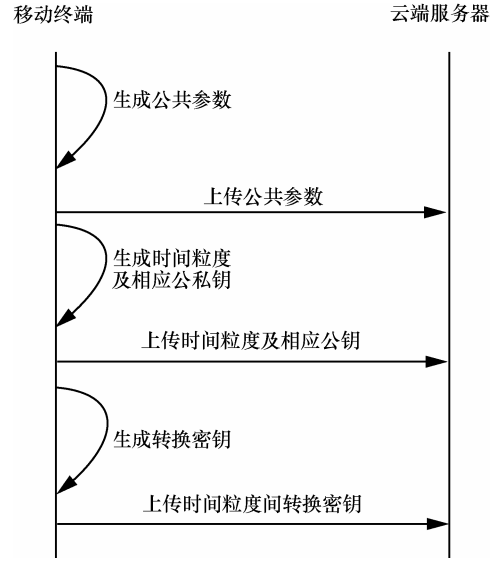


图 2 密钥初始化过程

2) 加密上传备份

如图 3 所示, 用户将需要备份的数据进行加密, 然后上传到云端服务器, 它涉及到的密码算法运算过程是 $Encrypt$ 。

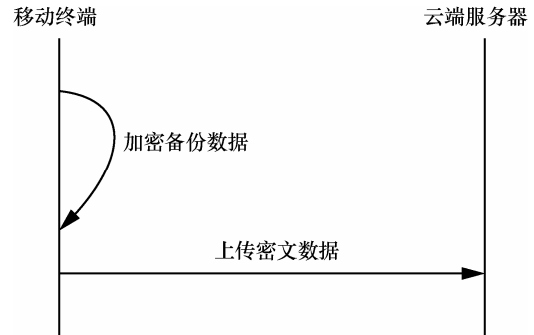


图 3 加密上传备份过程

3) 云端服务器定期进行数据整合

如图 4 所示, 云端服务器根据用户设定的时间粒度进行密文整合。它先向用户请求密文转换密钥的另一部分 Tk , 移动终端根据请求反馈转换密钥 Tk 。云端服务器根据获得的转换密钥和公共参数对密文进行转换, 它涉及的密码运算过程是 $TransformEncrypt$ 。

4) 用户进行数据访问

如图 5 所示, 用户根据需要在事先设定好的时间粒度向云端服务器请求文件。用户先向云端服务器发出数据下载请示, 然后进行数据传输, 最后使私钥对密文进行解密, 得到明文数据, 它涉及的密码运算过程是 $Decrypt$ 。

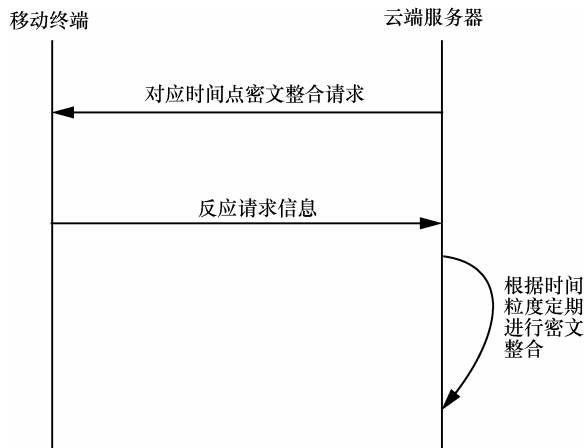


图4 云服务器定期数据整合过程

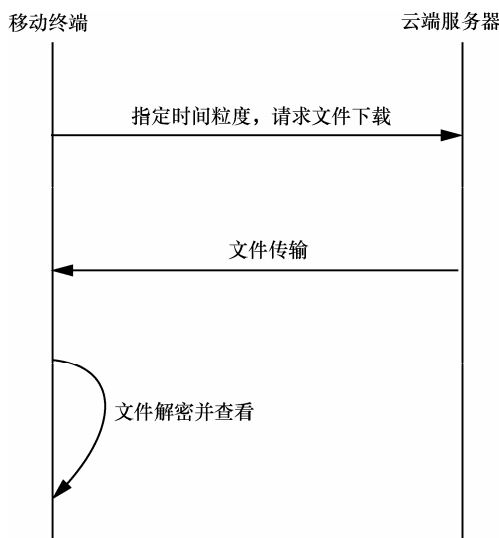


图5 用户数据下载访问过程

3.5 安全性分析

本文方案中引入摘要函数以保证密文完整性。该方案的安全性是基于 DBDH 假设的，并在标准模型 IND-PRE-CCA2 下是可证明安全的，其安全性证明方法可以参考文献[10]，证明过程如下。

该代理重公钥加密（PRE）方案的 IND-CCA 安全可以通过挑战者 C 与攻击者 A 之间的游戏来定义，具体如下。

系统建立：挑战者 C 首先运行算法 $Setup$ 来产生系统参数 $param$ ，然后将 $param$ 交给敌手 A 。

阶段 1 敌手 A 可以在本阶段自适应地进行如下的一系列查询。

1) 公钥查询(i): 敌手 A 输入索引 i ，挑战者 C 运行算法 $Setup(1^k)$ 产生公私钥对 (pk_i, sk_i) ，然后将 pk_i 交给敌手 A 。

2) 私钥查询(j): 敌手 A 输入索引 j ，挑战者 C 运行算法 $Setup(1^k)$ 来产生公私钥对 (pk_j, sk_j) ，然后将 (pk_j, sk_j) 交给敌手 A 。

3) 代理加密密钥查询(pk_j, sk_j): 挑战者 C 运行算法 $TransformKey(param, sk_{t_i}, pk_{t_j}) \rightarrow Tk_{t_i \rightarrow t_j}$ ，然后将 $Tk_{t_i \rightarrow t_j}$ 交给敌手。其中， pk_{t_i} 对应的私钥是 sk_{t_i} 。

4) 代理加密查询(pk_i, pk_j, C_{t_i}): 挑战者运行算法 $TransformEncrypt(param, C_{t_i}, Tk, Tk_{t_i \rightarrow t_j}) \rightarrow C_{t_j}$ ，其中， $Tk_{t_i \rightarrow t_j} = TransformKey(param, sk_{t_i}, pk_{t_j})$ ，然后将 C_{t_j} 交给敌手 A 。

5) 解密查询(C_{t_i}, sk_i): 挑战者运行算法 $Decrypt(Tk_b, C_{t_i}, sk) \rightarrow M$ ，从密文 C_{t_i} 中恢复出明文 M ，并将明文 M 交给敌手 A 。

挑战：一旦敌手 A 决定结束阶段 1，它输出一个欲挑战的公钥 pk^* 和 2 个比特长度相等的明文 $M_0, M_1 \in M$ 。挑战者 C 随机选取一个比特 $\delta \in \{0, 1\}$ ，将挑战密文设定为 $C^* = Encrypt(pk^*, m_\delta)$ ，然后将 C^* 交给敌手 A 。

阶段 2 敌手 A 继续进行一系列的解密查询，挑战者采取与阶段 1 相同的方法进行应答。此处要求敌手 A 不能进行解密查询(ID^*, C^*)。

猜测：最后，敌手 A 输出一个比特 δ' 来猜测在挑战阶段挑战者 C 所选取的比特是 0 还是 1。

当敌手 A 的优势满足 $Adv_{PRE,A}^{IND-CCA2} = |\Pr[\delta' = \delta] - \frac{1}{2}|$ 。若没有任何多项式有界的攻击者以一个不可忽略的优势完成上述过程，则该代理重加密方案在适应性选择密文的攻击下具有不可区分性（IND-PRE-CCA2）。

4 结束语

移动终端设备以灵活性强为优势，逐渐成为了人们生产、生活中不可获取的重要角色，本文针对移动云计算环境下数据的安全增量备份问题，结合数据加密、重加密等相关方案，设计了一种面向移动云计算的基于时间的数据安全增量备份方案，包含系统模型、基于时间粒度的加解密算法描述以及安全备份方案实施方案，具有如下特点。

1) 保证数据的加密性

数据在上传到云端前，由用户进行数据的首

次加密, 然后云端对数据进行基于时间粒度的数据重加密, 数据在传输和云端处理过程中均以密文的形式存在, 有效地保证了数据的机密性, 防止云服务商和其他攻击者对数据的窃取和挖掘。

2) 降低用户密钥泄露带来的数据丢失损失

数据在增量备份到云端时, 采用基于时间粒度的加密处理, 不再是所有数据的安全依托于用户的唯一公私钥对, 因此, 能够有效地解决由于用户密钥遗失造成的数据全部泄露问题。

该方案有别于现有的云平台数据增量备份方案, 将用户的备份时间作为加解密参数, 云服务器依据用户备份数据的时间, 将其划分到不同的时间阶段, 进行数据重加密并进行保存。用户使用数据的时候, 提供备份时间和自身私钥进行数据解密, 有效地防止了由于用户密钥遗失造成的数据大量泄露问题, 同时增加了用户数据增量备份的灵活性。

参考文献:

- [1] 中国互联网络发展状况统计报告: 2016-1[EB/OL]. <http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/201601/P020160122469130059846.pdf>. Report of China Internet development statistics: 2016-1[EB/OL]. <http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/201601/P020160122469130059846.pdf>.
- [2] 李瑞轩, 董新华, 辜希武, 等. 移动云服务的数据安全与隐私保护综述 [J]. 通信学报, 2013, 34(12): 158-166. LI R X, DONG X H, GU X W, et al. Overview of the data security and privacy-preserving of mobile cloud services[J]. Journal on Communications, 2013, 34(12): 158-166.
- [3] 何欢, 何倩. 数据备份与恢复[M]. 北京: 机械工业出版社, 2010. HE H, HE Q. Data backup and recovery[M]. Beijing: China Machine Press, 2010.
- [4] 张龙立. 云存储技术探讨[C]//中国云计算与SaaS大会. c2010. ZHANG L L. Cloud storage technology[C]//The 1st Chinese Conference on Cloud Computing and SaaS. c2010.
- [5] 张桂刚, 李超, 张勇, 等. 一种基于海量信息处理的云存储模型研究[J]. 计算机研究与发展, 2012, 49(z1):32-36. ZHANG G H, LI C, ZHANG Y, et al. A kind of cloud storage model research based on massive information processing[J]. Journal of Computer Research and Development, 2012, 49(z1):32-36.
- [6] 吴胜艳, 许力, 林昌露. 基于门限属性加密的安全分布式云存储模型[J]. 计算机应用, 2013, 33(7):1880-1884. WU S Y, XU L, LIN C L. Secure and distributed cloud storage model from threshold attribute-based encryption[J]. Journal of Computer Applications, 2013, 33(7):1880-1884.
- [7] JUELS A, KALISKI JR B S. Pors: proofs of retrievability for large files[C]//The 14th ACM Conference on Computer and Communications Security.c2007: 584-597.
- [8] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores[C]//The 14th ACM conference on Computer and Communications Security. c2007: 598-609.
- [9] ATENIESE G, PIETRO D R, MANCINI L V, et al. Scalable and efficient provable data possession[C]//The 4th International Conference on Security and Privacy in Communication Networks. ACM, c2008: 9.
- [10] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[M]//Advances in Cryptology—EUROCRYPT'98. Berlin Heidelberg: Springer, 1998: 127-144.
- [11] ATENIESE G, FU K, GREEN M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(1): 1-30.
- [12] IBRAIMI L, TANG Q, HARTEL P, et al. A type-and-identity-based proxy re-encryption scheme and its application in health-care[M]//Secure Data Management. Berlin Heidelberg: Springer, 2008: 185-198.
- [13] TABAN G, CÁRdenas A A, GLIGOR V D. Towards a secure and interoperable DRM architecture[C]//ACM Workshop on Digital rights Management. c2006: 69-78.
- [14] 王红兵. 基于双线性配对的代理重加密的研究[D]. 上海: 上海交通大学, 2013. WANG H B. Research on bilinear pairing based proxy re-encryption[D]. Shanghai: Shanghai Jiao tong University, 2013.

作者简介:



慈云飞 (1989-), 男, 安徽池州人, 北京电子科技学院硕士生, 主要研究方向为访问控制和信息安全。

史国振 (1974-), 男, 河南济源人, 博士, 北京电子科技学院副教授、硕士生导师, 主要研究方向为网络与系统安全、嵌入式安全。

谢绒娜 (1976-), 女, 山西永济人, 北京电子科技学院副教授, 主要研究方向为密码应用、网络与系统安全。

潘耀明 (1992-), 男, 安徽亳州人, 北京电子科技学院硕士生, 主要研究方向为嵌入式安全。

杨凤 (1990-), 男, 河南信阳人, 北京电子科技学院硕士生, 主要研究方向为片上多核系统、嵌入式系统。

叶思水 (1989-), 男, 江西南昌人, 硕士, 瑞庭网络技术 (上海) 有限公司软件工程师, 主要研究方向为网络安全。