基于秘密共享算法的云存储信息安全系统探究

□刘春辉　解放军 61213 部队场站　张鹏乐　北京系统工程研究所

【摘要】　云存储相比传统存储方式优势明显，但其安全性仍备受质疑。虽然云服务商采取了多种手段保证云存储数据安全，但由于其自身的安全缺陷，云存储中的数据安全仍存在威胁。本系统基于秘密共享算法，利用手机短信验证码技术、USB-KEY 安全认证技术，结合云服务商已有的安全机制，有效整合网络上多个免费云存储服务商，集成了一个免费虚拟云存储空间。系统在方便用户使用的同时，能有效保证用户数据的机密性、完整性，防止用户数据被破坏、被窃取和丢失。

【关键字】　秘密共享　云存储　信息安全

一、引言

随着当今时代信息化的不断发展，个人、企事业单位的信息数据量直线上升，越来越多的人选择使用云存储服务。云存储虽然可以满足用户不断增加的数据存储和管理需求，但却无法有效保证用户的数据安全。

目前，云存储服务商普遍采用多方式备份、高强度加密、跟踪、记录、监控用户数据等方式来保障用户数据安全。但云端数据依然面临如下风险：1) 由于运营商自身技术局限，不法分子侵入存储系统造成用户数据被篡改或破坏。2) 由于黑客攻击或运营商监守自盗，用户数据被非法窃取。3) 云存储服务依赖单一运营商，当该运营商遭受不可抗力（如地震、火灾等）破坏时，会造成用户数据丢失。

该系统利用（m,n）门限的秘密共享技术、手机短信验证码技术、USB-KEY 安全认证技术，结合云服务商已有的安全机制为用户提供更为安全的云存储服务。

二、关键技术分析

2.1 基于秘密共享算法实现源端数据的防窃取、防破坏、防丢失

秘密共享是一种将秘密分割存储的密码技术，它将拆分后的每一个份额交予不同参与者管理，单个参与者无法恢复秘密信息，只有若干个参与者一同协作才能恢复秘密消息，是分散风险和容忍入侵的有效方式，是信息安全和数据保密的常用手段。

本系统通过 (m,n) 门限秘密共享技术，将原文件不等分加密分割为 m 子块，分别储存在用户选定的不同云服务商处。取用时只需获取其中的 n（n<m）个完整子块，即可恢复出完整原始文件。数据的分割、加密过程对用户完全透明，不涉及用户身份信息，基本上杜绝了传输过程文件损坏、云服务商丢失文件、误删除子块文件、云服务商遭受不可抗力破坏等情况造成的原始文件损坏丢失，确保数据的安全、完整。

2.2 基于手机短信验证码或 USB-KEY 安全认证技术实现本地用户身份验证

根据用户安全需求不同，该系统可分为手机短信验证码认证和 USB-KEY 安全认证两种模式，用户可根据需求，选择适合自己的身份验证模式。

手机短信验证码是目前较为流行、成本最低、最简单便捷的安全验证方式。许多大型网站尤其是购物网站，都提供有手机短信验证码功能，可以比较准确安全地保证安全，验证用户身份的正确性。

基于 USB-KEY 的身份认证方式是近几年发展起来的一种方便、安全、经济的身份认证技术，它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用

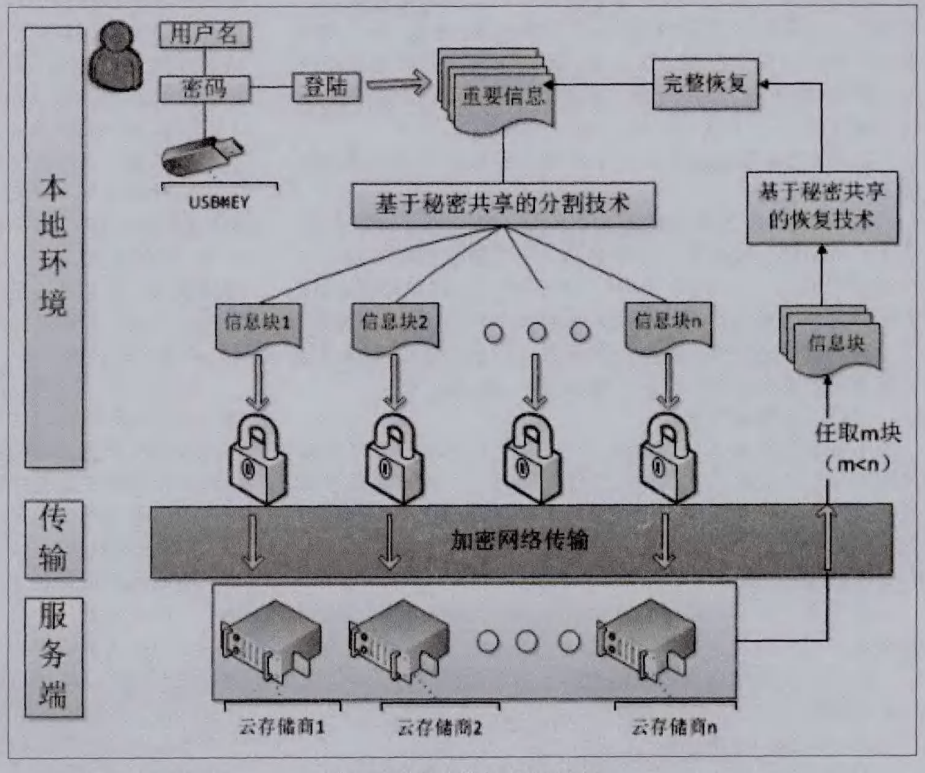

图 1　系统整体结构设计图

现代通信网络面临的安全现状与维护对策分析

□刘晓坦　中国人民解放军总医院海南分院

【摘要】　随着科学技术的发展以及人们生产生活中信息化水平的不断提升，现代通信技术也在充分发展的基础上在人们的生活中得到了广泛性的应用，这在一定程度上对通信网络安全提出了更高的要求。本文就从通信网络安全维护重要性入手，对当前我国通信网络安全维护方面存在的问题进行分析，并提出了相应的维护对策，希望能够推进我国现代通信行业获得更好的发展。
【关键词】　现代　通信网络　网络安全　维护

现代社会科学技术的进一步发展，计算机通信网络得到了普及性应用，给社会大众的生产生活带来了极大的便利，对人们精神生活质量的提升产生着相应的积极影响。但是伴随着通信网络影响力的逐步提升，对通信网络安全要求也随之增强，因此相关网络管理和维护部门必须加强对计算机通信网络安全维护和技术创新工作的重视，及时解决网络安全隐患，最大限度的避免通信网络安全问题对社会大众的生活造成不良影响，为人民营造健康的网络环境。

一、维护现代通信网络安全的重要性

通信网络安全维护工作就是采用一定的计算机技术和策略保证网络环境中信息安全、完整、可以继续应用。随着当代社会计算机科学技术的不断发展和创新，通信网络建设已经日渐成为网络技术革命的重要构成元素，是社会大众之间传递相关信息的重要桥梁，对社会上各种相关经济文化的传播和社会主义精神文明的构建产生了一定的积极影响[1]。但是从另一个方面进行分析，通信网络存在一定的安全隐患，一旦出现网络安全问题，不仅会造成网络使用人员在信息交流方面存在障碍，甚至会导致信息泄露，造成巨大的社会经济损失，对社会公共利益和价值也产生严重的不良影响。一般情况下，通信网络遭受到的攻击以攻击者非法偷盗和使用他人账号信息以及利用所盗用的账号进行其他各方面的诈骗为主。

因此在当前通信网络安全问题日渐增多的社会背景下，关注网络安全，进行安全技术创新，促使安全隐患得到有效

性之间的矛盾，现已广泛应用于银行 U 盾、加密电子狗等多种场合。本系统将验证机制写进 USB-KEY，通过 USB-KEY 来进行用户身份的识别，防止用户身份遭假冒，并提供了有限次数输错后自动锁死功能，进而有效保障用户数据在本地的安全性。

2.3 秘密共享安全机制与云服务商安全机制有机互补保证云端数据安全

基于（m,n）门限的秘密共享机制有效防止了用户数据丢失、被窃取、被破坏，云服务商自身安全机制对于用户加密数据流也有一定的保护作用。秘密共享安全机制能够保证在丢失部分数据的情况下仍可对原数据进行恢复，有效减小了用户对云服务商安全机制的依赖性。秘密共享安全机制与云服务商安全机制有机互补，确保用户云端数据安全。

三、系统实现方案

本系统主要关注云存储的安全问题，设计的安全环境涉及用户本机、服务云端及中间传输三个环节。无论用户进行何种操作，都必然将经历上述三个环节，因而这三个部分的安全性都需要给予高度关注。本系统的具体结构见图 1。

3.1 本地环境

本地环境是指直接运行本系统的用户环境，其安全机制是最基本也是相当重要的一环。

用户在本地环境中进行的操作，主要包括身份认证、文件操作两部分。

第一部分：身份认证。

身份认证是本地安全环境的基础部分，本作品的身份认证部分除包括传统的用户名、密码认证外，还加入了 USB-KEY 认证（或手机短信验证码认证），用户需同时通过两重认证才能进入系统实施相关操作。为防止攻击者穷举破解，系统还加入了尝试次数限制，若超过限制将锁死 USB-KEY（或限制用户认证手机）。

第二部分：文件操作。

文件操作是本地安全环境的核心部分，也是本系统主要关注的部分。文件操作涉及用户私密文件的秘密共享、门限容错、哈希加密等多个关键部分，以实现文件的分割合并、容错恢复、完整性检测、正确性保证等诸多功能，体现了本系统在安全性方面做的大部分工作。

3.2 传输环境

为防止用户私密文件在网络间传输过程中遭遇安全问题，系统在传输前对文件进行加密处理，保证网络间传输的内容为密文状态，即使被截获也无法直接破译出原始内容。且传输操作由系统全权托管，无需用户手动参与，避免了因用户操作不当导致的安全风险。

3.3 云端环境

本系统的设计初衷是防止云服务商的监守自盗，因而在每个云服务商处只上传单个经过加密的子块文件。单一服务商的窃取行为无法获得任何有意义信息。即便遭遇少数文件的丢失及破坏，系统也能够利用剩余完整子块还原出原始文件，进而大大降低了用户数据对云端安全环境的依赖。因此，在本系统的协助下，用户在使用云存储服务时不必过多担心云端环境的安全问题。