医院虚拟隔离私有云存储应用与设计*

徐 骁 李爱勤 陈敏莲 胡外光 胡珊珊

（湖南省儿童医院 长沙 410000）

〔摘要〕 为完善医疗信息安全中核心数据的访问和控制问题，构建医院虚拟隔离私有云存储架构，包括虚拟化改造、基于层次模型的元数据模块应用、基于虚拟隔离的访问远程客户端设计应用等方面，为医院内外网隔离和互通提供可靠的实施方法。

〔关键词〕 数据安全；云存储；虚拟化

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2018.01.007

Design and Application of Virtual Isolation Private Cloud Storage in Hospital *XU Xiao, LI Ai－qing, CHEN Min－lian, HU Wai－guang, HU Shan－shan, Hunan Children's Hospital Information Center, Changsha 410000, China*

〔**Abstract**〕 In order to improve the access and control of core data in medical information security, the paper builds a virtual isolation private cloud storage architecture in hospital, including virtualized reconstruction, metadata model application based on hierarchical model, access to remote clients design and application based on virtual isolation and so on, providing a reliable method for the isolation and intercommunication between the intranet and extranet.

〔**Keywords**〕 Data security; Cloud storage; Virtualization

1 引言

目前医疗机构中部署的应用多达 10 几甚至几十项之多，庞大复杂的软件应用、网络分布部署、存储与服务器应用给医疗机构信息系统的可控性带来极大的挑战。同时越来越多的医疗数据和病人信息接入到互联网，为医疗数据的共享、复制和传播提供极大的便利，伴随而来的是巨大的数据泄露风险，患者的个人隐私和医院核心机密数据都处于暴露状态。

为应对以上问题，关于存储以及私有云改造的研究得到了不断的发展深入[1]。基于主机、网络、存储的 3 层结构，通过虚拟化平台集中管理存储资源池，提高资源利用率，实现资源共享、按需分配的灵活机制，降低灾难恢复的硬件成本，提高存储利用率。李先锋[2]等人利用服务器虚拟化技术对物理服务器集群进行集中管控，提高主机的 CPU 利用率同时降低服务器使用的空间与能耗。结合客户端桌面虚拟化改造降低终端用户的故障率、优化办公环境、实现移动化医疗办公。孟群[3]等人阐述医院服务器虚拟化技术的整合思路，虚拟化整合能够实现动态管理和对分配资源进行计算，更加高效灵活地实现通用计算、存储及网络负载。服务器资源的虚拟化整合极大节省机房空间、机柜、网线、电耗、空调和人力成本等。孟庆伟[4]等人利用 3 方云产品对单位内部数据中心进行云端虚拟化改造工

〔修回日期〕 2017－09－30

〔作者简介〕 徐骁，硕士，工程师，发表论文 3 篇。

〔基金项目〕 湖南省科技厅重点研发计划（项目编号：2016JC2020）。

作，对服务器集群进行升级搭建虚拟机，整合服务器资源提升 CPU 计算能力利用率至 80%，可视化图像管理为日常维护、动态调配等工作提供了便利。近些年来对医院信息化存储虚拟化的综合性研究和应用也逐渐增多，如肖玮炜[5]综合介绍存储虚拟化技术的现状和重点关注点，对其应用及主要功能模块构成进行归纳总结。

2 整体架构设计

2.1 概述

为解决医院信息安全内外网中核心数据的访问、控制等问题，该架构设计首先基于院内原有存储设备对虚拟化存储进行扩展升级，对核心业务数据的通信、操控方式进行剥离控制，基于该架构构建开发一套远程访问客户端系统，实现安全的内、外网办公应用。分离文件流与控制流的数据通信设计，见图 1。通过特点算法实现文件数据分离，将文件数据流与操作控制流进行隔离，有效降低总控服务器的负载压力。同时，配备的热备服务器能够无缝启用，避免单点故障的发生。基于医院本身存储设备和已有虚拟化软件，利用云存储服务扩展虚拟化注册和动态容量功能，优化与核心业务服务的通信，降低和隔离访问客户端的接入建设成本。

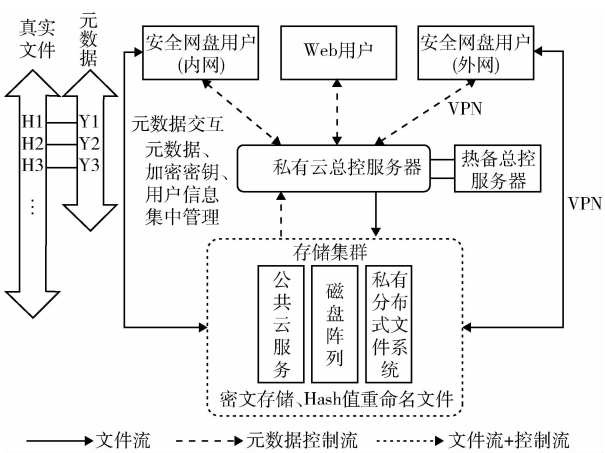

图 1 虚拟隔离存储应用架构设计

2.2 私有云存储虚拟化改造

由于企业组织私有云存储需要充分利用各种遗留存储资源，而这些存储资源从功能及形态上看往往是异构的，因此对异构存储资源进行虚拟化表示，对其进行严格生命周期管理，从而构建统一的私有云存储基础设施，就成为私有云存储构建中极为重要的环节。架构在原有存储设备基础之上，通过存储管理服务器重新定义存储资源虚拟化为存储能力（SC），对新添加的存储介质进行人工注册，虚拟层总控服务器实现动态算法监控以及空间分配。在虚拟层存储层面，架构利用哈希算法将数据文件数值化，在存储层屏蔽用户文件元数据细节，在物理层对数据的 I/O 拟采用透明加密解密处理，以密文的形式存在，以避免用户文件数据的泄露。

2.3 基于层次结构的元数据模型应用

为优化总控服务器负载和业务核心服务器存储通信，通过重新定义的数据 3 层结构：用户层、元数据层、文件存储层，将文件流和控制流进行分离，剥离用户和文件之间的直接交互行为，见图 2。通过哈希算法将文件碎片化并重新构成文件碎块树，从而保证用户访问数据的加密/解密操作的安全性。碎片化后的文件块以哈希值进行命名，依据特点算法分散存储在不同物理介质之中，当文件需要存取操作时将依据算法重新组装解密。此外利用文件碎块构成的文件树形结构能够基于时序存在多个版本，方便文件的追溯和版本管理。

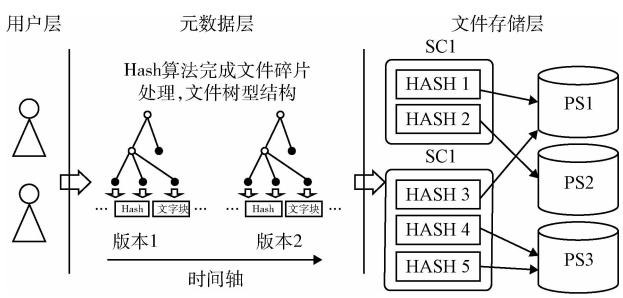

图 2 3 层数据结构

2.4 基于虚拟隔离的访问远程客户端设计应用

为保障医院远程应用办公的数据安全问题，设计客户端将利用虚拟隔离的方式进行文件存取及桌面应用的操作。远程客户端基于数字证书双向身份

认证，在设备初次注册时记录其硬件信息，保障用户身份的合法性。一旦完成身份验证，将通过对通信隧道的加密实现网络之间的加密传输，满足可信要求。隔离访问机制针对不同的异构存储通过强制读写分离进行管控，同时将强制关闭移动设备热点及 WIFI 功能直至客户端安全断开连接。隔离远程客户端在安装过程中将在本地生成一个安全数据拷贝盘，该数据拷贝盘是对私有云存储资源池中客户端历史访问文件的同步拷贝。当客户端和业务服务器进行通信时，数据访问和操作将作用于临时数据拷贝盘，从而减少网络通信压力。离线状态下，同样能够利用客户端访问本地数据拷贝盘读取文件数据。

3 结语

基于虚拟隔离机制的医院私有云存储架构为医院的内外网隔离和互通提供一个便捷、安全可靠的实施方案，改变以往需要配备两套网络的格局，节省了开支。系统立足于私有云存储系统架构，对异构存储资源虚拟化、文件分层组织管理、私有云客户端可信隔离访问、本地安全虚拟桌面构建及分布式目录同步等技术内容进行系统应用。一方面为医疗企业的虚拟化存储云架构实施应用提供一定的实践经验和理论架构，另一方面也是本地安全虚拟桌面构建远程桌面、私有云访问等虚拟化技术的综合应用，对创新型虚拟隔离数据保护环境构建技术虚拟化技术在医疗企业的应用具有一定的理论和现实意义。

参考文献

1 魏智，黄昊. 虚拟存储技术在医院信息化建设中的作用［J］. 中国数字医学，2013，(11)：86－88.

2 李先锋，王凯芸，吕强，等. 三甲医院虚拟化技术的研究与实践［J］. 中国医院，2012，16（2）：12－14.

3 孟群，屈晓晖. 虚拟化技术在医院信息平台服务器整合中的应用［J］. 中国数字医学，2011，6（7）：8－12.

4 孟庆伟，刘婷. 基于 Fstor Phantosys 云桌面虚拟化平台的构建［J］. 计算机安全，2014，(5)：24－27.

5 肖玮炜. 医院信息系统平台建设与存储虚拟化技术研究［J］. 电脑编程技巧与维护，2016，(12)：67－68.

（上接第 11 页）

17 Murphy S N, Weber G, Mendis M, et al. Serving the Enterprise and Beyond with Informatics for Integrating Biology and the Bedside (i2b2) [J]. J Am Med Inform Assoc, 2010, 17 (2): 124－130.

18 Bhattacharya S, Andorf S, Gomes L, et al. ImmPort: disseminating data to the public for the future of immunology [J]. Immunol Res, 2014, 58 (2－3): 234－239.

19 Payakachat N, Tilford J M, Ungar W J. National Database for Autism Research (NDAR): Big Data Opportunities for Health Services Research and Health Technology Assessment [J]. Pharmacoeconomics, 2016, 34 (2): 127－138.

20 Lowe H J, Ferris T A, Hernandez P M, et al. STRIDE—An integrated standards－based translational research informatics platform [J]. AMIA Annu Symp Proc, 2009, (2009): 391－395.

21 Tomczak K, P Czerwinska, M Wiznerowicz. The Cancer Genome Atlas (TCGA): an immeasurable source of knowledge [J]. Contemp Oncol (Pozn), 2015, 19 (1a): A68－77.

22 Clark K. The Cancer Imaging Archive (TCIA): maintaining and operating a public information repository [J]. J Digit Imaging, 2013, 26 (6): 1045－1057.

23 Wang X. Translational Integrity and Continuity: personalized biomedical data integration [J]. J Biomed Inform, 2009, 42 (1): 100－112.