灾害与突发事件 ICU 大数据平台的安全设计

罗福强,李 瑶,范展源
(四川大学锦城学院,四川 成都 611731)

摘 要:基于四川省“灾害与突发公共卫生事件重症救护大数据平台”建设项目展开研究。由于项目涉及到医疗机构、医生、病人等大量医疗信息的网络传输,对系统安全性的设计显得尤为重要。从系统、程序资源访问控制、功能性、数据域四个层次分析了现有的安全模型,找出了其中的限制与不足之处。根据现有的安全隐患,设计了新的基于云计算架构的应用系统的安全模型。该模型以成熟的虚拟化技术为基础,以追求高可用性、可伸缩性、安全性为目标,具有三重安全保障机制。以此模型提出项目的安全解决方案,确保项目的顺利实施。通过项目的运行检测,结果表明该安全设计方案可以保障平台信息不会轻易泄漏,从而保护用户的权益。

关键词:突发公共卫生事件;重症救治;大数据;安全模型;云计算架构;安全设计方案
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2016)10-0069-04
doi:10.3969/j.issn.1673-629X.2016.10.015

Safety Design of ICU Big Data Platform for Disaster and Sudden Event

LUO Fu-qiang,LI Yao,FAN Zhan-yuan
(Jincheng College of Sichuan University,Chengdu 611731,China)

Abstract:The research is based on the project of “the big-data platform of intensive care for disaster and emergency public health event”. Because the project involves the medical institutions and doctors,patients and other large medical information network transmission,the design of system security is particularly important. The existing security model is analyzed from four levels including the system,program resource access control,function and data domain,finding out their limits and shortcomings. Then according to the existing safety problems,a new security model of application system is designed based on cloud computing. The model is based on the mature of virtualization technology,in pursuit of high availability,scalability,security as the goal,with a triple security mechanism. It has offered a whole security design scheme to ensure the smooth implementation of the project. The test through the project shows that the security design can make the platform information will not be easy to leak,thus protecting the rights and interests of users.

Key words:sudden public health event;intensive care;big data;security model;cloud computing architecture;security design scheme

0 引 言

“灾害与突发公共卫生事件重症救护大数据平台”是一个集云计算技术、大数据技术、移动互联技术以及物联网技术为一体的新型智能系统,是一个为重症伤病人员提供咨询、抢救、运送、手术、监护、康复、心理干预等全方位服务的大数据软件系统,也是一个整合不同级别、不同区域的医疗资源为一体,实现重症救护统一指挥和调度的集成系统,还是一个各级政府、医疗机构、医生、病人、公众在参与重症救护时的开放信息互动平台。这个平台的定位就决定它必须运行在互联网中并能及时通信,另一方面,对于系统中的信息又要做到绝对的安全,这就对平台的安全性提出了挑战。

1 传统的安全模型分析

通常,一个应用系统安全性问题[1]可按粒度从粗到细的顺序划分为以下 4 个层次。

(1)系统级安全[2]。实现办法包括:访问 IP 段的限制、登录时间段的限制、连接数的限制、特定时间段内登录次数的限制等。这是应用系统第一道防护大门。

(2)程序资源访问控制安全。对程序资源的访问进行安全控制[3],在客户端上为用户提供与其权限相关的用户界面,如只出现与其权限相符的菜单或操作按钮;在服务端则对 URL 请求的资源或业务服务类方法的调用进行访问控制。

收稿日期:2015-09-20 **修回日期**:2015-12-24 **网络出版时间**:2016-09-18
基金项目:2015 年四川省第一批科技支撑项目(2015SZ0056)
作者简介:罗福强(1970-),男,副教授,研究方向为物联网、云计算和大数据。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160918.1707.018.html

(3)功能性安全。功能性安全会对程序流程产生影响,如针对用户的操作记录是否需要审核,对上传的附件是否要限制其大小,等等。这些安全限制已经不是一般的限制,而是业务流程内的限制,在一定程度上影响了业务流程的运行。

(4)数据域安全[4]。数据域安全包括两个层次:一是行级数据域安全,即用户可以访问哪些数据记录,一般以用户的岗位角色或所在单位为条件进行过滤;二是字段级数据域安全,即用户可以访问数据记录的哪些字段。

在以上四个层次的安全问题中,不同应用系统的系统级安全关注点往往差异很大。该项目对上述的安全问题均有较高要求。

传统的应用系统关注系统级安全,通常在 Windows 平台上进行开发,其网络通信限于局域网之内,与互联网物理隔离。这种系统架构一般被认为是最有安全保证的架构。实际上,因为设计考虑不周,系统经常遭受中间人攻击[5],因此同样存在安全问题。此外,整个系统通常由用户组织力量进行运营和维护,受资金、技术、人力资源的限制,常常出现一些意想不到的灾难性问题,例如,服务器物理损坏、设备被盗、机房火灾等。为了保证整个系统正常运营,不得不承受高昂的运维代价。

随着 Internet 的普及,基于 B/S 的 Web 应用系统的安全性解决方案发生了重大变革,如图 1 所示。在图 1 中,左边是传统的基于 C/S 的应用系统的安全模型,右边是传统的基于 B/S 的 Web 应用系统的安全模型[6]。

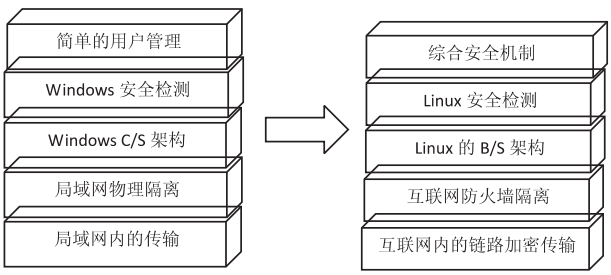

图 1 传统的应用系统安全模型的变革

在基于 B/S 的 Web 应用系统的安全模型中,位于最底层的传输层直接借助 Internet 通信,出于加强安全设计的考虑,引入诸如 IPSec、SSL 协议进行链路加密或引入 VPN[7] 技术,以避免数据传输之中的安全隐患。

网络的安全从原来依靠物理隔离转变为依靠互联网与内网之间的防火墙隔离。之后,借助开源的 Linux 并以此为基础构建的 B/S 系统架构,可有效解决 Windows 总是不令人放心的安全疑虑。

最上层的 Web 应用系统在设计时通常更加重视 Internet 技术本身的安全隐患,因此所采用的安全机制与手段往往更加丰富,例如数据加密、身份认证、权限管理等。

在传统 Web 应用系统的安全模型之中,其安全性得到了很大的保障,但是应用系统以网站的形式部署在物理操作系统平台之上的网站服务器中,例如部署到 Apache 中,这种部署方式的主要安全隐患是在突发尖峰时刻无法有效应对大规模的访问请求,从而造成拒绝服务攻击。传统的解决方案是尽可能多地准备镜像服务器,通过服务集群来提高整个系统的并发访问能力,但常常收效甚微。

2 基于云计算架构的应用系统的安全模型

为了解决传统 Web 应用系统存在的安全隐患,文中设计了一种全新的基于云计算架构的安全模型[8],如图 2 所示。

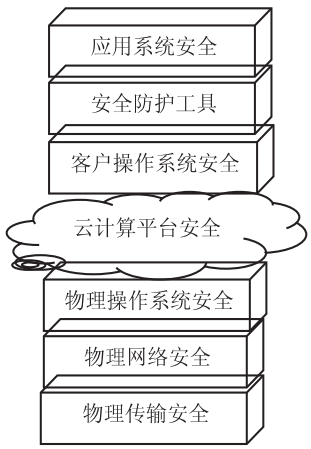

图 2 基于云计算架构的应用系统的安全模型

在基于云计算架构的应用系统的安全模型中,首先利用虚拟化技术将传统的物理网络系统、物理存储系统、物理服务器硬件系统分别抽象为虚拟网络[9]、虚拟存储和虚拟服务器[10]。然后借助云计算平台(例如 OpenStack)将这些资源分配用户。用户在云计算平台上部署自己的系统,包括客户操作系统、安全检测工具和应用系统等。

相对两种传统模型来说,基于云计算架构的安全模型以成熟的虚拟化技术为基础,以追求高可用性、可伸缩性、安全性为目标,具有无可比拟的优势。

高可用性保证云服务器可以在其物理系统发生故障时可动态迁移到其他物理系统而不影响其中的应用系统的正常运行。

可伸缩性[11]提供弹性计算、弹性存储功能,可根据用户并发访问的规模进行自动扩展,能有效地解决突发尖峰时刻可能出现的系统拒绝服务的问题。

安全性机制首先以传统物理传输安全、网络安全和操作系统安全为基础,然后提供了专门针对云计算

架构而设计的安全策略[12],例如 OpenStack 平台借助 Keystone 的令牌控制机制实现系统的安全性。最后授权给用户的云服务器本身还可以像传统物理服务器一样,构建属于云服务器自身的安全解决方案,包括操作系统的安全、专业级的安全检测工具和应用系统安全机制等。

因此,基于云计算架构的应用系统的安全模型事实上具有三重安全保障机制。

3　本项目的安全解决方案

本项目的目标是要实现当灾害与突发公共卫生事件发生并造成重大人员伤亡时的伤病数据采集、现场筛检、转运、导航、入院、治疗、护理、康复、出院的全流程管理,还要实现四川省范围内所有重症救治资源的统一调度与管理,包括救灾单兵设备、救护车、医务人员、各级各类 ICU 中心、床位、血液、药器、医疗设备等所有可统一调度的资源。因此,决定采用基于云计算架构的应用系统的安全模型。

(1)以阿里云的安全性为基础。

本项目选择阿里云平台,主要依据是:阿里云是一个经过淘宝网和阿里巴巴电子商务平台运营实践证明的成熟可靠的公有云,不存在传统安全模型中的安全隐患问题,同时还可以借助阿里云的安全解决方案和技术团队来规避 Internet 本身存在的安全性问题。阿里云允许根据业务规模的增长自动扩展云服务器的配置[13],能有效应对尖峰时刻的大规模并发访问问题。

安全解决模型如图 3 所示。

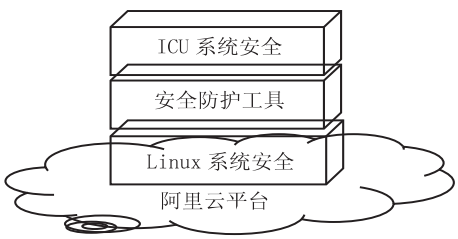

图 3　本项目的安全解决模型

(2)以开源的 LAMP 技术的安全性为依托。

本项目在阿里云基础上安装和配置云服务器。云服务器采用开源的 LAMP 技术(即 Linux、Apache、MySQL 和 PHP)。这些开源的软件不仅解决了软件知识产权问题,还具备比传统 Windows+C#+ASP. NET+SQL Server 技术更经济的优势。更重要的是,LAMP 技术是经国内外多达上百万个网站测试证明是安全可靠的技术,具有公认的安全性。除此之外,在云服务器之中,还可以安装和配置各种安全防护与检测工具,提供防火墙、防木马、防病毒等功能。

总之,本项目的底层技术架构就以 Ubuntu Linux 操作系统为基础,再搭配 Apache 和 PHP 的 Web 服务器技术以及 MySQL 数据库技术,最终通过构造服务器集群来打造大规模灾害与突发公共卫生事件的重症救护的 SaaS[14]平台(即“软件即服务”)。

(3)系统架构的安全设计。

本项目以 LAMP 技术为基础,系统采用云计算架构,结合多租户[15]的设计思想,最终打造一个能提供 SaaS 功能的大数据平台。每一个租户代表一个独立的重症医学科(即各级医院的 ICU 中心)。

首先,在数据存储方面,每个租户拥有独立的数据库,该数据库可独享一台云服务器中的计算、存储和网络性能。独立的数据存储架构确保了每个租户的数据资源具有完全的封闭性,也为 ICU 中心的正常运营奠定了安全性基础。创建租户时系统自动创建属于该租户的数据库、自动完成该数据库表的初始化。此外,系统预设向 Hadoop 和 HBase 的大数据平台迁移数据的接口。

其次,在系统管理方面,每个租户拥有独立的系统管理员和后台管理系统。每个租户(即 ICU 中心)的系统管理员由租户内部指定,其他内部工作人员的账户管理、角色分配、系统权限管理均由属于租户的系统管理员统一管理。这种架构确保了每个 ICU 中心内部业务的独立性。

最后,在技术实现方面,引入开源的 Laravel 和 ArgularJS架构,用流行的 SOA(即面向服务的架构)思想、按 RESTful 风格进行代码实现。这种全新的云计算设计模式决定了最终用户(无论是医务人员还是伤病患者及亲属)可使用任何设备(包括台式计算机、笔记本电脑、平板电脑和智能手机)在任何时间访问本系统平台且安全可靠。

(4)数据域与功能性安全设计。

在数据域安全层面上,首先借助 Linux 的强制访问控制机制实现数据库文件级的安全,其次引入加密技术将系统中敏感信息加密存储,以确保在发生极端安全灾难的情况下的信息泄露问题。

在功能性安全层面上,整个系统的可操作功能划分为两个类别,即前台业务和后台管理。前台业务主要面向租房内部的医务工作人员开放,由后台管理员进行权限管理。系统提供灵活的根据岗位角色的权限分配机制,以确保 ICU 中心内部员工在工作上的独立性。

(5)日志记录的安全性设计。

为了确保在发生不可预测的安全性问题时能通过追溯来锁定安全事件的源头,提供了完善的日志记录功能,通过分析这些日志记录即可寻找安全解决方法。

详细的日志记录包括系统级的日志记录,也包括重症救治业务级的日志记录。整个系统除了能记录系

统的运行状态之外,还能记录每个操作人员的操作。所有日志记录保存到 HBase 数据库之中,借助 Mahout 数据挖掘功能可以做到系统发生的所有事件均可追溯相关责任人。

(6)ICU 业务流程的安全性设计。

根据 ICU 业务的管理流程进行严格设计,提供业务审核机制,不仅确保 ICU 中心内部的每一项工作业务按规定进行,还直接提升了 ICU 中心的工作质量。

4 结束语

随着互联网的发展,越来越多的企业或部门依托网络进行宣传或传递信息。对于医院来说,为了更好地整合资源、更方便地服务群众,建立一个灾害与突发公共卫生事件重症救护大数据平台很有必要,那么系统的安全性则成了必须要考虑的问题。文中提出的大数据平台安全性设计方案从各个方面分析了系统的安全性,并提出了相应的设计方案用以提高安全性,保障平台信息不会轻易泄漏,保护用户的权益。同时该设计方案也可为其他系统的安全性设计提供参考。

参考文献:

[1] 朱琳彤. 物联网安全模型分析与研究[D]. 南京:南京理工大学,2013.

[2] 曹利峰. 面向多级安全的网络安全通信模型及其关键技术研究[D]. 郑州:解放军信息工程大学,2013.

[3] 刘 畅. 资源访问控制网关管理系统的设计与实现[D]. 北京:北京邮电大学,2012.

[4] 冯志伟. 网络安全设备联动策略的研究与应用[D]. 北京:华北电力大学,2014.

[5] 于 波. 针对无线网络中间人攻击的检测与防御[D]. 北京:北京邮电大学,2015.

[6] 宋 旭. Web 应用安全确保技术研究与应用[D]. 成都:电子科技大学,2013.

[7] 杨 铎. 基于 MPLS VPN 技术的组网的设计与实现[D]. 长春:吉林大学,2014.

[8] Fernandes D A B,Soares L F B,Gomes J V. Security issues in cloud environments:a survey[J]. International Journal of Information Security,2014,13(2):113-170.

[9] Amaldi E. On the computational complexity of the virtual network embedding problem[J]. Electronic Notes in Discrete Mathematics,2016,52:213-220.

[10] 叶可江,吴朝晖,姜晓红,等. 虚拟化云计算平台的能耗管理[J]. 计算机学报,2012,35(6):1262-1285.

[11] 杨靖琦. 云化业务平台可伸缩性研究[D]. 北京:北京邮电大学,2014.

[12] Safa N S,Solms R V,Furnell S. Information security policy compliance model in organizations[J]. Computers & Security,2016,56:70-82.

[13] 吴 丽,余文春. 基于多服务器最优配置的云计算利润最大化技术研究[J]. 计算机应用研究,2015,32(1):194-197.

[14] Tsai W T,Bai Xiaoying,Huang Yu. Software-as-a-service (SaaS):perspectives and challenges[J]. Science China Information Sciences,2014,57(5):1-15.

[15] 顾平莉. SaaS 应用中多租户若干关键技术研究[D]. 北京:北京邮电大学,2012.