云环境下移动视频监控系统安全性研究

卞艺杰,马玲玲
(河海大学 商学院,江苏 南京 210098)

摘 要:云环境下移动视频监控系统是指在云计算框架下,运用云计算来解决视频数据存储、管理和切分等问题的视频监控系统。该系统与传统视频监控系统相比能够有效提高存储空间、通信带宽的利用率及事后检索的方便性,但由于云计算服务自身存在的安全隐患问题使得移动视频监控系统的信息安全性也受到了威胁。基于以上不足,文中根据该系统的特点分析了其所面临的安全性问题。文中将身份认证、授权限制和审计、核心数据分类与加密、SaaS 技术以及基于 SSL 协议的安全加密操作等技术应用到云环境下移动视频监控系统前端、后台以及网络三个方面,并在此基础上增加了一定的安全性措施,从而提高了系统的安全性。

关键词:移动视频;监控系统;云计算;云存储;安全性
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2013)09-0119-04
doi:10.3969/j.issn.1673-629X.2013.09.030

Research on Security of Mobile Video Surveillance System under Cloud Environment

BIAN Yi-jie, MA Ling-ling
(Business School, Hohai University, Nanjing 210098, China)

Abstract: Mobile video surveillance system under the cloud environment is a system that can use cloud computing to solve video data storage, management and segmentation. The system can more effectively improve the storage space, increase communications bandwidth utilization and the convenience of later retrieval compared with the traditional mobile video surveillance system, but the security risks of cloud computing result in the scarcity of information security of mobile video surveillance system. Describe the security problems existed in the system based on the above shortage. Respectively apply the user authentication, license restrictions, audit, core data classification and encryption, SaaS technology and security encryption technology based on the SSL protocol into the client terminal, background and network of mobile video surveillance system under the cloud environment. Furthermore, supplement some safe measurement based on the above-mentioned technology to improve the system security.

Key words: mobile video; surveillance system; cloud computing; cloud storage; security

0 引 言

移动视频监控系统以嵌入式系统为核心,以移动便捷为目标,以智能分析为特色,是网络视频监控系统的最新发展方向,具有移动性、实用性、即时性、亲临性等特点[1]。目前,国内移动视频监控系统有了长足的发展,如 2008 年的北京奥运会,中国移动为其提供的移动视频监控服务;中国联通开展的“智能家居”视频监控业务;2010 年的上海世博会,各园区应用了多层次的移动视频监控业务[2]。

随着云计算研究的不断深入,国内外学者都提出了云环境下移动视频监控系统,如国内的上海交通大学的唐新怀教授、曾碧教授都做了很深入的研究。这里所说的云环境下移动视频监控系统是指在现有移动视频监控系统的基础上,通过将视频数据存储及处理部署在监控系统的云端,从而有效地提高了存储空间、通信带宽的利用率及事后检索的方便性的一种新的视频监控系统[3]。

然而发现云环境下的移动视频监控系统虽然很大程度上提高了数字资源共享性与可用性[4],但云计算提供了低成本的超级计算服务,这使得黑客可以轻而

收稿日期:2012-11-17 **修回日期**:2013-02-24 **网络出版时间**:2013-05-09
基金项目:国家自然科学基金资助项目(50979024)
作者简介:卞艺杰(1964-),男,江苏南通人,教授,博导,研究方向为信管管理与电子商务;马玲玲(1988-),女,安徽滁州人,硕士研究生,研究方向为信息管理与电子商务。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130509.1057.009.html

易举地获得超强的网络计算能力,从而给用户的数据安全等方面带来了威胁。2009 年 2 月,Google Gmail 邮箱中断服务长达 4 小时。3 月中旬,微软 Azure 停止运行约 22 个小时。

针对这些问题,文中主要从移动视频监控系统的前端安全、后台安全和网络安全三个方面来研究,有针对性地采取措施来保证云环境下移动视频监控设备的安全性。

1 总体架构

总体架构如图 1 所示,每一个网络摄像机(ip camera)及代理都成为一个云终端(cloud)。用户通过 Web 浏览器访问代理及相应的网络摄像机从而获得相应的服务。其中每个网络摄像机及代理都是互联互通的,当有异常情况发生时,所捕获的异常数据会立即传递到网络代理,网络代理进行数据分析,并制定相应的补丁,然后将补丁分发到每一个网络摄像机。

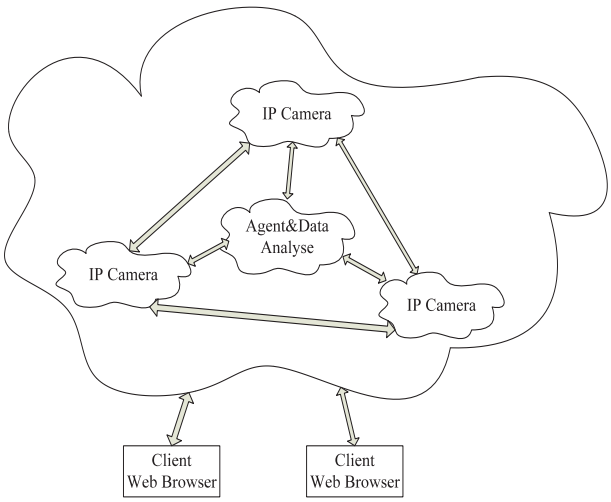

图 1 总体架构图

2 该系统的功能

1)每一台网络摄像机都将其提供的服务发布到网络上,用户可以根据其所需的服务通过代理找到服务提供者(例如某个区域的网络摄像机)。

2)每当用户通过代理访问网络摄像机时,代理都会记录用户的信息并保存到云数据库中。当用户下一次访问代理时,可以自动显示用户可能需要的服务。

3)每一网络摄像机都提供服务定制功能(根据每一用户的喜好将使用频率高的服务置顶)。

4)每当用户在使用某一服务时出现异常状况,都会将异常信息发送到代理进行数据分析,然后将结果反馈给每一网络摄像机(更新安全模块)。

5)此系统中提供的安全机制主要有三个方面:后台、网络及前端的安全。

3 用户调用服务架构

用户通过浏览器调用服务的架构如图 2 所示。

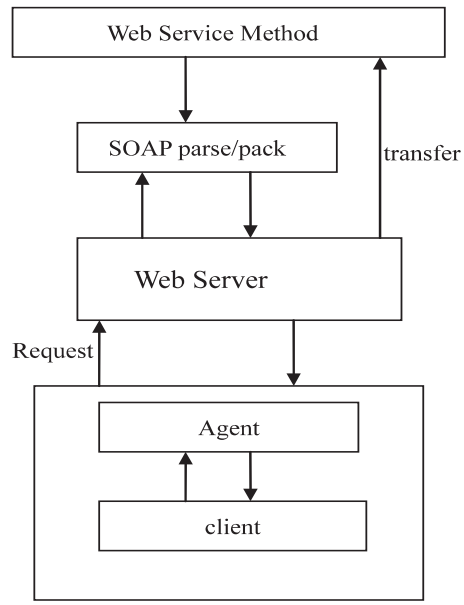

图 2 客户端调用 Web 服务

客户端通过代理访问 Web 服务器,Web 服务器收到的 HTTP Web Service 请求分为两种:HTTP GET/POST 和 SOAP。当服务器收到 SOAP 请求后,就通过 SOAP 解析器进行解析,确定其调用的 Web Service 方法,调用相应的服务后,将结果包装成 SOAP 文档返回给客户。

4 系统安全的实现方案

4.1 后台安全问题:服务器端保存用户身份信息及日志数据

在云环境下使用移动视频监控系统,要确保服务器端用户身份信息以及日志数据的安全,降低系统的安全威胁,提高服务的连续性。

4.1.1 云环境中数据资源的安全存储与管理

数据资源的安全存储与管理是整个移动视频监控系统的安全核心[4]。云环境下的移动视频监控系统是利用虚拟化海量存储技术来对数据资源进行存储和管理的,不必建立冗余备份设备,而是为每个虚拟盘创建多个副本来容错。这样虽提高了数据的访问性能和可用性,却给信息的存储、传输和管理带来了新的威胁。移动视频监控系统将信息资源存储于公共“云”中,以便遍布各地的用户可以快速地共享云资源。但是这样却又引发了新的数据安全问题,如当用户注销账户后,资源所在的云存储空间有可能被重新分配给新用户。这时,原来存储介质上的数字信息被擦除了,但是它的物理信息却有可能被重建,系统内的文件、数据库记录等数据都可能被非法恢复和窃取。为此,必须保证存储对象在存入存储空间前,必须对存储空间进行完整

的数据擦除,避免安全问题的发生[4]。

文中认为应当对移动视频监控系统中的核心机密数据进行加密,再向“云”传输或者直接加密磁盘上的数据,从而避免一些不法的“云”服务提供商和在同一个物理“云”中的用户刻意对数据进行截取或篡改[3]。但加密不仅影响了数据的完整性,更增加了数据的复杂性,这会妨碍用户对移动视频监控系统的索引和搜索性能,降低其使用效率。因此,对于移动视频监控系统中的数据资源应当进行分类,有选择地进行加密或者放入私有“云”中[4]。

4.1.2 SaaS 应用中用户身份信息及日志数据的存取安全问题

SaaS(软件即服务)是一种通过 Internet 提供软件的模式[5]。用户可以直接向提供商租用基于 Web 的软件来管理企业活动,不需要购买、管理和维护软件。通过对 SaaS 的应用,移动视频监控系统用户可以利用网络实现集中存取数据[6],但却也因此降低了对自身数据的控制能力,提高了云数据存取时的安全风险[4]。

因此,对于用户身份信息及日志数据的存取,可以采取以下措施:

1)为了降低黑客的单点攻击成功率,可以将监控系统的数据服务器、Web 服务器和应用服务器相互隔离,从而增加恶意攻击的成本[4]。

2)对于数据库服务器必须进行云备份。当数据被破坏了,就可以通过备份来进行信息修复,从而保证服务的不间断性。

3)对移动视频监控系统绝密数据进行加密存储。当用户需要使用数据时,必须由移动视频监控系统与用户进行身份认证、协商加密算法、交换加密密钥,并且在数据传输时采用传输协议加密,从而保证了数据传输过程的安全性[4]。这样,即使数据被非法获取了,也不一定能被正确识别出来。

另外,由于服务商有时只是通过客户认证标识符,在应用中的逻辑执行层将客户结构化和非结构化数据实现逻辑上的隔离,而实际上却将这两种数据进行了混乱的存储。云服务商进行应用审计或数据存储一旦海量增大,就会导致应用层的管理混乱。因此,SaaS 提供商必须使用安全的虚拟数据存储架构和预防机制,使得软件安全问题在整个开发周期中,一直处于重要地位,从而保证用户在同一个虚拟环境中的安全隔离[4]。

4.2 网络安全问题:视频传输过程中的加密

对于网络的安全,主要考虑到视频传输的安全,其安全威胁可分为被动攻击和主动攻击两类。

1)被动攻击:被动攻击不会造成原数据的更改,因此不容易被发现,具体有以下几种:

(1)窃听:目前,以安全性较低的明文形式进行通信是大部分网络通信的选择,但是这样的方式给攻击者提供了更多的机会,他们只要设法取得数据通信路径就可以轻易地截获明文数据流。而对于网络视频监控系统,攻击者可以直接获得网络中所传输的画面[7]。

(2)流量分析:这里,假设对于网络中传输的重要信息已经进行了加密,攻击者虽然已经截获了信息,但是不能直接查看信息的具体内容。但是,攻击者还是可以通过流量分析来判断出信息的模式。攻击者可以根据流媒体和 RTP 协议的特质来推测出所传视频画面的某些规律性的信息,因为发送静态画面时,流量较小;而发送快速运动画面时,流量则较大[7]。

2)主动攻击。

(1)数据篡改:现在很多网络攻击者可以做到让数据的发送方和接收方都不察觉的情况下,读取数据后,并对数据进行更改。而对于视频监控系统来说,攻击者可以完全更换掉原来的视频,从而给用户带来巨大的损失。

(2)中间人攻击:中间人攻击发生在合法通信对象之间,即通信过程以及通信数据遭到第三方的监视、截取和控制[8]。如果是在网络低层协议下,攻击者可以在通信两端不觉察的情况下,将数据进行重定向,甚至可以获得通信两端的全部信息和通信数据。

(3)主机欺骗:主机欺骗是指攻击者通过 ARP 欺骗或 DNS 欺骗来非法增加节点,使用假冒主机去欺骗合法用户及主机。对于移动视频监控系统而言,攻击者可诱使客户端连接到他设计好的主机上,从而发表虚假视频或者窃取用户信息[7]。

(4)重放攻击:攻击者可以使用协议分析器来截获一个加密数据包,如果攻击者无法解密,他可以制作一个数据包的副本然后再使用协议分析器发给客户端。客户没有意识到并进行了正常的解密,那么攻击者就可以获得解密方法了。对于视频监控系统,攻击者可以查看视频的内容,并且对视频进行掉包、更改等操作[7]。

对于上面出现的问题,将 SSL 和各类加密算法、消息摘要算法和数字签名等结合来解决。SSL 层协议位于应用层和 TCP/IP 之间[9],从上层协议进入该层的数据被加密,并通过 TCP/IP 传送,而当数据到达目的主机,从 TCP/IP 流入之 SSL 层后又被解密,通过为客户端和服务器提供双向认证,对隐私数据的加密,和用数字签名来保证数据完整性,从而提供了一个安全的通信通道。最后提供了以下三个方面的安全服务:

(1)认证:利用数字证书技术和可信任的第三方认证机构,为客户机和服务器之间的通信提供身份认证功能,以便于彼此之间进行身份识别。

(2)机密性:在 SSL 客户机和服务器之间传输的所有数据都经过了加密处理,以防止非法用户进行窃取、篡改和冒充。

(3)完整性:SSL 利用加密算法和 Hash 函数来保证客户机和服务器之间传输的数据的完整性[7]。

4.3 前端安全问题:用户身份验证、授权及审计

通常对计算机信息安全的认识是要保证计算机信息系统中信息的机密性、完整性、可控性、可用性和不可否认性(抗抵赖),简称"五性"。在云环境下的信息安全也不外乎是保证这"五性"。保证这"五性"的安全措施主要有认证、授权与审计,统称为 AAA 或 3A,即英文 Authentication(认证)、Authorization(授权)和 Accounting(审计)。

4.3.1 身份认证

身份认证(Authentication)是系统审查用户身份的过程,从而确定该用户是否具有对某种资源的访问和使用权限,它能够通过标识和鉴别用户的身份,提供一种判别和确认用户身份的机制。身份认证技术在信息安全中处于非常重要的地位,是其他安全机制的基础。只有实现了有效的身份认证,才能保证访问控制、安全审计、入侵防范等安全机制的有效实施[10]。

基于密码的身份认证是最常用也是最容易实现的身份认证机制之一[7]。但是对于密码的设置必须要保证足够的安全性,这里提出几点在使用密码时应当注意的事项:

(1)设置足够长的密码;

(2)不要使用结构简单的词或数字组合;

(3)尽量增加密码的组合复杂度;

(4)使用加密;

(5)定期更换密码。

然而具体到移动视频监控设备的密码安全问题,文中提出应该具备下列安全性:

(1)为了防止攻击者破译密码后直接登录,必须给系统增加其他的认证方式,如物理地址认证。因此,这里采用的是密码和物理地址的双重认证法,从而提高系统的安全性。

(2)为了防止攻击者通过监听网络上传送的信息而获得密码,这里对数据进行加密。

4.3.2 授 权

授权是指当用户或实体的身份被确定为合法后,赋予该用户的系统访问或资源使用权限。只有通过认证的用户才允许访问系统资源,然而在许多情况下当一个用户通过认证后通常不可能赋予访问所有系统资源的权限。

授权是继身份认证之后的又一个常用的安全机制。授权不仅可以预防非法入侵者破坏重要信息,也可以阻止合法用户访问非法信息,在更近的层次上保护数据。

4.3.3 审 计

审计是指所有用户的行为都要留下记录,以便进行核查。所采集的数据主要包括用户名、主机名、时间、操作等[11]。使用审计可以达到用户对自己行为的不可抵赖性。不可抵赖性包括对自己行为的不可抵赖及对行为发生的时间的不可抵赖。用户对资源的访问过程如图 3 所示。

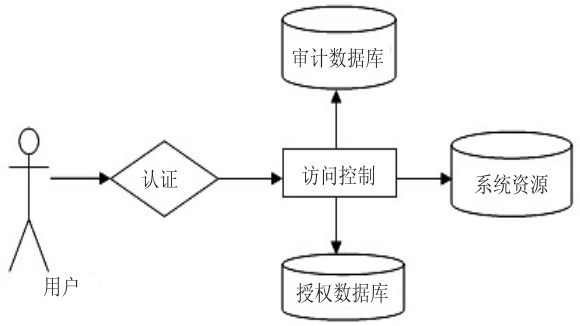

图 3 用户对资源的访问过程

总之,在云环境下移动视频监控设备首先经身份认证阻止一些非法入侵者的访问信息,其次通过授权限制一些非法和合法的用户访问受保护的信息,最后经过审计不仅可以追查相应入侵者的信息,又阻止了用户对自己行为的可抵赖性,从而有针对性地对设备进行安全加固。经过上面三种安全进制的保护,移动视频监控设备在云环境下的安全性得到了一定程度的提高。

5 结束语

云环境下的移动视频监控系统是网络视频监控系统的最新发展方向,但对于此系统的安全问题,很多学者只从单个方面去考虑,没有给出一个多方面的系统安全机制。文中从三个方面来保证移动视频监控系统的安全性。首先在系统的前端将身份认证、授权限制和审计等技术相结合,并在这几个技术的基础上,增加了具有该系统特色的安全保障措施,从而保证了系统的不可入侵性;其次在后台对系统的信息进行分类并对核心机密数据进行加密操作,并且在采用 SaaS 的基础上,结合系统的特点,增加了用户身份信息和日志数据的存取时的安全措施,从而保证了系统信息的安全性;最后在网络安全方面,在采用 SSL 协议的同时,将其与各类加密操作相结合,保证了视频信息传输过程中的安全。通过对这三个方面有针对性地采取措施,并经过实践的验证,云环境下移动视频监控设备的安全性得到了一定的提高。

(下转第 127 页)

usergroup、groupuser 等数据对象的 list 泛型实体类同时,比对功能对象实体类 userPA 的 PrivilegeID 项,存在一个权限就显示一个权限的菜单项。所有权限相关菜单项原本就是存在于 UI 中,通过 userPA 进行比对,来控制其显示还是隐藏。

该系统在 RAD(快速应用开发)工具的支持下,比较快速地完成了 UI 设计。图 4 为角色管理 UI 简图。

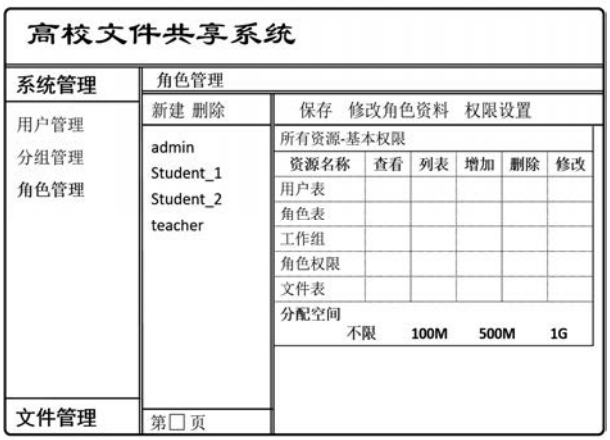

图 4　角色管理 UI 简图

4　结束语

文中通过对基于数据对象的 RBAC 访问模型进行了简化和改进,基于高校文件共享系统的实际需求,设计并解决了文件共享系统中存在的对于不同数据对象具有不同操作权限的分配问题,并将此 RBAC 模型在学校文件共享系统中进行了三层架构的实现。经过测试,证明该 RBAC 模型稳定可靠,三层架构实现了数据操作与逻辑操作的分离,为高校文件共享系统的安全保障在理论和实现上提供了双重的可靠保证。

参考文献:

[1] Luo Junzhou, Ni Xudong, Yong Jianming. A trust degree based access control in grid environments[J]. Information Sciences, 2009, 179(15): 2618-2628.

[2] Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies[J]. ACM Transactions on Information and System Security, 2000, 3(2): 85-106.

[3] Shan Zhiyong. Enforcing Mandatory Access Control in Commodity OS to Disable Malware[J]. Dependable and Secure Computing, 2012, 9(4): 541-555.

[4] 刘宏波,罗　锐,王永斌. 一种采用 RBAC 模型的权限体系设计[J]. 计算机技术与发展,2009,19(9):154-156.

[5] 樊金生,关保灿,李晓东. 基于角色的访问控制扩展模型及其实现[J]. 计算机工程与设计,2008,29(18):4718-4721.

[6] Strembeck M, Mendling J. Modeling process-related RBAC models with extended UML activity models[J]. Information and Software Technology, 2011, 53(5): 456-483.

[7] Ranmswamy C, Sandbu R. Role-based Access Control Features in Commercial Database Management Systems[J]. ACM Trans. on Inf. Syst. Secur., 2001(1): 1-5.

[8] Agrawal R, Ramakrishnan S. Fast algorithms for mining association rules in large databases[C]//Proceedings of the Twentieth International Conference on Very Large Databases. Santiago: ACM Press, 1994: 487-499.

[9] 欧阳凯,沈晴霓,周敬利. 基于 RBAC 模型的同名角色研究与设计[J]. 小型微型计算机系统,2007,28(8):1402-1406.

[10] 吴一民,王玲亚. 扩展角色与权限的 RBAC 访问控制模型[J]. 计算机应用与软件,2008,25(3):192-194.

[11] 冀汶丽. 基于 RBAC 模型的权限管理系统的研究与应用[J]. 微电子学与计算机,2007,24(8):86-88.

(上接第 122 页)

参考文献:

[1] 高海辉. 智能移动视频监控系统的设计与实现[D]. 北京:北京工业大学,2010.

[2] 叶雄杰. 基于云存储的移动视频监控系统研究[D]. 广州:广东工业大学,2011.

[3] Xia Yongquan, Shen Han, Dong Xiangying. The Design of 3G Mobile Video Surveillance System Based on J2ME Platform[J]. Procedia Engineering, 2011, 15: 2423-2427.

[4] 马晓亭,陈　臣. 云安全 2.0 技术体系下数字图书馆信息资源安全威胁与对策研究[J]. 现代情报,2011,31(3):62-66.

[5] 李　波,杨从有,武　浩,等. 云计算环境中 SaaS 的接入控制和调度策略研究[J]. 计算机技术与发展,2012,22(8):9-12.

[6] Kim W, Lee J H. An innovative method for data and software integration in SaaS[J]. Computer and Mathematics with Applications, 2012, 64(5): 1252-1258.

[7] 余　璠. 网络视频监控系统的安全传输研究和实现[D]. 武汉:华中科技大学,2008.

[8] 陈　曦. 基于 IPSec 的 VPN 实现与安全性研究[J]. 无线互联科技,2011(12):18-19.

[9] Oppliger R, Hauser R, Basin D. SSL/TLS session-aware user authentication revisited[J]. Computers and Security, 2008, 27(3): 64-70.

[10] 刘红波. 基于 USBKEY 的身份认证系统的设计[J]. 硅谷,2010(20):59-59.

[11] 乔佩利,李明明. 一种改进的内网用户行为审计模型研究[J]. 哈尔滨理工大学学报,2011,16(5):57-60.

云环境下移动视频监控系统安全性研究

作者： 卞艺杰， 马玲玲， BIAN Yi-jie， MA Ling-ling
作者单位： 河海大学 商学院,江苏 南京,210098

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2013(9)