基于云存储的智能视频监控系统安全风险及应对策略

张雅丽 编著

中国人民公安大学出版社
群 众 出 版 社

基于云存储的智能视频监控系统安全风险及应对策略

张雅丽　编著

中国人民公安大学出版社
群众出版社
·北　京·

图书在版编目（CIP）数据

基于云存储的智能视频监控系统安全风险及应对策略 / 张雅丽编著. —北京：中国人民公安大学出版社，2018.3

2017年度中国人民公安大学优秀学术著作出版项目

ISBN 978-7-5653-3213-5

Ⅰ.①基… Ⅱ.①张… Ⅲ.①视频系统—监控系统—安全风险—风险管理 Ⅳ.①TN948.65

中国版本图书馆CIP数据核字（2018）第029679号

基于云存储的智能视频监控系统安全风险及应对策略

张雅丽 编著

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
印　　刷：北京市泰锐印刷有限责任公司

版　　次：2018年5月第1版
印　　次：2018年5月第1次
印　　张：8.75
开　　本：787毫米×1092毫米　1/16
字　　数：139千字

书　　号：ISBN 978-7-5653-3213-5
定　　价：32.00元

网　　址：www.cppsup.com.cn　www.porclub.com.cn
电子邮箱：zbs@cppsup.com　zbs@cppsu.edu.cn

营销中心电话：010-83903254
读者服务部电话（门市）：010-83903257
警官读者俱乐部电话（网购、邮购）：010-83903253
教材分社电话：010-83903259

前 言

近年来，随着安防视频监控系统规模不断扩大，以及高清视频的大规模应用，人们对视频监控系统中数据存储的规模和应用的复杂程度的要求都在不断提高。为了应对智能视频监控存储系统对容量、扩展性、稳定性和可靠性等方面的要求，运用云存储技术，通过云计算和虚拟化等关键技术实现海量级的存储规模效应和存储空间的弹性扩展，避免了存储资源的浪费，整体可降低建设和维护的成本。

本书主要研究的是基于云存储的智能视频监控系统存在的潜在风险及安全应对策略，从介绍基于云存储的智能视频监控系统的相关概念和关键技术出发，详细分析了云存储架构下智能视频监控数据可能受到的各种安全威胁，以及监控云服务中潜在的各种安全风险，并从安全认证技术、传输加密技术、数据备份与恢复、存储虚拟化安全及管理策略等几方面，分析了相关的应对策略，特别针对云存储的 H. 264 编码视频的特征，专门研究了适用其共享编码视频的安全策略，有效解决了存储资源高效访问的问题及相关的安全隐患。

具体来说，本书的主要特点有以下几个方面：一是科学性强。本书在分析云存储的智能视频监控系统的基础上，吸收了国内外最新的研究成果，全面分析了其存在的安全隐患，并给出了相应的安全策略。二是针对性强。安全是云存储的智能视频监控的关键词，本书针对云存储的高清视频数据如何避免网络化带来的安全隐患、实现安全高效访问和应用提出了积极的技术策略和管理建议。三是服务公安。作为安防视频管理系统信息的最终集散地，存储的压力近年来也随着高清视频监控系统需求的提升而

变得不断增大，尤其当传统的存储模式遇到今天的爆炸式信息发展形势时，使公安在开展视频侦查、视频指挥、视频巡控等实战工作过程中遇到了一些瓶颈，解决好云存储的安全问题将为公共安全视频的健康持续发展提供助力。

本书是中国人民公安大学信息技术与网络安全学院副教授张雅丽结合自身多年在安全防范领域的理论研究和实践调研成果等积累完成的，该研究的相关成果对云存储在公共安全视频监控领域的发展具有积极的参考意义。书中难免有不当之处，敬请读者指出。

编著者
2018 年 3 月

目录

第 1 章　云技术

当前，云计算被认为是继微型计算机、互联网后的第三次 IT 革命，是互联网发展的大趋势。它不仅是互联网技术发展、优化、组合的结果，也为信息化社会带来了全新的商业服务模式，将为人类社会生活带来重大变革。云计算不是纯粹的商业炒作，它的确会改变信息产业的格局，许多人已经用上了 Google Docs 和 Google Apps，用上了许多远程软件，如 Office 字处理，而不是用自己本地机器上安装的这些应用软件。最简单的云计算技术在网络服务中已经随处可见，如搜寻引擎、网络信箱等，使用者只要输入简单指令即能得到大量信息。未来如手机、GPS 等行动装置都可以通过云计算技术发展出更多的应用服务。进一步的云计算不仅可以用做信息的分析搜寻，未来还可以应用于 DNA 结构分析、基因图定序，以及解析癌症细胞等。

云技术可以看作是对计算机网络的一种高级形式的利用。网络速度的发展比以前更快了，增加了如 IPV6 的互联网协议，但基本的 TCP/IP 协议没有变化。云计算的目标就是将这些复杂的协议略去，让它成为计算中心统一管理的内部事务，而终端的计算机会跟电子屏幕一样，没有任何数据分析和处理的功能，仅仅是各种视频或画面的呈现。云计算有了统一的数据管理中心，整体的资源利用率显著提高，不再需要用光盘或 U 盘来拷贝文件了。用户只要能够访问网络，就可以访问授权的所有资源，因此也不需要对文件进行下载和存储管理。在云计算系统中，只要有一台可以连接到网络的设备，就不再需要大型硬件，就可以在任何时间从任何地点访问用户所存储的数据资源，使用户的成本大大降低，而用户则只需要支付一

定的费用。用户的数据资源存储在一个可靠的地方，完全是密封和安全的，计算中心将对它的安全负责，而不需要用户再去考虑它的安全问题。这种云计算的服务模式，将大幅度减少碳的排放量和对周边的影响，用户的数据、应用程序和用户的服务器在用户需要的任何时候都可以使用，完全没有基础设施或者资本开支的问题。因此，云计算具有其他方法无法获得的强大的计算能力。

云计算代表了一个时代发展的需求，也反映了网络发展所带来的变化，只要拥有更为庞大的数据规模和存储运算能力就可以提供更为广阔的信息服务，而软件和硬件的影响相对缩小。云计算的最终目标是把一切资源都拿到网络上，或者说云就是网络。

当众多运行机构分布在全国各地的时候，或者众多人在移动中办公、在家里办公的时候，可以考虑把一些数据和相关的处理需求交给第三方来完成，这样随时随地就可以通过手机或移动电脑等其他设备访问整个网络上的一切资源。所有存储在网络上的数据均可由口令保护，并且能够在整个网络上加密，就像使用本地网络一样去处理任务，因此完全可以由第三方的虚拟化计算机完成，实现最大限度地处理能力，从而减少机构和团体的碳排放量。

云计算领域是与不断增长的 Linux 系统、高性能计算和虚拟化技术等有关的一个领域。超大型计算机和刀片式服务器的发展，以及数据中心的数据处理能力的提高和处理器利用率的提高，这些都已经使云计算成为了现实。云技术的一个主要发展方向是云计算理论和半成熟的理论，如架构即服务，软件即服务，实现将用户的各种应用和功能置于云中。用户可以将一些已经成熟的服务加入云应用中，也可以根据用户的需求将某些系统加入云应用中，实现实时链接。用户也可以将业务流程和功能分割成小的功能块，并与云技术结合，创造和提供一些个性化的业务功能。用户应用架构即服务的云功能可以缩短搭建平台架构的周期，提高整体工作效率。

1.1 云技术的含义

云技术（Cloud technology）即云计算技术，是基于云计算（cloud com-

puting）模式应用的信息处理技术、网络技术、数据管理技术、支撑应用技术等的总称，可以组成庞大的资源池，实现按需所用，同时具有灵活便利的优点。云计算的概念是由 Google 公司提出的，具体可分为狭义和广义两种云计算：狭义的云计算主要是指 IT 基础设施的共享模式，是通过网络实现的按需分配资源，具有易扩展的特性；广义的云计算，主要是指某些服务的共享应用模式，这种服务可以是硬件或软件的服务，或是互联网提供的相关服务，也可以是任意其他的 IT 服务，这种广义的云计算具有超大规模、虚拟化和可靠安全等独特的功能。“云计算”是当前很时尚的一个概念，它既不是一种具体的技术，也不是一种具体的理论，而是一种运营和计算服务模式的体现。

云计算是分布式计算技术的一种，其最基本的概念，是透过网络将庞大的计算处理程序自动分拆成无数个较小的子程序，再交由多部服务器进行处理，这样构成的一个庞大系统，经搜寻、计算分析之后，再将处理结果回传给用户。通过这项云计算技术，网络服务提供者可以在短短的数秒之内达到处理数以千万计甚至亿计信息的计算量，可以达到和“超级计算机”同样强大的网络服务效能。

云计算是多种技术融合发展的产物，具体包括的技术有网格计算（Grid Computing）、分布式计算（Distributed Computing）、并行计算（Parallel Computing）、效用计算、虚拟化、负载均衡、网络存储等。它的主要功能是通过网络将多个不同的资源或成本相对较低的计算实体整合成一个具有强大计算能力的系统，并借助软件即服务（Software as a Service，SaaS）、基础设施即服务（Infrastructure as a Service，IaaS）以及成功的项目群管理（Managing Successful Program，MSP）等先进的服务模式，把强大的计算能力按需分配到终端用户手中。

云计算的一个核心理念就是通过提高数据中心“云”的处理能力，达到减少用户终端处理负担的目的，实现使用户终端简化为一个仅有输入输出功能的设备，并可以按需享受“云”的计算和服务处理能力。

云计算的基本原理是使大量的计算通过分布式计算机来执行，而不需要本地计算机或远程服务器执行，整个云计算系统的数据中心的运行将与互联网相类似，如图 1.1 所示。这使得管理中心可以将不同的资源投入到用户所需要的应用上，并根据用户提出的需求来访问计算机和存储系统。

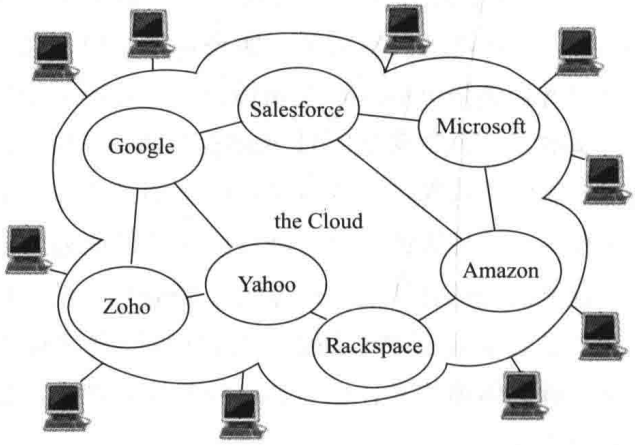

图 1.1　分布式计算机示意图

云是可以实现自我维护和自我管理的虚拟计算资源，通常是一些大型服务器集群，可以包括计算机服务器、存储服务器和宽带资源等。云计算可以将所有的计算资源都集中起来，通过各种软件实现自动管理。云使得应用或服务的提供者无需为很多烦琐的细节而烦恼，可以有精力更加专注于自己的业务，整体有利于实现创新和降低成本。在整个云系统中，用户不需要关心自己所享有的应用和服务来自哪一台服务器或数据来自哪一台存储器。云计算意味着计算能力和信息应用服务也可以与商品一样，通过互联网进行传输，而且成本低廉、使用简便。

1.2　云技术的特性

分布式的网络信息处理技术解决了互联网发展所带来的大量数据存储和处理难题，而物联网的数据量远远超过互联网的数据量，物联网中海量数据的存储与计算处理更加需要云计算技术的支撑。云技术主要具有以下几个特点：

1.2.1　超大规模

大多数云计算中心都具有相当的规模，如 Google 云计算中心已经拥有几百万台服务器，而 Amazon、IBM、Microsoft、Yahoo 等企业所掌握的云计

算规模也毫不逊色，均拥有几十万台服务器。并且云计算中心能通过整合和管理这些数目庞大的计算机集群来赋予用户前所未有的计算和存储能力。

1.2.2　虚拟化

云计算支持用户在任意位置使用各种终端获取应用服务。所请求的资源来自云，而不是固定有形的实体。资源以共享资源池的方式统一管理，利用虚拟化技术，将资源分享给不同用户，资源的放置、管理与分配策略对用户透明。

云计算是基于网络提供的一种服务，只要有网络，使用任何终端（笔记本电脑或手机等），都可以实时连接到云计算服务器去享受云的服务。在享受服务的时候，用户不知道也没必要知道这个服务是由哪台服务器提供的。例如，每天在用 Google 搜索文档的时候，根本不用知道是由 Google 在什么地方的服务器提供的服务，我们只需要知道搜索到的结果就可以了。

1.2.3　高可靠性

云计算中心在软件、硬件的各不同层面采用了数据多副本容错技术、检测技术和计算节点同构可互换等措施，以提高系统服务的可靠性，因此使用云计算比使用本地计算机更可靠。此外，它还可以对设施层采取节能、制冷和网络连接等措施，采用冗余设计来进一步确保服务的高可靠性。由于云计算系统由大量商用计算机组成集群向用户提供数据处理服务，随着计算机数量的增加，系统出现错误的概率大大增加，因而在没有专用的硬件可靠性部件的支持下，需采用软件的方式，即数据冗余和分布式存储来保证数据的可靠性。

1.2.4　通用性和高可用性

云计算不针对特定的应用，云计算中心很少为特定的应用存在，但它有效支持业界的大多数主流应用，并且一个云可以支撑多个不同类型的应用同时运行，在云的支撑下可以构造出千变万化的应用，并保证这些服务的运行质量。

通过集成海量存储和高性能的计算能力，云能提供较高的服务质量。云计算能容忍节点的错误，因它能自动检测失效节点，并将失效节点排除，而不影响系统的正常运行。

1.2.5 高可扩展性

云计算是可以随着用户规模进行扩展的，可以保证支持用户业务的发展。因为用户所使用的云资源可以根据其应用的需要进行调整和动态伸缩，并且再加上前面所提到的云计算中心本身的超大规模，云能够有效地满足应用和用户大规模增长的需要。云计算能够无缝地扩展到大规模的集群之上，甚至包含数千个节点同时处理。

1.2.6 按需服务

云是一个庞大的资源池，它以服务的形式为用户提供应用程序、数据存储、基础设施等资源，用户可以按需购买，就像自来水、电和煤气等公用事业那样，根据用户的使用量计费，无需任何软硬件和设施等方面的前期投入。并且可以根据用户需求，自动分配资源，而不需要系统管理员干预。显然用户可以支付不同的费用，以获得不同级别的服务等。而且服务的实现机制对用户透明，用户无需了解云计算的具体机制就可以获得需要的服务。

1.2.7 经济廉价

由于云的特殊容错措施可以采用廉价的节点来构成云，云的自动化集中式管理具有使大量企业无需负担日益高昂的数据中心管理成本的优势。通常只要花费几百美元、几天时间就能完成以前需要数万美元、数月时间才能完成的任务。显然组建一个采用大量的商业机组成的集群，相对于组建同样性能的超级计算机花费的资金要少很多。

1.2.8 自动化

在云计算中，不论是提供应用服务和计算资源的部署，还是对软硬件的实时管理，主要是通过自动化的方式实现执行和管理，极大地降低了整个云计算数据中心的人力成本。

1.2.9　节能环保

云计算技术将许多分散的、利用率低的、在服务器上工作的各负载整合到云中，以提升系统资源的利用率，而且云数据中心由专业管理团队进行运维，其电源使用效率比普通数据中心强很多，因此这种云计算中心模式能够起到节能环保的作用。

1.2.10　高层次的编程模型

云计算系统提供高层次的编程模型。用户通过简单学习就可以编写自己的云计算程序，在云系统上执行，满足自己的需求。

1.2.11　完善的运维机制

在云计算数据中心端有最专业的团队来帮用户维护、存储和管理数据信息。同时，采取严格的权限管理策略，以保证这些数据的安全。这种完善的运维机制可以使用户享受到最专业的服务。

1.2.12　资源配置动态化

云计算根据消费者的需求动态划分或释放不同的物理和虚拟资源，当增加一个需求时，可通过增加可用的资源进行匹配，实现资源的快速弹性提供；当用户不再使用这部分资源时，可释放这些资源。云计算为客户提供的这种能力是无限的，实现了IT资源利用的可扩展性。

1.2.13　以网络为中心

云计算的组件和整体构架由网络连接在一起并存在网络中，同时通过网络向用户提供服务。用户可借助不同的终端设备，通过标准的应用实现对网络的访问，从而使得云计算的服务无处不在。

1.2.14　资源的池化和透明化

对云服务的提供者而言，各种底层资源（如计算、储存、网络、资源逻辑等）的异构性被屏蔽，边界被打破，所有的资源可以被统一管理和调度，成为所谓的“资源池”，从而为用户提供按需服务；对用户而言，这

些资源是透明的、无限大的，用户无需了解内部结构，只关心自己的需求是否得到满足即可。

此外，云计算还以其部署迅速、资源利用率高、易管理、几乎可以提供无限的廉价存储和计算能力等特性深受市场关注。

这些特点使得云计算能为用户提供更方便的体验，它为人们解决大规模计算、资源存储等问题提供了一条新的途径。正因为如此，云计算才能脱颖而出，并被业界推崇。

1.3 云计算技术发展面临的问题及发展方向

1.3.1 云计算技术发展面临的主要问题

尽管云计算模式具有许多优点，但是也存在下列一些问题。

（1）云元的问题

云计算的云由云元构成。由于云在未来的应用场景广阔，而云元是构建云的关键部件，因此对云元设备的研究和制造、设备规范和接口规范，都应该高度重视。云元能否支撑以后的应用是个大问题。设计云元的时候，面临着几点困惑：高端的云元如何支持低端云元的应用？低端云元支持高端应用的条件是什么？如何设计云元，以适应今后的发展？

（2）网络传输及宽带网络的问题

云计算服务依赖网络，目前网速低且不稳定，使云应用的性能不高。因此，云计算的普及依赖网络技术的发展，并且云元之间、云元和用户之间，需要高速宽带网络来连接。因此如果没有宽带网络就没有云。

目前，云元和云元之间靠得很近，一般认为靠高速交换机即可，但实际云元之间要求高速并行总线才行，但目前网络设备还无法完全满足此要求。当云元之间离得很远的时候就需要广域网来连接，而目前的广域网无法实现高速、无阻塞、全交换的连接。因此，广域网将会是云计算中的一个很大的技术难题。

（3）数据安全与数据隐私问题

在云计算系统中，用户数据存储在云端，如何保证用户的数据不被非法

访问和泄露是系统必须要解决的重要问题，即数据的安全和隐私问题。目前，互联网数据中心 IDC（Internet Data Center）中云的技术应用得最广泛、效果最明显。因此，从 IDC 入手讨论云的安全问题比较有价值。IDC 的安全问题有两部分：一部分是 IDC 本身的安全问题，另一部分是由于云技术的引入而带来的安全问题，应把这两者分清楚。用户在 IDC 中存放数据的安全性问题和数据私密性问题，无论用传统技术还是云技术并无本质差别，其主要差别在于数据虚拟化的过程，这当中包括了计算能力的虚拟化。

由于有些数据是企业的商业机密，数据的安全性关系到企业的生产和发展。因此，云计算数据的安全性问题解决不了，会影响云计算在企业中的应用。如何保证存放在云服务提供商的数据隐私不被非法利用，不仅需要技术的改进，也需要法律的进一步完善。

（4）资源池与资源虚拟化技术问题

云的弹性好坏，取决于资源池算法的优劣，算法也是云计算技术的核心所在。该技术分为时分技术和空分技术。其中，时分技术在计算机操作系统中被广泛应用，在云计算中也得到广泛使用。但虚拟化技术除了采用时分技术还将采用空分技术，而通信中还有频分、码分、波分技术。从技术角度分析，当前的 IT 资源虚拟化方面这些技术很难被使用。目前看来，在云计算中的虚拟化技术，主要也就是时分技术和空分技术。

（5）云计算系统的管理问题

云计算系统本身的可扩展性、可用性、可靠性、可管理性等都是要重点解决的问题，在服务的层次上，云计算系统必须解决服务的描述及转换问题。如何将用户的业务理念需求转换成对基础设施的需求，如何确定高层的服务需求和度量到基础设施的需求到度量之间的映射，如何保证多级别的 QoS，这些都是云计算系统要解决的问题。

在云计算系统的管理方面，云系统之间的互操作是必须要考虑的一个问题。当一个云系统需要使用另一个云系统的计算资源时，要能够提供跨云的管理策略，从而使得云系统之间能够自动交互。同时为了保证 SLA（Service－Level Agreement），系统必须能够进行 SLA 的监测，当有服务失败时，能自动地进行资源重新分配。在基础设施层次上，云计算系统要能够进行服务的动态迁移，目前的虚拟机只支持共享存储的迁移，如何将虚拟机迁移到没有共享存储的其他物理主机上也是云计算系统面临的挑战之一。

（6）用户使用习惯问题

在云计算环境下，用户的使用观念也需发生彻底的变化，即实现从“购买产品”到“购买服务”的转变。因为他们直接面对的将不再是复杂的硬件和软件而是最终的服务。

由于云计算把连接“显示器”和“主机”的电线变成了网络，把“主机”变成云服务提供商的服务器集群了，因此，如何改变用户的使用习惯，使用户适应网络化的软硬件应用是长期而艰巨的挑战。

（7）云计算系统的标准化问题

现有的云计算系统的部署相对分散，各自内部能够实现虚拟内存的自动分配、管理和容错等，但云计算系统之间的交互还没有统一的标准。在云计算系统的标准化方面，还有一系列亟待解决的问题。

1.3.2 云计算技术的发展方向

云计算技术存在的上述问题，是今后云计算技术领域必须要研究解决好的问题，否则将阻碍云计算技术的发展。据此，结合云计算技术本身的发展，笔者认为，其发展方向可归纳为下述几点。

（1）健全云计算的法律法规及其标准规范

云计算技术的应用与推广，需要政府政策的支持。对于政府来说，一个运转良好的云计算公共服务平台不仅可带动区域软件产业的发展，还能吸引更多的商业投资，促进地方经济的发展，有助于政府与企业实现共赢。

而由于云计算是新生事物，其特点就是用户将自己的基础设施、数据、应用都托管在运营商的平台上，而云平台又是以池化资源的方式组织的，其传统的用户、应用、设备、地理等边界都被打破。因此，一旦发生安全事故、服务中断等意外，如何溯源、定损，如何界定运营商与用户的责任，这些都需要相关的法律法规进行规范。并且要满足什么条件才能成为运营商，境外云运营商如何在国内落地，在运营过程中如何对运营商进行有效监管等，这些也都离不开相应的法律法规规定。

众所周知，标准化工业是相当重要的，何况云计算的标准化工业尚处于起步阶段。云计算核心技术和服务标准，云互操作性及接口标准，云存储、云安全的标准，云测试基准，以及云计算环境的管理与互操作性等，