项目五　应用层安全技术

- 5.1　云计算安全
- 5.2　中间件安全
- 5.3　数据安全
- 5.4　数据隐私保护
- 5.5　位置隐私保护
- 5.6　轨迹隐私保护
- 5.7　本章小结

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

1. 云计算思想的产生

传统模式下，企业建立一套 IT 系统不仅仅需要购买硬件等基础设施，还有买软件的许可证，需要专门的人员维护。当企业的规模扩大时还要继续升级各种软硬件设施以满足需要。对于企业来说，计算机等硬件和软件本身并非他们真正需要的，它们仅仅是完成工作、提供效率的工具而已。对个人来说，电脑需要安装许多软件，而许多软件是收费的，对不经常使用该软件的用户来说购买是非常不划算的。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

可不可以有这样的服务，能够提供我们需要的所有软件供我们租用？这样我们只需要在用时付少量“租金”即可“租用”到这些软件服务，为我们节省许多购买软硬件的资金。

我们每天都要用电，但我们不是每家自备发电机，它由电厂集中提供；我们每天都要用自来水，但我们不是每家都有井，它由自来水厂集中提供。这种模式极大得节约了资源，方便了我们的生活。面对计算机给我们带来的困扰，我们可不可以像使用水和电一样使用计算机资源？这些想法最终导致了云计算的产生。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

云计算的最终目标是将计算、服务和应用作为一种公共设施提供给公众，使人们能够像使用水、电、煤气和电话那样使用计算机资源。

云计算模式即为电厂集中供电模式。在云计算模式下，用户的计算机会变的十分简单，或许不大的内存、不需要硬盘和各种应用软件，就可以满足我们的需求，因为用户的计算机除了通过浏览器给“云”发送指令和接受数据外基本上什么都不用做便可以使用云服务提供商的计算资源、存储空间和各种应用软件。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

这就像连接“显示器”和“主机”的电线无限长，从而可以把显示器放在使用者的面前，而主机放在远到甚至计算机使用者本人也不知道的地方。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。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

在云计算环境下，用户的使用观念也会发生彻底的变化：从“购买产品”到“购买服务”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。用户不需要拥有看得见、摸得着的硬件设施，也不需要为机房支付设备供电、空调制冷、专人维护等等费用，并且不需要等待漫长的供货周期、项目实施等冗长的时间，只需要把钱汇给云计算服务提供商，我们将会马上得到需要的服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

2. 云计算的概念

云计算是一种新兴的商业计算模型，它利用高速互联网的传输能力，将数据的处理过程从个人计算机或服务器转移到一个大型的计算中心，并将计算能力、存储能力当作服务来提供，就如同电力、自来水一样按使用量进行计费。

云计算基本原理是计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，从而使企业数据中心的运行与互联网相似。这使企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

云计算的核心是新一代数据中心技术，包括绿色 IT 、高性能（网格）计算、分布式计算以及数据中心虚拟化等。云计算作为传统计算机技术与网络融合的产物，可以将各类资源以服务的形式向用户提供，具有可虚拟化性、动态性和可伸缩性，被认为是信息产业的又一次重大革命。虚拟化及虚拟机概念是 20 世纪 60 年代由 IBM 提出，主要通过将有限的固定的资源根据不同需求进行重新规划以达到简化管理，优化资源的目的。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

“云”是一些可以自我维护和管理的虚拟计算资源，通常为一些大型服务器集群，包括计算服务器、存储服务器、 web 服务器、宽带资源等等。云计算将所有的计算资源集中起来，并由软件实现自动管理，无需人为参与。这使得应用提供者无需为繁琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。有人打了个比方：这就好比是从古老的单台发电机模式转向了电厂集中供电的模式。它意味着计算能力也可以作为一种商品进行流通，就像煤气、水电一样，取用方便，费用低廉。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

最大的不同在于，它是通过互联网进行传输的。云计算是并行计算（ Parallel Computing ）、分布式计算（ Distributed Computing ）和网格计算（ Grid Computing ）的发展，是虚拟化（ Virtualization ）、效用计算（ Utility Computing ）、 IaaS （基础设施即服务）、 PaaS （平台即服务）、 SaaS （软件即服务）等概念混合演进并跃升的结果。云计算是网格计算的商业演化版。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

目前，云计算并没有统一的定义，这也与云计算本身特征很相似。维基百科对云计算的定义是：云计算是一种基于互联网的计算新方式，通过互联网上异构、自治的服务为个人和企业提供按需即取的计算。由于资源是在互联网上，而互联网通常以云状图案来表示，因此以云来类比这种计算服务，同时云也是对底层基础设施的一种抽象概念。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

云计算的资源是动态扩展且虚拟化的，通过互联网提供，终端用户不需要了解云中基础设施的细节，不必具有专业的云技术知识，也无需直接进行控制，只关注自身真正需要什么样的资源以及如何通过网络来获得相应的服务。关于云计算的描述，在当前具有的共同特征是：云是一种服务，类似水电一样，按需使用、灵活付费，使用者只关注服务本身。 H3C 的云计算理念认为云计算是一种新的 IT 服务模式，支持大规模计算资源的虚拟化，提供按需计算、动态部署、灵活扩展能力。

项目五　应用层安全技术

5.1　云计算安全

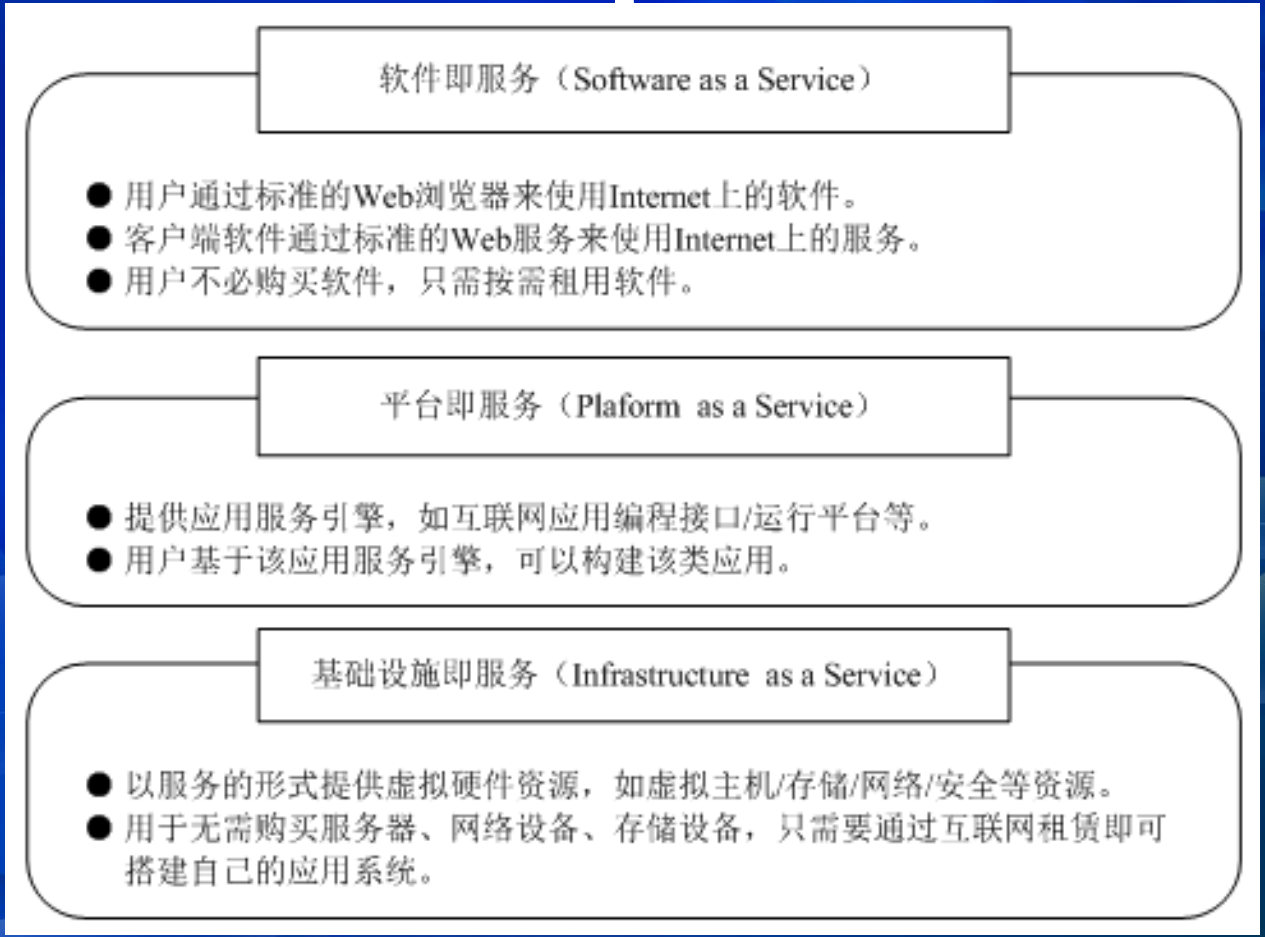

图 6-1　云计算服务模式

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

3. 云计算的服务模式

云计算平台包括图 6-1 所示的三种典型服务模式：

① 基础设施即服务（ Iaas ， Infrastructure as a Service ）

基础设施即服务指的是为用户提供网络、计算和存储一体化的基础架构服务，通过 Iaas 服务，客户端无须购买服务器、软件等网络设备，即可任意部署和使用存储、网络和其它基本的计算资源。在 Iaas 服务中，用户不能控制底层的基础设施，但是可以控制操作系统、储存装置和已部署的应用程序。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

在 IaaS 中，一台物理机器往往被划分为多台虚拟机器进行使用。由于同一物理服务器的虚拟机之间可以相互访问，而不需要经过之外的防火墙与交换机等设备，因此虚拟机之间的攻击变得更加容易。另外，服务商提供的是一个共享的基础设施，例如 CPU 缓存、 GPU 等，这些基础设施对使用者来说并不是完全隔离的，当一个攻击者得逞时，全部服务器都向攻击者敞开了大门，因此对 Iaas 服务的分区和服务环境监控是云安全中的重要研究领域，如何保证同一物理机上不同虚拟机之间的资源隔离，包括 CPU 调度、内存虚拟化、 VLAN 、 I/O 设备虚拟化之间，是当前 IaaS 服务模式下首要解决的安全技术问题。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

② 平台即服务（ Paas ， Platform as a Service ）

把服务器平台或者开发环境作为一种服务提供的商业模式。 PaaS 实际上是指将软件研发的平台作为一种服务，具体可以归类为应用服务器、业务能力接入、业务引擎、企业进行定制化研发的中间件平台等，通过 PaaS 提供的 API 开放给 PaaS 用户。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

PaaS 可以提高在 Web 平台上利用的资源数量。例如，可通过远程 Web 服务使用数据即服务（ Data-as-a-Service ：数据即服务）。用户或者厂商基于 PaaS 平台可以快速开发自己所需要的应用和产品。同时， PaaS 平台开发的应用能更好地搭建基于 SOA 架构的企业应用，如云平台通过提供二次开发接口、软件定制接口等功能以及开放式的支撑服务功能，提供完善的应用服务引擎和应用编程接口，用户能通过应用服务引擎，无需专业程序员，直接在线开发相应的企业应用。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

③ 软件即服务（ Saas ， Software as a Service ）

软件即服务与“ on-demand software”（按需软件）， the application service provider （ ASP ，应用服务提供商）， hosted software （托管软件）具有相似的含义。它是一种通过 Internet 提供软件的模式，厂商将应用软件统一部署在自己的服务器上，客户可以根据自己实际需求，通过互联网向厂商定购所需的应用软件服务，按定购的服务多少和时间长短向厂商支付费用，并通过标准的 Web 浏览器来使用云平台上的各类在线服务

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

用户不必购买软件，只需按需租用云平台上的各类正版软件和在线软件服务功能，且无需对软件进行维护，服务提供商会全权管理和维护软件，软件厂商在向客户提供互联网应用的同时，也提供软件的离线操作和本地数据存储，让用户随时随地都可以使用其定购的软件和服务。

对于许多小型企业来说，SaaS 是采用先进技术的最好途径，它消除了企业购买、构建和维护基础设施和应用程序的需要，减少了企业运维和购买软件的成本。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

4. 云计算部署模式

在部署模式上，云计算有三种模式，如图 6-2 所示。

① 公共云

公共云是指为外部客户提供服务的云，它所有的服务是供别人使用，而不是自己用。目前，典型的公共云有微软的 Windows Azure Platform 、亚马逊的 AWS 、 Salesforce.com ，以及国内的阿里巴巴、用友伟库等。对于使用者而言，公共云的最大优点是，其所应用的程序、服务及相关数据都存放在公共云的提供者处，自己无需做相应的投资和建设。

项目五　应用层安全技术

5.1　云计算安全

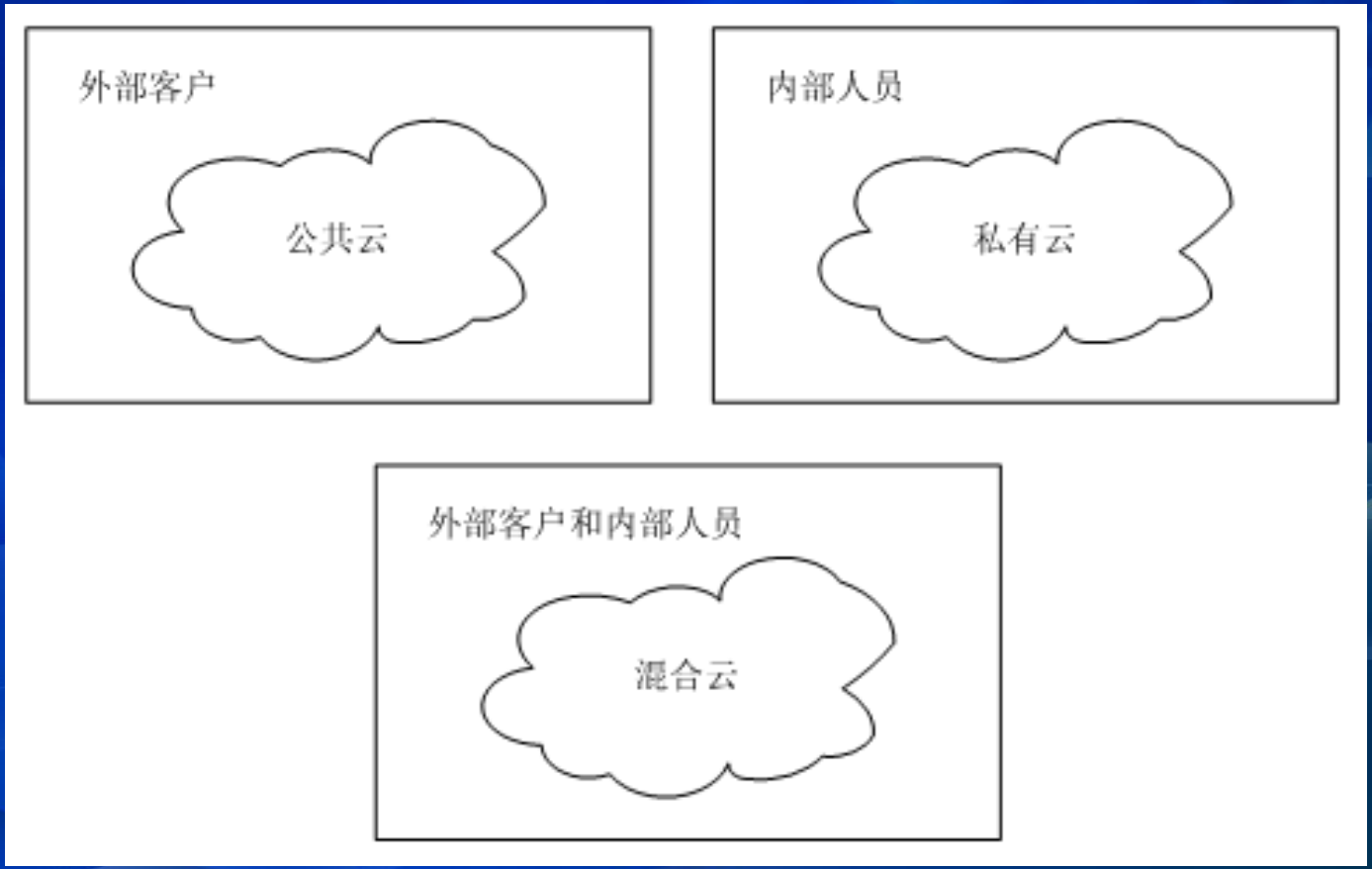

图 6-2　云计算的三种部署模式

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

② 私有云

私有云是指企业自己使用的云，它所有的服务不是供别人使用，而是供自己内部人员或分支机构使用。私有云的部署比较适合于有众多分支机构的大型企业或政府部门。随着这些大型企业数据中心的集中化，私有云将会成为他们部署 IT 系统的主流模式。相对于公共云，私有云部署在企业自身内部，因此其数据安全性、系统可用性都可由自己控制。但其缺点是投资较大，尤其是一次性的建设投资较大。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

③ 混合云

混合云是指供自己和客户共同使用的云，它所提供的服务既可以供别人使用，也可以供自己使用。相比较而言，混合云的部署方式对提供者的要求较高。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

5. 云计算的发展

云计算从 1959 年概念的提出到今天的初步成熟，已经经历了几十年的发展历程。

1959 年， ChristopherStrachey 发表虚拟化论文，虚拟化是今天云计算基础架构的基石。

1961 年， JohnMcCarthy 提出计算力和通过公用事业销售计算机应用的思想。

1962 年， J.C.R.Licklier 提出“星际计算机网络”设想。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

1984 年， Sun 公司的联合创始人 JohnGage 提出“网络就是计算机”的名言，用于描述分布式计算技术带来的新世界，今天的云计算正在将这一理念变成现实。

1997 年，南加州大学教授 RamnathK.Chellappa 提出云计算的第一个学术定义”，认为计算的边界可以不是技术局限，而是经济合理性。

1998 年， VMware （威睿公司）成立并首次引入 X86 的虚拟技术。

1999 年， MarcAnreessen 创建 LouClou ，是第一个商业化的 IaaS 平台。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

2004 年， Google 发布 MapReuce 论文。 Hadoop 就是 Google 集群系统的一个开源项目总称，主要由 HFS 、 MapReuce 和 Hbase 组成，其中 HFS 是 GoogleFileSystem （ GFS ）的开源实现；MapReuce 是 GoogleMapReuce 的开源实现； HBase 是 GoogleBigTable 的开源实现。

2005 年， Amazon 宣布 Amazon Web Services 云计算平台，并在 2006 年相继推出在线存储服务 S3 和弹性计算云 EC2 等云服务。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

2007 年， Google 与 IBM 在大学开设云计算课程。戴尔成立数据中心解决方案部门，先后为全球 5 大云计算平台中的三个（包括 WinowsAzure 、 Facebook 和 Ask.com ）提供云基础架构。亚马逊公司推出了简单队列服务（ SimpleQueueService ， SQS ），这项服务使托管主机可以存储计算机之间发送的消息。IBM 首次发布云计算商业解决方案，推出”蓝云”（ BlueClou ）计划。

2008 年， Salesforce.com 推出了随需应变平台 evForce, Force.com 平台是世界上第一个平台即服务的应用。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

2009 年，思科发布统一计算系统（ UCS ）、云计算服务平台， VMWare 推出业界首款云操作系统 Vmware vSphere 4, Google 推出 Chrome OS 操作系统。

2010 年 , Microsoft 正式发布 Microsoft Azure 云平台服务。英特尔在 IDF 上提出互联计算，用 X86 架构统一嵌入式、物联网和云计算领域。戴尔推出源于 DCS 部门设计的 PowerEdgeC 系列云计算服务器及相关服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

在我国，云计算的发展也颇为迅猛。

2008 年 3 月 17 日， Google 全球 CEO 埃里克•斯密特（ Eric Schmidt ）在北京访问期间，宣布在中国大陆推出“云计算（ Cloud Computing ）”计划。而 2008 年初， IBM 与无锡市政府合作建立了无锡软件园云计算中心，开始了云计算在中国的商业应用。 2008 年 7 月份瑞星推出了“云安全”计划。

2009 年， VMware 在中国召开的 vForum 用户大会，第一次将开放云计算的概念带入中国。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

2010 年 10 月 18 日发布《国务院关于加快培育和发展战略性新兴产业的决定》中，将云计算定位于“十二五”战略性新兴产业之一。同一天，工信部、发改委联合印发《关于做好云计算服务创新发展试点示范工作的通知》，确定在北京、上海、深圳、杭州、无锡等五个城市先行开展云计算服务创新发展试点示范工作，让国内的云计算热潮率先从政府云开始熊熊燃烧。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

云计算在中国有些巨大的市场潜力，不仅仅在于中国幅员辽阔，人口众多。更重要的是中国从 2009 年已经成为全球最大的 PC 消费国，也会成为最大的 PC 服务器拥有国。庞大的 IT 投资也成为国家节能减排中值得重点关注的一环，云计算将成为绿色 IT 、节能减排最为重要的手段，提高了 IT 灵活性和可持续发展，也将积极推动和谐社会的构建，这也是为什么政府在“十二五”规划中为什么将云计算定位为战略性新兴产业的原因之一。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

云计算作为一种应用模式，它的出现和应用范围日益扩大，必将对产业链的上下游产生重要影响，它在不断的适应着企业的需求。未来云计算的发展，将朝着平台化、公共云和混合云、大数据等方向发展，未来的云计算将更强调安全性和性能，云游戏的领域也将会是云的另一个主要的发展趋势。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

5. 云计算平台简介

目前，比较优秀的云计算平台主要包括： Google 云计算平台、 IBM” 蓝云” 云计算平台、 Amazon 的弹性计算云、微软的云计算架构等。

① Google 云计算平台

Google 云计算平台是全球最大的搜索引擎，包括： Google Maps 、 Google Earth 、 Gmail 、 YouTube 等一系列产品，这个平台先是为 Google 最重要的搜索应用提供服务，现在已经扩展到其他应用程序，其特点是数据量庞大、面向全球用户提供实时服务。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

Google 的硬件条件优势、大型的数据中心和搜索引擎的支柱应用，促进 Google 云计算迅速发展。 Google 的云计算基础架构模式包括 4 个相互独立又紧密结合在一起的系统：Google File Systemt 分布式文件系统，针对 Google 应用程序的特点提出的 MapReduce 编程模式，分布式的锁机制 Chubby 以及 Google 开发的模型简化的大规模分布式数据库 BigTable 。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

Google File System 文件系统（ GFS ）：除了性能，可伸缩性、可靠性以及可用性以外， GFS 设计还受到 Google 应用负载和技术环境的影响。体现在 4 个方面： 1 ）充分考虑到大量节点的失效问题，需要通过软件将容错以及自动恢复功能集成在系统中 ;2 ）构造特殊的文件系统参数，文件通常大小以 G 字节计，并包含大量小文件 ;3 ）充分考虑应用的特性，增加文件追加操作，优化顺序读写速度 ;4 ）文件系统的某些具体操作不再透明，需要应用程序的协助完成。

图 6-3 给出了 Google File System 的系统架构。

项目五　应用层安全技术

5.1　云计算安全

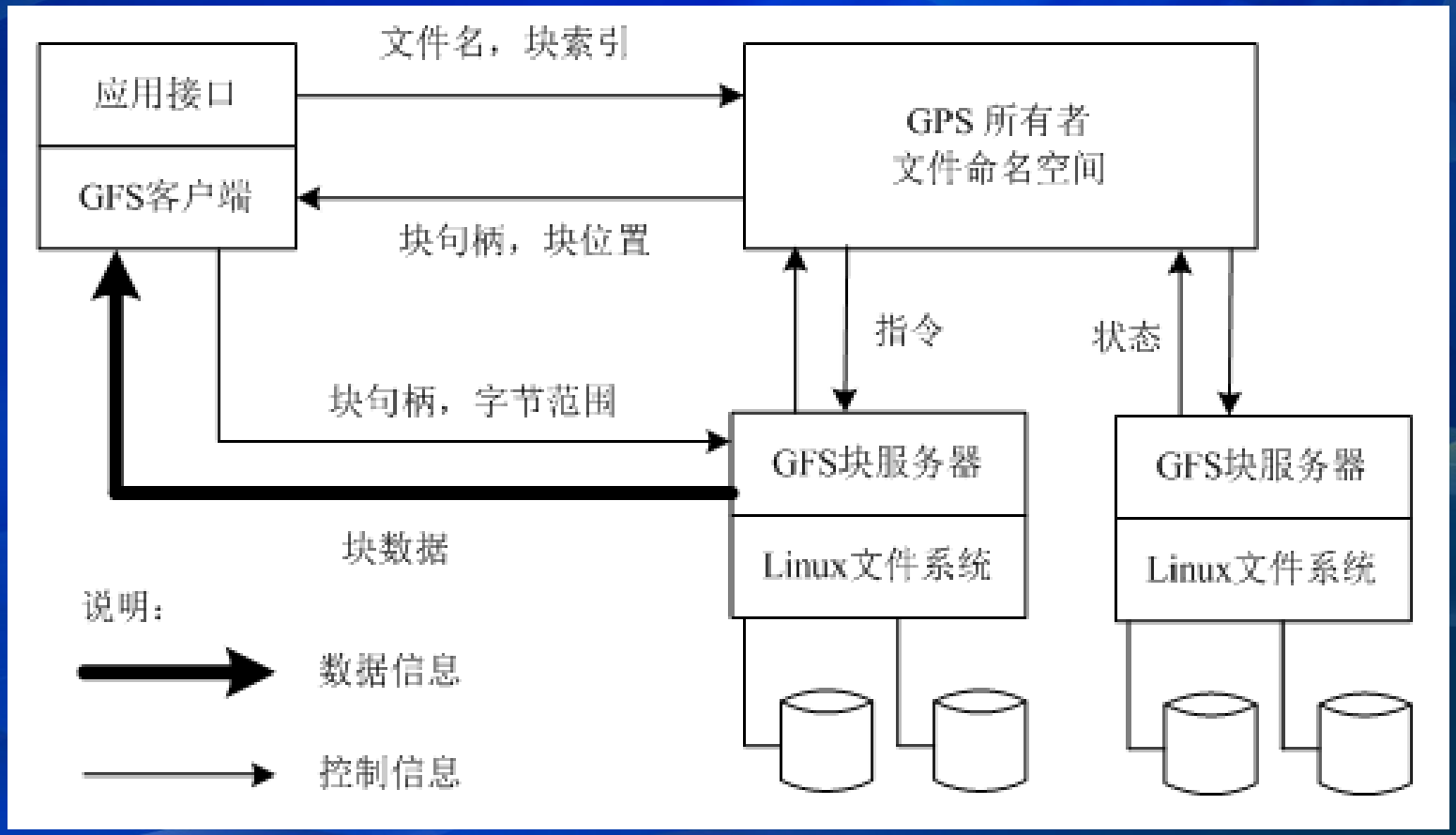

图 6-3　Google File System

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

一个 GFS 集群包含一个主服务器和多个块服务器，被多个客户端访问。文件被分割成固定尺寸的块。在每个块创建的时候，服务器分配给它一个不变的、全球惟一的 64 位块句柄对它进行标识。块服务器把块作为 linux 文件保存在本地硬盘上，并根据指定的块句柄和字节范围来读写块数据。为了保证可靠性，每个块都会复制到多个块服务器上，缺省保存三个备份。主服务器管理文件系统所有的元数据，包括名字空间、访问控制信息和文件到块的映射信息，以及块当前所在的位置。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

GFS 客户端代码被嵌入到每个程序里，它实现了 Google 文件系统 API ，帮助应用程序与主服务器和块服务器通信，对数据进行读写。客户端跟主服务器交互进行元数据操作，但是所有的数据操作的通信都是直接和块服务器进行的。客户端提供的访问接口类似于 POSIX 接口，但有一定的修改，并不完全兼容 POSIX 标准。通过服务器端和客户端的联合设计， Google File System 能够针对它本身的应用获得最大的性能以及可用性效果。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

Map Reduce 分布式编程环境： Google 构造 Map Reduce 编程规范来简化分布式系统的编程。应用程序编写人员只需将精力放在应用程序本身，而关于集群的处理问题，包括可靠性和可扩展性，则交由平台来处理。 MapReduce 通过“ Map （映射）”和“ Reduce （化简）”这样两个简单的概念来构成运算基本单元，用户只需提供自己的 Map 函数以及 Reduce 函数即可并行处理海量数据。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

分布式的大规模数据库管理系统 BigTable ：由于一部分 Google 应用程序需要处理大量的格式化以及半格式化数据， Google 构建了弱一致性要求的大规模数据库系统 Big Tablet 。 Big Table 的应用包括 Search History ， Maps ， Orkut ， RSS 阅读器等。

Big Table 是客户端和服务器端的联合设计，使得性能能够最大程度地符合应用的需求。 Big Table 系统依赖于集群系统的底层结构。一个是分布式的集群任务调度器，一个是前述的 Google 文件系统，还有一个分布式的锁服务 Chubby 。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

Chubby 是一个非常鲁棒的粗粒度锁， Big Table 使用 Chubby 来保存根数据表格的指针，即用户可以首先从 Chubby 锁服务器中获得根表的位置，进而对数据进行访问。 Big Table 使用一台服务器作为主服务器，用来保存和操作元数据。主服务器除了管理元数据之外，还负责对 tablet 服务器（即一般意义上的数据服务器）进行远程管理与负载调配。客户端通过编程接口与主服务器进行元数据通信，与 tablet 服务器进行数据通信。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

② IBM“蓝云”云计算平台

“蓝云”解决方案是由 IBM 云计算中心开发的企业级云计算解决方案。该解决方案可以对企业现有的基础架构进行整合，通过虚拟化技术和自动化技术，构建企业自己拥有的云计算中心，实现企业硬件资源和软件资源的统一管理、统一分配、统一部署、统一监控和统一备份，打破应用对资源的独占，从而帮助企业实现云计算理念。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

IBM 的“蓝云”计算平台是一套软、硬件平台，将 Internet 上使用的技术扩展到企业平台上，使得数据中心使用类似于互联网的计算环境。“蓝云”大量使用了 IBM 先进的大规模计算技术，结合了 IBM 自身的软、硬件系统以及服务技术，支持开放标准与开放源代码软件。

“蓝云”基于 IBM Almaden 研究中心的云基础架构，采用了 Xen 和 PowerVM 虚拟化软件， Linux 操作系统映像以及 Hadoop 软件（ Google File System 以及 MapReduce 的开源实现）。 IBM 已经正式推出了基于 x86 芯片服务器系统的“蓝云”产品。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

“蓝云”计算平台由一个数据中心、IBM Tivoli 部署管理软件（Tivoli provisioning manager）、IBM Tivoli 监控软件（IBM Tivoli monitoring）、IBM WebSphere 应用服务器、IBM DB2 数据库以及一些开源信息处理软件和开源虚拟化软件共同组成。“蓝云”的硬件平台环境与一般的 x86 服务器集群类似，使用刀片的方式增加了计算密度。“蓝云”软件平台的特点主要体现在虚拟机以及对于大规模数据处理软件 Apache Hadoop 的使用上。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

“蓝云”平台的一个重要特点是虚拟化技术的使用。虚拟化的方式在“蓝云”中有两个级别，一个是在硬件级别上实现虚拟化，另一个是通过开源软件实现虚拟化。硬件级别的虚拟化可以使用 IBM p 系列的服务器，获得硬件的逻辑分区 LPAR （ logic partition ）。逻辑分区的 CPU 资源能够通过 IBM Enterprise Workload Manager 来管理。通过这样的方式加上在实际使用过程中的资源分配策略，能够使相应的资源合理地分配到各个逻辑分区。 p 系列系统的逻辑分区最小粒度是 1/10 颗 CPU 。 Xen 则是软件级别上的虚拟化，能够在 Linux 基础上运行另外一个操作系统。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

③ Amazon 的弹性计算云

亚马逊是互联网上最大的在线零售商，但是同时也为独立开发人员以及开发商提供云计算服务平台。亚马逊将他们的云计算平台称为弹性计算云（ Elastic Compute Cloud ， EC2 ），它是最早提供远程云计算平台服务的公司。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

③ Amazon 的弹性计算云

与 Google 提供的云计算服务不同， Google 仅为自己在互联网上的应用提供云计算平台，独立开发商或者开发人员无法在这个平台上工作，因此只能转而通过开源的 Hadoop 软件支持来开发云计算应用。亚马逊的弹性计算云服务也和 IBM 的云计算服务平台不一样，亚马逊不销售物理的云计算服务平台，没有类似于“蓝云”一样的计算平台。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

亚马逊将自己的弹性计算云建立在公司内部的大规模集群计算的平台之上，而用户可以通过弹性计算云的网络界面去操作在云计算平台上运行的各个实例（ Instance ），付费方式则由用户的使用状况决定，即用户仅需要为自己所使用的计算平台实例付费，运行结束后计费也随之结束。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

弹性计算云从沿革上来看，并不是亚马逊公司推出的第一项这种服务，它由名为亚马逊网络服务的现有平台发展而来。早在 2006 年 3 月，亚马逊就已经发布了简单存储服务（ Simple Storage Service ， S3 ），这种存储服务按照每个月类似租金的形式进行服务付费，同时用户还需要为相应的网络流量进行付费。亚马逊网络服务平台使用 REST （ Representational State Transfer ）和简单对象访问协议（ SOAP ）等标准接口，用户可以通过这些接口访问到相应的存储服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

2007 年 7 月，亚马逊公司推出了简单队列服务（ Simple Queue Service ， SQS ），这项服务使托管主机可以存储计算机之间发送的消息。通过这一项服务，应用程序编写人员可以在分布式程序之间进行数据传递，而无须考虑消息丢失的问题。通过这种服务方式，即使消息的接收方还没有模块启动也没有关系。服务内部会缓存相应的消息，而一旦有消息接收组件被启动运行，则队列服务将消息提交给相应的运行模块进行处理。同样的，用户必须为这种消息传递服务进行付费使用，计费的规则与存储计费规则类似，依据消息的个数以及消息传递的大小进行收费。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

④ 微软的云计算架构

微软最新发布的服务器和云平台网站已经可以提供包括管理云应用、部署服务器等多种功能在内的一站式云服务。除了可为消费者构建私有云外，该网站还提供虚拟服务器、虚拟桌面、管理云应用、部署服务器、管理员身份认证、数据分析等服务。

此外，用户还可以从该网站浏览新闻、查看微软最新产品、公告等，实现量身定制的个性上网方案。

项目五　应用层安全技术

5. 1　云计算安全

5.1.1　云计算概述

基于图 6-4 的架构，微软为企业提供两种云计算部署类型，即公共云和私有云。

公共云：由微软自己运营，为客户提供部署和应用服务。在公共云中， Windows Azure Platform 是一个高度可扩展的服务平台，提供基于微软数据中心随用随付费的灵活的服务模式。

私有云：部署在客户的数据中心内部，基于客户个性化的性能和成本要求、面向服务的内部应用环境。这个云平台基于成熟的 Windows Server 和 System Center 等系列产品，并且能够与现有应用程序兼容。

项目五　应用层安全技术

5.1　云计算安全

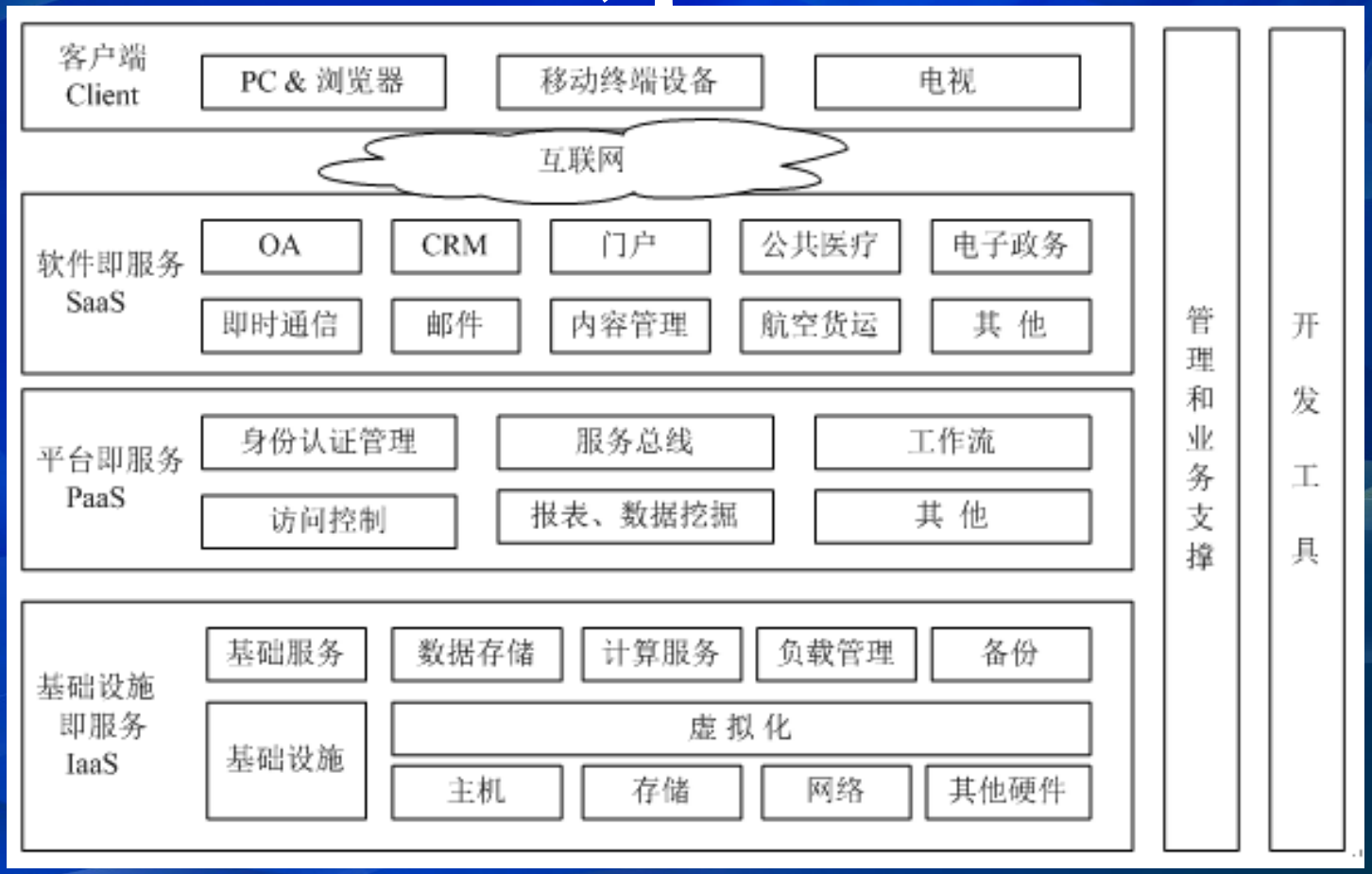

图 6-4　微软云计算架构图

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

有鉴于云计算如火如荼的快速发展，微软针对几乎全线产品也都提出了明确的云战略，其云计算解决方案包括公共云和私有云，既可以帮助企业搭建私有云，又可以帮助企业构建公共云，或让企业选择基于微软云平台运营企业的公共云服务。微软为自己的客户和合作伙伴提供三种不同的云计算运营模式：

公有云：微软自己构建及运营公共云的应用和服务，同时向个人消费者和企业客户提供云服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

合作伙伴运营：独立软件开发商或系统集成商等各种合作伙伴可基于微软 Windows Azure Platform 开发 ERP 、 CRM 等各种云计算应用，并在这一平台上为最终使用者提供服务。

客户自建私有云：客户可以选择微软的云计算解决方案构建自己的云计算平台。微软可以为用户提供包括产品、技术、平台和运维管理在内的全面支持。

微软云战略包括三大部分，为客户和合作伙伴提供三种不同的云计算运营模式：

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

1）微软运营：微软自己构建及运营公共云的应用和服务，同时向个人消费者和企业客户提供云服务。例如，微软向最终使用者提供的 Online Services 和 Windows Live 等服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

2）伙伴运营：　ISV/SI 等各种合作伙伴可基于 Windows Azure Platform 开发 ERP 、 CRM 等各种云计算应用，并在 Windows Azure Platform 上为最终使用者提供服务。另外一个选择是，微软运营在自己的云计算平台中的 Business Productivity Online Suite （ BPOS ）产品也可交由合作伙伴进行托管运营。BPOS 主要包括 Exchange Online, SharePoint Online, Office Communications Online 和 LiveMeeting Online 等服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

3) 客户自建：客户可以选择微软的云计算解决方案构建自己的云计算平台。微软可以为用户提供包括产品、技术、平台和运维管理在内的全面支持。
即企业既会从云中获取必需的服务，也会自己部署相关的 IT 系统。

在云计算时代，一个企业是否可以不用部署任何的 IT 系统，一切都从云计算平台获取？或者反过来，企业还是像以前一样，全部的 IT 系统都部署在企业内部，不从云中获取任何的服务？

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

很多企业认为有些 IT 服务适合从云中获取，如 CRM 、网络会议、电子邮件等；但有些系统不适合部署在云中，如自己的核心业务系统、财务系统等。因此，微软认为理想的模式将是“软件 + 服务”，即企业既会从云中获取必需的服务，也会自己部署相关的 IT 系统。图 6-5 是微软的软件 + 服务战略。

项目五　应用层安全技术

5.1　云计算安全

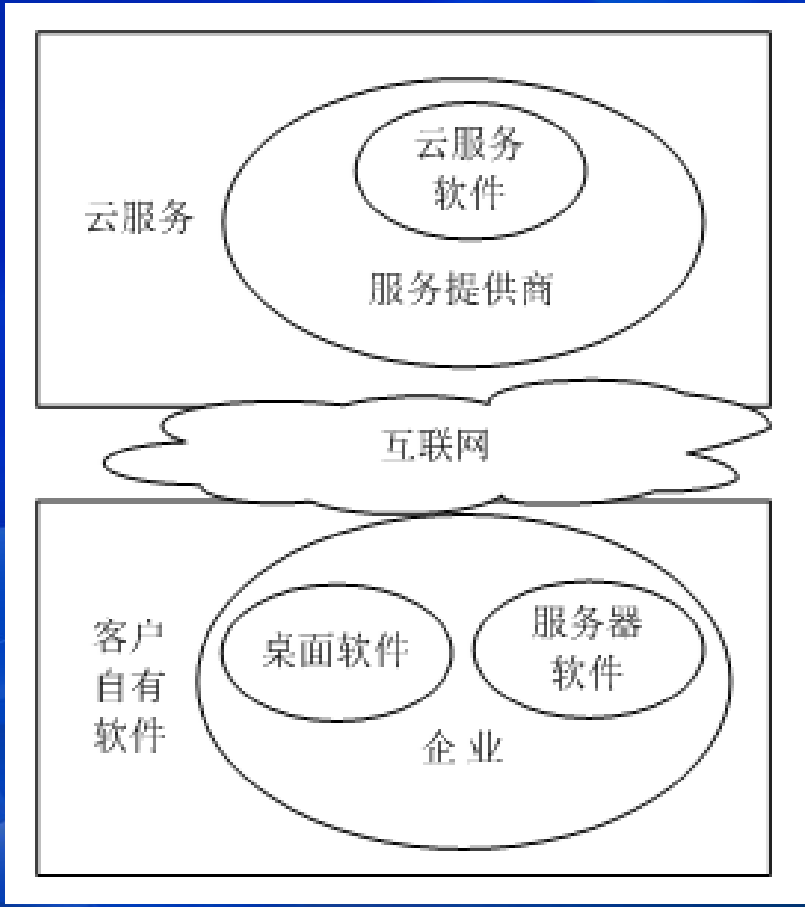

图 6-5　微软的软件 + 服务战略

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

“软件 + 服务”可以简单地描述为两种模式：

1) 软件本身架构模式是软件加服务。例如，杀毒软件本身部署在企业内部，但是杀毒软件的病毒库更新服务是通过互联网进行的，即从云中获取。

2) 企业的一些 IT 系统由自己构建，另一部分向第三方租赁、从云中获取服务。例如，企业可以直接购买软硬件产品，在企业内部自己部署 ERP 系统，而同时通过第三方云计算平台获取 CRM 、电子邮件等服务，而不是自己建设相应的 CRM 和电子邮件系统。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

“软件+服务”的好处在于，既充分继承了传统软件部署方式的优越性，又大量利用了云计算的新特性。
在云计算时代，有三个平台非常重要，即开发平台、部署平台和运营平台。 Windows Azure Platform 是微软的云计算平台，其在微软的整体云计算解决方案中发挥关键作用。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

它既是运营平台，又是开发、部署平台；上面既可运行微软的自有应用，也可以开发部署用户或 ISV 的个性化服务；平台既可以作为 SaaS 等云服务的应用模式的基础，又可以与微软线下的系列软件产品相互整合和支撑。事实上，微软基于 Windows Azure Platform ，在云计算服务和线下客户自有软件应用方面都拥有了更多样化的应用交付模式、更丰富的应用解决方案、更灵活的产品服务部署方式和商业运营模式。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

企业可以根据自身的具体需求和特征，微软为用户提供自由选择的机会。

为用户提供自由选择的机会是微软云计算战略的第三大典型特点。这种自由选择表现在以下三个方面：

1) 用户可以自由选择传统软件或云服务两种方式自己部署 IT 软件、采用云服务、或者两者都用，无论是用户选择哪种方式，微软的云计算都能支持。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

2）用户可以选择微软不同的云服务

无论用户需要的是 SaaS（ Software-as-a-Service ）、 PaaS（ Platform-as-a- Service ）还是 IaaS（ Infrastructure-as-a- Service ），微软都有丰富的服务供其选择。微软拥有全面的 SaaS 服务，包括针对消费者的 Live 服务和针对企业的 Online 服务；也提供基于 Windows Azure Platform 的 PaaS 服务；还提供数据存储、计算等 IaaS 服务和数据中心优化服务。用户可以基于任何一种服务模型选择使用云计算的相关技术、产品和服务。

项目五　应用层安全技术

5.1　云计算安全

5.1.1　云计算概述

3) 用户和合作伙伴可以选择不同的云计算运营模式

微软提供多种云计算运营模式。用户和合作伙伴可直接应用微软运营的云计算服务；用户也可以采用微软的云计算解决方案和技术工具自建云计算应用；合作伙伴还可以选择运营微软的云计算服务或自己在微软云平台上开发云计算应用。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

云计算系统运用了许多技术，其中以编程模型、数据管理技术、数据存储技术、虚拟化技术、云计算平台管理技术最为关键。

1. 编程模型

Map Reduce 是一种编程模型，用于大规模数据集（大于1TB ）的并行运算。概念 “ Map （ 映射 ）” 和 “ Reduce （ 归约 ）” ，和它们的主要思想，都是从函数式编程语言里借来的，还有从矢量编程语言里借来的特性。它极大地方便了编程人员在不会分布式并行编程的情况下，将自己的程序运行在分布式系统上。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

当前的软件实现是指定一个 Map （映射）函数，用来把一组键值对映射成一组新的键值对，指定并发的 Reduce （归约）函数，用来保证所有映射的键值对中的每一个共享相同的键组。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

Map Reduce 是 Google 开发的 java 、 Python 、 C++ 编程模型，它是一种简化的分布式编程模型和高效的任务调度模型，用于大规模数据集（大于 1TB ）的并行运算。严格的编程模型使云计算环境下的编程十分简单。 Map Reduce 模式的思想是将要执行的问题分解成 Map （映射）和 Reduce （化简）的方式，先通过 Map 程序将数据切割成不相关的区块，分配（调度）给大量计算机处理，达到分布式运算的效果，再通过 Reduce 程序将结果汇整输出。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

① 有多个 Map 任务，每个任务的输入为 DFS 中的一个或者多个文件块。 Map 将文件块转换为一个 Key-Value 对序列，而此处的逻辑就是 Mapper 的业务算法。

② 主控制器（ master controller ），从每个 Map 任务中收集一系列键值对， 并将它们按照键大小排序，而这些键值再次被分割，然后分配给所有的 Reduce 任务中，相同键值的对集合会被分配到同一个 Reduce 任务。该部分就是 Map Reduce 和核心 Shuffle 的任务。在 Mapper 端结果进行：分区、排序、分割。在 Reduce 端将 Map 的结果分割后的任务派发给 Reduce，最核心的就是 merge 过程。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

③ Reduce 任务每次作用于一个键，并将与此键关联的所有值以某种方式组合起来。具体的组合方式取决于用户所编写的 Reduce 函数代码。

如图 6-6 所示， Hadoop 任务被分解为几个节点，而 Map Reduce 任务则被分解为跟踪器（ tracker ）。

图 6-7 显示了 Map Reduce 如何执行任务，它将获取输入并执行一系列分组、排序和合并操作，然后呈现经过排序和散列的输出。

项目五　应用层安全技术

5.1　云计算安全

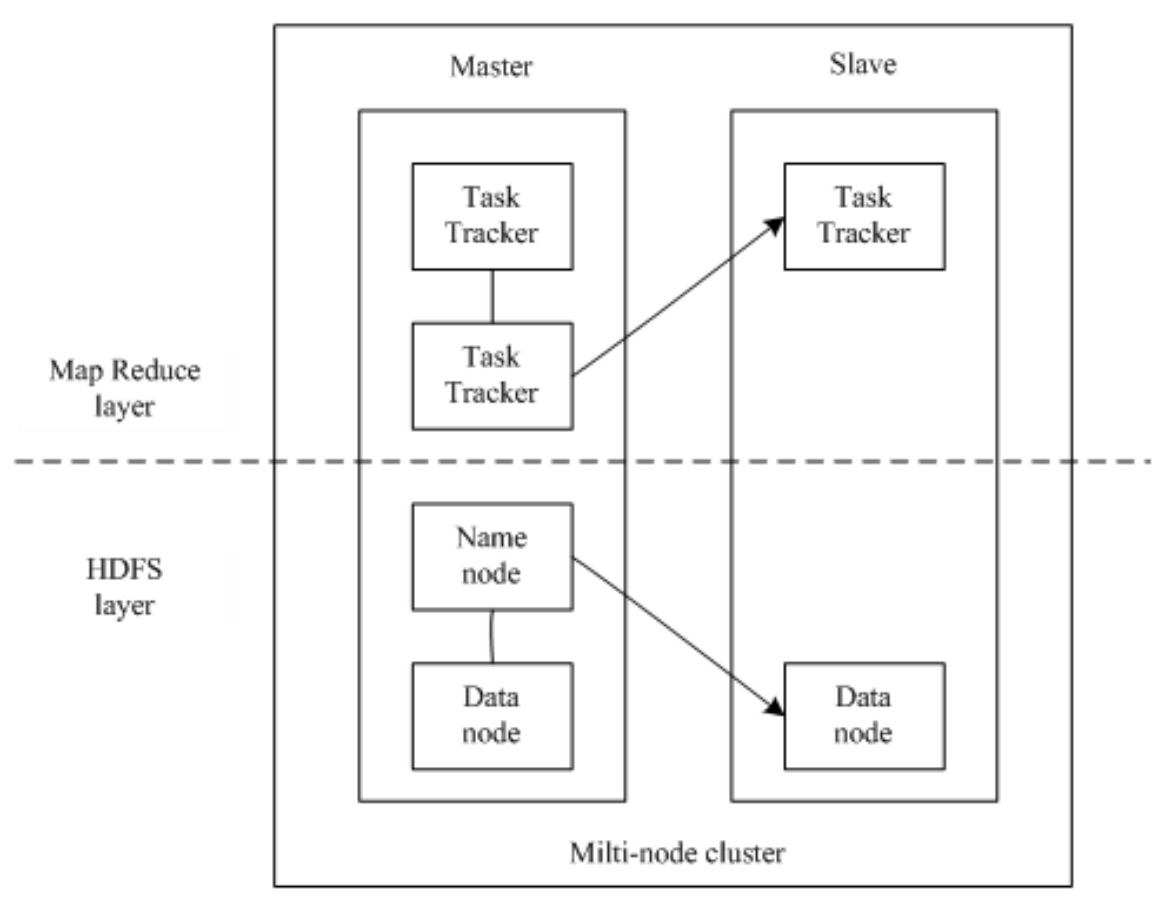

图 6-6　HDFS/Map Reduce 层的组成部分

项目五　应用层安全技术

5.1　云计算安全

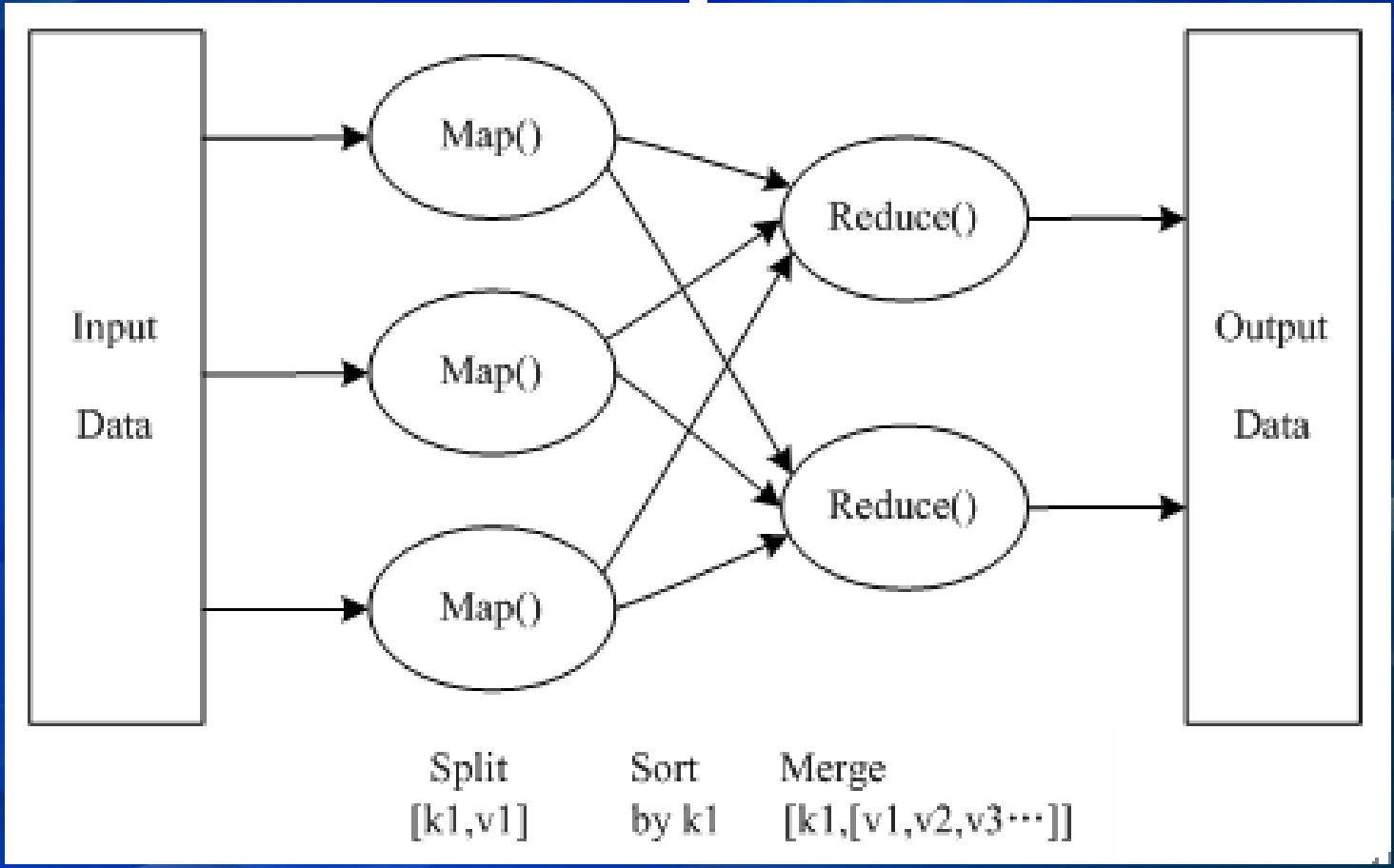

图 6-7　Map Reduce 执行任务图

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

图 6-7 演示了一个更复杂的 Map Reduce 任务及其组成部分。用户提交一个任务以后，该任务由 Job Tracker 协调，先执行 Map 阶段（图中 M1 ， M2 和 M3 ），然后执行 Reduce 阶段（图中 R1 和 R2 ）。 Map 阶段和 Reduce 阶段动作都受到 Task Tracker 监控，并运行在独立于 Task Tracker 的 Java 虚拟机中。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

输入和输出都是 HDFS 上的目录。输入由 Input Format 接口描述，它的实现如 ASCII 文件， JDBC 数据库等，分别处理对于的数据源，并提供了数据的一些特征。通过 Input Format 实现，可以获取 Input Split 接口的实现，这个实现用于对数据进行划分（图中的 splite1 到 splite5 ，就是划分以后的结果），同时从 Input Format 也可以获取 Record Reader 接口的实现，并从输入中生成 <k,v> 对。有了 <k,v> ，就可以开始做 Map 操作了。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

Map 操作通过 context.collect （最终通过 OutputCollector.collect ）将结果写到 context 中。当 Mapper 的输出被收集后，它们会被 Partitioner 类以指定的方式区分地写出到输出文件里。我们可以为 Mapper 提供 Combiner ，在 Mapper 输出它的 <k,v> 时，键值对不会被马上写到输出里，他们会被收集在 list 里（一个 key 值一个 list ），当写入一定数量的键值对时，这部分缓冲会被 Combiner 中进行合并，然后再输出到 Partitioner 中（图中 M1 的黄颜色部分对应着 Combiner 和 Partitioner ）。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

Map 的动作做完以后，进入 Reduce 阶段。这个阶段分 3 个步骤：混洗（ Shuffle ），排序（ sort ）和 reduce 。
混洗阶段， Hadoop 的 Map Reduce 框架会根据 Map 结果中的 key ，将相关的结果传输到某一个 Reducer 上（多个 Mapper 产生的同一个 key 的中间结果分布在不同的机器上，这一步结束后，他们传输都到了处理这个 key 的 Reducer 的机器上）。这个步骤中的文件传输使用了 HTTP 协议。

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

排序和混洗是一块进行的，这个阶段将来自不同 Mapper 具有相同 key 值的 <key,value> 对合并到一起。Reduce 阶段，上面通过 Shuffle 和 sort 后得到的 <key, （ list="" of="" values ）=""> 会送到 Reducer. reduce 方法中处理，输出的结果通过 OutputFormat ，输出到 DFS 中。

Map Reduce 数据流图解如图 6-8 所示。

项目五　应用层安全技术

5.1　云计算安全

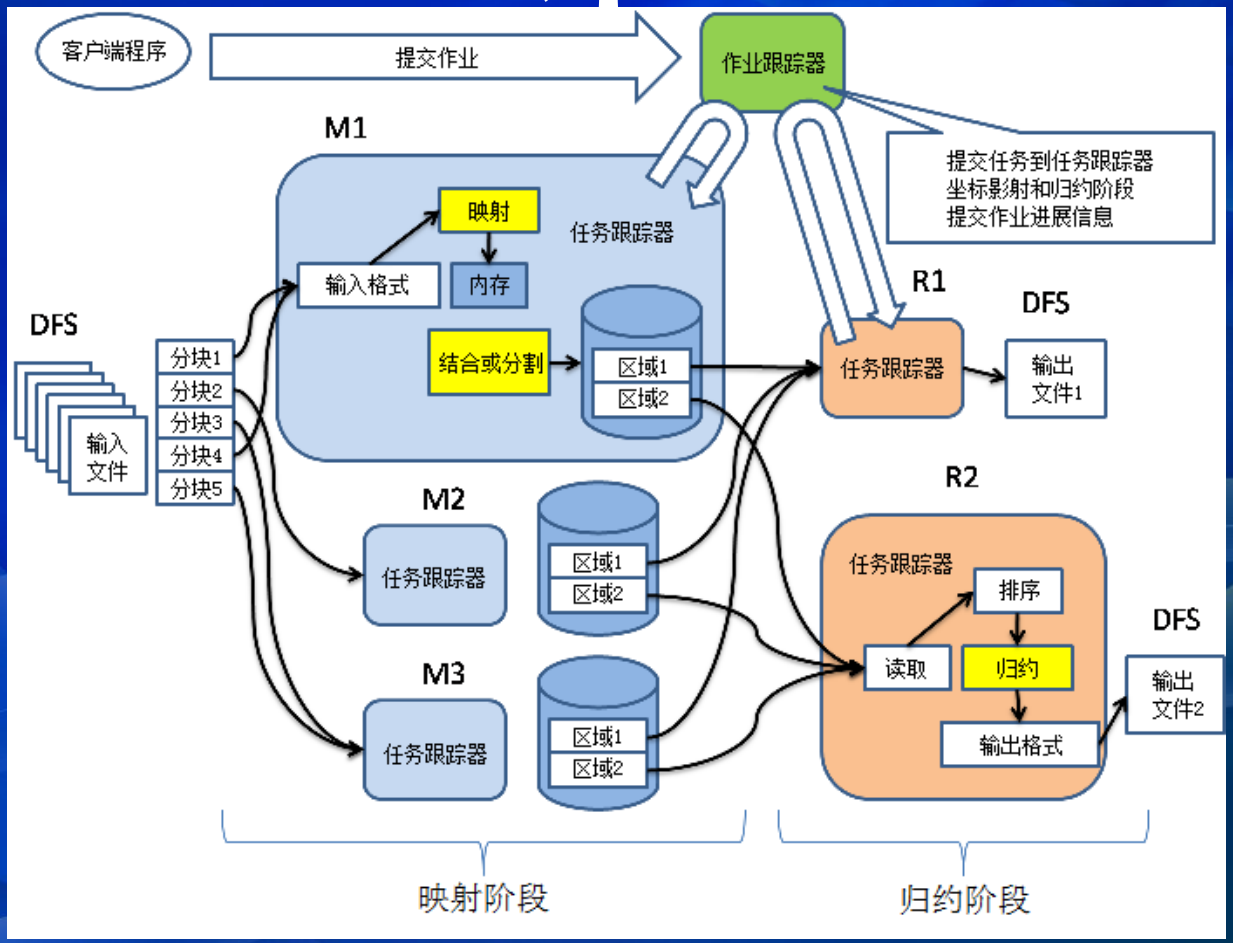

图 6-8　Map Reduce　数据流图解

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

尽管 Hadoop+Map Reduce 要比传统的分析环境（如 IBM Cognos 和 Satori proCube 在线分析处理）更复杂一些，但它的部署仍然具有可扩展能力和高成本效益。

2. 海量数据分布存储技术

云计算系统由大量服务器组成，同时为大量用户服务，因此云计算系统采用分布式存储的方式存储数据，用冗余存储的方式保证数据的可靠性。云计算系统中广泛使用的数据存储系统是 Google 的 GFS 和 Hadoop 团队开发的 GFS 的开源实现 HDFS 。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

GFS 即 Google 文件系统（ Google File System ），是一个可扩展的分布式文件系统，用于大型的、分布式的、对大量数据进行访问的应用。 GFS 的设计思想不同于传统的文件系统，是针对大规模数据处理和 Google 应用特性而设计的。它运行于廉价的普通硬件上，但可以提供容错功能。它可以给大量的用户提供总体性能较高的服务。

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

一个 GFS 集群由一个主服务器（ master ）和大量的块服务器（ Chunk Server ）构成，并被许多客户（ Client ）访问。主服务器存储文件系统所以的元数据，包括名字空间、访问控制信息、从文件到块的映射以及块的当前位置。它也控制系统范围的活动，如块租约（ lease ）管理，孤立块的垃圾收集，块服务器间的块迁移。主服务器定期通过 Heart Beat 消息与每一个块服务器通信，给块服务器传递指令并收集它的状态。 GFS 中的文件被切分为 64MB 的块并以冗余存储，每份数据在系统中保存 3 个以上备份。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

客户与主服务器的交换只限于对元数据的操作，所有数据方面的通信都直接和块服务器联系，这大大提高了系统的效率，防止主服务器负载过重。

项目五　应用层安全技术

5.1　云计算安全

5.1.2　云计算核心技术

3. 海量数据管理技术

云计算需要对分布的、海量的数据进行处理、分析，因此，数据管理技术必需能够高效的管理大量的数据。云计算系统中的数据管理技术主要是 Google 的 BT （ BigTable ）数据管理技术和 Hadoop 团队开发的开源数据管理模块 HBase 。

BT 是建立在 GFS, Scheduler, Lock Service 和 MapReduce 之上的一个大型的分布式数据库，与传统的关系数据库不同，它把所有数据都作为对象来处理，形成一个巨大的表格，用来分布存储大规模结构化数据。

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

Google 的很多项目使用 BT 来存储数据，包括网页查询，Google earth 和 Google 金融。这些应用程序对 BT 的要求各不相同：数据大小（从 URL 到网页到卫星图象）不同，反应速度不同（从后端的大批处理到实时数据服务）。对于不同的要求，BT 都成功的提供了灵活高效的服务。

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

4. 虚拟化技术

通过虚拟化技术可实现软件应用与底层硬件相隔离，它包括将单个资源划分成多个虚拟资源的裂分模式，也包括将多个资源整合成一个虚拟资源的聚合模式。虚拟化技术根据对象可分成存储虚拟化、计算虚拟化、网络虚拟化等，计算虚拟化又分为系统级虚拟化、应用级虚拟化和桌面虚拟化。

项目五　应用层安全技术

5. 1　云计算安全

5.1.2　云计算核心技术

5.　云计算平台管理技术

云计算资源规模庞大，服务器数量众多并分布在不同的地点，同时运行着数百种应用，如何有效的管理这些服务器，保证整个系统提供不间断的服务是巨大的挑战。
云计算系统的平台管理技术能够使大量的服务器协同工作，方便的进行业务部署和开通，快速发现和恢复系统故障，通过自动化、智能化的手段实现大规模系统的可靠运营。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

在云计算出现之后，云计算就与安全有着密切的联系，云安全指的是针对云计算自身存在的安全隐患，研究相应的安全防护措施和解决方案，如云计算安全体系架构、云计算应用服务安全、云计算环境的数据保护等，云计算安全是云计算健康可持续发展的重要前提。

项目五　应用层安全技术

5. 1　云计算安全

5.1.3　云计算安全威胁

1. 云计算安全事故实例

云计算系统的可靠性、性能以及其他技术问题都会带来云计算的相关风险。而且云计算在安全性和风险管理方面仍有不足：即便是最出色的云服务供应商也会遭遇服务中断或速度变慢的问题，比如：

① 2009 年 2 月 24 日，谷歌的 Gmail 电子邮箱爆发全球性故障，服务中断时间长达 4 小时。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

② 2009 年 3 月 17 日，微软的云计算平台 Azure 停止运行约 22 个小时。 Azure 平台的宕机可能引发微软客户对该云计算机服务平台的安全担忧，也暴露了云计算的一个巨大隐患。

③ 2009 年 6 月， Rackspace 遭受了严重的云服务中断故障。供电设备跳闸，备份发电机失效，不少机架上服务器停机。这场事故造成了严重的后果。

④ 2010 年 1 月，几乎 6 万 8 千名的 Salesforce.com 用户经历了至少 1 个小时的宕机。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

⑤ 2011 年 4 月 21 日凌晨，亚马逊公司在北弗吉尼亚州的云计算中心宕机，导致包括回答服务 Quora 、新闻服务 Reddit 、 Hootsuite 和位置跟踪服务 FourSquare 在内的一些网站受到了影响。

以上安全事故使得人们进一步思考公有云面临的安全问题。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

2. 云计算安全的特征

由于云计算资源虚拟化、服务化的特有属性，与传统安全相比，云计算安全具有一些新的特征：

① 传统的安全边界消失，在传统安全中，通过在物理上逻辑上划分安全域，可以清楚的定义边界，但是由于云计采用虚拟化技术以及多租户模式，传统的物理边界被打破于物理安全边界的防护机制难以在云计算环境中得到有效应用；

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

② 动态性，在云计算环境中，用户的数量和分类不同化频率高，具有动态性和移动性强的特点，其安全防护也要进行相应的动态调整；

③ 服务安全保障，云计算采用服务的交互模式，涉及服务的设计、开发和交付，需要对服务的全生命周期进行保障保服务的可用性和机密性；

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

④ 数据安全保护，在云计算中数据不在当地存储，数据密、数据完整性保护、数据恢复等数据安全保护手段对于据的私密性和安全性更加重要；

⑤ 第三方监管和审计，由于云计算的模式，使得服务提商的权利巨大，导致用户的权利可能难以保证，如何确保维护两者之间平衡，需要有第三方监管和审计。

项目五　应用层安全技术

5. 1　云计算安全

5.1.3　云计算安全威胁

3. 云计算安全核心技术

云计算安全的核心技术包括以下五个方面：

① 云计算安全面临的威胁

2013 年，云安全联盟（ CSA ）对云计算的威胁进行排名，以下是 2013 年几个最严重的云计算安全威胁因素：

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

1）数据泄露

数据泄露其实每天都在发生，但云计算加重了这种威胁。一个设计不当的多租户云服务数据库将使攻击者不仅仅进入一个帐户，而且会进入每一个与该服务相关的其他帐户

2）数据丢失

设备被损坏、意外删除、天灾不可抗力等都会造成永久性的数据丢失，除非供应商提供备份。如果一个企业的数据在上传到云之前就行加密，他们就能更好地保护加密密钥或数据。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

3) 账户或服务流量劫持

黑客通过网络钓鱼、欺诈或利用软件漏洞来劫持无辜的用户。通常黑客根据一个密码就可以窃取用户多个服务中的资料，因为用户不会为每个服务设立一个不一样的密码。对于供应商，如果被盗的密码可以登陆云，那么用户的数据将被窃听、篡改，黑客将向用户返回虚假信息，或重定向用户的服务到欺诈网站。对用户将可能造成严重的损失。

项目五　应用层安全技术

5. 1　云计算安全

5.1.3　云计算安全威胁

4) 拒绝服务

剥夺用户访问他们的资源和数据，并造成延迟是破坏一个云服务的一个攻击方法，可能意味着在线服务的死亡。其他形式的攻击，如非对称应用级的 DoS 攻击，在不消耗大量的资源的情况下就可利用弱点将 Web 服务器、数据库和其他云资源作为目标。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

5）恶意的内部人员

恶意的内部人员风险是每个组织必须考虑的方面。这种情况不一定发生，但当它发生时，它造成的伤害就会很大。鹏宇成安全专家表示，完全依赖于云服务提供商的安全系统，是最大的风险。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

② 身份与权限控制

身份与权限控制解决方案是云安全的核心问题之一，在虚拟的、复杂的环境下，如何保证用户的应用、数据清晰可控。简化认证管理、强化端到端的可信接入方面将会是云安全发展的方向之一。

③ WEB 安全防护

云计算模式中， WEB 应用是用户最直观的体验窗口，也是唯一的应用接口。而近几年风起云涌的各种 WEB 攻击手段，则直接影响到云计算的顺利发展。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

④ 虚拟化安全

虚拟化是云计算的标志之一。然而，虚拟化的结果，却使许多传统的安全防护手段失效。从技术层面上讲，云计算与传统 IT 环境最大的区别在于其虚拟的计算环境，也正是这一区别导致其安全问题变得异常“棘手”。虚拟化的计算，使得应用进程间的相互影响更加难以捉摸；虚拟化的存储，使得数据的隔离与清除变得难以衡量；虚拟化的网络结构，使得传统的分域防护变得难以实现；虚拟化的服务提供模式，使得对使用者身份、权限和行为的鉴别、控制与审计变得极其重要。

项目五　应用层安全技术

5.1　云计算安全

5.1.3　云计算安全威胁

⑤ 云安全服务

面对云计算的安全问题，现如今有许多基于云服务提供的安全，包括 Web 和邮件过滤、网络流量访问控制和监控以及用于支付卡业务的标记化。不同安全服务的一个重要区别是，一些是“在云中”的一些是“针对云”的，即那些集成到云环境中作为虚拟设备提供给用户使用和控制的安全服务。
在选择云安全服务时，要多同服务提供商沟通，了解他们能具体提供什么以及自己的需求他们是否能满足，最好签订一份服务协议，这有助于降低企业的风险。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

云计算安全关键技术主要包括虚拟机安全技术、海量用户的身份认证、隐私保护与数据安全等三个方面。

1. 虚拟机安全技术

虚拟机中的安全问题主要指针对虚拟机控制器的各类攻击（对虚拟机控制器的恶意修改和嵌套等），以及基于虚拟机的 Rootkit 。目前针对这些问题，主要采用的防护方法有基于虚拟机的入侵检测，基于虚拟机的内核保护和基于虚拟机的可信计算等。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

① 基于虚拟机的入侵检测技术

虚拟化技术带来了计算机系统结构的变化，也改变了传统安全软件的应用环境。目前，对虚拟机中的入侵检测技术的研究主要集中在基于主机的入侵检测上。但是，在实际的应用环境中，大部分的安全威胁都是来自于网络中，在虚拟机环境中对基于网络的入侵检测系统的研究更能有效的保障虚拟机的运行安全。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

虚拟机利用虚拟机管理器来管理和调度多个客户操作系统对底层单一物理资源的共享访问。通过在虚拟机内部虚拟一个网桥设备，并把各个客户操作系统的网络设备挂接到该虚拟网桥上，由此虚拟机实现了对网络设备的虚拟化。由于虚拟机系统的出现导致传统的操作系统直接运行于硬件层之上的结构发生变化。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

在虚拟机系统之中，VMM 层位于硬件层和操作系统层之间，运行于系统最高特权级，由 VMM 实现对系统所有物理资源的虚拟化和调度管理；另外，同一个虚拟机平台上现在可以部署多台虚拟机，和传统的单一系统占据整台机器也有了本质的不同。这些特征都使得传统的入侵检测系统已经不能完全适应机器体系结构上发生的变化。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

在一个虚拟机系统中，可以部署多个虚拟机，并且每个虚拟机部署不同的服务，因此会产生不同的安全级别，在面向虚拟机网络入侵检测系统的设计中，需要针对这些不同的安全级别采取不同的安全配置。同时，也能针对各个虚拟机进行单独配置，用户可以按照各个虚拟机所配置的服务类型选择所需要的服务。

在虚拟机中，由虚拟网桥负责转发虚拟机中所有的数据流，各个虚拟机的虚拟网络接口直接挂接在虚拟网桥的输出端，数据探测器部署在各个虚拟网络接口上，直接捕获到进出虚拟机的网络数据包，基于虚拟机的入侵检测机制如图 6-9 所示：

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

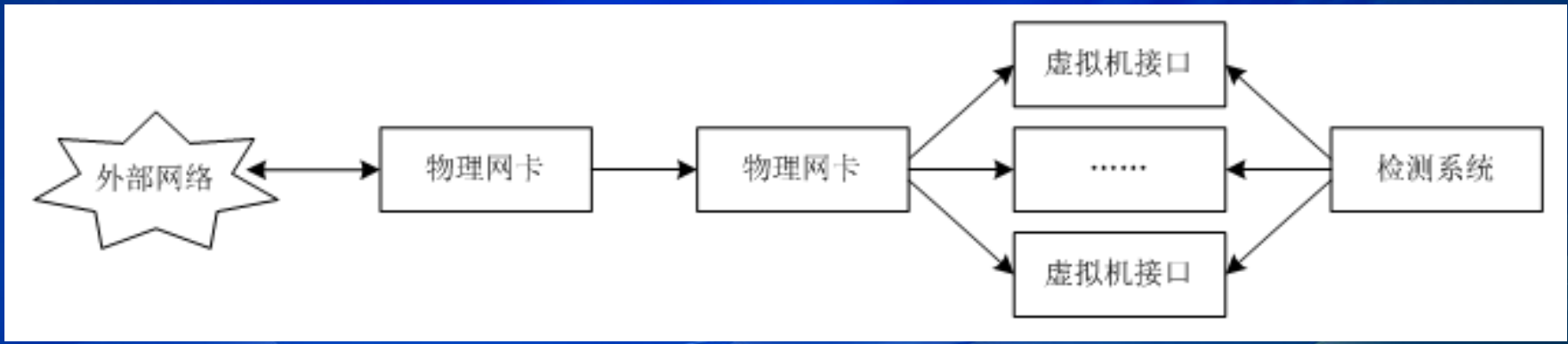

图 6-9　基于虚拟机的入侵检测机制

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

② 基于虚拟机的内核保护技术

基于虚拟机的 Rootkit 是运行在虚拟机系统内核空间的恶意程序，可以修改内核程序的控制流程，从而对虚拟环境的安全构成巨大威胁。而基于虚拟机的内核保护技术主要通过分析内核中影响程序控制流程的资源，并对这些资源进行保护，从而防止 Rootkit 对内核控制流程的篡改。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

rootkit 按其运行的权限不同可以分为应用层 rootkit 和内核级 rootkit 。应用层 rootkit 主要是通过修改或替换系统工具或者系统库来达到其攻击目标，有的应用层 rootkit 还会修改替换了的系统工具和系统库的最后修改时间更具一定的欺骗性。目前对应用层 rootki 的主要检测方法是文件的完整性检查法：新系统安装完毕后通过这类工具获得并保存系统的各种信息比如校验和、最后修改时间等等，检测的时候通过比较文件的当前信息和保存的基准信息，如果不匹配说明攻击发生。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

内核层 rootkit 主要攻击内核的系统调用表、中断描述符表等等。当内核被攻击后，其提供给应用层的信息将不可靠，因此很少有纯应用层工具能检测到内核级 rootkit ，即使能检测到某些内核级 rootkit ，但当此 rookit 升级后就失效了。

目前内核级检测工具通常都是应用层和内核层或者是应用层和能结合 /dev/[k]mem 设备文件比较可靠的获得内核某些信息的工具的结合，例如 kern_check 、 checkidt 和 StMichael 等。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

kern_check 主要手段是比较各个内核符号在 System.map 文件中的地址和系统运行时的地址； checkidt 主要通过检查中断描述符表的完整性检测到攻击中断描述表这一特定类型 rootkit ； StMichael 主要手段是验证内核关键区域如代码段和系统调用表的完整性来达到检测目的，它截获了可加载模块的加载等系统调用，在每次模块加载等操作时都会触发完整性的检查操作。它还设置了一个定时器，以固定时间间隔运行完整性检查操作。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

③ 基于虚拟机的可信计算

虚拟机的可信计算也是虚拟机安全的一个重要发展方向。由斯坦福大学 Tal Garfinkel 等人提出的 Terra 结构是目前在虚拟机可信计算方面的代表，它提供了一个简单与可变通的设计模型，准许应用设计者在闭合平台上以同样的方法建立安全的应用。同时 Terra 支持目前的多数操作系统和应用。 Terra 结构是通过可信虚拟机监控器（ Trusted Virtual Machine Monitor,TVMM ）来实现上面的目标的， TVMM 是一个高可信的虚拟机监控器，将单一的、抗攻击的通用平台划分成多个相互隔离的虚拟机。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

通过可信虚拟监控器，现有的操作系统和应用都能运行在一个与现有开放平台类似的明箱（ open-box ）虚拟机上；它们也可以运行在一个提供专用闭合平台功能的自己的暗箱（ closed-box ）虚拟机之上。可信虚拟机监控器保护暗箱虚拟机内容的保密性和完整性，在暗箱虚拟机里运行的应用程序可以修改自己的软件堆以适应它们的安全要求， TVMM 还允许应用加密地向远端证明运行软件堆的身份，这一过程称之为证明（ attestation ）。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

Terra 的核心是虚拟机监控器，像普通的虚拟机监控器一样，Terra 通过虚拟化硬件资源，使很多虚拟机能独立并发地运行，除此之外，它还提供额外的安全性能，如扮演信任方的角色向远端方证明虚拟机上软件的身份。

TVMM 保障了虚拟机监控器是可信的。虚拟机监控器即使整个虚拟机安全的瓶颈，也是整个系统安全的基础，TVMM 保障了 VMM 的安全性，从而奠定了在 VMM 上实现其他软件的安全基础。面向虚拟机的网络入侵检测系统需要以安全的 VMM 为实现保障。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

2. 海量用户的身份认证

在互联网时代的大型数据业务系统中，大量用户的身份认证和接入管理往往采用强制认证方式，例如指纹认证、 USB Key 认证、动态密码认证等。但是在这种身份认证和管理主要是基于系统自身对于用户身份的不信任作为主要思想而设计的。在云计算时代，因为用户更加关心的云计算提供商是否按照 SLA 实施双方约定好的访问控制策略，所以在云计算模式下，研究者开始关注如何通过身份认证来保证用户自身资源或者信息数据等不会被提供商或者他人滥用。当前比较可行的解决方案就是引入第三方 CA 中心，由后者提供为双方所接受的私钥。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

云计算系统应建立统一、集中的认证和授权系统，以满足云计算多租户环境下复杂的用户权限策略管理和海量访问认证要求，提高云计算系统身份管理和认证的安全性。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

① 集中用户认证

集中用户认证是指采用主流认证方式，如 LDAP 、数字证书认证、令牌卡认证、硬件信息绑定认证、生物特征认证等，支持多因子认证。对不同类型和等级的系统、服务、端口采用相应等级的一种或多种组合认证方式，以满足云计算系统中不同子系统的安全等级与成本及易用性的平衡要求。提供用户访问日志记录，记录用户登录信息，包括系统标识、登录用户、登录时间、登录 IP 、登录终端等标识。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

② 集中用户授权

集中用户授权是指根据用户、用户组、用户级别的定义来对云计算系统资源的访问进行集中授权。采用集中授权或分级授权机制。支持细颗粒度授权策略。

③ 访问授权策略管理身份认证策略

即采用用户身份与终端绑定的策略、完整性认证检查策略和口令策略。授权策略：支持采用集中授权或分级授权策略。账号策略：设置账号安全策略，包括口令连续错误锁定账号、长期不用导致账号失效、用户账号未退出时禁止重复登录等。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

④ 其他功能要求和日志管理

支持对用户认证信息、授权信息等详细日志的集中存储和查询。加密机制：支持对认证、授权等敏感数据的加密存储及传输。

项目五　应用层安全技术

5. 1　云计算安全

5.1.4　云计算安全关键技术

3. 隐私保护与数据安全技术

虽然云计算从服务提供方式上可以划分为 IaaS （基础设施即服务）、 PaaS （平台即服务）和 SaaS （软件即服务） 3 个层次，但本质上都是将数据中心外包给云计算服务提供商的模式。因此，如何保证用户数据的私密性及如何让用户相信他们的数据能够获得必要的隐私保护是云计算服务提供商需要特别关注的问题。用户隐私保护和数据安全主要包括各类信息的物理隔离或者虚拟化环境下的隔离；基于身份的物理或者虚拟安全边界访问控制；数据的异地容灾与备份以及数据恢复；数据的加密传输和加密存贮；剩余信息保护等。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

在云计算应用中，数据量规模之巨已经远远超出传统大型 IDC 数据规模，同时不同用户对于隐私和数据安全的敏感度也各不相同。对数据隐私的保护是云计算服务能够被大众广泛认可并获得深入推广的必要前提，它要求为用户交付的服务的每一个环节都能得到安全性保证。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

在数据传输方面，企业数据通过网络传递给云计算服务提供商进行处理，而这些数据中保存了大量企业的重要核心数据，如企业的销售数据、客户信息、财务信息等。如何确保企业的数据在网络传输过程中不被窃取、修改，保证数据的完整性、保密性和可利用性。需要对网络监测技术、数据加密技术和权限认证技术进行研究。在云计算应用环境下，数据传输加密可以选择在链路层、网络层、传输层、甚至应用层等层面实现。主要的技术措施包括 IPSec VPN 、 SSL 等 VPN 技术，保证用户数据在网络传输中机密性、完整性和可用性。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

在数据存储方面，企业数据存储在云中心，但用户并不清楚自己的数据被放置在哪一台服务器上，甚至根本不了解这台服务器放置在哪个地方，以及服务器所在地是否会有相关政策从而导致信息泄露。在这种数据存储资源的共享环境下，云计算服务提供商要能保证数据之间的有效隔离；另外，云计算服务提供商需要对企业托管的数据进行备份，以备在出现重大事故时及时恢复用户数据，并且要保证数据本身及其所有备份在不需要时能被完全删除而不留任何痕迹。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

因此，云计算服务提供商必须针对这些问题对共享环境下的数据存储技术进行深入研发，以保证用户在任何时候都可以安全地访问数据。另外对于云存储类服务，一般的提供商都支持对数据进行加密存储，防止数据被他人非法窥探。一般会采用效能较高的对称加密算法，如 AES 、 3DES 等国际通用算法等。

项目五　应用层安全技术

5.1　云计算安全

5.1.4　云计算安全关键技术

在运营策略方面，由于企业关键的数据存储在云端，用户会因担心隐私被泄露而产生顾虑。云计算服务提供商需要对其运营策略进行改进，通过借助商业规则和信誉，树立良好的企业形象和公信力，在保障用户隐私的同时，又必须对用户行为进行必要的监督和管制。例如，云计算的按需提供资源并按需计费的模式降低了不良用户通过网络发起不良行为的成本，会助长其破坏互联网安全的行为。对于这类情况，云计算服务提供商必须给予监督并在政策指导下坚决予以打击，这也是服务提供商的安全责任所在。

项目五　应用层安全技术

5. 1　云计算安全

5.1.5　云计算与物联网

1. 云计算与物联网关系

由于云计算从本质上来说就是一个用于海量数据处理的计算平台，因此，云计算技术是物联网涵盖的技术范畴之一。随着物联网的发展，未来物联网将势必产生海量数据，而传统的硬件架构服务器将很难满足数据管理和处理要求，如果将云计算运用到物联网的传输层和应用层，采用云计算的物联网，将会在很大程度上提高运作效率。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

运用云计算模式，使物联网中数以兆计的各类物品的实时动态管理、智能分析变得可能。 物联网通过将射频识别技术（ RFID ）、传感器技术、纳米技术等新技术充分运用在各行各业之中。将各种物体充分连接，并通过无线等网络将采集到的各种实时动态信息送达计算处理中心，进行汇总、分析和处理，从而将各种物体连接。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

物联网和互联网的融合，需要更高层次的整合，需要“更透彻的感知、更全面的互联互通、更深入的智能化”。这同样也需要依靠高效的、动态的、可以大规模扩展的计算机资源处理能力，而这正是云计算模式所擅长的。同时，云计算的创新型服务交付模式，简化服务的交付，加强物联网和互联网之间及其内部的互联互通，可以实现新商业模式的快速创新，促进物联网和互联网的智能融合。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

2. 云计算在物联网中的应用

将云计算的云计算、云储存、云服务、云终端等技术应用于物联网的感知层、应用层及网络层，解决物联网中海量信息和数据的管理问题：

① 节点不可信的问题

可以有效的解决服务器的节点不可信的问题，可以最大限度的降低服务器的出错的概率。随着科技的不断进步发展，物联网已经从原来的局域网逐渐的发展成为城域网，其信息量也随之不断的增多，这样也就导致服务器的数量不断的增加，这样就会导致节点的出错概率的增加。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

在云计算中，可以有不同数目的虚拟服务器组，其可以按照先来先提供服务的方式，以此来完成节点之间的分布式的调度，这样在屏蔽相关节点的时候，也会提升响应的速率，云计算可以有效的保障物联网无间断安全服务的实现。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

② 获得很好的经济收益

可以保障物联网在低的投人下，获得很好的经济收益，一般情况下，服务器的硬件资源都是有一定的限度的，当服务器的响应的数量超出了自身承载数量的最大值，可能会造成服务器的瘫痪现象的发生。而云计算的出现，就可以通过采用机群均衡的调度方式，在服务器访问数量达到最大的负载的时候，通过改变星级的级别，以此来动态的减少或者是增加服务器的数量以及质量，达到释放访问压力的作用。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

③ 实现物联网的广泛连接

可以实现物联网由局域网到互联网的广泛连接，其能够很大程度上对信息资源进行共享，能够保障物联网的相关的信息放在互联网的云计算中心上，这样就能够保障信息的空间性，在任何地方只要有相应的传感器芯片，就能够从服务器中收到相关的信息。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

3. 云计算与物联网中的结合方式

云计算与物联网的结合方式我们可以分为以下几种：

① 单中心，多终端

在此类模式中，分布范围的较小各物联网终端（传感器、摄像头或 3G 手机等），把云中心或部分云中心做为数据 / 处理中心，终端所获得信息、数据统一由云中心处理及存储，云中心提供统一界面给使用者操作或者查看。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

这类应用非常多，如小区及家庭的监控、对某一高速路段的监测、幼儿园小朋友监管以及某些公共设施的保护等都可以用此类信息。这类主要应用的云中心，可提供海量存储和统一界面、分级管理等功能，对日常生活提供较好的帮助。一般此类云中心为私有云居多。

②　多中心，大量终端

对于很多区域跨度加大的企业、单位而言，多中心、大量终端的模式较适合。譬如，一个跨多地区或者多国家的企业，因其分公司或分厂较多，要对其各公司或工厂的生产流程进行监控、对相关的产品进行质量跟踪等等。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

当然同理，有些数据或者信息需要及时甚至实时共享给各个终端的使用者也可采取这种方式。举个简单的例子，如果北京地震中心探测到某地和某地 10 分钟后会有地震，只需要通过这种途径，仅仅十几秒就能将探测情况的告信息发出，可尽量避免不必要的损失。中国联通的“互联云”思想就是基于此思路提出的。这个的模式的前提是我们的云中心必须包含公共云和私有云，并且他们之间的互联没有障碍。这样，对于有些机密的事情，比如企业机密等可较好地保密而又不影响信息的传递与传播。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

③ 信息与应用分层处理、海量终端

这种模式可以针对用户的范围广、信息及数据种类多、安全性要求高等特征来打造。当前，客户对各种海量数据的处理需求越来越多，针对此情况，我们可以根据客户需求及云中心的分布进行合理的分配。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

对需要大量数据传送，但是安全性要求不高的，如视频数据、游戏数据等，我们可以采取本地云中心处理或存储。对于计算要求高，数据量不大的，可以放在专门负责高端运算的云中心里。而对于数据安全要求非常高的信息和数据，我们可以放在具有灾备中心的云中心里。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

4. 云计算与物联网结合面临的问题

① 规模问题

规模化是云计算与物联网结合的前提条件。只有当物联网的规模足够大之后，才有可能和云计算结合起来，比如行业应用：智能电网、地震台网监测等等需要云计算。而对一般性的、局域的、家庭网的物联网应用，则没有必要结合云计算。如何使两者发展至相应规模，尚待解决。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

② 安全问题

无论是云计算还是物联网，都有海量的物、人相关的数据。若安全措施不到位，或者数据管理存在漏洞，它们将使我们的生活无所遁形。使我们面临黑客、病毒的威胁，甚或被恐怖分子轻易跟踪、定位，这势必带来对个人隐私的侵犯和企业机密泄露等问题。破坏了信息的合法有序使用要求，可能导致人们的生活、工作陷入瘫痪，社会秩序混乱。因此，这就要求政府、企业、科研院所等各有关部门运用技术、法律、行政等各种手段，解决安全问题。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

③ 网络连接问题

云计算和物联网都需要持续、稳定的网络连接，以传输大量数据。如果在低效率网络连接的环境下，则不能很好工作，难以发挥应用的作用。因此，如何解决不同网络（有线网络、无线网络）之间的有效通信，建立持续、大容量、高可靠的网络连接，需要深入研究。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

④ 标准化问题

标准是对任何技术的统一规范，由于云计算和物联网都是由多设备、多网络、多应用通过互相融合形成的复杂网络，需要把各系统都通过统一的接口、通信协议等标准联系在一起。这将是在两者发展中不断发展，有效健全的问题。

总之，物联网是指“把所有物品通过射频识别等信息传感设备与互联网连接起来，实现智能化识别和管理”，“云计算”是指“利用互联网的分布性等特点来进行计算和存储”。前者是对互联网的极大拓展，而后者则是一种网络应用模式，两者存在着较大的区别。

项目五　应用层安全技术

5.1　云计算安全

5.1.5　云计算与物联网

然而，对于物联网来说，本身需要进行大量而快速的运算，云计算带来的高效率的运算模式正好可以为其提供良好的应用基础。没有云计算的发展，物联网也就不能顺利实现，而物联网的发展又推动了云计算技术的进步，因为只有真正与物联网结合后，云计算才算是真正意义上从概念走向应用，两者缺一不可。

项目五　应用层安全技术

5. 2　中间件安全

5.2.1　中间件概述

顾名思义，中间件（ Middleware ）是处于操作系统与应用程序中间的软件。中间件的结构如图 6-10 所示。

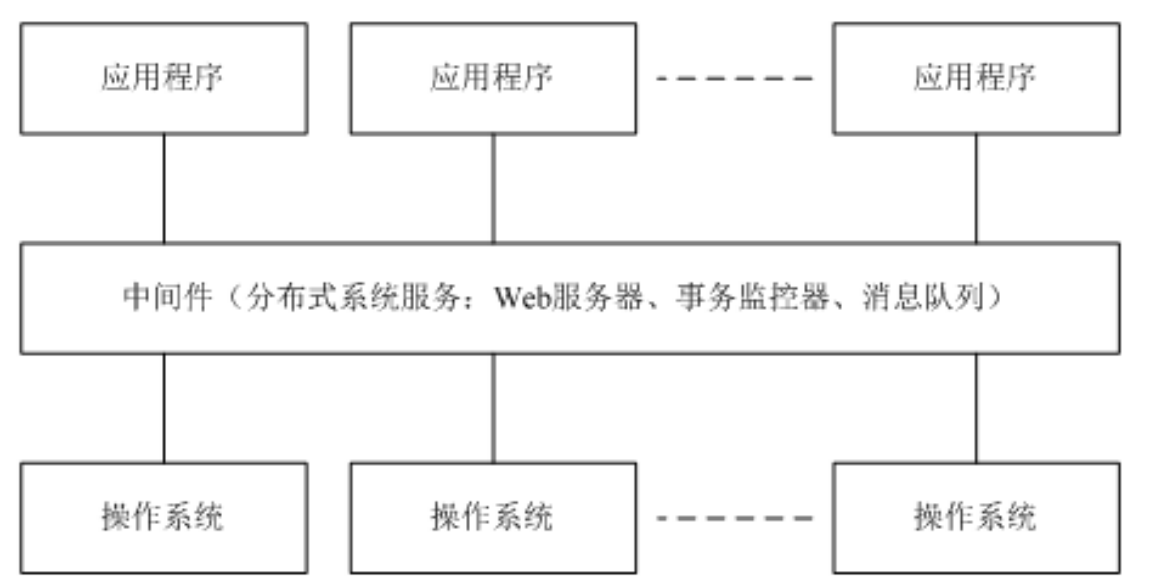

图 6-10　中间件的结构

项目五　应用层安全技术

5. 2　中间件安全

5.2.1　中间件概述

在众多关于中间件的定义中，被各界广泛地接受的是IDC 的表述：中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源，中间件位于客户机服务器的操作系统之上，管理计算资源和网络通信。

IDC 对中间件的定义表明，中间件是一类软件，而非一种软件；中间件不仅仅实现互连，还要实现应用之间的互操作；中间件是基于分布式处理的软件，最突出的特点是其网络通信功能。

项目五　应用层安全技术

5. 2　中间件安全

5.2.1　中间件概述

中间件是基础软件的一大类，属于可复用软件的范畴。人们在使用中间件时，往往将一组中间件集成在一起，构成一个平台（包括开发平台和运行平台），但在这组中间件中必需要有一个通信中间件，即中间件 = 平台 + 通信，这个定义也限定了只有用于分布式系统中才能称为中间件，同时还可以把它与操作系统和应用软件区分开来。

项目五　应用层安全技术

5. 2　中间件安全

5.2.1　中间件概述

中间件是一类连接软件组件和应用的计算机软件。它包括一组服务，以便于运行在一台或多台计算机上的多个软件通过网络进行交互。该技术所提供的互操作性，推动了一致分布式体系架构的演进。中间件架构通常用于支持分布式应用软件，并简化了其复杂程度。它包括 web 服务器、事务监控器和消息队列软件等。

目前，中间件技术发展很快，已经与操作系统和数据库并列为 3 大基础软件。

项目五　应用层安全技术

5. 2　中间件安全

5.2.1　中间件概述

中间件位于操作系统、网络和数据库的上层，应用程序的下层。中间件的核心作用是通过管理计算资源和网络通信，为各类分布式应用软件共享资源提供支撑。广义地看，中间件的总体作用是为处于自己上层的应用软件提供运行与开发的环境，帮助用户灵活地、高效地开发和集成复杂的应用软件。

项目五　应用层安全技术

5. 2　中间件安全

5.2.1　中间件概述

中间件的产生与迅速发展的原因可以用表 5.1 清楚地描述。

由于计算机网络环境的日益复杂，为了支持各种不同的交互模式，产生了适应各种不同网络环境和应用系统的中间件。

项目五　应用层安全技术

5.2　中间件安全

5.2.1　中间件概述

表 6.1　操作系统、数据库管理系统与中间件的比较

基础软件类型	操作系统	数据库管理系统	中间件
产生原因	硬件过于复杂	数据过于复杂	网络环境过于复杂
主要作用	管理各种资源	管理各类数据	支持不同的交互模式
理论基础	各种调度算法	各种数据模型	各种协议、各种接口
产品形态	功能类似	功能类似	种类多，功能差别大

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

中间件所包括的范围十分广泛，针对不同的应用需求涌现出多种各具特色的中间件产品。但至今中间件还没有一个比较精确的定义，因此，在不同的角度或不同的层次上，对中间件的分类也会有所不同。由于中间件需要屏蔽分布环境中异构的操作系统和网络协议，它必须能够提供分布环境下的通讯服务，我们将这种通讯服务称之为中间件平台。

基于目的和实现机制的不同，可以将中间件平台分为以下几类：远程过程调用（ Remote Procedure Call Middleware ，RPC ）、面向消息的中间件（ Message-Oriented Middleware ，MOM ）、对象请求代理（ Object Request Broker ， ORB ）和事务处理监控（ Transaction Processing Monitor ， TPM ）。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

它们可向上提供不同形式的通讯服务，包括同步、排队、订阅发布、广播等等，在这些基本的通讯平台之上，可构筑各种框架，为应用程序提供不同领域内的服务，如事务处理监控器、分布数据访问、对象事务管理器 OTM 等。平台为上层应用屏蔽了异构平台的差异，而其上的框架又定义了相应领域内的应用的系统结构、标准的服务组件等，用户只需告诉框架所关心的事件，然后提供处理这些事件的代码。当事件发生时，框架则会调用用户的代码。用户代码不用调用框架，用户程序也不必关心框架结构、执行流程、对系统级 API 的调用等，所有这些由框架负责完成。因此，基于中间件开发的应用具有良好的可扩充性、易管理性、高可用性和可移植性。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

1. 远程过程调用

远程过程调用（ Remote Procedure Call ， RPC ）是一种广泛使用的分布式应用程序处理方法。一个应用程序使用 RPC 来“远程”执行一个位于不同地址空间里的过程，并且从效果上看和执行本地调用相同。事实上，一个 RPC 应用分为两个部分： server 和 Client 。 server 提供一个或多个远程过程； client 向 server 发出远程调用。 server 和 client 可以位于同一台计算机，也可以位于不同的计算机，甚至运行在不同的操作系统之上。它们通过网络进行通讯。 client 运行相应的 server 提供的数据转换和通讯服务，从而屏蔽不同的操作系统和网络协议。在这里 RPC 通讯是同步的。采用线程可以进行异步调用。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

在 RPC 模型中， client 和 server 只要具备了相应的 RPC 接口，并且具有 RPC 运行支持，就可以完成相应的互操作，而不必限制于特定的 server 。因此， RPC 为 client/server 分布式计算提供了有力的支持。同时，远程过程调用 RPC 所提供的是基于过程的服务访问， client 与 server 进行直接连接，没有中间机构来处理请求，因此也具有一定的局限性。比如， RPC 通常需要一些网络细节以定位 server ；在 client 发出请求的同时，要求 server 必须是活动的等等。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

2. 面向消息的中间件

面向消息的中间件（ Message-Oriented Middleware, MOM ）指的是利用高效可靠的消息传递机制进行平台无关的数据交流，并基于数据通信来进行分布式系统的集成。通过提供消息传递和消息排队模型，它可在分布环境下扩展进程间的通信，并支持多通讯协议、语言、应用程序、硬件和软件平台。流行的 MOM 中间件产品有 IBM 的 MQSeries 、 BEA 的 MessageQ 等。消息传递和排队技术有以下三个主要特点：

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

① 通讯程序可在不同的时间运行

程序不在网络上直接相互通话，而是间接地将消息放入消息队列，因为程序间没有直接的联系。所以它们不必同时运行。消息放入适当的队列时，目标程序甚至根本不需要正在运行；即使目标程序在运行，也不意味着要立即处理该消息。

② 对应用程序的结构没有约束

在复杂的应用场合中，通讯程序之间不仅可以是一对一的关系，还可以进行一对多和多对一方式，甚至是上述多种方式的组合。多种通讯方式的构造并没有增加应用程序的复杂性。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

③ 程序与网络复杂性相隔离

程序将消息放入消息队列或从消息队列中取出消息来进行通讯，与此关联的全部活动，比如维护消息队列、维护程序和队列之间的关系、处理网络的重新启动和在网络中移动消息等是 MOM 的任务，程序不直接与其它程序通话，并且它们不涉及网络通讯的复杂性。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

3. 对象请求代理中间件

随着对象技术与分布式计算技术的发展，两者相互结合形成了分布对象计算，并发展为当今软件技术的主流方向。 1990 年底，对象管理集团 OMG 首次推出对象管理结构 OMA(Object Management Architecture) ，对象请求代理中间件（ Object Request Broker ， ORB ）是这个模型的核心组件。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

它的作用在于提供一个通信框架，透明地在异构的分布计算环境中传递对象请求。 CORBA 规范包括了 ORB 的所有标准接口。 1991 年推出的 CORBA 1.1 定义了接口描述语言 OMG IDL 和支持 Client/Server 对象在具体的 ORB 上进行互操作的 API 。 CORBA 2.0 规范描述的是不同厂商提供的 ORB 之间的互操作。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

对象请求代理是对象总线，它在 CORBA 规范中处于核心地位，定义异构环境下对象透明地发送请求和接收响应的基本机制，是建立对象之间 client/server 关系的中间件。 ORB 使得对象可以透明地向其他对象发出请求或接受其他对象的响应，这些对象可以位于本地也可以位于远程机器。 ORB 拦截请求调用，并负责找到可以实现请求的对象、传送参数、调用相应的方法、返回结果等。 client 对象并不知道同 server 对象通讯、激活或存储 server 对象的机制，也不必知道 server 对象位于何处、它是用何种语言实现的、使用什么操作系统或其他不属于对象接口的系统成分。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

值得指出的是 client 和 server 角色只是用来协调对象之间的相互作用，根据相应的场合， ORB 上的对象可以是 client ，也可以是 server ，甚至兼有两者。当对象发出一个请求时，它是处于 client 角色；当它在接收请求时，它就处于 server 角色。大部分的对象都是既扮演 client 角色又扮演 server 角色。另外由于 ORB 负责对象请求的传送和 server 的管理， client 和 server 之间并不直接连接，因此，与 RPC 所支持的单纯的 Client/Server 结构相比， ORB 可以支持更加复杂的结构。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

4. 事务处理监控中间件

事务处理监控（ Transaction Processing Monitor ， TPM ）最早出现在大型机上，为其提供支持大规模事务处理的可靠运行环境。随着分布计算技术的发展，分布应用系统对大规模的事务处理提出了需求，比如商业活动中大量的关键事务处理。事务处理监控界于 client 和 server 之间，进行事务管理与协调、负载平衡、失败恢复等，以提高系统的整体性能。它可以被看作是事务处理应用程序的“操作系统”。总体上来说，事务处理监控有以下功能：

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

① 进程管理

包括启动 server 进程、为其分配任务、监控其执行并对负载进行平衡。

② 事务管理

即保证在其监控下的事务处理的原子性、一致性、独立性和持久性。

③ 通讯管理

为 client 和 server 之间提供了多种通讯机制，包括请求响应、会话、排队、订阅发布和广播等。

项目五　应用层安全技术

5. 2　中间件安全

5.2.2　中间件的分类

事务处理监控能够为大量的 client 提供服务，比如飞机定票系统。如果 server 为每一个 client 都分配其所需要的资源的话，那 server 将不堪重负。但实际上，在同一时刻并不是所有的 client 都需要请求服务，而一旦某个 client 请求了服务，它希望得到快速的响应。事务处理监控在操作系统之上提供一组服务，对 client 请求进行管理并为其分配相应的服务进程，使 server 在有限的系统资源下能够高效地为大规模的客户提供服务。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

1. RFID 中间件的工作原理

RFID 中间件扮演 RFID 的标签和应用程序之间的中介角色，从应用程序端使用中间件提供一组通用的应用程序接口（ API ）。中间件可以连接到 RFID 的读写器，读取 RFID 标签中的数据。因此，尽管存储 RFID 标签信息的数据库软件或后端应用程序被修改或被其他软件取代，甚至 RFID 读写器的种类发生变化等情况发生时，应用端不需修改也同样能够处理。这样，解决了多对多连接的维护复杂性问题。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

2. RFID 中间件的分类

RFID 中间件可以从架构上分为两类。

① 以应用程序为中心

这种设计模式是通过 RFID 读写器厂商提供的应用程序接口，以 Hot Code 方式直接编写特定的 RFID 阅读器的读写数据适配器，并传送至后端系统的应用程序或数据库，从而达到与后端系统或服务连接的目的。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

② 以软件架构为中心

随着企业物联网应用系统的复杂度的提高，企业将无法负荷以 Hot Code 方式为每个应用程序编写适配器，同时还将会面临对象标准化等技术难题。此时，企业可以考虑采用厂商提供的标准规格的 RFID 中间件。这样，尽管发生 RFID 标签信息的数据库软件改由其他软件替代，或者 RFID 标签的读写器种类变化等情况，应用端也不需要做任何修改。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

3. RFID 中间件的特点

① 独立与架构

RFID 中间件独立并介于 RFID 的读写器与后端应用程序之间，并且能够与多个 RFID 读写器以及多个后端应用程序连接，从而减轻架构和维护的复杂性。

② 数据流

RFID 的主要目的是将实体对象转换为信息环境下的虚拟对象，因此数据处理是 RFID 的最重要的功能。 RFID 中间件具有数据的收集、过滤、整合与传递等特性，以便将正确的对象信息传送到企业后端的应用系统。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

③ 处理流

RFID 中间件采用程序逻辑以及存储再转送的功能来提供顺序的消息流，具有数据流的设计与管理的能力。

④ 标准

RFID 系统为自动数据采样技术与辨析实体对象的应用。 EPC global 制定了适用于全球各种产品的唯一识别号码的统一标准，即电子产品编码（ Electronic Product Code ， EPC ）。EPC 在供应链系统中以一串数字来识别某种特定的商品。通过无线射频辨识标签，由 RFID 的读写器读入后，传送到计算机或应用系统中的过程称为对象命名服务。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

对象命名服务系统会锁定计算机网络中的固定点，抓取有关商品的信息。 EPC 存放在 RFID 的标签中，被 RFID 读写器读出后，即可提供追踪 EPC 所对应的物品名称及相关信息，并立刻识别和分享供应链中的物品数据，显著地提高了信息的透明度。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

4. RFID 中间件的发展

从发展趋势来分析， RFID 中间件可以分为以下三个发展阶段：

① 中间件应用程序阶段

RFID 初期的发展，多以整合串接 RFID 读写器为目的。在这个阶段， RFID 生产厂商一般都主动提供简单的应用程序接口（ API ），供企业将后端系统与 RFID 读写器连接。从整体发展架构来看，此时企业的导入必须自行花费许多成本去处理前后端系统的连接问题。通常，企业在这个阶段会通过试点工程方式来评估成本效益与导入的关键问题。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

② 中间件架构阶段

中间件架构阶段是 RFID 中间件成长的关键阶段。由于 RFID 的强大应用，沃尔玛与美国国防部等关键使用者相继进行 RFID 技术的规划，并进行导入的试点工程，促使大型厂商持续关注 RFID 相关市场的发展。在这个阶段， RFID 中间件的发展，不但已经具备基本数据收集、过滤等功能，同时也满足了企业多对多的连接需求，并且具备平台的管理和维护功能。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

③ 中间件解决方案阶段

在 RFID 标签、读写器与中间件的发展成熟过程中，各大厂商针对不同领域提出了各项创新应用解决方案。例如，曼哈特联合软件公司提出了 RFID 一盒子解决方案（ RFID in a box ），企业不需要再为前端 RFID 的硬件与后端应用系统的连接而烦恼。曼哈特联合软件公司与艾邻技术公司在 RFID 硬件端合作，开发了以 Microsoft.Net 平台为基础的中间件。原本使用曼哈特联合软件公司供应链执行解决方案的 900 多家企业，只需要通过 RFID 一盒子解决方案，就可以在原有应用系统上快速利用 RFID 来加强供应链管理的透明度。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

5. RFID 中间件技术的发展现状

① 国际 RFID 中间件产品的发展现状

最早提出 RFID 中间件概念的国家是美国。美国企业在实施 RFID 项目改造期间，发现最耗时、耗力、复杂度和难度最高的问题，是如何保证 RFID 数据正确导入企业的管理系统。为此企业做了大量的工作用于保证 RFID 数据的正确性。经过企业与研究机构的多方研究、论证、实验，终于找到了一个比较好的解决方法，这就是 RFID 中间件。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

目前，在国际上比较知名的 RFID 中间件厂商，有 IBM 、 Oracle 、 Microsoft 、 SAP 、 Sun 、 Sybase 、 BEA 等国际知名企业。由于这些软件厂商本身就具备比较雄厚的技术实力，其开发的 RFID 中间件产品又经过实验室、企业实地的反复测试，因此，这些 RFID 中间件产品的稳定性、先进性、海量数据的处理能力都比较完善，得到了企业的广泛认可。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

1) IBM RFID 中间件

IBM RFID 中间件是一套基于 JAVA 并遵循 J2EE 企业架构开发的一套开放式 RFID 中间件产品，可以帮助企业简化实施 RFID 项目的步骤，能满足企业处理海量货物数据的要求；基于高度标准化的开发方式， IBM 的 RFID 中间件产品可以与企业信息管理系统无缝联接，有效缩短企业的项目实施周期，降低了 RFID 项目实施出错率、企业实施成本。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

目前 IBM RFID 中间件产品已经成功应用于全球第四大零售商 Metro 公司的供应链之中，不仅提高了整个供应链商品的流转速度、减少产品差错率，还提高了整个供应链的服务水平，降低了整个供应链的运营成本。此外，还有约 80 多家供应商表示，将与 IBM 公司签订采用这项新的 IBM WebSphere RFID 中间件解决方案。

为了进一步提高 RFID 解决方案的竞争力，目前 IBM 与 Intermec 公司进行合作，将 IBM RFID 中间件成功地嵌入 Intermec 的 IF5 RFID 读写器中，共同向企业提供一整套 RFID 企业或供应链解决方案。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

2) Oracle RFID 中间件

Oracle RFID 中间件是甲骨文公司着眼于未来 RFID 的巨大市场而开发的一套基于 JAVA 遵循 J2EE 企业架构的中间件产品。Oracle 中间件依托 Oracle 数据库，充分发挥 Oracle 数据库的数据处理优势，满足企业对海量 RFID 数据存储和分析处理的要求。 Oracle RFID 中间件除最基本的数据功能外，还向用户提供了智能化的手工配置界面。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

实施 RFID 项目的企业可根据业务的实际需求，手工设定 RFID 读写器的数据扫描周期、相同数据的过滤周期，并指定 RFID 中间件将电子数据导入指定的服务数据库，并且企业还可以利用 Oracle 提供的各种数据库工具对 RFID 中间件导入的货物数据进行各种指标数据分析，并做出准确的预测。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

3) Microsoft 的 RFID 中间件

微软公司在 RFID 巨大的市场面前自然不会袖手旁观，投入巨资组建了 RFID 实验室，着手进行 RFID 中间件和 RFID 平台的开发，并以微软 SQL 数据库和 Windows 操作系统为依托，向的大、中、小型企业提供 RFID 中间件企业解决方案。

与其他软件厂商运行的 JAVA 平台不同， Microsoft 中间件产品主要运行于微软的 Windows 系列操作平台。企业在选用中间件技术时，一定要考虑 RFID 中间件产品与自己现有的企业管理软件的运行平台是否兼容。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

根据微软的 RFID 中间件计划，微软准备将 RFID 中间件产品集成为 Windows 平台的一部分，并专门为 RFID 中间件产品的数据传输进行系统级的网络优化。依据 Windows 占据的的全球市场份额及 Windows 平台优势，微软的 RFID 中间件产品拥有了更大的的竞争优势。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

4) SAP 中间件

SAP RFID 中间件产品也是基于 JAVA 语言遵循 J2EE 企业架构开发的产品。 SAP RFID 中间件产品具有两个显著的特征：系列化产品和整合中间件。首先， SAP 的 RFID 中间件产品是系列化产品；第二， SAP 的 RFID 中间件是一个整合中间件，它可以将其他厂商的 RFID 中间件产品整合在一起，作为 SAP 整个企业信息管理系统应用体系的一部分进行实施。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

SAP RFID 的中间件产品主要包括： SAP 自动身份识别基础设施软件、 SAP 事件管理软件和 SAP 企业门户。为增强 SAP RFID 中间件的企业竞争力， SAP 又联合 Sun 和 Sybase ，将这两家的 RFID 中间件产品整合到 SAP 的中间件产品中。与 Sybase 的 RFID 安全中间件整合，大大提高了 SAP 中间件数据传输的安全性；与 Sun 的 RFID 中间件结合，则使得 SAP 中间件的功能得到了极大的扩展。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

SAP 的企业用户大多数是世界 500 强企业，原来已经采用 SAP 的管理系统。这些企业实施 RFID 项目的规模一般都比较大，对相关软件和硬件的性能要求也比较高。这些企业实施 RFID 项目改造，应用 SAP 提供的 RFID 中间件技术可以和 SAP 的管理系统实现无缝集成，能为企业节省大量的软件测试时间、软件的集成时间，有效缩短了 RFID 项目实施步骤、时间。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

5) Sun 的 RFID 中间件

Sun 公司开发的 JAVA 语言，目前被广泛应用于开发各种企业级的管理软件。目前， Sun 公司根据市场需求，利用 JAVA 在企业的应用优势开发的 RFID 中间件，也具有独特的技术优势。

Sun 公司开发的 RFID 中间件产品从 1.0 版本开始，经历了较长时间的测试，随着产品不断完善，已经完全达到了设计要求。随着 RFID 标准 Gen2.0 的推出，目前 SUN 中间件已推出了 2.0 版本，实现了 RFID 中间件对 Gen2.0 版本的全面支持和中央系统管理。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

其中间件分为事件管理器和信息服务器两个部分。事件管理器用来帮助处理通过 RFID 系统收集的信息或依照客户的需求筛选信息；信息服务器用来得到和储存使用 RFID 技术生成的信息，并将这些信息提供给供应链管理系统中的软件系统。

由于 Sun 公司在 RFID 中间件系统中集成了 Jini 网络工具，有新的 RFID 设备接入网络时，立刻能被系统自动发现并集成到网络中，实现新设备数据的自动收集。这一功能的在储存库环境中是非常实用的。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

为了进一步扩大 SUN RFID 中间件产品的影响力， SUN 公司已经与 SAP 等几家厂商组建了 RFID 中间件联盟，将各个厂家的 RFID 中间件产品整合到一起，利用各自的企业资源，进行 RFID 中间件产品推广工作。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

6) Sybase 中间件

Sybase 原来是一家数据库公司，其开发的 Sybase 数据库在上世纪八九十年代曾辉煌一时。在收购 Xcellenet 公司后， Sybase 公司正式介入 RFID 中间件领域，并开始使用 Xcellenet 公司技术开发 RFID 中间件产品。

Sybase 中间件包括 Edgeware 软件套件、 RFID 业务流程、集成和监控工具。该工具采用基于网络的程序界面，将 RFID 数据所需要的业务流程映射到现有企业的系统中。客户可以建立独有的规则，并根据这些规则监控实时事件流和 RFID 中间件取得的信息数据。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

Sybase 中间件的安全套件被 SAP 看中，被 SAP 整合进 SAP 企业应用系统，双方还签定了 RFID 中间件联盟协议，利用双方资源共同推广 RFID 中间件的企业 RFID 解决方案。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

7) BEA 的 RFID 中间件

BEA RFID 中间件是目前 RFID 中间件领域最具竞争力的产品之一，尤其是在 2005 年 Bea 收购了 RFID 中间件技术领域的领先厂商 ConnecTerra 公司之后， ConnecTerra 的中间件整合进 BEA 的中间件产品，使 BEA 的 RFID 中间件功能得到极大的扩展。因此， BEA 可以向企业提供完整的一揽子产品解决方案，帮助企业方便地实施 RFID 项目，帮助客户处理从供应链上获取的日益庞大的 RFID 数据。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

BEA 公司的 RFID 解决方案由以下四个部分构成：

①BEA WebLogic RFID Edition ：先进的 EPC 中间件，支持多达 12 个阅读器提供商的主流阅读器，支持 EPC Class0 、 0+ 、 1 ， ISO15693 ， ISO18000-6Bv1.19EPC ， GEN2 等规格的电子标签；

②BEA WebLogic Enterprise Platform ：专门为构建面向服务型企业解决方案而设计的统一的、可扩展的应用基础架构；

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

③BEA RFID 解决方案工具箱：是实施 RFID 解决方案的加速器，包含快速配置和部署 RFID 应用系统所必需的代码、文档和最佳实践路线。主要内容包括事件模型框架、消息总线架构、预置的 portlet 等；

④ 为开发、配置和部署该解决方案提供帮助的咨询服务。该解决方案可以为客户实施 RFID 应用提供完整的基础架构，用户可以围绕 RFID 进行业务流程创新，开发新的应用，从而提高 RFID 项目投资的回报率。

目前，BEA 已成为基于标准的端到端 RFID 基础设施——从获取原始的 RFID 事件直到把这些事件转换成重要的商业数据的厂家。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

② 中国 RFID 中间件的发展现状

RFID 技术进入中国的时间比较短，各方面的工作还处于起步阶段。虽然中国政府在国家十一五规划和 863 计划中，对 RFID 应用提供了政策、项目和资金的支持，并且 RFID 在国内的发展也较为迅速，但是与国际先进技术的发展相比，在很多方面还存在明显的差距。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

中国在 RFID 中间件和公共服务方面已经开展了一些工作。依托国家 863 计划“无线射频关键技术研究与开发”课题，中科院自动化所开发了 RFID 公共服务体系基础架构软件和血液、食品、药品可追溯管理中间件。华中科技大学开发了支持多通信平台的 RFID 中间件产品 Smarti ，上海交通大学开发了面向商业物流的数据管理与集成中间件平台。此外，国内产品还包括东方励格公司的 LYNKO-ALE 中间件，清华同方的 ezRFID 中间件、 ezONE 、 ezFramework 基础应用套件等。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

目前，虽然中国已经有了一些初具规模的 RFID 中间件产品，但大多数都还没有在企业进行实际应用测试，与国外的 RFID 中间件产品相比，尚处于实验室阶段。与国外经历了很长时间企业实际测试的 RFID 中间件产品相比，还有较大的差距。国内的相关企业和研发机构应尽快完成 RFID 中间件产品的企业测试，完善 RFID 中间件的相关功能，为国内中小企业的 RFID 项目实施提供方便、实用、低成本的 RFID 中间件解决方案。

项目五　应用层安全技术

5. 2　中间件安全

5.2.3 RFID 中间件

如果中国的研发机构能够赶在企业开始大规模实施 RFID 项目之前，开发出完善、成熟、可靠的 RFID 中间件产品，加上天时、地利、人和、成本等优势，占据中国国内的 RFID 中间件市场是完全有可能的。

通过对比国内外 RFID 中间件的实际情况，不难发现，国外的 RFID 中间件产品发展的时间并不比中国 RFID 中间件早很多；只要中国的软件公司奋起直追，依托国内较低的成本优势、众多优秀的软件工程师和技术人员共同努力，在短时间内完全有可能开发出与国外的同类产品相匹敌的 RFID 中间件产品。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

物联网是一个在互联网的基础上，结合 RFID 技术和传感器技术构建的连接范围更为广阔的网络。因此，物联网安全既包括当前互联网的安全问题，又包括 RFID 和传感器技术特有的安全问题。由于物联网感知识别层中大量应用 RFID 标签和无线传感器，因此物联网特有的安全问题，主要是 RFID 系统安全和无线传感器网络安全。 RFID 标签中保存着个人私密信息，随着定位技术的发展，假如 RFID 标签受到跟踪、定位，或者个人私密信息受到窃取，就会对用户的隐私造成伤害。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

1. 中间件安全设计原则

RFID 中间件的设计，要遵循功能全面、容易设计、便于维护、具有良好的扩展性和可移植性的原则。设计 RFID 中间件至少要解决以下几个问题。

1) 屏蔽下层硬件，兼容不同的 RFID 读写器

不同生产厂家的硬件设备在读取频率、支持协议、读写范围、防冲突性能等方面有所差异。因此屏蔽物理设备的差异，能方便地进行集成扩展，这是 RFID 中间件应具有的特点。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

2) 对硬件设备进行统一管理

对硬件设备进行统一管理，包括打开、关闭、获取设备参数、发出读取指令、缓存标签、定义逻辑阅读器等，使上层的软件感觉不到设备的差异，提供透明的硬件服务。

3) 对数据流进行过滤和分组

安全中间件必须采用特定的算法和数据结构，过滤和剔除用户不感兴趣的、大量的、重复的、无规则的数据，否则，大量的垃圾数据流入上层，对企业应用程序将是一个沉重的负担，甚至会造成上层应用程序崩溃。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

4) 数据接收和数据格式转换

中间件要接收来自 RFID 设备的标签数据，并向上层传输。由于数据标签编码方式多种多样，规范标准不统一，如果不进行数据格式处理，将会导致数据混乱，难以识别。

5) 中间件的安全问题

电子标签的安全和隐私问题，制约着 EPC 技术的发展和应用。 RFID 系统在进行数据采集和数据传输时，电子标签和读写器容易受到信号的干扰，再加上电子标签容易被跟踪和定位，侵犯个人隐私，因此安全问题不可避免。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

6) 与企业应用程序的通信

企业应用程序具有自己特定的数据格式，采用何种方式与中间件进行交互，并且高效地实现中间件有应用程序之间的数据交换，也是中间件需要解决的重要问题。

2. 通用的中间件安全模型

针对中间件的安全需求，中国学者吴景阳和毋国庆等提出了一种通用的中间件安全模式。他们认为由于针对中间件层的特点进行分析，访问控制的实现依赖于引用监视器和访问策略的所在位置和实施。因此，可以根据安全逻辑的实现，将引用监视器的功能分成决策和执行两部分。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

1) 决策部分

决策部分根据访问策略来决定一个主体是否具有权限来访问它所请求的客体资源，采用决策机制的可以是自主访问控制，也可以是强制访问控制，或者是其它机制。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

2) 执行部分

执行部分接受主体的访问请求，该请求是通过下层传送上来的，由执行部分负责将该请求传递给中间层中的决策部分，并将执行结果返回决策部分。执行部分根据此决策来执行相应的动作，如果访问被允许，则根据访问请求将主体的请求信息传送给目标对象。如果需要的话，可能还要调用中间件的其他部件，执行某些特定的功能，如事务处理、数据库访问等。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

通用中间件安全模式如图 6-11 所示。

从图 6-11 中可以看出，决策部分给目标对象提供了接口，用于目标对象的注册。这是供应用层对象调用的，用于获得目标对象的相关信息，从而提供安全策略，以辅助决策部份实现其功能。这个接口的实现，一方面有效地解决了对于应用层目标对象特定信息的访问控制，另一方面也是该模型对于应用层灵活性的体现，可以很容易地满足不同应用中不同的目标对象所要求的安全机制。

项目五　应用层安全技术

5.2　中间件安全

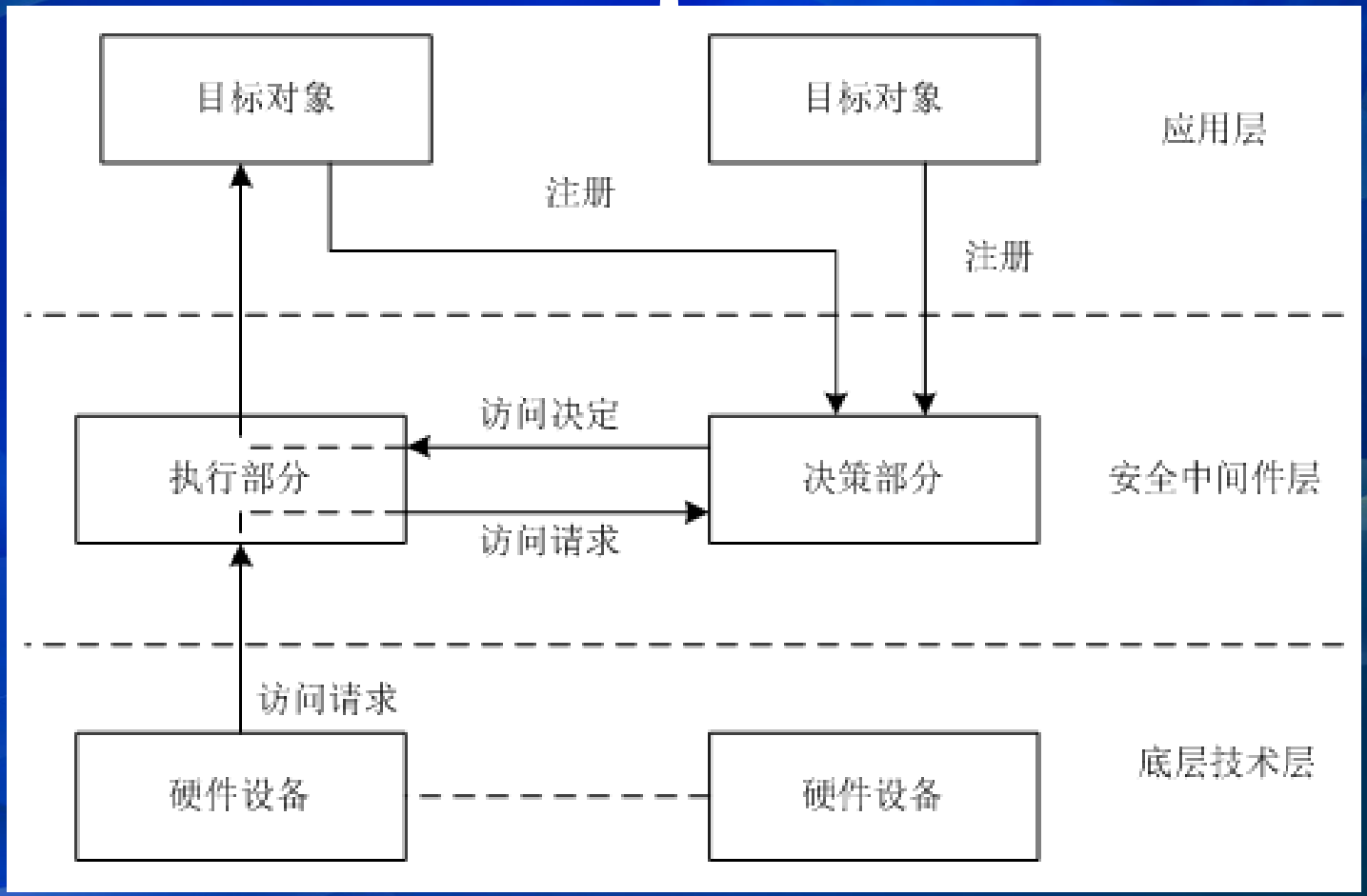

图 6-11　通用中间件安全模式

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

3. 基于中间件的物联网安全模型

中国学者姚远在 2011 年提出了一个基于中间件的物联网安全模型，认为物联网安全问题要从三个方面进行保护：存储信息安全问题、传输安全问题和设备安全问题。

一般来说，中间件的设计应遵循整体的分层原则，中间件的设计框架如图 6-12 所示。

自下向上的第一层，是包含各种不同设备的硬件、操作系统和驱动程序层。这一部分的差异较大，从低端的单片机到高端的 DSP 数字信号处理器或者 PowerPC 通信处理器都会出现在这一层。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

自下向上的第二层，是运行于各种硬件之上的软件环境，这一部分的差异较硬件层小，通常由 Linux 和 Windows CE 等各种移动终端操作系统和驱动程序组成，其功能类似。

在图 6-12 中，中间最大的一块区域是中间件的实际范围。

1）移植层

移植层用作屏蔽底层差异，实现中间件的统一实施接口，同时也是平台的主要功能的体现接口。一般来说移植层的各种软硬件分别实现各自不同的功能，其接口包括线程或任务移植接口、显示移植接口、网络和通信移植接口、平台控制和属性移植接口、 RFID 读写移植接口等。

项目五　应用层安全技术

5.2　中间件安全

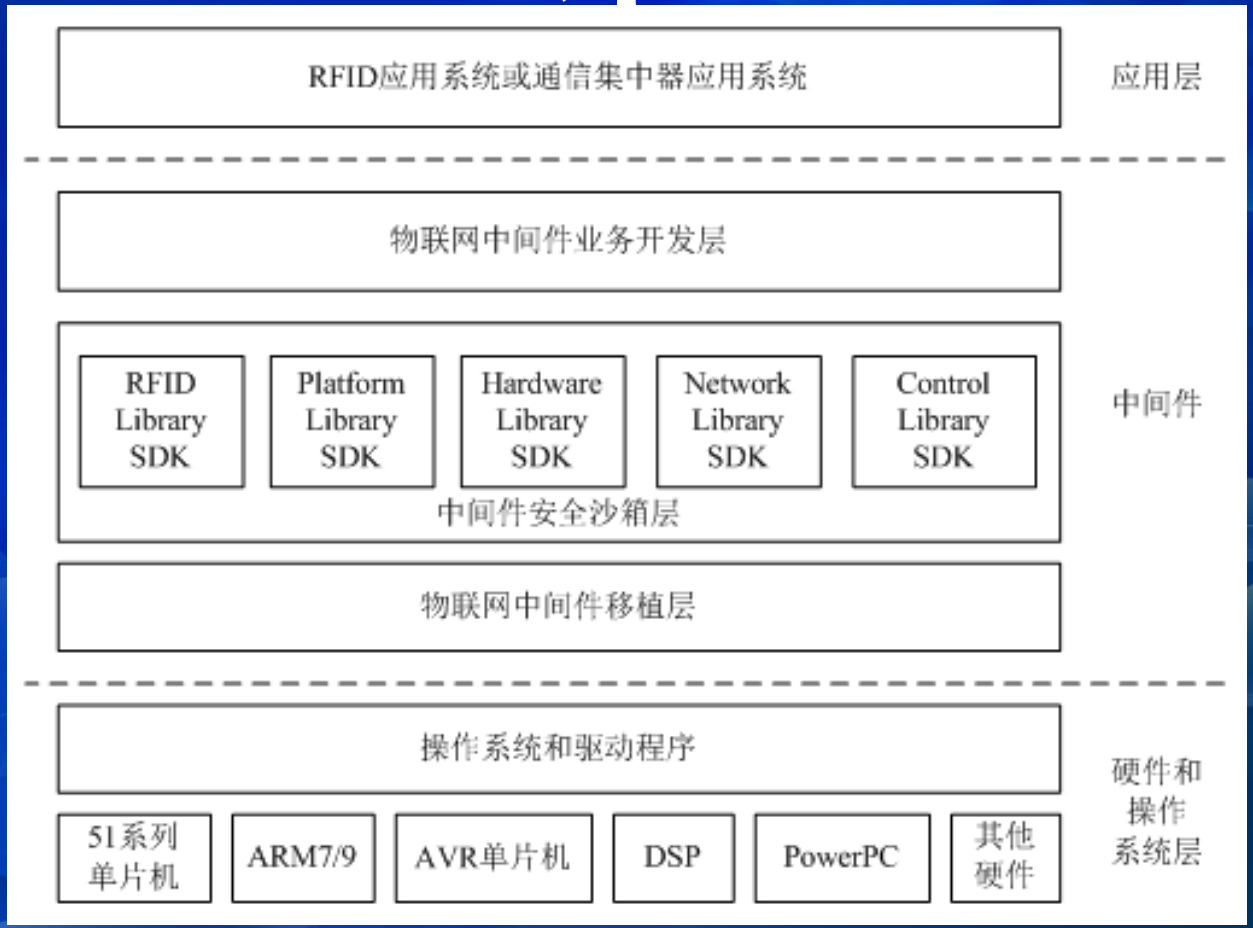

图 6-12　中间件框图

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

2) 安全沙箱层

中间件的关键模块是中间件安全沙箱层，其内部包含多种执行模块，如 RFID 模块、通讯模块和硬件控制模块等，所有的模块统一位于一个安全沙箱中。该安全沙箱可以保证通信协议和远程控制对本地资源的安全访问。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

沙箱（ Sandbox ）模型是一种保护本机安全的虚拟技术。利用沙箱技术，可以将系统关键数据进行虚拟化映射。外界对数据的获取和修正首先在沙箱映射层中实现。只有经过严格的授权才能访问底层实际硬件和资源，因此保证了设备本身不会受到病毒或恶意程序的攻击和崩溃。中间件中使用此模型时，通过远程调用和通信协议执行的一般信令，不可能访问真正的硬件设备资源。但是由于沙箱中的关键数据与系统中的数据时刻保持同步，沙箱模型并不会影响获取数据的实时性。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

3) 业务开发层

中间件的最上层是业务开发层，该层提供给本地或远程应用程序调用，以实现相应的业务功能。其接口设计一般包含物联网设备的控制，信息读写、通信、显示、授权认证等通用接口，并将这些模块的实现映射到安全沙箱中解析或执行。

物联网中间件从以下三个方面建立一个通用的安全模型：使用安全沙箱保证只有明确授权的应用程序才可以访问底层资源；支持基于 SSL 、 TSL 和 VPN 等加密通道传输信息；使用基于 X509 证书的授权方式保证终端和设备授权认证的通过。

项目五　应用层安全技术

5. 2　中间件安全

5.2.4 RFID 中间件安全

中间件支持通过插件模式挂接不同的通信适配组件，如 SSL 安全层或 TSL 传输安全层，也可以配置及挂载 VPN 通道，实现数据的安全传输。传统的网络层加密机制是逐跳加密，即信息在发送过程中和传输过程中是加密的，但是在每个节点处却没有加密。

- 谢谢各位同学！

项目五　未完待续

- 再 见 ！