云消费者以及云提供商的作用已经讨论过了。总结起来说，**云提供商**可以提供一种或多种云服务，以满足**云消费者**的 IT 和商业需求。对三种服务模型（SaaS、PaaS、IaaS）中的每一种，云提供商为该服务模型提供所需的存储空间以及处理设备。对 SaaS 而言，云服务商对云基础设施上的软件应用程序进行部署、配置、维护以及更新操作，以便为云消费者提供他所期望级别的服务。SaaS 的客户可以是向其成员提供软件应用程序的访问入口的企业组织，也可以是直接使用该软件应用程序的终端用户，还可以是为终端用户配置应用程序的软件应用程序管理者。

对 PaaS 而言，云提供商管理着平台上的计算基础设施，运行该平台上的云端软件程序，如实时软件执行堆栈，数据库以及其他中间件元件。PaaS 的云消费者可以使用云提供商提供的工具和执行资源来进行开发、测试、部署以及管理在云端的应用程序。

对 IaaS 而言，云提供商可以获得完成服务所需的物理计算资源，包括服务器、网络、存储空间以及承载基础设施。IaaS 云消费者，比如虚拟计算机，为了满足它们的基本计算需求，依次使用这些计算资源。

云载体是一个在云消费者以及云提供商之间提供连接功能以及云服务传输的网络设备。一般来说，云提供商会跟云载体之间建立服务级别协议（SLA）以便为云消费者提供与该协议级别一致的服务，同时有可能需要云载体在云消费者与云提供商之间提供专用的安全连接。

当云服务特别复杂，以至于云消费者没法轻易进行管理时，**云代理商**就显得非常重要。云代理商可以提供三种类型的支持服务：

- **服务中介**：这些都是增值服务，比如身份管理、性能报告、安全增强。
- **服务聚合**：云代理商结合了多种云服务以便满足消费者需求，这些服务不局限于由一家云提供商提供，最终的目的是性能最优化或者成本最低化。
- **服务套利**：它跟服务聚合类似，唯一的不同是，被聚合的服务并不是固定不变的。服务套利意味着代理商可以灵活地从多个代理机构中选择服务。比如，云代理商可以使用信用评分服务，从中选择一家得分最高的代理机构。

云审计商可以依据安全控制、隐私影响、性能等诸多因素评估云提供商提供的服务。审计商是一个独立的实体，它可以保证云提供商符合一系列的标准要求。

5.5　云安全风险和对策

一般来讲，云计算中的安全控制跟任何 IT 环境中的安全控制类似。但是，云服务中使用的操作模型和技术，使得云计算中有可能会出现与特定云环境相关的风险。在这方面的基本观点是，企业虽然丧失了大量的对资源、服务以及应用程序的控制，但是必须保持对安全和隐私策略的可计量性。

下面列出了云安全联盟[CSA 10]提出的云安全方面的主要威胁，同时提供了一些防护对策：

- **滥用和恶意使用云计算**：对许多云提供商来说，注册并且使用它们提供的云服务是相对容易的，而且，有些提供商甚至提供免费有限的试用期。这使得攻击者可以进入云并且进行一系列的攻击，比如发送垃圾邮件，恶意代码攻击以及拒绝服务攻击。