



中山大學 软件工程学院  
SUN YAT-SEN UNIVERSITY SCHOOL OF SOFTWARE ENGINEERING

# SSE316 : 云计算技术 Cloud Computing Technology

陈壮彬

软件工程学院

<https://zbchern.github.io/sse316.html>



# 云计算安全

- ❖ 云计算安全介绍
- ❖ 用户关心的云安全问题
- ❖ 云计算部署和交付模型的安全性
- ❖ 云计算安全问题实例



# 云计算安全

- ❖ 云计算安全介绍
- ❖ 用户关心的云安全问题
- ❖ 云计算部署和交付模型的安全性
- ❖ 云计算安全问题实例

# 云计算的优势



- 更低的 IT 初始/运营成本 ( Pay-as-you-go )
- 可扩展性和灵活性
- 更高的可用性与可靠性 ( 数据备份 , 自动系统运维 )
- 随时随地可访问 ( 使用任何网络设备执行相同的任务 )
- ...

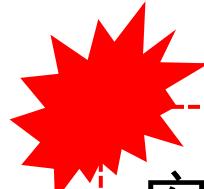
# 使用云计算的顾虑



如果云计算这么好，为什么不是人人都用呢？



安全和隐私是用户最大的顾虑！



# 新技术早期顾虑



- 事实上，在技术生命周期的早期，人们对如何使用这项技术有很多担忧
- 对于要把数据运行在第三方平台，用户存在顾虑
- 然而，随着时间的推移，这种担忧逐渐消失，特别是对价值追求的意向足够强大时

# ChatGPT 存在类似的顾虑



- 2023年4月10日新闻：Yoshua Bengio 和马斯克一起，联合众多科学家签署了关于“**暂停6个月 AI 大模型研究**”的呼吁申请
- Andrew Ng 和 Yann LeCun 对此有不同意见

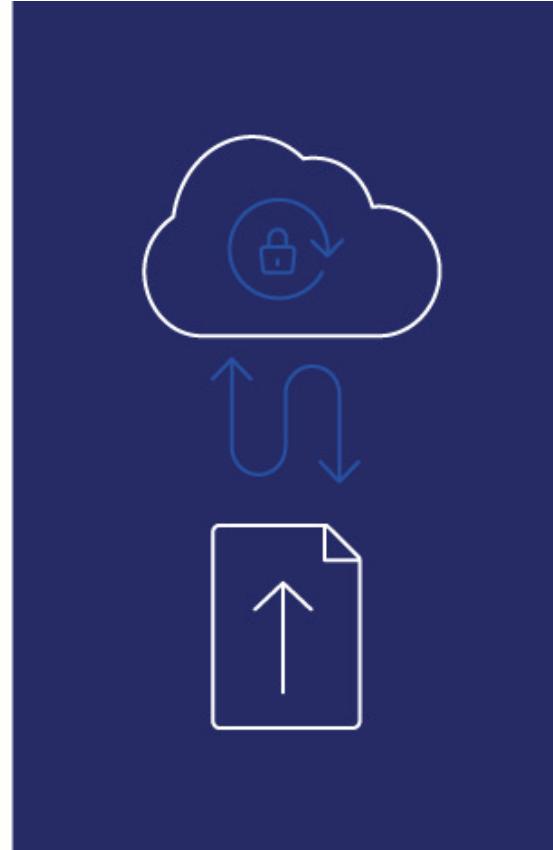
**GPT-5不能停！吴恩达LeCun直播回怼：**  
**汽车都还没发明要什么安全带**

▷ 播报文章

# 现今云计算安全的表现



94% of business claimed saw an improvement in security after switching to the cloud. 91% said it the cloud makes it easier to meet government compliance requirements.



# 但是，云安全问题仍频繁发生



## McDonald's discloses data breach after theft of customer, employee info

Jun 11, 2021



"While we were able to close off access quickly after identification, our investigation has determined that a small number of files were accessed, some of which **contained personal data including Korea and Taiwan customer data**"

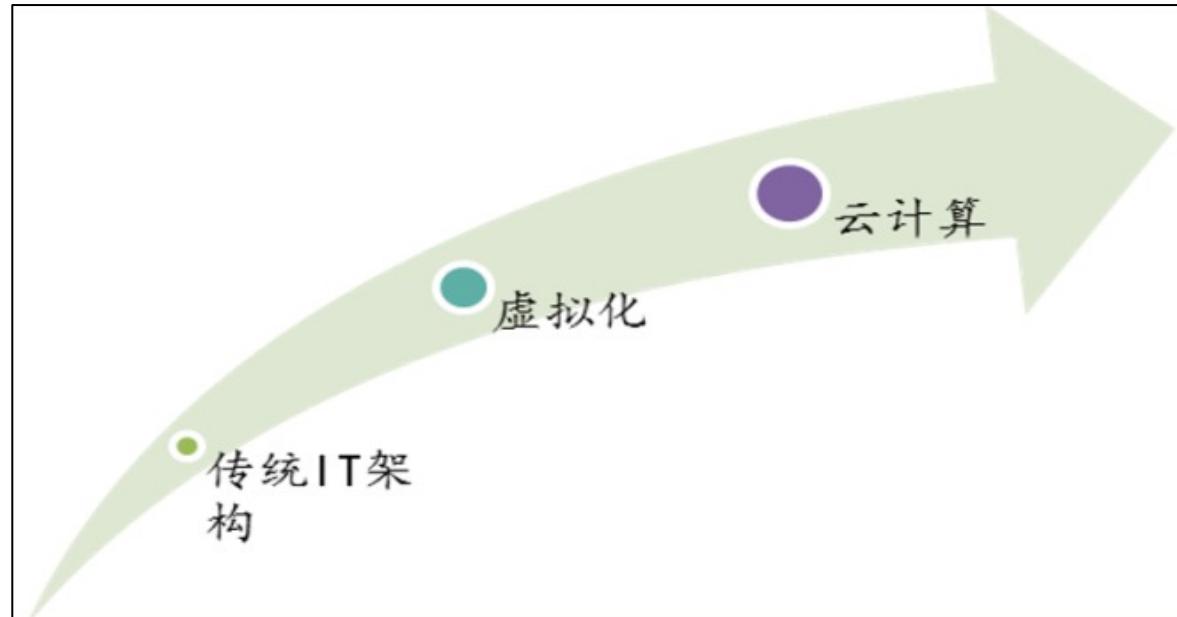
## Audi, Volkswagen data breach affects 3.3 million customers

Jun 12, 2021



"The data also included more sensitive information relating to eligibility for a purchase, loan, or lease. **More than 95% of the sensitive data** included was driver's license numbers. "

# 信息安全 “云化”



IT 基础架构的变迁

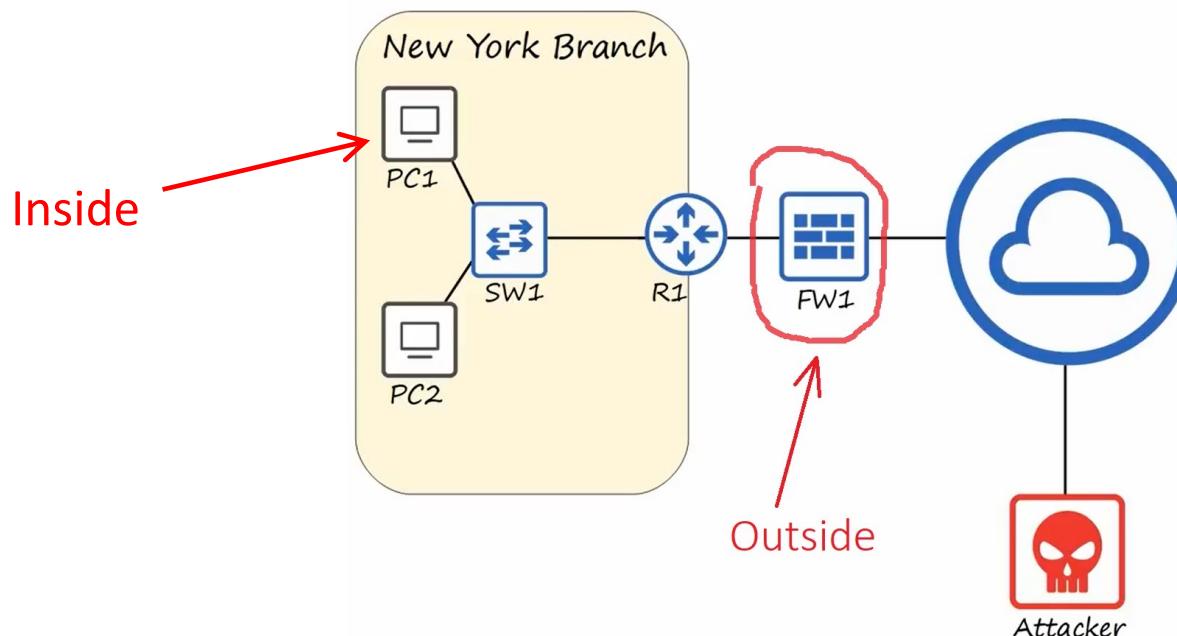
**IT 基础架构的改变是信息安全 “云化” 的根本原因**

**“云安全” 的诞生其实是信息安全对 “云架构” 的适应的结果，可以说是云环境下的信息安全**

# 传统 IT 基础架构的信息安全



- 最初的传统网络安全防护措施主要以网络边界上的防御为主，  
边界内的主机一般不具有或只具有很弱的防御能力
  - ✓ 边界上的防护措施：防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）
  - ✓ 边界内的主机防御：防恶意软件，如病毒、木马



# 传统 IT 基础架构的信息安全

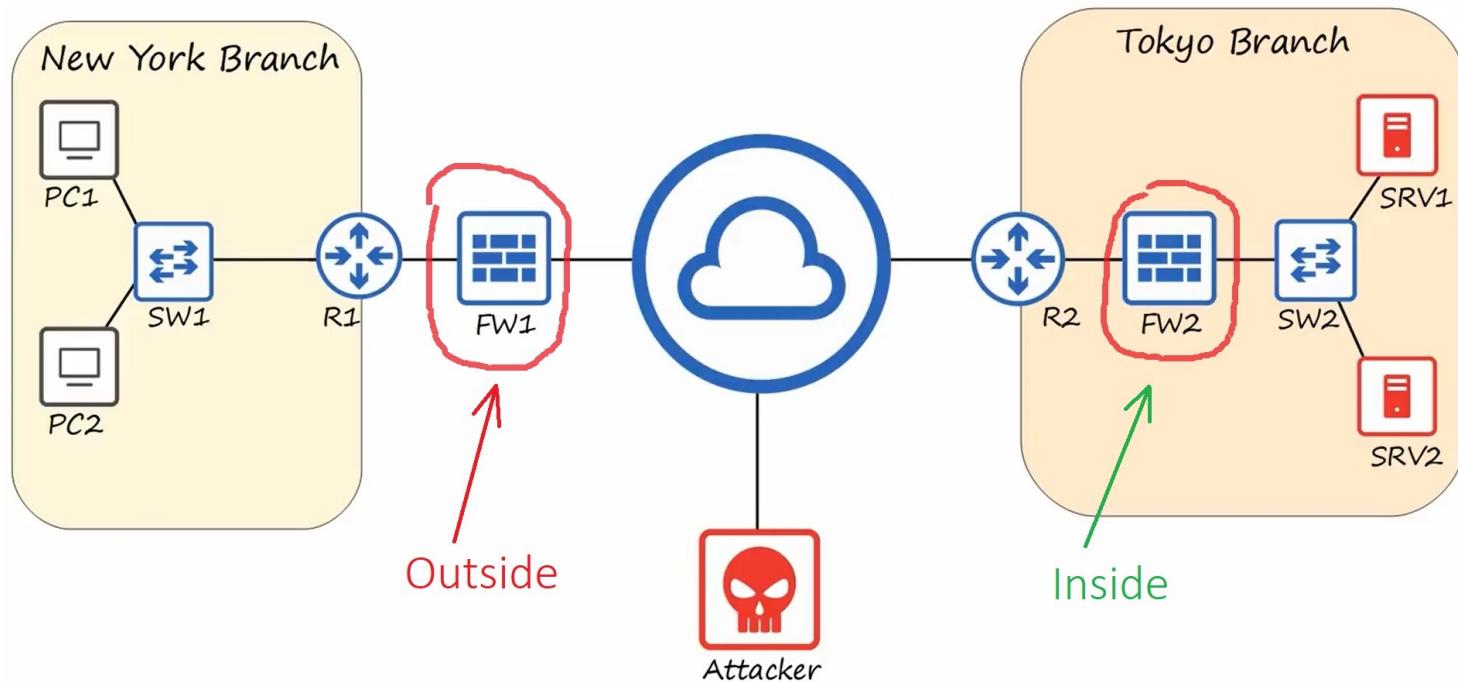


- 但是网络边界上的防护措施并不能阻隔所有的威胁
  - ✓ 首先，防火墙自身可能存在**设计上的漏洞**
  - ✓ 其次，内部黑客可以**从网络内部发起攻击**
  - ✓ 再次，外部的黑客可以通过**绕过防火墙的连接**（如拨号上网）**等方式攻入内部网络**

# 传统 IT 基础架构的信息安全



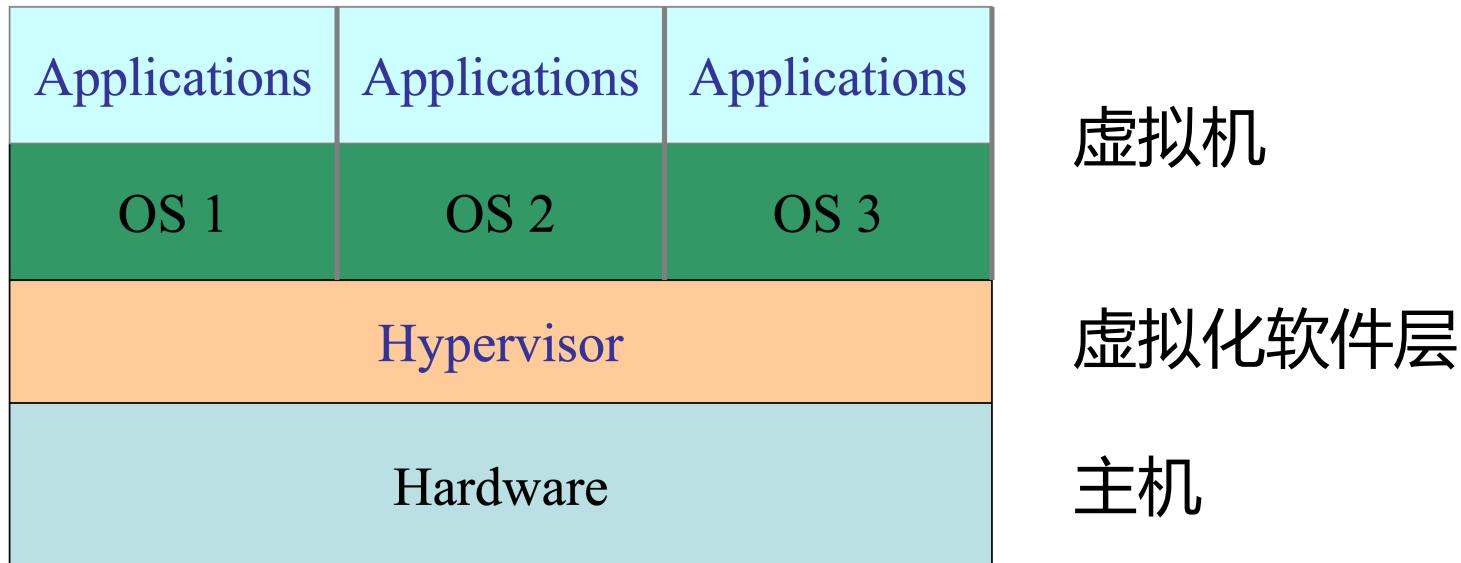
- 所以有必要对边界内的主机进行更深层次的防护，与内部一样采取防火墙、防恶意软件、IDS/IPS的防御方式
- 与网络边界上的安全措施共同组成一个防护网



# 虚拟化架构



- 虚拟化技术使得实时创建、删除虚拟机，并使在虚拟机之间迁移应用和数据成为可能



# 虚拟化架构的信息安全问题



安全问题	说明
Hypervisor 安全	(1) Hypervisor 本身代码量巨大、功能结构复杂存在大量已知的和未知的安全漏洞 (2) Hypervisor 承载了大量虚拟机，一旦被攻陷，所有受其管辖的虚拟机都将遭受未授权访问
虚拟机（VM）加固	虚拟机镜像可能存在安全漏洞，易导致用户遭受攻击，云服务提供商应该对虚拟机实施安全加固和保护
不同可信级别的虚拟机混杂	同一个物理机存在多个可信级别的 VM，如果低可信级别的虚拟机遭受攻击，很可能成为对其他高可信级别虚拟机进行进一步攻击的跳板，从而降低整体的安全级别
虚拟机间攻击	多租户环境下，多个用户共享计算、存储、网络等资源，如果某些共享模块存在漏洞，则租户可对其他租户发动攻击
虚拟机盲点	(1) 传统网络流量都会经过路由器和交换机，从而可以对流量进行安全分析和处理，但是通过虚拟化网络传输的流量不经过任何网络设备，从而对安全设备不可见 (2) 同一物理主机上的虚拟机可能通过硬件背板而不是网络进行通信，这些流量的安全性不可见
安全防护过期	当虚拟机被关闭时其配置是安全的，但是一段时间过后被再次启动时，所处环境可能已经发生重大变化，由于虚拟机未更新而导致安全防护过期，产生漏洞
虚拟机蔓延	(1) 由于业务需求保留一定量冗余的虚拟机，或虚拟机在创建时没有经过审核和验证导致不必要的配置，因为不知道这些虚拟机创建的原因，从而不敢删除和回收，不得不任其消耗计算资源； (2) 由于虚拟机生命周期管理流程的缺陷，许多虚拟机镜像文件及其副本依然保存在硬盘上，从而占据大量服务器存储资源
虚拟机镜像安全	虚拟机镜像有被窃取和篡改的脆弱漏洞，且以文件形式存在能够轻易通过网络传输到其他位置
虚拟机迁移安全	(1) 虚拟机在不同的物理服务器之间迁移增加了审计和安全监测的复杂度 (2) 在迁移过程（通道）中，可能发生被盗取和窃听的问题 (3) 一些重要虚拟机可能迁移到不安全的物理服务器上
虚拟机数据安全清除	当虚拟机从一个物理服务器上迁出或用户撤除云服务时，要确保没有任何数据残留在磁盘上从而避免被恶意恢复

资料来源：《云计算信息安全管理——CSA C-STAR 实施指南》，兴业证券研究所

# 虚拟化架构的信息安全问题



## 安全问题

## 说明

### Hypervisor 安全

- (1) Hypervisor 本身代码量巨大、功能结构复杂存在大量已知的和未知的安全漏洞
- (2) Hypervisor 承载了大量虚拟机，一旦被攻陷，所有受其管辖的虚拟机都将遭受未授权访问

### 虚拟机（VM）加固

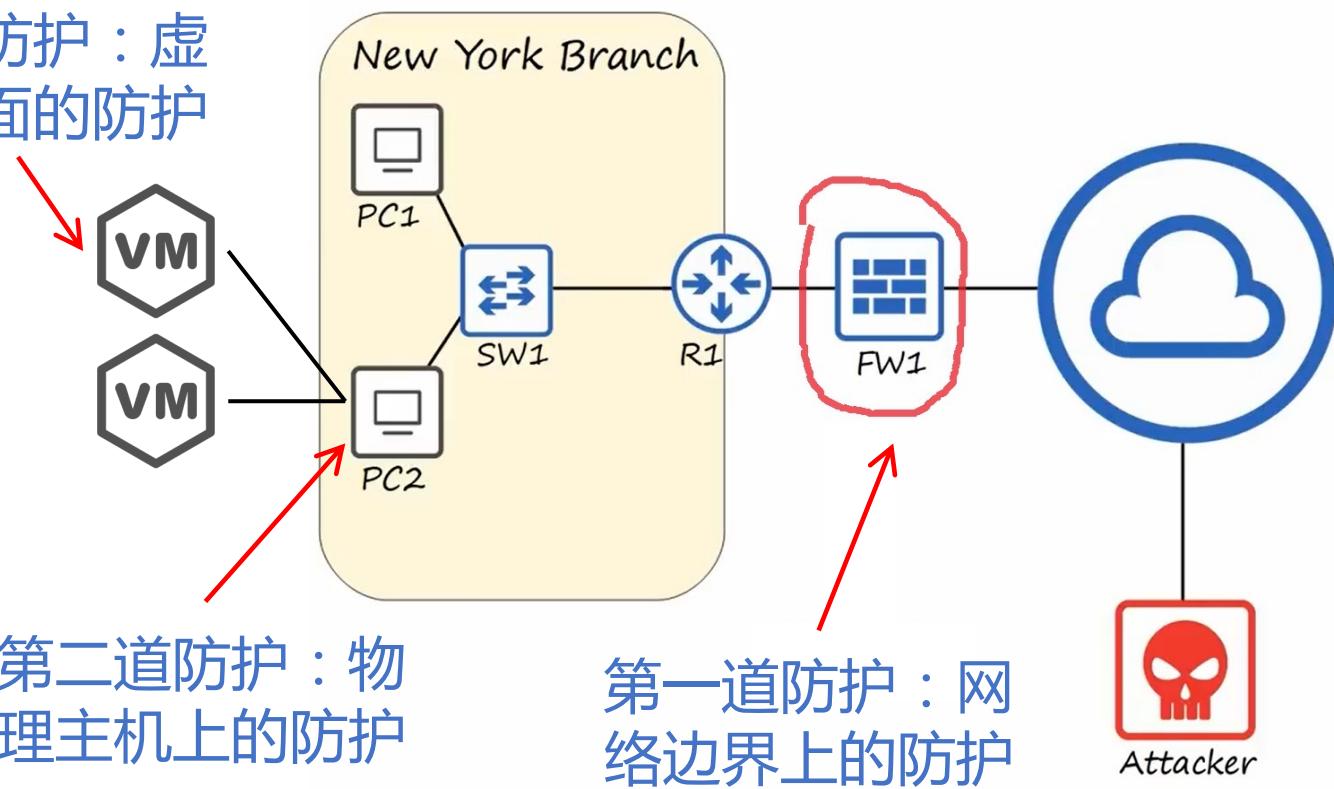
虚拟机镜像可能存在安全漏洞，易导致用户遭受攻击，云服务提供商应该对虚拟机实施安全加固和保护

# 虚拟化架构的信息安全



- 安全措施需要覆盖至每一个逻辑主机节点上，即将原来只延伸到物理主机上的防护扩展至每一个虚拟机（VM）上

第三道防护：虚拟机层面的防护



第二道防护：物理主机上的防护

第一道防护：网络边界上的防护



# 云计算安全

- ❖ 云计算安全介绍
- ❖ 用户关心的云安全问题
- ❖ 云计算部署和交付模型的安全性
- ❖ 云计算安全问题实例

# 用户关心的安全性问题

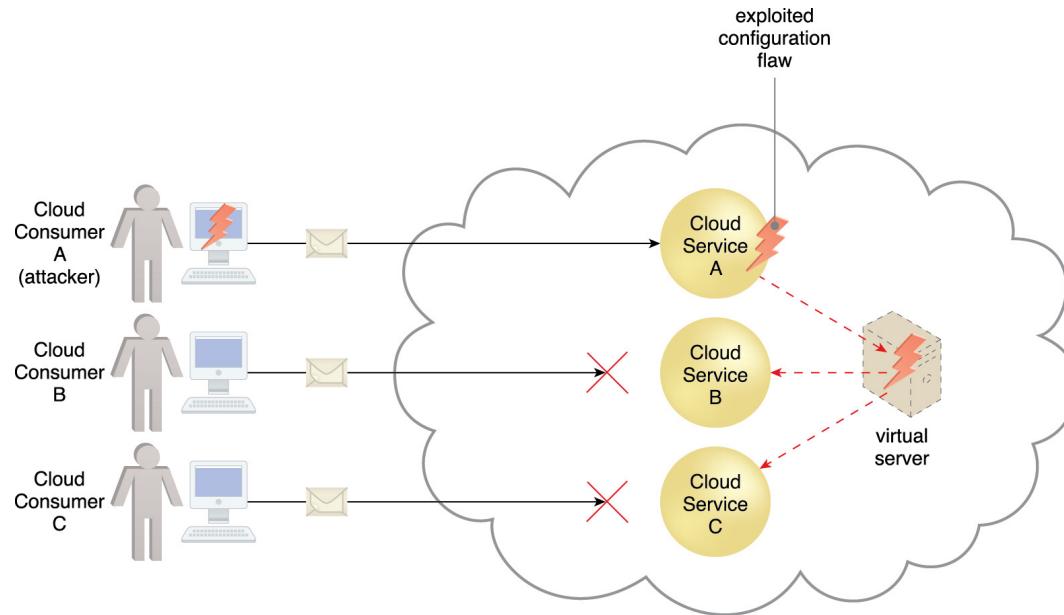


- 云就像一个**大黑匣子**，客户**不知道**云内的具体情况
- 即使云提供商是诚实的，它也可能有**恶意的系统管理员**违反安全准则
- 云仍然受制于传统的数据机密性、完整性、可用性和隐私问题，以及一些**额外的攻击**

# 云计算安全问题的根因



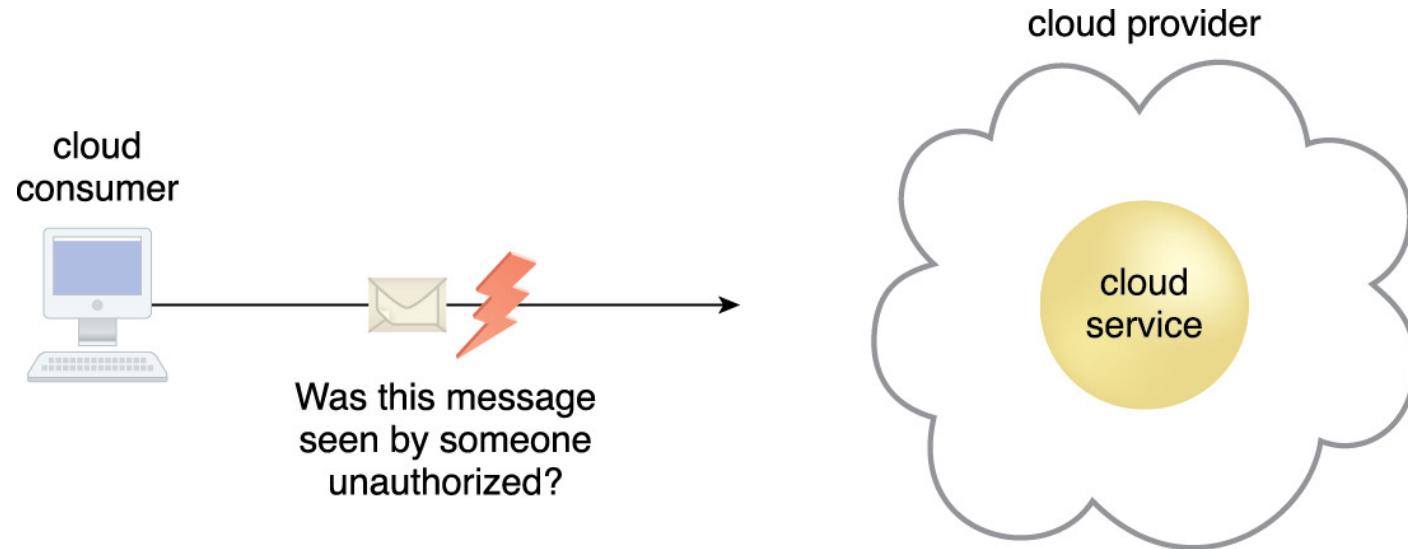
- 大多数云计算安全问题由下列因素导致
  - ✓ 用户缺乏控制权（访问/安全策略由云提供商制定）
  - ✓ 用户缺乏对云服务提供商的信任
  - ✓ 多租户架构



共享底层计算资源使得租户间的攻击成为可能

# 安全问题的类型

- 保密性（Confidentiality）：事物只有被授权才能访问。  
在云中，保密性主要是关于对**数据的传输和存储的访问限制**

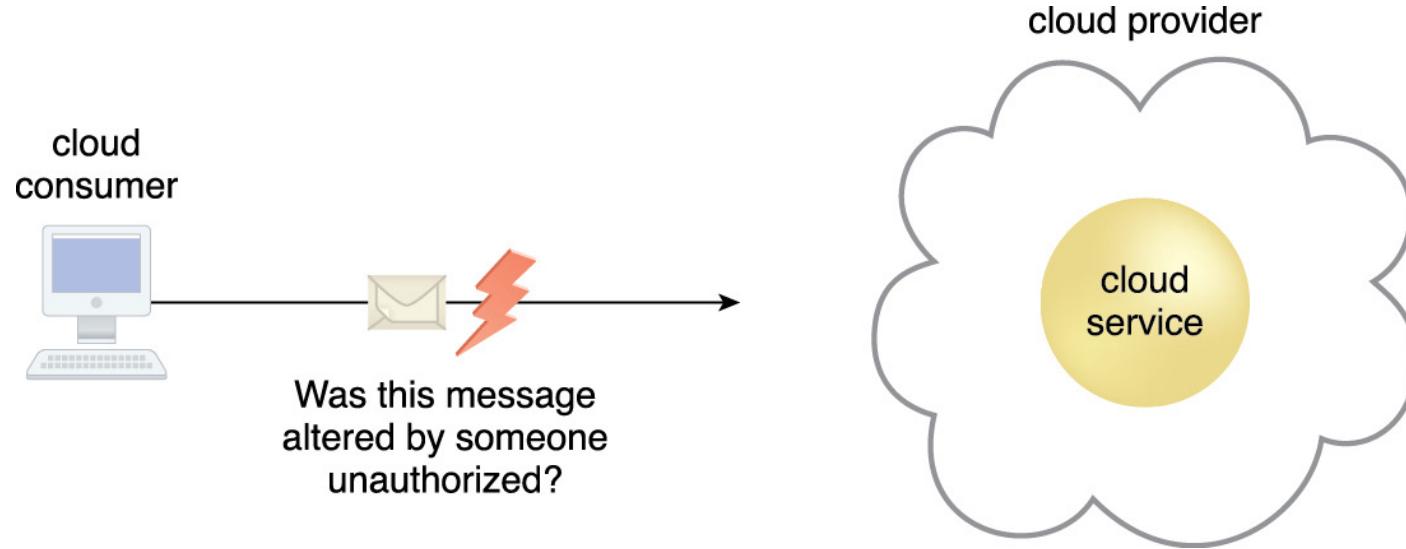


- 用户担心的问题
  - ✓ 失去对数据的控制（由于恶意的攻击或无意的失误）
  - ✓ 云提供商本身是否会诚实，不会窥探数据？

# 安全问题的类型



- 完整性 (Integrity) : 是指数据未被篡改的特性



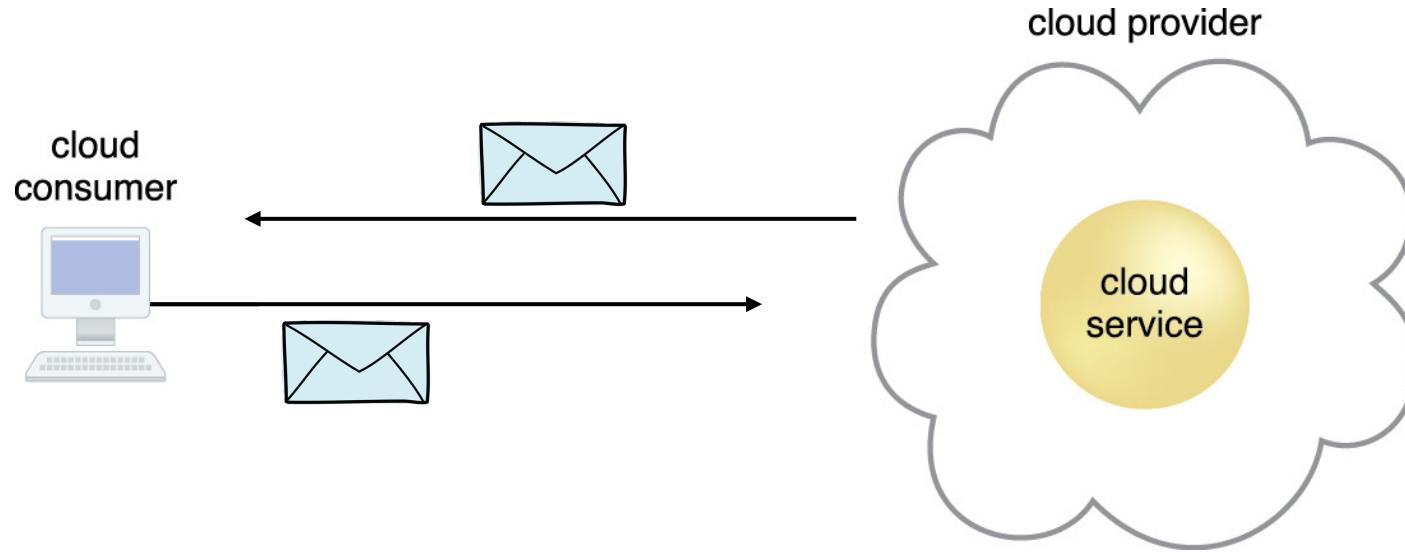
- 用户关心的问题

- ✓ 我如何知道数据在传输过程中未被篡改？
- ✓ 我如何确保云提供商在不篡改我存储的数据？

# 安全问题的类型



- 可用性（Availability）：用户在特定时间段内可以访问和使用数据的特性



- 用户关心的问题
  - ✓ 如果提供商受到攻击，客户的关键系统会崩溃吗？
  - ✓ 如果云提供商倒闭，会发生什么？
  - ✓ 云的规模足够存储所有数据吗？



# 安全问题的类型

- 大规模数据挖掘引发的隐私问题 ( Privacy issues raised via massive data mining )
  - ✓ 云存储来自许多客户的数据，可以运行数据挖掘算法来获取客户端的大量信息

**OpenAI confirms ChatGPT data breach**

Some users payment information may have been visible to other users

# 安全问题的类型



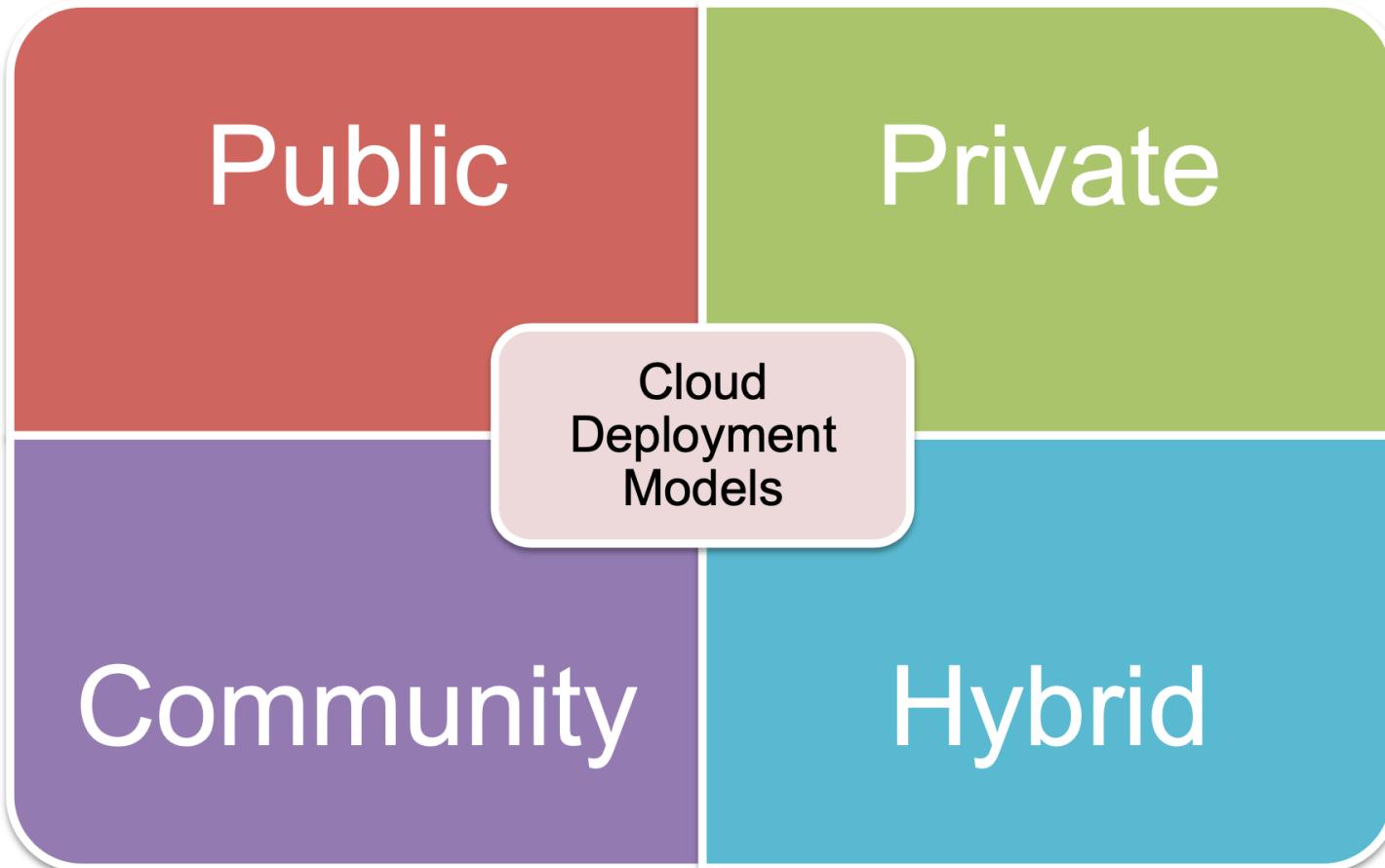
- 法律与可信任转移问题 ( Legal and transitive trust issues )
  - ✓ 取证困难，更新迅速，操作历史被擦除
  - ✓ 如果云提供商分包给第三方机构，数据是否仍然安全？
- 更多的攻击点 ( Increased attack surfaces )
  - ✓ 攻击者瞄准云提供商和客户端之间的通信链路
  - ✓ 直接窃取存储用户数据的存储介质
  - ✓ ...



# 云计算安全

- ❖ 云计算安全介绍
- ❖ 用户关心的云安全问题
- ❖ 云计算部署和交付模型的安全性
- ❖ 云计算安全问题实例

# 云部署模型



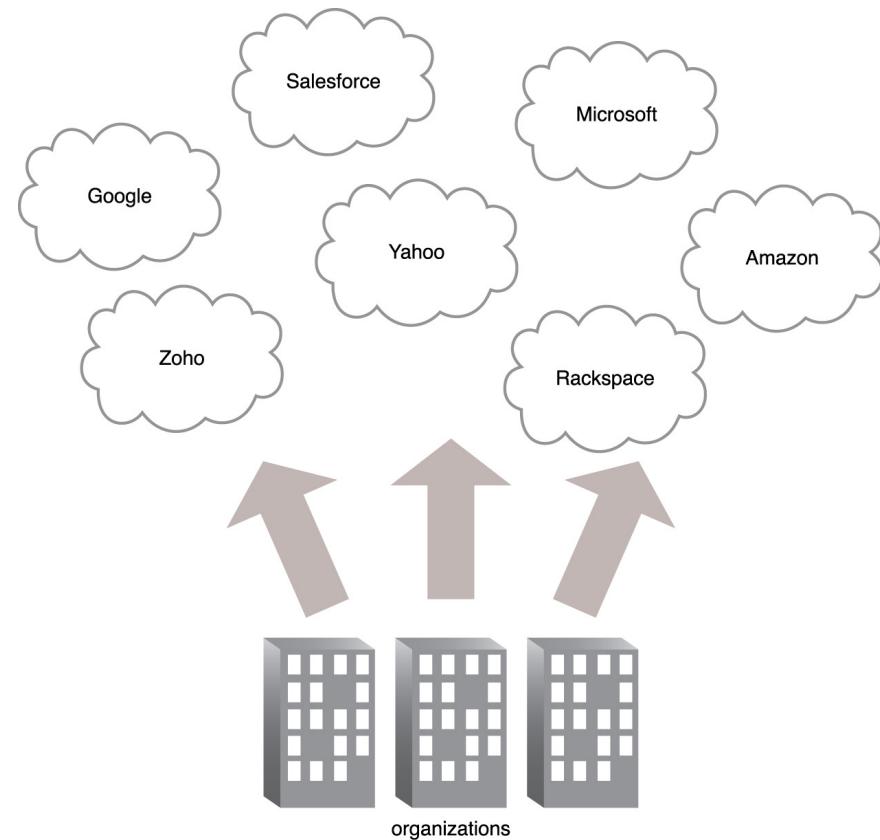
# 公有云的安全性



- 由第三方运营，如阿里云、华为云
- 通常离用户所在地较远，通过互联网访问
- 通过复用硬件和软件提供 IT 资源，价格优惠

## 安全性

- ✓ 安全性由云提供商提供
- ✓ 控制权限更低



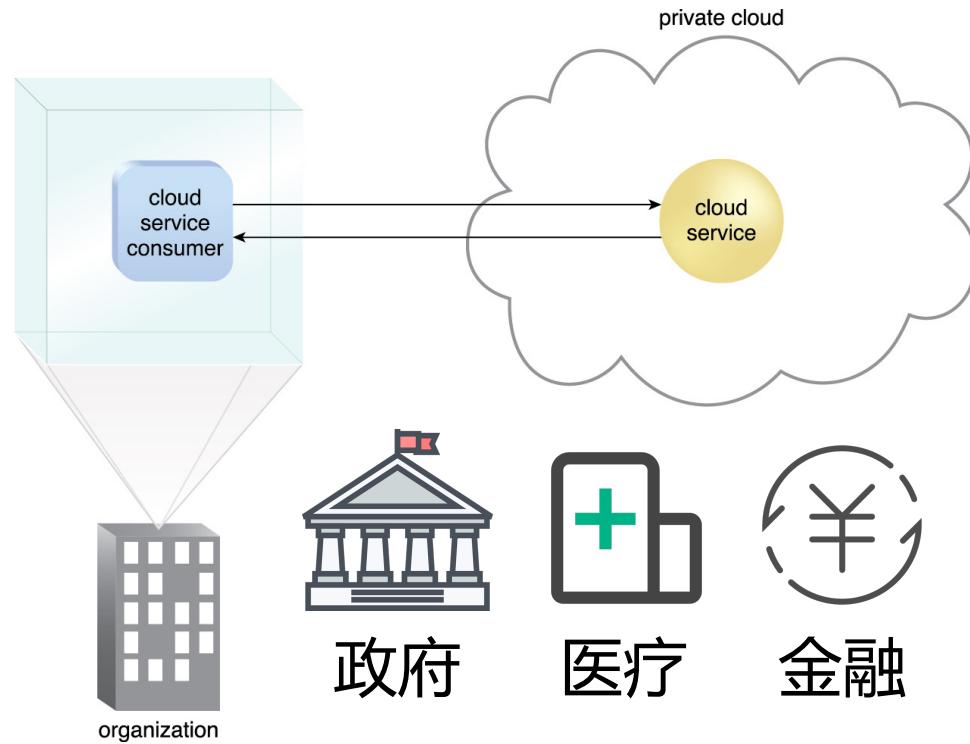
# 私有云的安全性



- 客户专属的云资源，价格较高
- 部署在企业数据中心或临近的办公地点

## 安全性

- ✓ 对数据、安全性和 QoS 的完全控制
- ✓ 控制权限高但更复杂



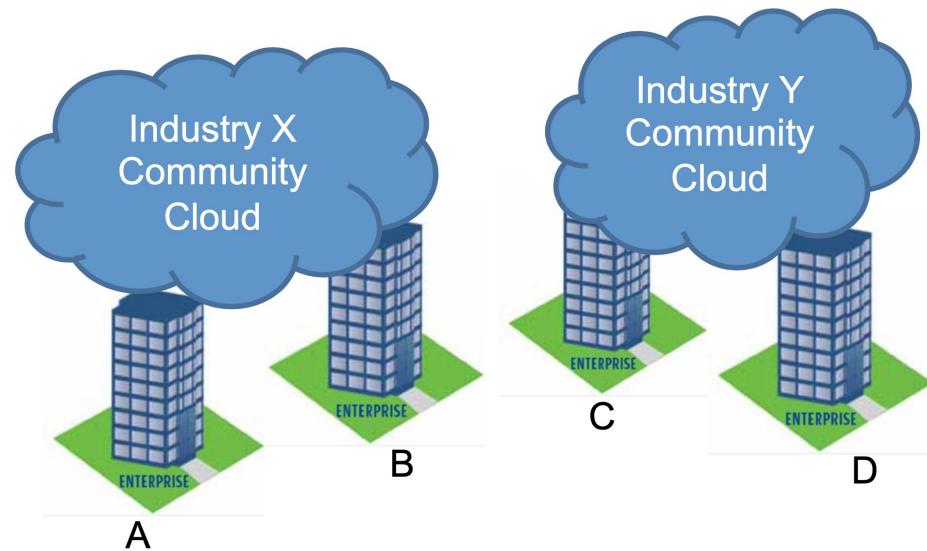
# 社区云的安全性



- 来自同一社区的多个组织共享云基础设施
- 共享在安全措施和基础设施方面的成本

## 安全性

- ✓ 控制权限比公有云高但也有来自社区内部的威胁
- ✓ 需要协调所有成员的安全策略和控制



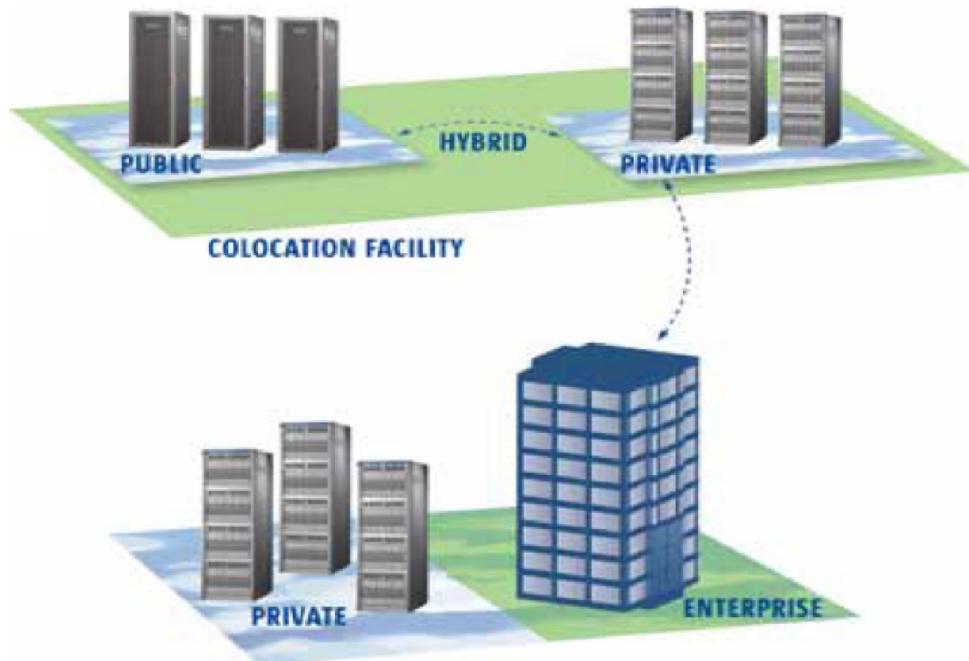
# 混合云的安全性



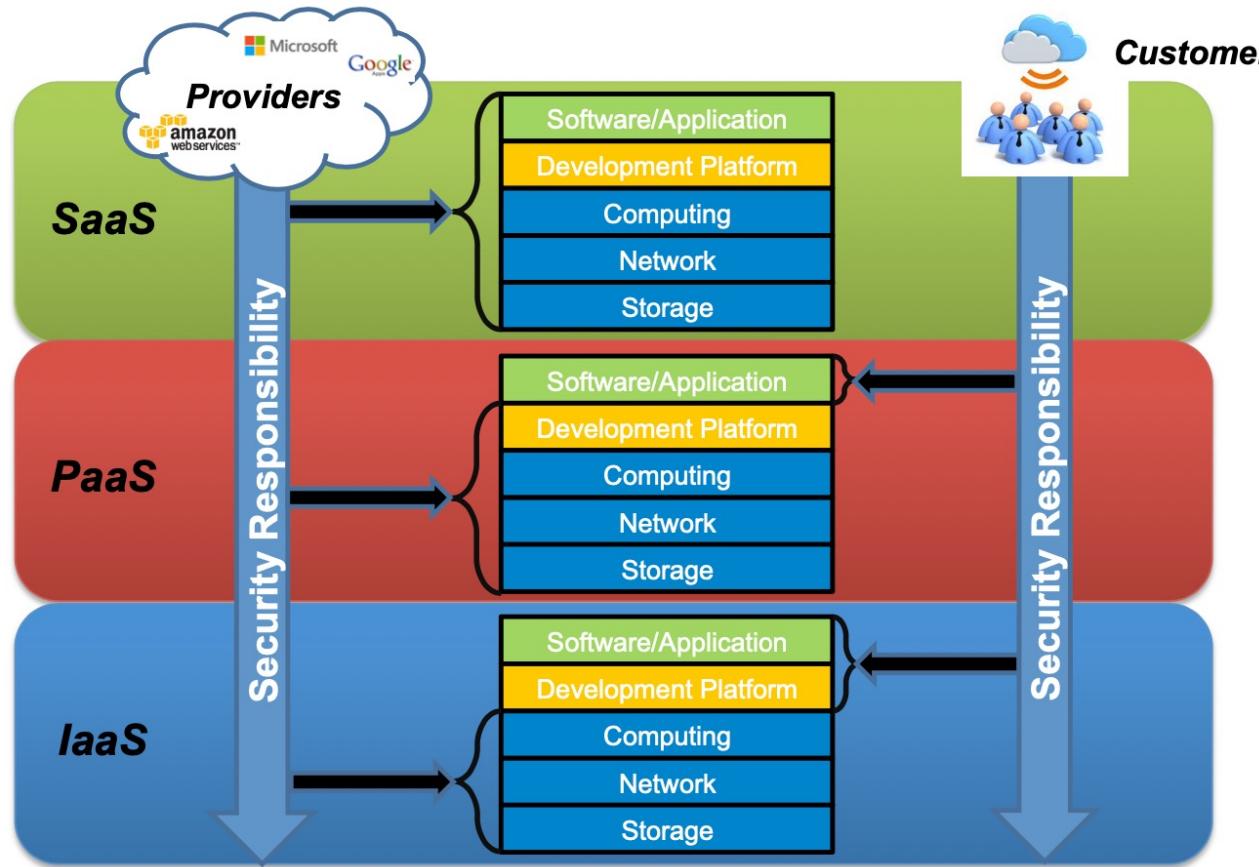
- 结合了私有云和公共云
- 重要隐私数据存储在私有云，公有云提供额外计算资源处理隐私性低的数据，经济效益高

## 安全性

- ✓ 控制权限灵活
- ✓ 网络配置复杂，造成安全隐患
- ✓ 数据传输至公有云可能导致隐私数据泄漏



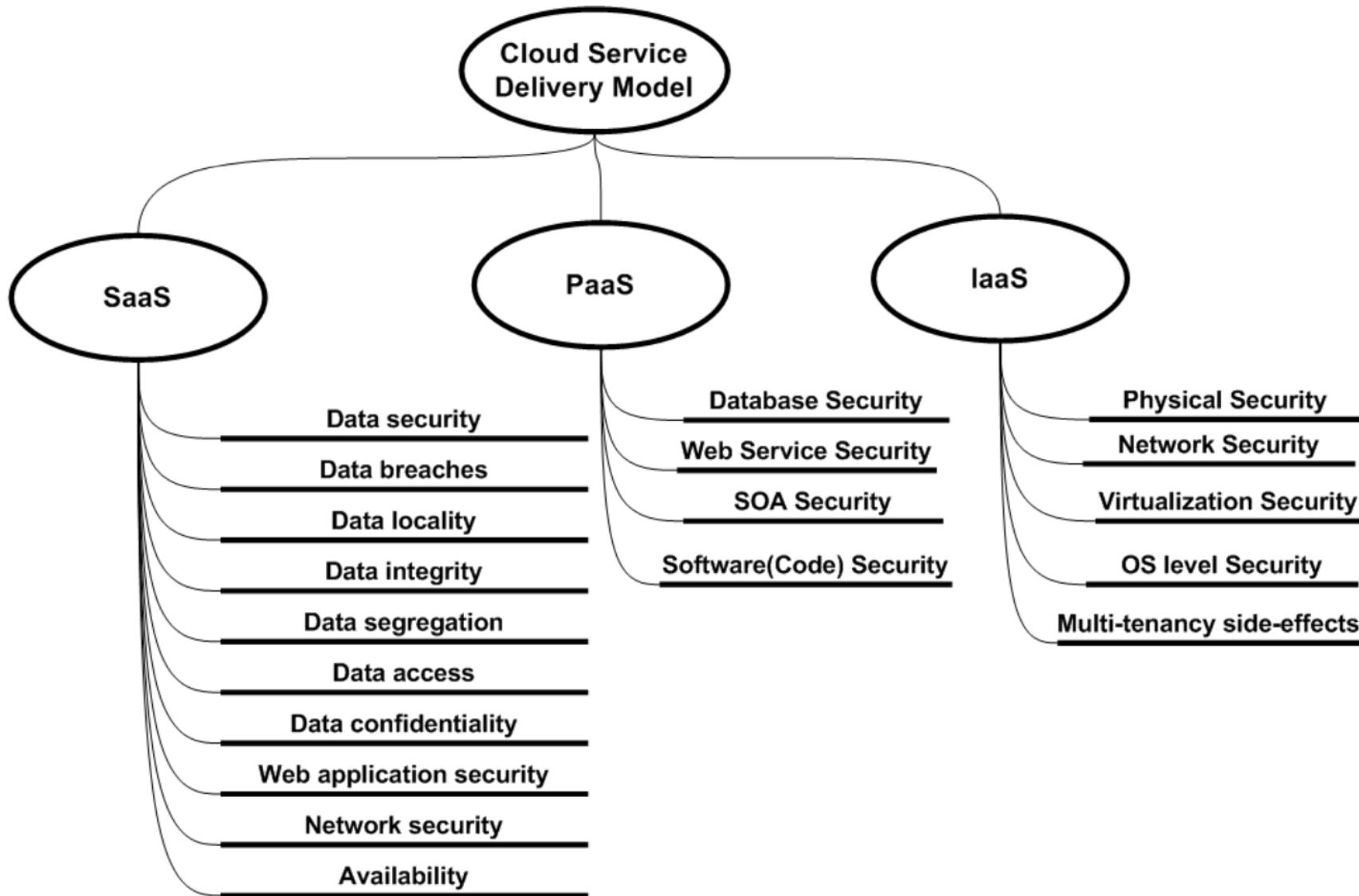
# 云计算交付模型的安全性



越底层的交付  
模型需要用户  
负责越多的安  
全性问题

云计算时代下，信息安全的防护越来越多地**需要**  
**用户（云租户）密切参与**，即整体的安全责任是  
由**云租户和云服务商共担**。

# 不同云交付模型的安全问题



# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁

# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁



- **数据安全等级划分**

不同用户（个人、政府、企业）的数据安全级别划分不同，多个用户数据存储在同一位置，**安全级别划分策略比较混乱**

- **审计策略指定**

云环境下用户对自己的数据进行**跟踪审计**难上加难

# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁



- **数据存放位置不确定**

云环境下用户无法确定数据存放的地理位置

- **数据混合存储**

不同用户的各类数据都存放在云端，需要有效的数据隔离策略

- **数据丢失或者被篡改**

造成这一后果的可能因素有：云服务器被病毒或木马入侵、云提供商不可信或管理措施不当、云服务器遭受自然灾害

# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁



- **访问控制**

如果云提供商制定的**访问策略不合理、不全面**，那么可能造成非授权用户非法访问

- **数据传输风险**

用户通过网络使用云端数据，数据可能被非法拦截，或因网络攻击而无法获得数据

# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁



- **信息丢失**

由于不同云数据共享时要对数据格式进行转换，转换格式后面临**数据可能丢失的风险**

- **应用安全**

数据共享可能通过特定的应用实现，如果**应用本身有安全漏洞**，则应用上的数据就有泄漏、丢失、篡改的风险

# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁



注：数据归档是指将不常用的数据移到一个单独的存储设备长期保存的过程

- **法律和合规**

特殊数据对归档所使用介质和使用有特殊规定，云提供商可能**不支持这些规定而造成无法归档**

# 云环境下的数据安全问题



## 云环境下数据生命周期

产生

存储

使用

共享

归档

销毁



- **数据被删除后可能被重新恢复**

- **云提供商不可信**

用户无法确认云服务是否真正执行了删除命令，云服务可能留有被删除数据的多个备份



# 云计算安全

- ❖ 云计算安全介绍
- ❖ 用户关心的云安全问题
- ❖ 云计算部署和交付模型的安全性
- ❖ 云计算安全问题实例

# 云计算安全问题实例



- 2013 年云安全联盟 ( CSA, Cloud Security Alliance ) 指出云计算面临的**九大威胁**：
  1. 数据泄漏 ( Data breaches )
  2. 数据丢失 ( Data loss )
  3. 账号劫持 ( Account hijacking )
  4. 不安全的 API ( Insecure APIs )
  5. 拒绝服务攻击 ( Denial of service )
  6. 恶意内部人员 ( Malicious insiders )
  7. 云计算滥用 ( Abuse of cloud services )
  8. 审查不充分 ( Insufficient due diligence )
  9. 共享技术带来的问题 ( Shared technology issues )

# 数据泄漏



- 数据泄漏是当未经授权的个人或实体访问、检索或查看存储在云中的敏感信息时发生的
- 常见例子
  - ✓ 黑客剽窃、散播用户数据
  - ✓ 云数据库因配置错误导致数客户的个人数据泄漏

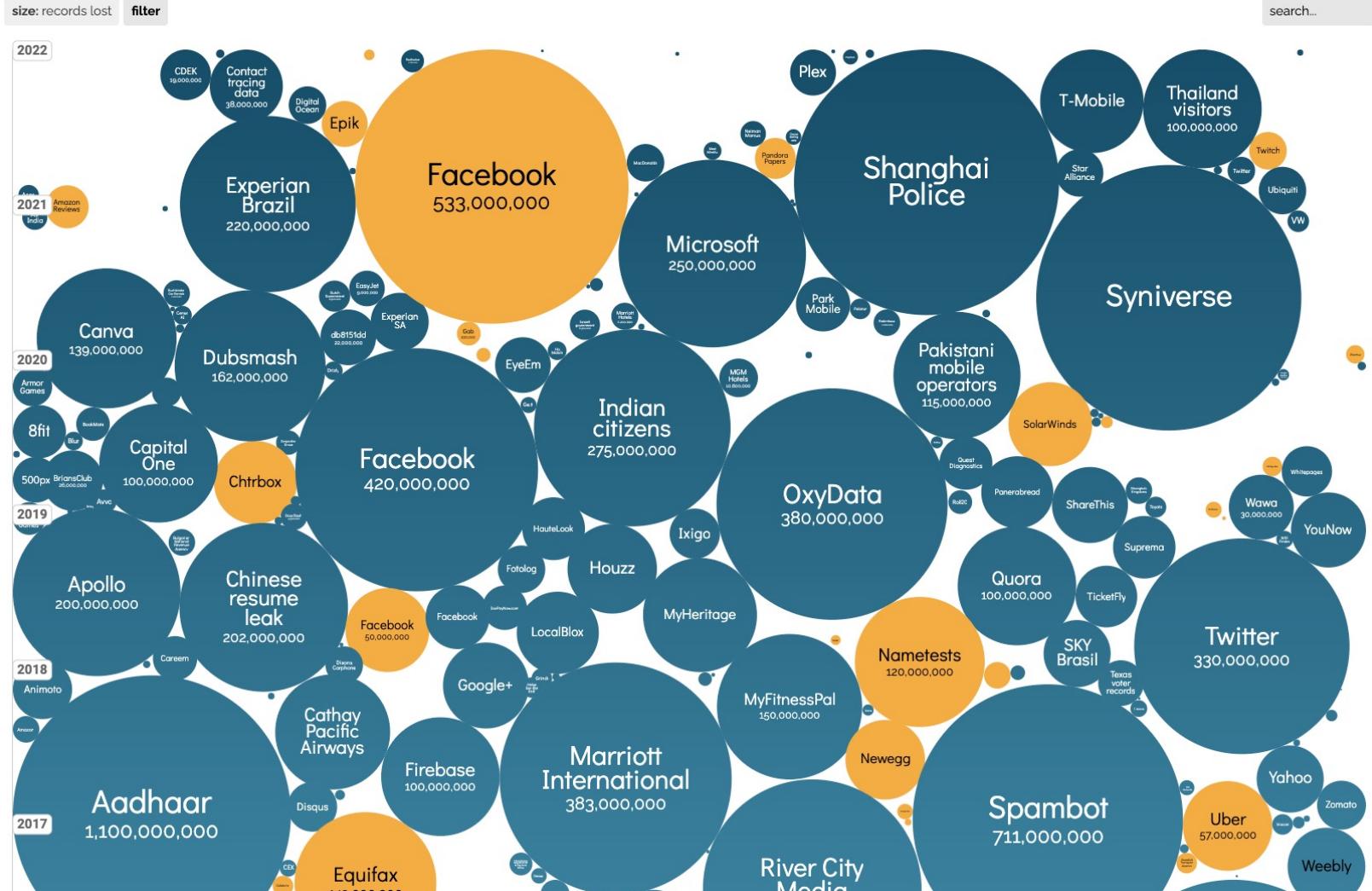
# 数据泄漏统计



## World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

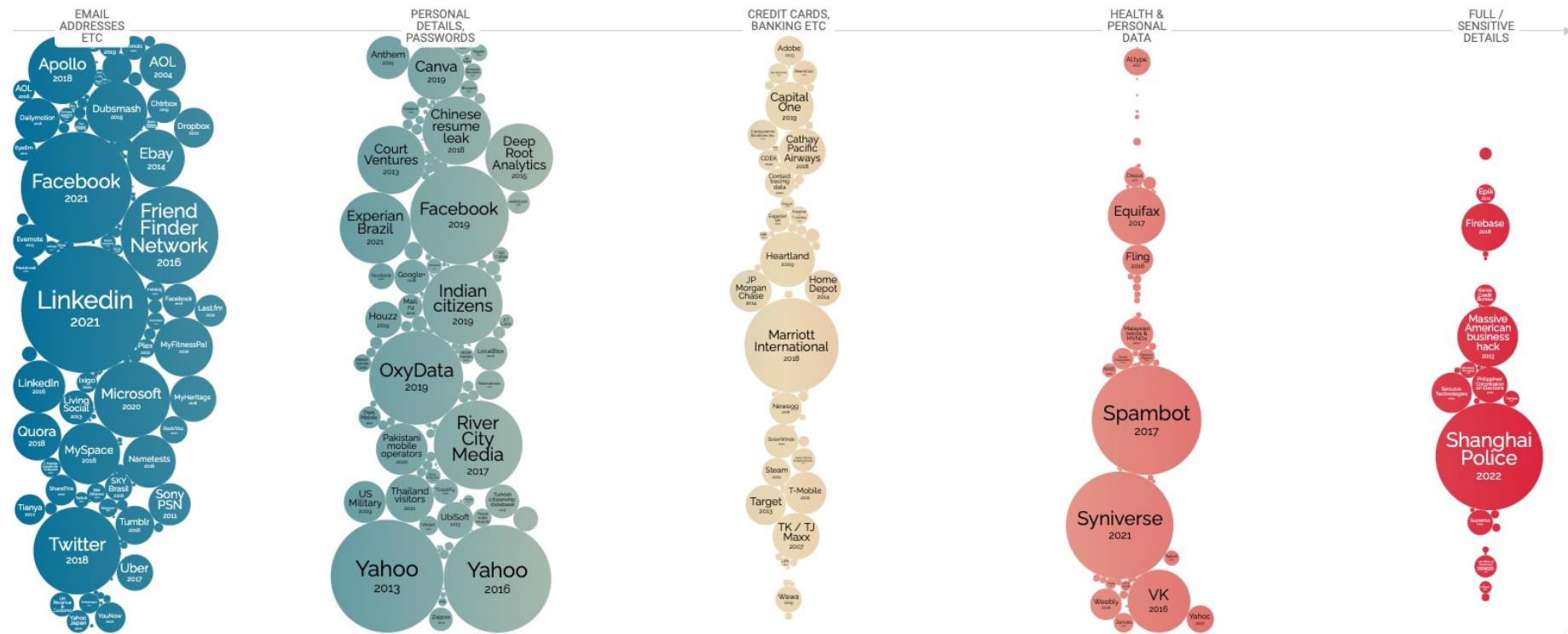
UPDATED: Sep 2022



# 数据泄漏类型



## Data Breaches by data sensitivity



Email、地址、个人信息、密码、银行信息等

# 数据泄漏的应对策略



- 实施强大的访问控制机制（多重认证）
- 强大的数据加密和解密功能
- 识别敏感信息并增加额外的保护

# 数据丢失



- 数据丢失可能是由于各种原因，如自然灾害、人为错误或恶意攻击，导致存储在云中的数据无法恢复
- 常见例子
  - ✓ 没有备份的数据因存储机器损坏而丢失
  - ✓ 丢失编码密钥是导致数据丢失

# 数据丢失的应对策略



- 实施强有力的密钥生成、存储和管理以及销毁实践
- 维护数据备份并及时更新
- 定期进行数据恢复演练

# 账户、服务和流量劫持



- 账号劫持是指攻击者获取了用户的**登录凭证**并获得对其云服务的控制权
- 常见例子
  - ✓ 在钓鱼邮件中输入个人凭证导致云账户被劫持
  - ✓ 密码长期不更新，并对不同的帐户使用重复的密码

# 劫持攻击的应对策略



- 遵循密码规则创建强密码
  - ✓ 包含大小写字母、数字、特殊符号
  - ✓ 长度不小于 8 位
  - ✓ 不包含简单数字组合
  - ✓ ...
- 及时更改密码
- 禁止在未知机器上使用密码，并禁止与其他用户共享密码

# 最常用的密码



# 暴力破解密码所需时间



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

TIME IT TAKES  
A HACKER TO  
BRUTE FORCE  
YOUR  
PASSWORD  
IN 2022



› Learn about our methodology at [hivesystems.io/password](https://hivesystems.io/password)

# 新型 AI 诈骗



## 和AI网聊10分钟被骗430万！官方：AI诈骗成功率接近100%

2023-05-24 16:58:26 来源: 科学大观园 ◎ 北京

举报

“从头到尾都没有和我提借钱的事情，就说会先把钱给我打过来，再让我给他朋友账户转过去，而且当时是给我打了视频的，**我在视频中也确认了面孔和声音，所以才放松了戒备**”，郭先生说。

# 不安全的 API



- API 是云服务之间进行数据交换的方式，如果 API 设计不安全，可能会被利用来进行恶意行为
- 常见例子
  - ✓ 若 API 未能正确验证用户身份，攻击者可能会利用这一点来获得未经授权的访问权

# 不安全 API 的应对策略



- 对云提供商的接口进行安全测试
- 确保在加密传输的同时实施强有力的身份验证和访问控制

# 拒绝服务攻击

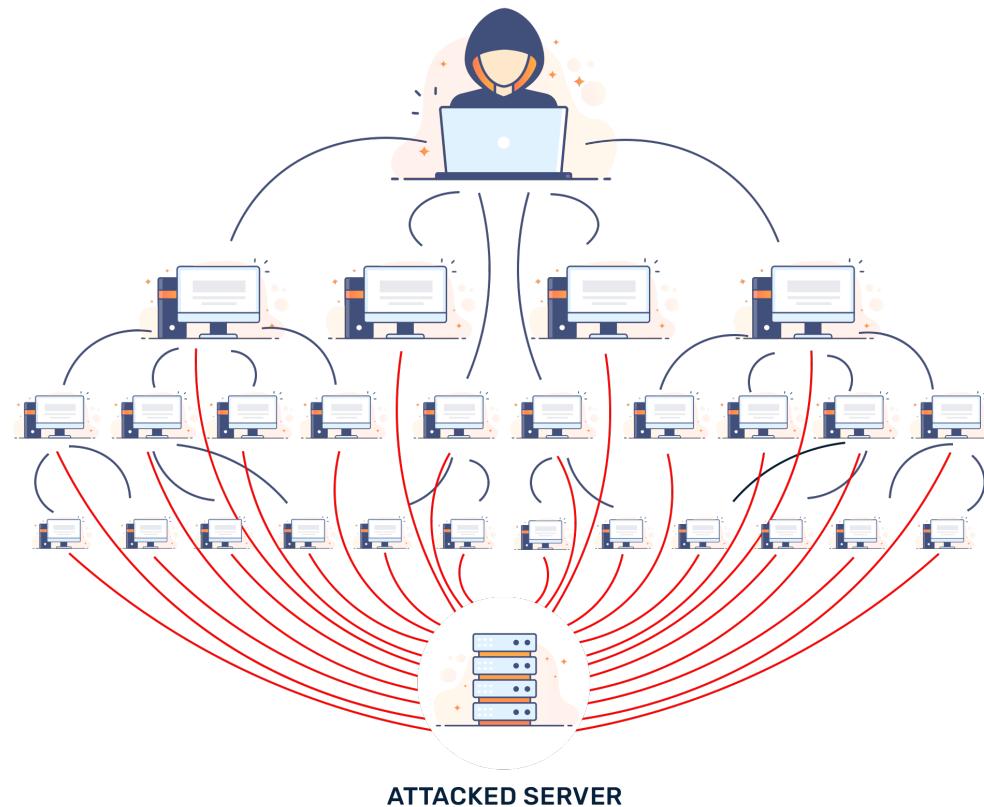


- 在 DoS 攻击中，攻击者通过向云服务发送大量的请求，导致服务过载并无法处理合法用户的请求
- 常见例子
  - ✓ 一家在线零售商在节假日销售高峰期可能会遭受 DoS 攻击，导致其网站瘫痪，无法处理客户的订单

# 分布式拒绝服务攻击 ( DDoS )



- 攻击者通过利用多台计算机同时向目标系统发送大量请求，以达到使目标系统服务降级甚至瘫痪的目的



# 拒绝服务攻击的应对策略



- 算法检测攻击并自动清洗可疑流量
- 使用负载均衡和自动缩放来分散和处理流量

# 恶意内部人员



- 指那些有权访问云服务的内部人滥用他们的访问权来进行恶意活动
- 常见例子
  - ✓ 窃取公司敏感数据获利
  - ✓ 删库跑路

百度 95 后程序员删库跑路被判刑，动机是工作变动及对领导不满

播报文章



黑马程序员

2022-06-09 17:03 北京 | 黑马程序员官方帐号,优质教育领域创作者

关注

6月9日，前百度员工金先生，因涉嫌破坏计算机信息系统罪，判处有期徒刑9个月，缓刑一年。

# 恶意内部人员的应对策略



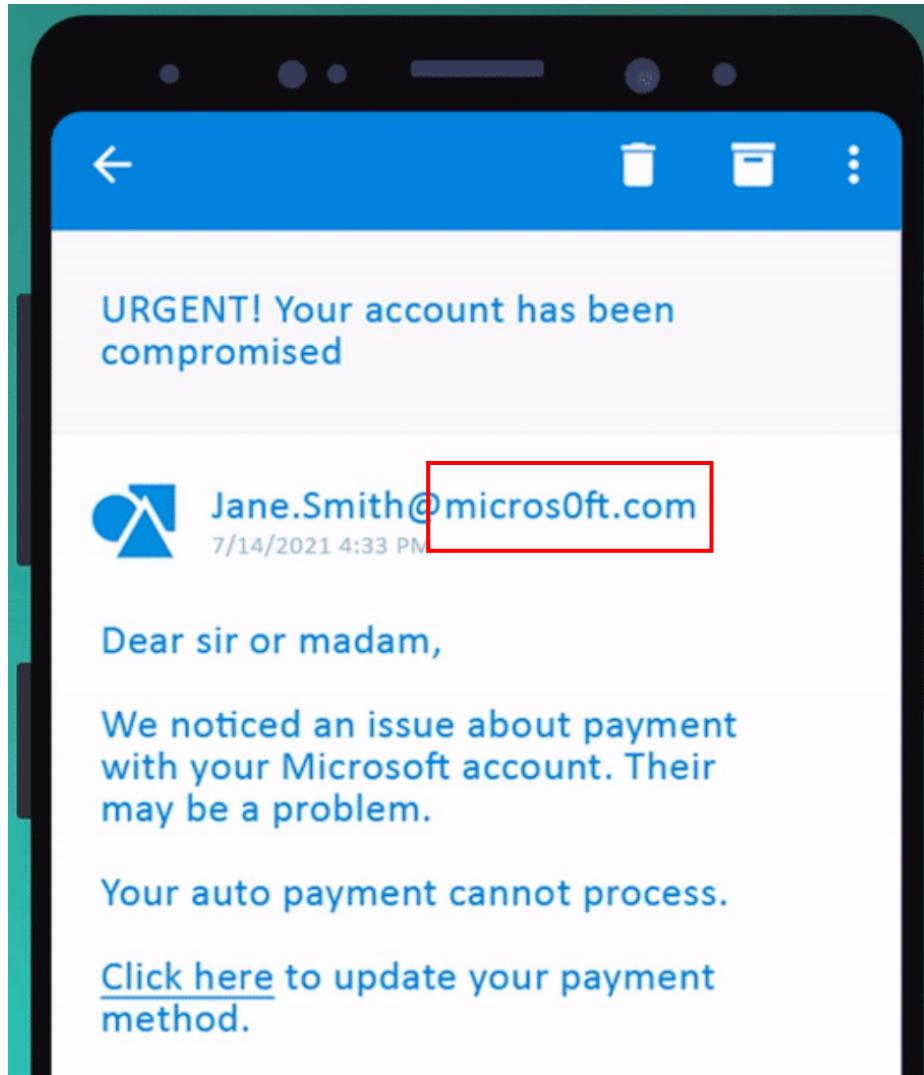
- 人力资源需求规范应成为法律合同的一部分
- 只给员工完成工作的最小权限，定期审查和更新权限
- 建立健全的员工意见反馈机制

# 云计算滥用



- 指攻击者利用云服务进行恶意活动，如发送垃圾邮件或进行密码破解攻击
- 常见例子
  - ✓ 利用未经保护的云服务器来派发恶意软件

# 钓鱼邮件



# 恶意软件



Search - att.net    Windows Official Support

https://serversupport08.azurewebsites.net/1sdafgdfvdsert44bdsbfj2342x/

support.windows.com says:

Windows Warning Alert

Malicious Pornographic Spyware/Riskware Detected

# Windows protected your PC

Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk. For technical support call on **+1-855-595-7999 (Toll Free)**.

Publisher: Unkonwn Publisher  
App: windows10manager (1).exe

Run anyway    Back to Safety

Your computer with the IP has expired & Your information stolen. Call Windows +1-855-595-7999 to protect your files and identity from further damage.

Call Windows : +1-855-595-7999 (Toll Free)

Automatically report details of possible security incidents to Google. Privacy policy

Call Windows : +1-855-595-7999 (Toll Free)    Back to safety

# 上网搜索类似案件



855-595-7999

ALL WORK IMAGES VIDEOS MAPS NEWS SHOPPING

21,200 Results Any time ▾

Microsoft See work results for 855-595-7999 >

Why am I seeing this

**Windows Warning Alert +1-855-595-7999 - Anti-spyware 101**  
<https://anti-spyware-101.com/remove-windows-warning-alert-1-855-595-7999> ▾  
Windows Warning Alert +1-855-595-7999 may try to trick you into contacting a fake Windows Technical Support. According to our specialists, the false notification claims a computer is infected with a dangerous threat called Pornographic Spyware and that it is necessary to ask for assistance from the support center to get rid of it.

**Windows Warning Alert +1-855-595-7999 Removal Guide ...**  
<https://spyware-techie.com/windows-warning-alert-1-855-595-7999-removal-guide> ▾  
Jul 05, 2019 · Windows Warning Alert +1-855-595-7999 is a fake alert that can scare you into doing something you shouldn't. Although this warning looks very real, it has been designed to trick unsuspecting users into spending their money for a service that doesn't exist.

**Remove Windows Warning Alert +1-855-595-7999**  
<https://www.pcthreat.com/parasitebyid-97038en.html> ▾  
Windows Warning Alert +1-855-595-7999 is one of those fake alerts that claim your system is in danger. It shows up on a grey pop-up warning displayed in the background of a website that imitates Microsoft's site. Also, it should urge users to call a fictitious support center said to be for Windows users.

**Uninstall 855-595-7999 Pop-up Virus From PC - Help Delete ...**  
<https://www.helpdeletemalware.com/uninstall-855-595-7999-pop-up-virus-from-pc> ▾  
Mar 27, 2019 · 855-595-7999 Pop-up infection is a pernicious and notorious threat. It will keep creating new problems into your machine, so it's very important to delete this malware permanently. Keep in mind that this virus may have created its several copies and distributed into different locations on your system under different names.

# 云服务滥用的应对策略



- 严格的注册和验证机制
- 监控网络公共黑名单
- 持续监控客户网络流量并进行异常行为检测

# 审查不充分



- 指公司在选择云服务提供商或迁移到云服务时，未能充分考察和理解相关的安全和合规风险
- 常见例子
  - ✓ 公司可能因为未能充分理解云提供商的数据管理政策，而导致其无法合规地处理敏感客户数据

# 审查不充分的应对策略



- 在选择云服务提供商或迁移到云服务时，**充分考察和理解相关的安全和合规风险**
- 制定详尽的迁移和使用策略

# 共享技术带来的问题



- 在云计算环境中，许多资源（例如硬件、网络等）是被多个用户共享的。如果共享技术的隔离机制出现问题，可能导致一个用户的活动影响到其他用户
- 常见例子
  - ✓ 如果云服务提供商的**虚拟化软件存在漏洞**，那么攻击者可能会通过这个漏洞，从一个虚拟机窥探或者干扰另一个虚拟机的运行

# 共享技术中的安全问题类比



Securing a house

单机中的安全问题，  
防范外部攻击为主



Securing a motel

共享技术带来的新的安  
全问题，同时防范内  
部和外部的攻击

# 共享技术问题的应对策略



- 确保云服务提供商有足够的隔离机制，并且定期审计和测试这些机制
- 持续监控系统以检测未经授权的活动
- 对所有关键操作实施严格的访问控制和强身份验证



中山大學 软件工程学院  
SUN YAT-SEN UNIVERSITY SCHOOL OF SOFTWARE ENGINEERING

谢谢

陈壮彬  
软件工程学院

<https://zbchern.github.io/sse316.html>