Privacy Regulations, Smart Roads, Blockchain, and Liability Insurance: Putting Technologies to Work

金融信息与工程管理系

龚林　2001210250

问题研究：智能道路、车联网产生的大量数据可用于提升交通运行效率，但同时可能侵害个人隐私（GDPR：《通用数据保护条例》）。

智能道路 Smart roads

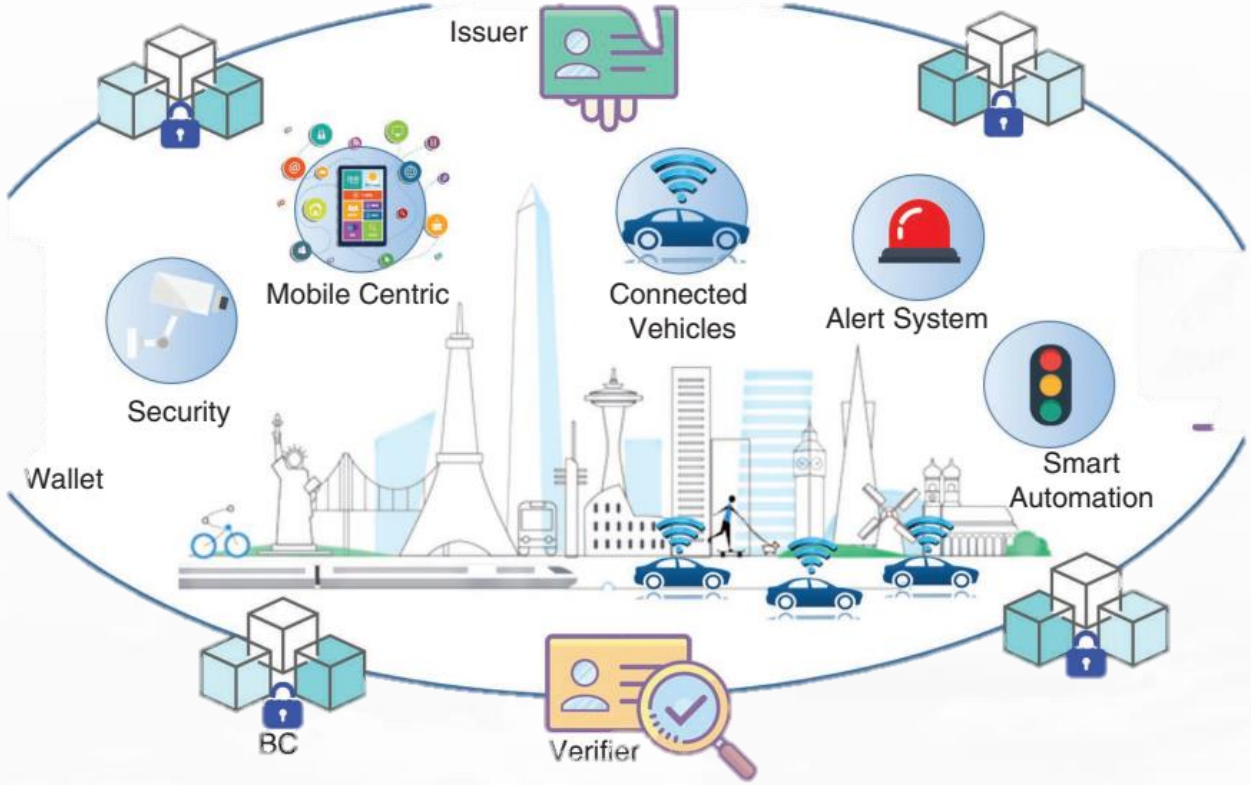
提供网络传输、路况监视、道路安全等服务

车联网 IoV

实现交通数据的信息联通，所有智能交通工具均配备网络设备与传感器设备

区块链 Blockchain

可以妥善解决信息安全问题；非对称加密技术可以用于保障隐私



Smart roads and IoV in the Blockchain shell

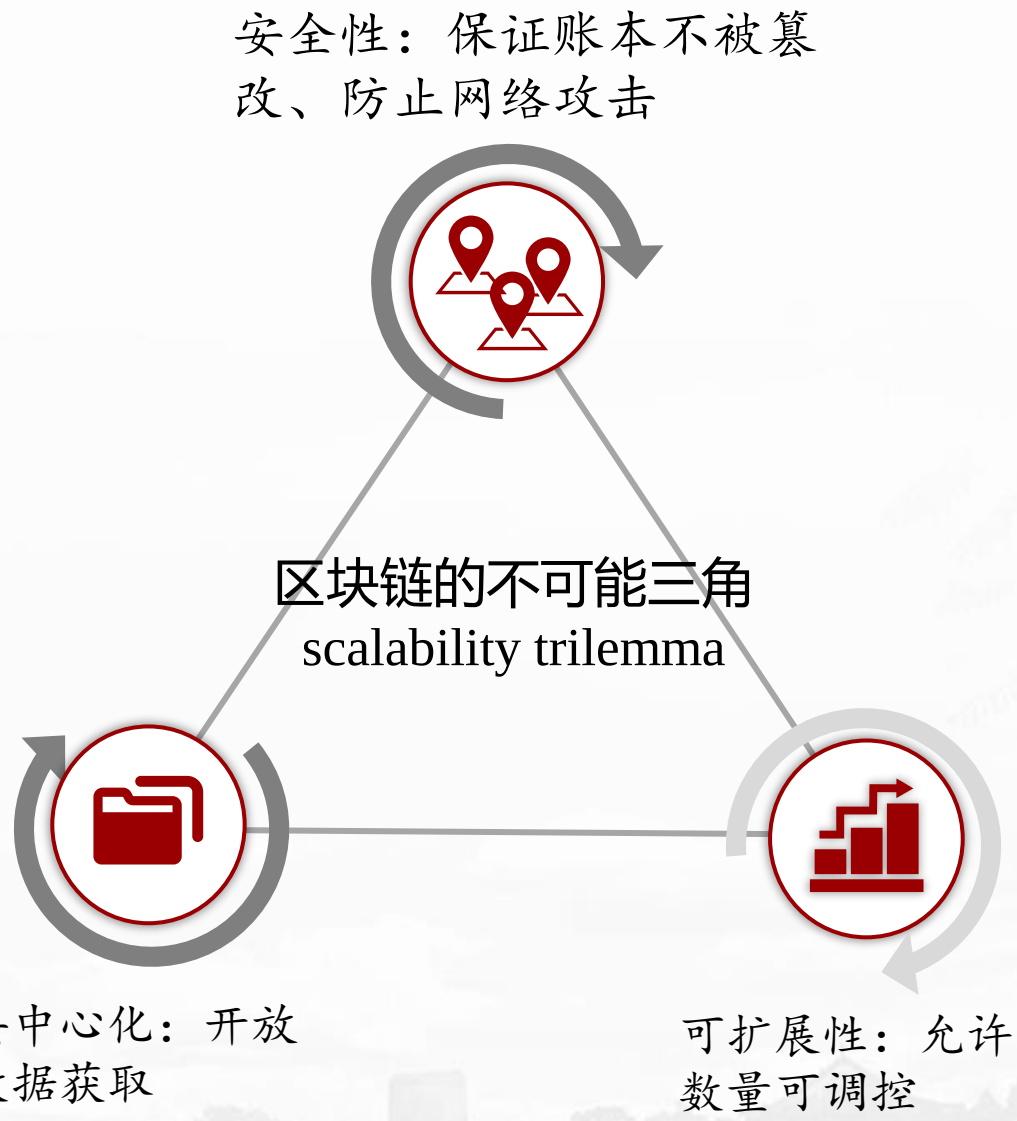
- **智能道路**：

  1. 提升道路安全性；
  2. 起到震慑作用。

  } 可能侵犯用户隐私

- **区块链**：

  1. 去中心化：降低单个参与者的数据获取和存储成本；权力机构掌控私钥的使用权保护隐私
  2. 安全性：保证数据的安全性。

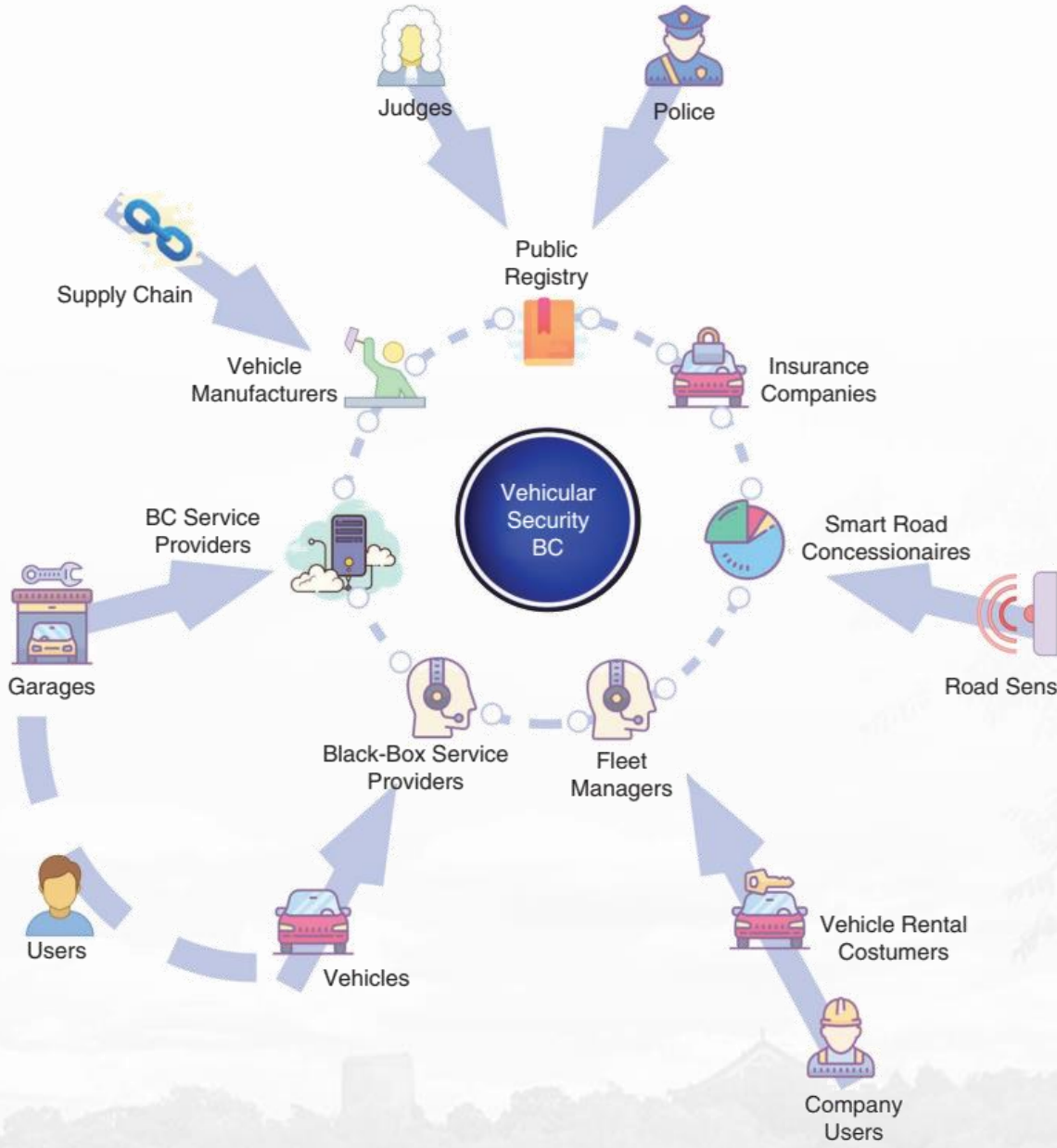


通过让投资者变成获利者，提升投资激励：

- 保险公司可以降低诉讼成本
- 交通工具制造商可以提高和监控产品质量
- 私人许可商可以依靠提供数据服务获利

信息保护机制：

- 用非对称加密技术保障隐私，只有拥有私钥才能解密数据。
- 法官、警察等权力机构拥有私钥的控制权，保证隐私安全。



北京大学
PEKING UNIVERSITY

Why Does Your Data Leak Uncovering the Data Leakage in Cloud from Mobile Apps

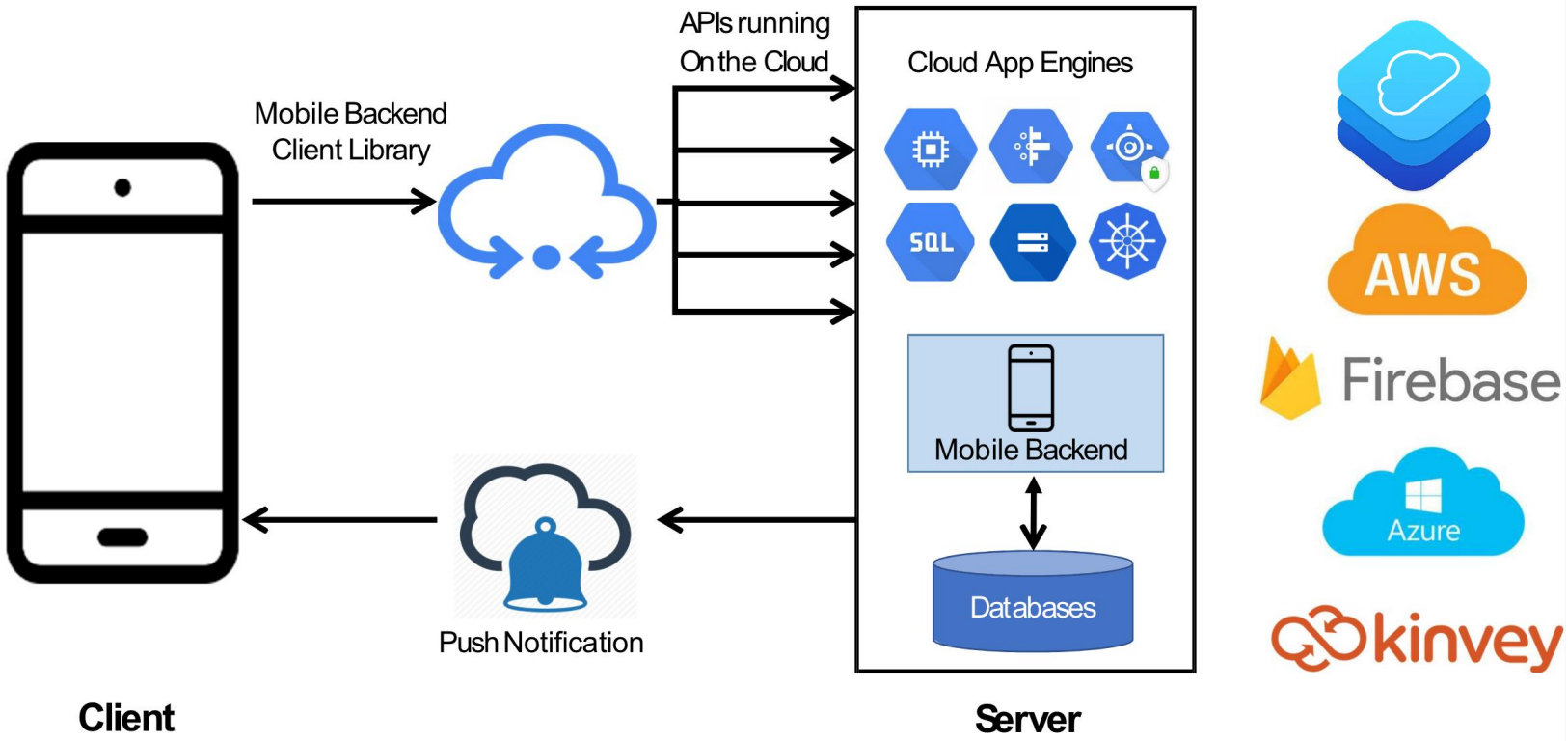
刘琛 2001210628

云后端

云后端相对于传统后端的优势

1、关注应用的核心逻辑，不再重复写CRUD。

2、伸缩性和可用性



云后端信息泄露的两个主要原因

1、滥用不同权限的Key
高权限key
低权限key
2、权限配置错误
firebase配置

Service	Key Type	Example
Azure Storage	Account Key	DefaultEndpointsProtocol=https; AccountName=*;AccountKey=*
	SAS	https://*.blob.core.windows.net/* ?sv=*&st=*&se=*&sr=b& sp=rw&ip=*&spr=https&sig=*
Notification Hub	Listening Key	Endpoint=sb://*.servicebus.windows.net /; SharedAccessKeyName= DefaultListenSharedAccessSignature; SharedAccessKey=*
	Full Access Key	Endpoint=sb://*.servicebus.windows.net /; SharedAccessKeyName= DefaultFullSharedAccessSignature; SharedAccessKey=*

```
{
  "rules": {
    ".read": true,
    ".write": true
  }
}
```

(a)

```
{
  "rules": {
    "users": {
      "$uid": {
        ".read": "$uid === auth.uid",
        ".write": "$uid === auth.uid"
      }
    }
  }
}
```

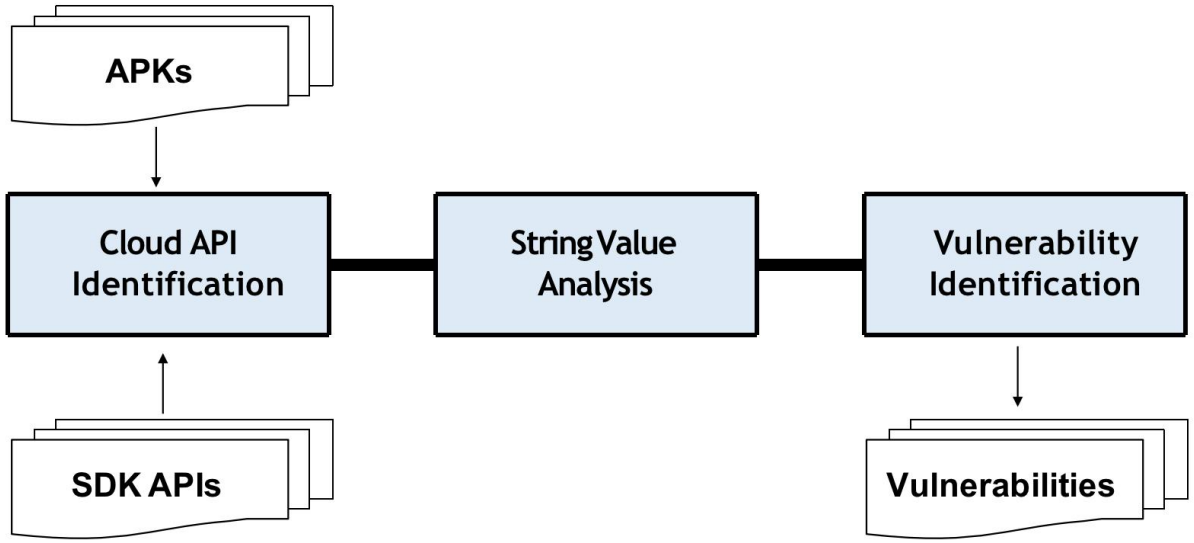
自动化识别信息泄露漏洞

三个需要解决的问题：

1、定位到云API的调用函数

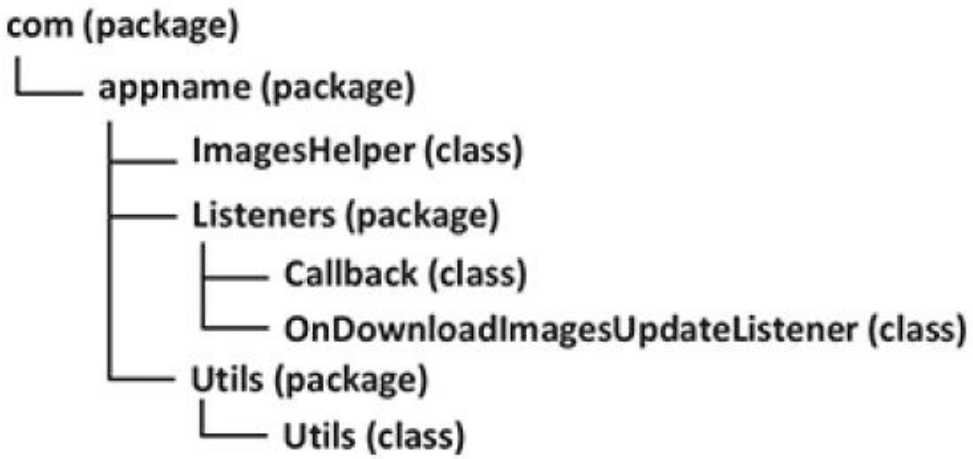
2、提取API的参数，得到密钥

3、信息不泄露的情况下验证漏洞



抗混淆的云API识别

混淆后，变量名，函数名会变，不能直接定位
混淆后的不变量：包结构和调用关系
在SDK中的API对这两个不变量进行编码得到每个API的签名
在源程序中根据签名寻找API，定位到API的位置



字符串分析

1、后向切片Java字节码
寻找会影响密钥的计算相关的变量和指令，构造出CFG，DDG以及String Stack

2、利用CFG，DDG和Stack计算密钥的值

```
1 package com.appname
2 public class ImagesHelper {
3   private final String storageAccountKey;
4private final String storageAccountName;  5
6 private ImagesHelper(Context arg3) {  7          int v0 =
2131099713;
8     int v1 = 2131099712;
9     this.storageAccountName =
10       this.getResources().getString(v0);
11    this.storageAccountKey =
12this.getResources().getString(v1);  13 }
14
15   public void downloadImages(Callback arg5,
16       OnDownloadImagesUpdateListener arg6) {
17     StringBuilder v0 = new StringBuilder();
18     v0.append("DefaultEndpointsProtocol=http;AccountName=");
19     v0.append(this.storageAccountName);
20     v0.append(";AccountKey=");
21     v0.append(this.storageAccountKey);
22     String v1 = v0.toString();
23     CloudStorageAccount v7 = CloudStorageAccount.parse(v1);


24 ...
```

零泄漏漏洞验证

1、在AWS中检测密钥类型

https：//ec2.amazonaws.com/?Action=Describe Instances＆InstanceId.1 = X，不同的密钥会返回不同的结果。“ InvalidInstanceID” “ UnauthorizedOperation

2、Firebase权限配置错误

利用firebase的rest接口，传入root path和indexon字段，不同的配置会返回不同的结果。字段不存在说明权限正确。

```
{
  "rules": {
    ".read": true,
    ".write": true
  }
}
```

(a)

Did App Privacy Improve After the GDPR?

俞鼎耀 200120699

问题引入

General Data Protection Regulation(GDPR)是一个针对个人数据安全的保护条例，于2016年制定，2018年实行。文章提出了如下问题：GDPR对消费者有影响吗？代码的世界改变了吗？GDPR对移动应用程序的行为有**可测量**的影响吗？如何衡量这种行为上的变化？

提出假设

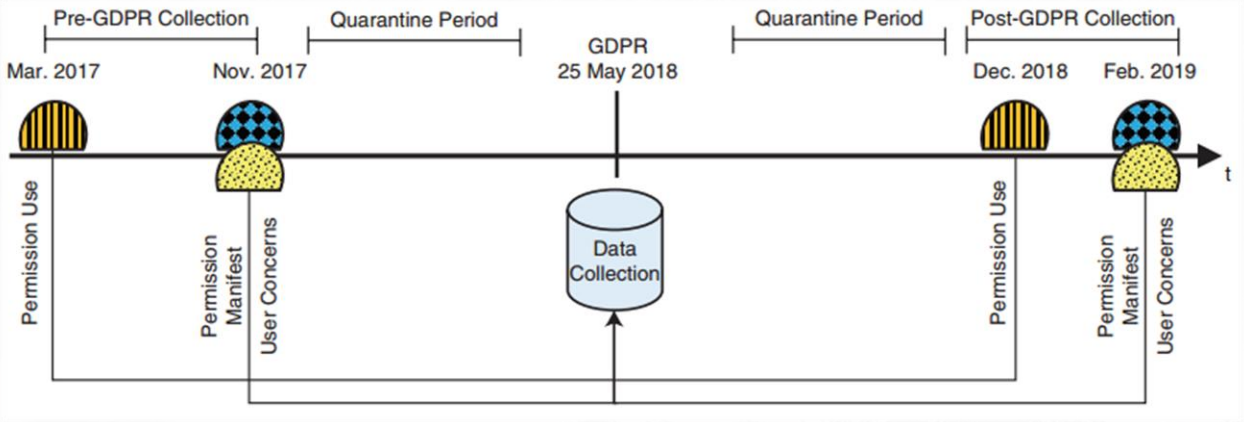
针对GDPR条例中的几条：目的明确原则，数据最小化原则和透明原则，作者提出以下假设改进。

- 更少的权限**声明**
- 更少的权限**使用**
- 更少的用户担忧

数据收集

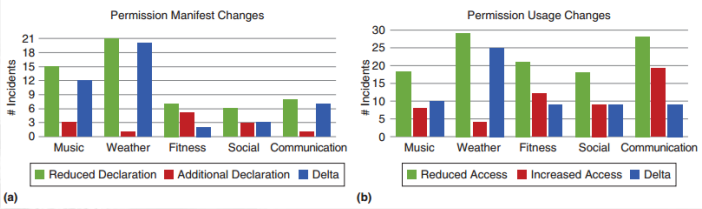
针对**权限的声明和使用**，作者参考了Android dangerous permission privileges和安卓端App的软件，针对**用户反馈**，作者收集了Google Play app market的数据。

数据收集的时间包括GDPR实行前后数月，共有50个apps被列入观察列表。



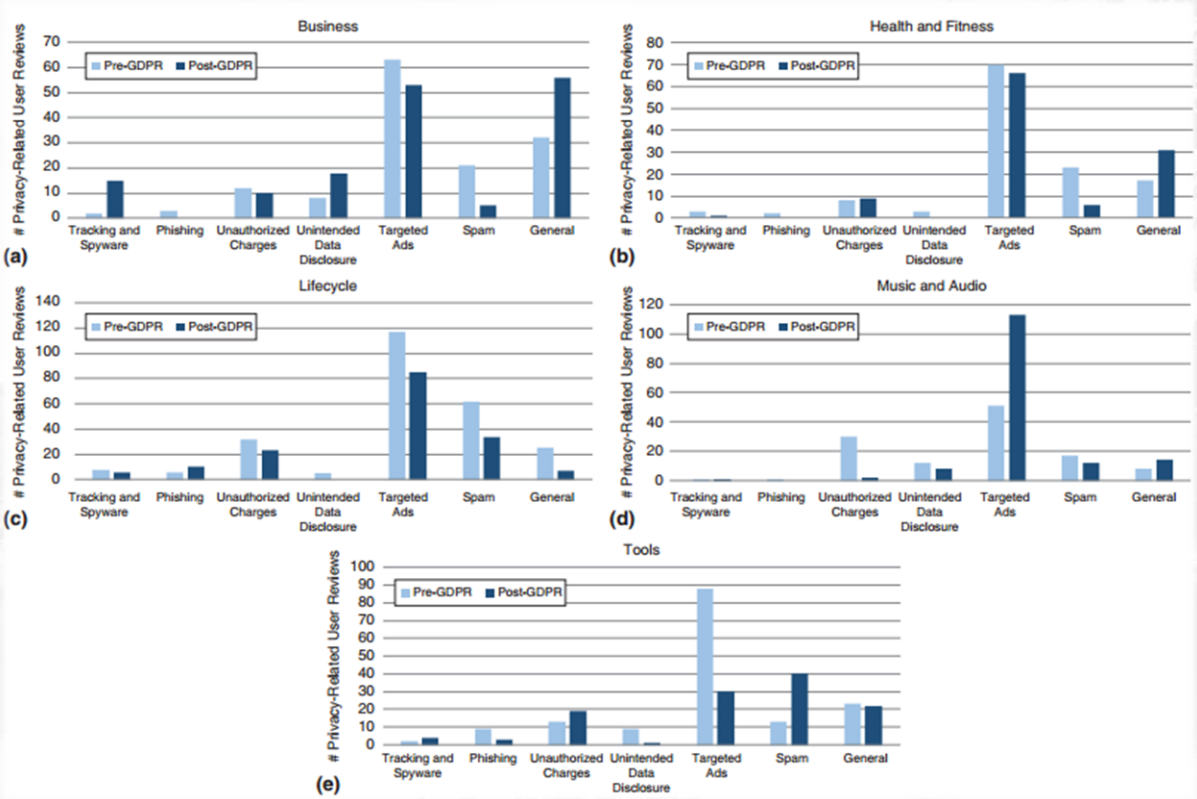
实验结果

对于权限的声明和使用，图中(a)表是许可协议的变化，(b)表是实际使用监测到的变化。绿色表示**许可数量减少**，红色表示**许可数量增加**，白色表示**未使用无变化**，灰色表示**已使用无变化**。对于（a），日历权限被删除（绿色，−），麦克风权限被添加（红色，+），电话权限被删除（绿色，−）。对于（b），位置权限访问减少了100%（绿色，−100），传感器权限访问增加了10%（浅红色，+10），SMS权限访问减少了6%（浅绿色，−6）。



实验结果

本图是作者利用机器学习方法提取了用户反馈的关键词，包括间谍软件、网络钓鱼、非官方收费、非预期数据、定向广告、垃圾邮件和其它普通的问题。主要是能看到实行 GDPR 后与隐私相关的投诉减少，且与GDPR前的投诉相比，General的投诉变成第二大类。



总结与分析

- 如数据显示，许可数量总体减少，声明权限的意图降低。
- 显示使用的权限数量减少，尽管某些权限使用的频率更高
- 除了对定向广告和一般安全问题的担忧外，Google Play app market用户在其它类别上的担忧总体减少。

尽管GDPR可能没有减少apps对某些权限的使用，但它在保护用户隐私上确实做出了贡献。

Security and Privacy Challenges in Cloud Computing Environments

—— Hassan Takabi and James B.D. Joshi

报告人：凌晨

2020.11.10

云计算中存在的隐私与安全问题

1.云服务提供商问题

2.多租户环境下的问题

3.虚拟化问题

4.监管问题

5.异构性问题

6.数据所有权问题

一、云服务提供商问题

在云计算中，数据的搜集和汇总都是通过第三方，即云服务商提供的，这与传统的一台电脑处理自己的数据，是完全不同的。因此我们需要用适当的机制来防止云提供商以未经同意的方式使用客户的数据。

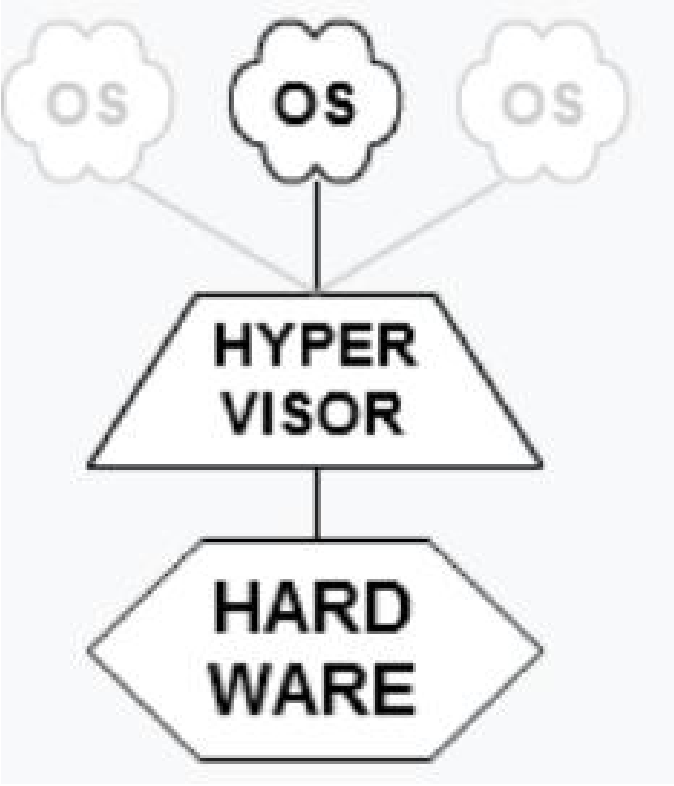
但是要想做到这一点，在技术上难度很大。因此在现实情况中，客户常常选择那些技术能力和经济稳定性有高度信誉的公司。

二、多租户环境下的问题

云计算的另一大特点是多租户，即多个客户同时使用云服务，这就是所谓“多租户环境”。这种多租户的环境，为安全和隐私带来了诸多挑战。比如在 SAAS (Software as a Service，基础设施即服务)中，由于每个租户是从不同的提供商处获取和使用组件和数据，因此云服务商需要考虑如何安全地组合这些组件与数据，并确保它们得到了良好的保护。

对此，亚马逊采用了虚拟机监控器(Hypervisor)的技术，所谓虚拟机监控器，顾名思义就是监控虚拟机的。而这又涉及到第三个问题，即云计算中虚拟化的问题。

三、虚拟化问题



在云计算中，为了满足不同租户的需求，云服务提供商会在一台服务器上装多个操作系统，这就是所谓的虚拟化。

虚拟化的技术，提高了资源利用率，但同时也带来了安全上的风险，主要有以下两方面：

1.因为装入多个操作系统，攻击者便有了更多的攻击手段。

2.因为虚拟化隐藏了硬件信息，因此一些关键数据的安全性得不到保证。

四、监管问题

在云计算出现以前，组织通常有完善的合规监控和执行流程。但是随着云计算越来越成为一种全球性的现象，它获取的计算和基础设施资源也越来越多，这引起了一些监管的问题。作者举了两个例子，分别是Sarbanes-Oxley法案和HIPPA法案。

所谓HIPPA，是健康保险便利和责任法案(Health Insurance Portability and Accountability Act)，这个法案要求在确保私密性的情况下保存病人信息档案六年，还详细规定了医疗机构处理病人信息规范，以及违法保密原则、通过电子邮件或未授权的网络注销病人档案的处罚方案。

Sarbanes-Oxley法案。该法案主要是针对上市公司财务进行审计的，简单的理解，就是，如果公司都不能保证自己的内部控制的可靠性（例如IT系统可能存在安全隐患等），那么，公司所提供的财务报告就很难具备足够的公信力。

五、异构性问题

所谓异构性，是指统一租户在接收来自不同提供商提供的云服务时，所面临的数据整合问题。

举个例子，租户从A提供商获取a数据，从B提供商获取b数据结合，然后将a与b一起送到C服务商那里处理，得到最终的结果c。

这里有三个云提供商，那么就可能有三个不同的安全协议，那么如何处理这三个安全协议之间的差异，就成为一个问题。这就是所谓的异构性。

六、数据所有权与访问控制问题

云中的数据通常驻留在一个共享环境中，但是数据所有者应该完全控制谁有权使用这些数据，以及一旦他们获得访问权限，他们可以对数据做些什么。为了在云中提供这种数据控制，我们需要想出一种合适的方法。

此外，访问控制也是一个问题。因为租户访问云的设备和地点不可能只有一个，比如他可以在家里、公司里、出差地，使用不同的品牌的手机或者电脑使用云服务，那么云服务商就要能够辨别出，哪些是真实的场景转换，哪些是黑客恶意伪造的攻击手段。如果不能解决访问控制，那么云服务也是存在很大的隐私和安全挑战的。

谢谢观看！

Blockchain-Based Distributed Cloud Storage Digital Forensics: Where's the Beef?

2001210694

杨璧鸿

本文重点

- 数字取证面临的问题
- 现存的基于云、P2P、分布式存储的数字取证实践
- 基于区块链的分布式云存储实现STORJ的简介
- 针对STORJ的数字取证尝试
- 提出未来应做的研究

数字取证行为的构成

1. 鉴定
2. 准备
3. 进场策略
4. 保护现场
5. 收集
6. 检查和分析

——Digital Forensics Research Workshop

数字取证难度总结

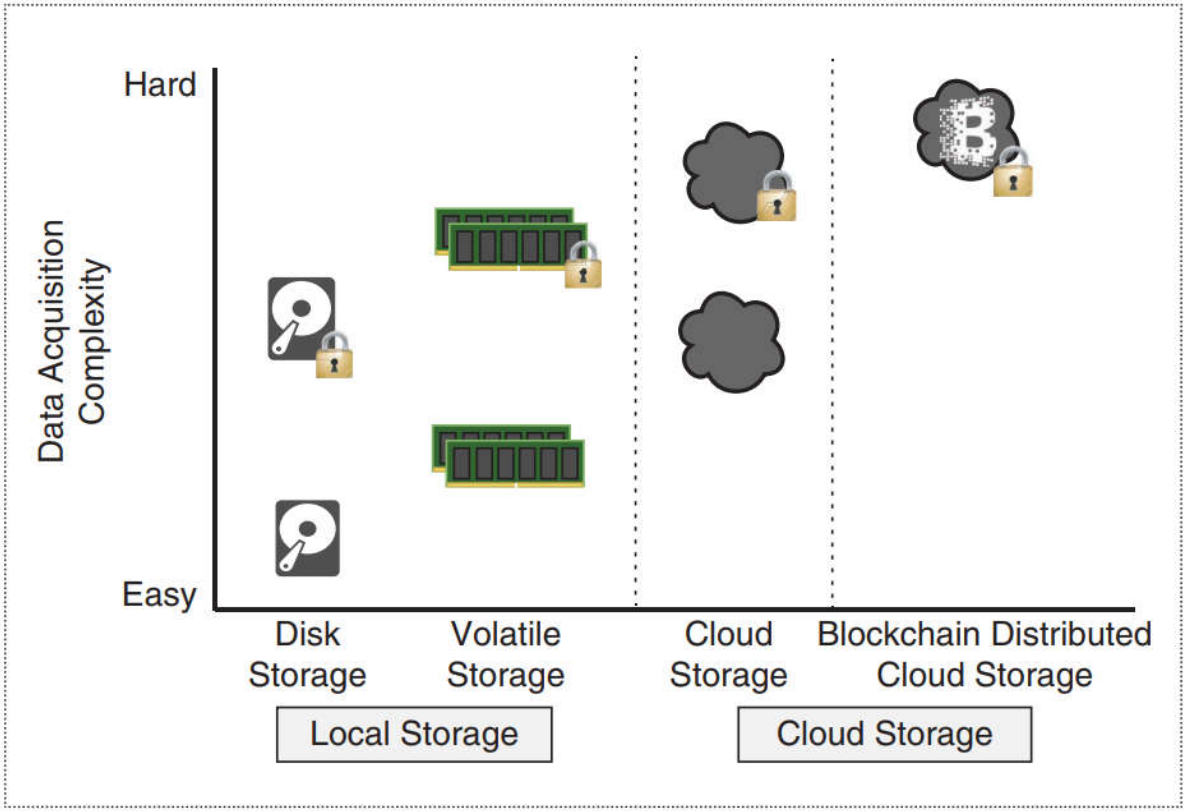


Figure 1. The progressive difficulty and complexity of data acquisition in changing storage technologies.

针对区块链的数字取证

- 在线
  - 交易历史
- 本地
  - Bitcoin地址
  - 公钥
  - 公钥哈希
  - IP地址
  - 时间戳
  - 交易
  - 交易金额

针对云存储的数字取证

- 本地数据
  - 虚拟机账号密码
  - 网络流量分析数据
  - 存储分析
- 客户端的元数据
  - 同步元数据
  - 文件管理元数据
  - 缓存
  - 认证数据
  - 加密元数据
- 服务器端元数据
  - 文件管理元数据
  - 存储的文件
  - 认证数据
  - 加密元数据
  - 登陆数据
- 工具
  - kumodd
    基于api
    可以获得云上文件列表
    可以下载指定文件

针对分布式文件系统的数字取证

- 易失性环境元数据
  - 网络逻辑地址
- 非易失性元数据
  - 登陆数据
  - 备份数据
- 配置元数据
  - 认证配置
  - 网络配置
  - 执行

P2P文件分享系统

- 感兴趣的文件
- 给peer报告的自身IP

- 工具 RoundUp

STORJ

- Kademlia 、 Blockchain

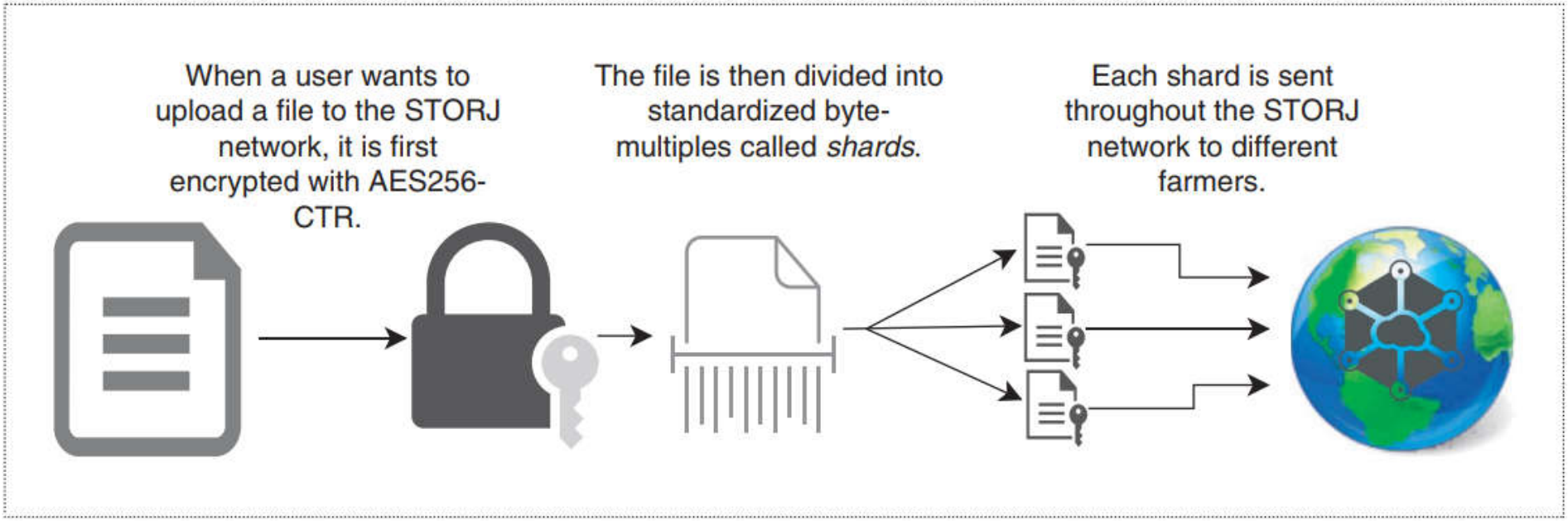


Figure 4. An overview of the client-side process.

STORJ取证难点

- 发现使用STORJ
- 通过 STORJ API 获取数据
  - 获取用户凭证
  - 获取密码
- 通过物理手段获取数据
  - 定位碎片
  - 确定碎片的地理位置
  - 获得许可令
  - 恢复碎片
  - 加盐碎片的处理
  - 与其他碎片结合的碎片的处理

STORJ分析

- 作为存储提供者
  - 分析存储的.ldb文件
    - 无法检测存储的文件类型

- 作为使用者
  - 分析请求交易
    - 合约号
    - farmer ID
    - 签名
    - 付款地址
  - 从本地恢复上传的数据
    - 文件名
    - 文件大小
    - 文件类型
    - 上传日期
  - 无法恢复已删除的文件

未来需要的工作

- 通过计算机上遗留痕迹判断用户是否使用STORJ的方法
- 开发分析取证基于区块链的分布式云存储系统的工具