基于全同态加密的医疗数据隐私保密系统

目录/Contents

应用背景

数据库隐私泄露？

2010年360搜集百万用户账号
2011年天涯、CSDN用户账号泄露
2015年互联网金融平台铜掌柜60万用户隐私泄露
2015年美医疗保险公司CareFirst被黑 110万用户信息泄露
2015年全球最大婚外情网站Ashley Madison被黑

这样，你还敢把隐私赤裸裸地放在数据库里吗？

云平台安全性


医院数据库被恶意攻击
管理员的恶意操作导致资料外泄
隐私易泄露
患者不信任
医疗
云平台
云计算服务大幅削弱
加解密密钥管理复杂
如何高效解决？

方案设计

加密之后，如何统计计算？

全同态加密技术

病人隐私泄露怎么办？

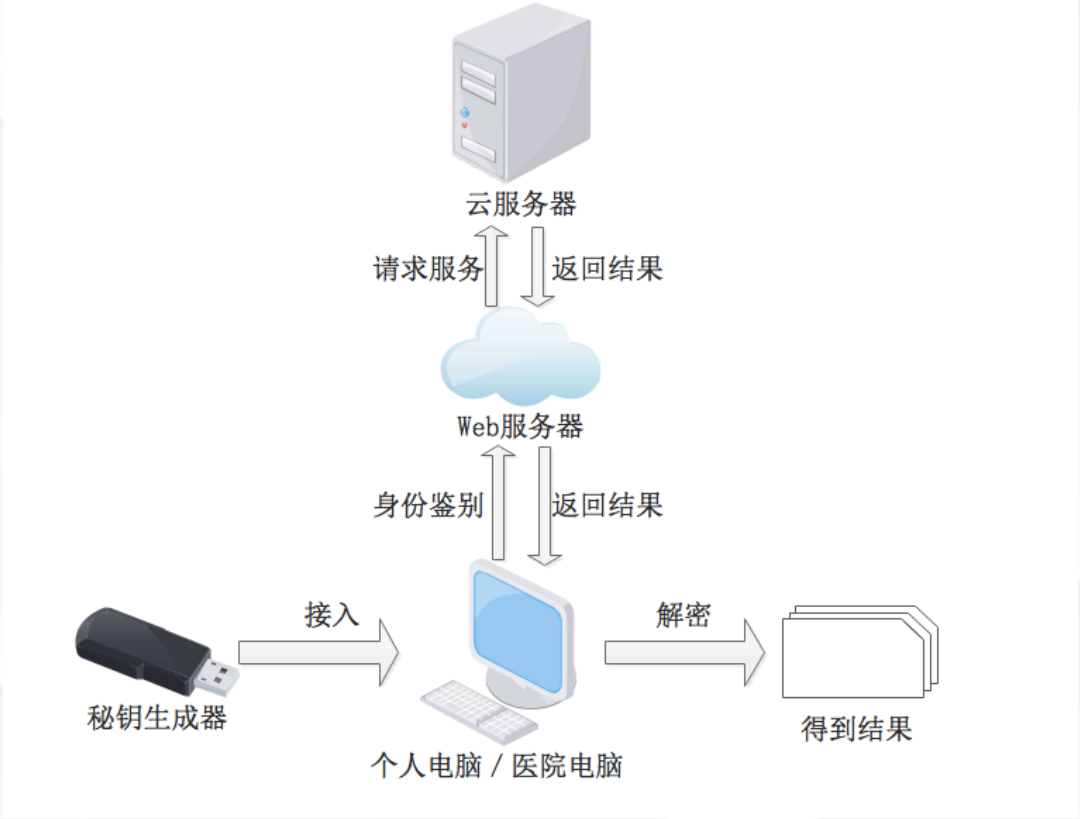
对病历进行加密后存储在云平台上

患者病历怎么存储？

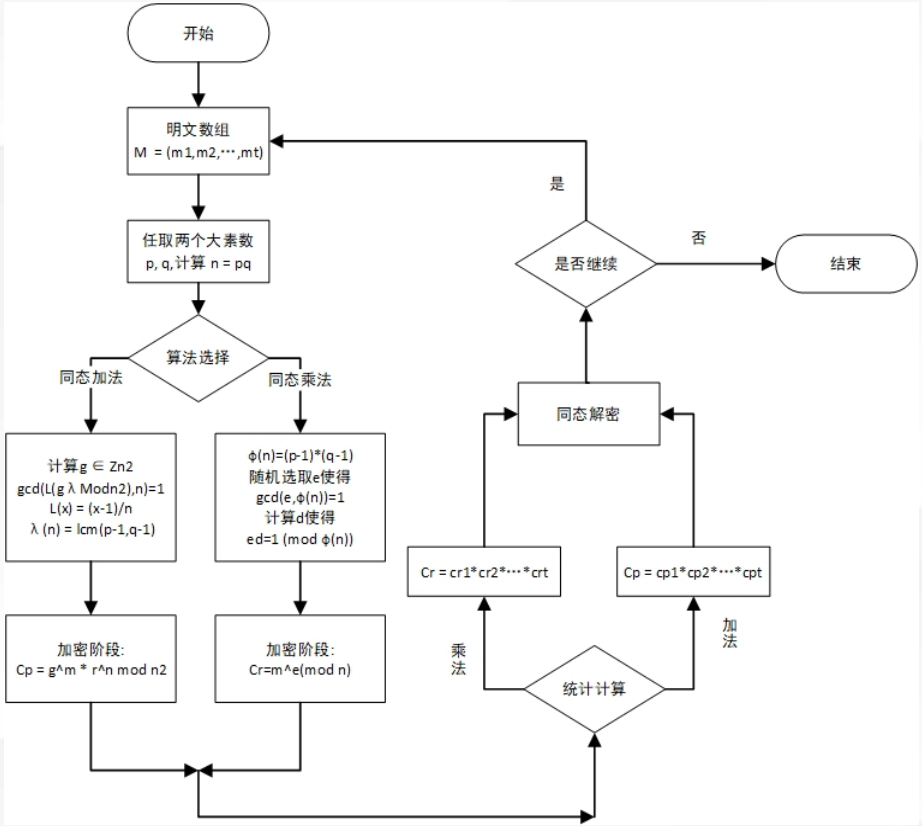
将所有病历制作为电子病历存储在云平台上

如何防止管理员恶意泄露病人隐私？

密钥生成器


云服务器
请求服务
返回结果
Web服务器
身份鉴别
返回结果
接入
解密
秘钥生成器
个人电脑 / 医院电脑
得到结果

关键技术——全同态加密算法



加密后限制了云计算的能力

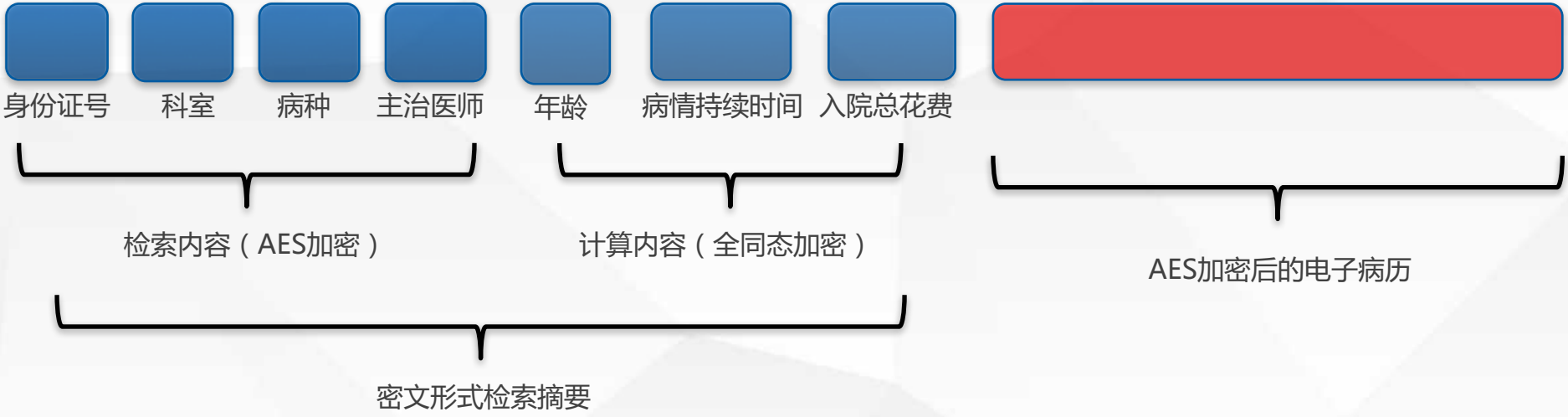
全同态加密算法

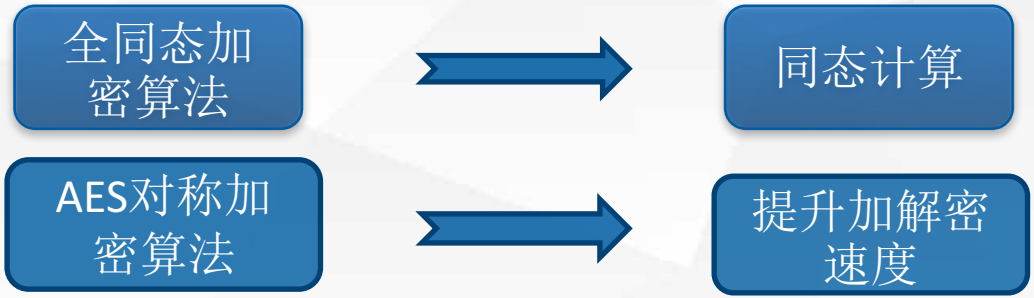
$e = E(m)$

$F(e) = E(f(m))$

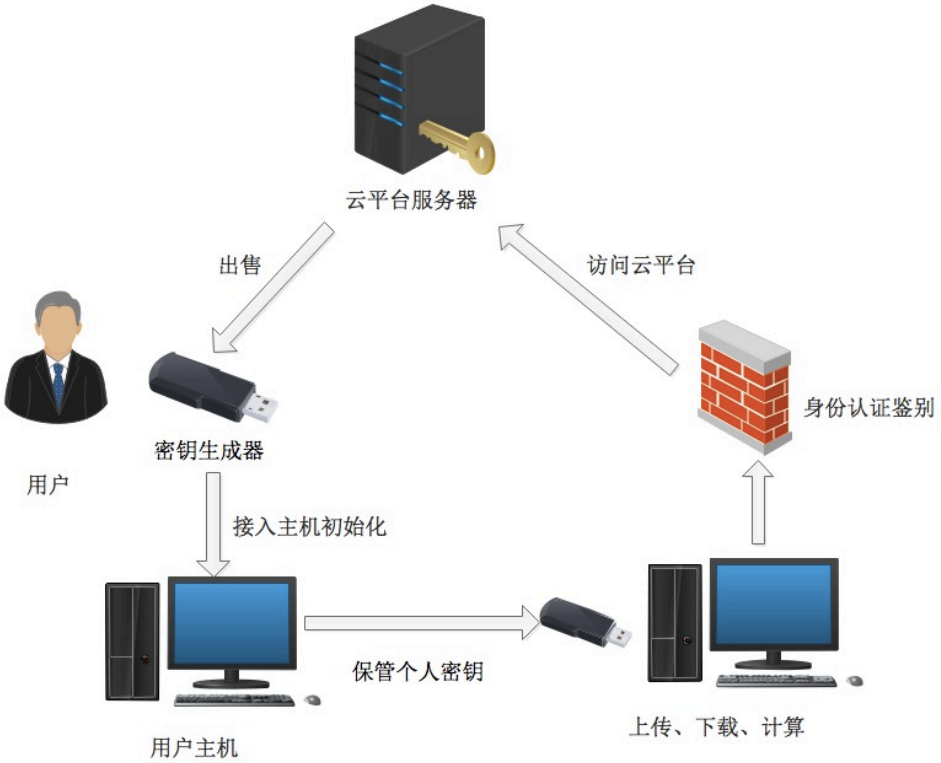
保留云平台计算能力

关键技术——密文检索摘要


身份证号
科室
病种
主治医师
年龄
病情持续时间
入院总花费
检索内容（AES加密）
计算内容（全同态加密）
AES加密后的电子病历
密文形式检索摘要


全同态加密算法
同态计算
AES对称加密算法
提升加解密速度

关键技术——密钥生成器



产生唯一的身份鉴别码

自动完成加解密操作

云平台不保留用户的任何密钥

性能分析

系统安全性分析

全同态加密技术

加密时间极短

解密效率低

大小1G的文件：

加密需1分钟

解密需65小时

用于加密需要计算的少量信息

性能改进

AES对称加密技术

加密时间与加密文件的大小呈正相关

解密时间是加密时间的两倍

大小1G的文件：

加密需4分钟

解密需8分钟

用于加密完整病历

用例测试

序号	原文件大小（KB）	加密后文件大小（KB）	加密用时（秒）	解密用时（秒）
1	6	6	0	1
2	12	12	0	3
3	24	24	0	5
4	45	45	0	10
5	90	90	1	21
6	180	180	2	40

RSA的测试数据

序号	原文件大小（MB）	加密后文件大小（MB）	加密用时（秒）	解密用时（秒）
1	1.639	3.335	0	0
2	3.278	6.669	0	1
3	6.556	13.338	1	2
4	13.111	26.676	3	5
5	26.226	53.351	6	11
6	52.441	106.701	12	23

AES的测试数据

总结展望

基于全同态加密的医疗数据隐私保密系统

全同态加密技术

密文摘要检索

密钥生成器

保护用户隐私
保留云平台计算能力

密钥管理简单
加解密效率高

可扩展性强

未来展望

谢谢观看