**6.系统安全保密设计**

6.1说明

  随着移动信息化技术的迅猛发展，我们会在信息化建设中发现，随着业务系统移动化的需求越来越多，内部移动应用的数量也随之激增，使用起来十分繁琐。为了解决这一问题，很多集团制定了移动信息化发展战略，根据这一战略要求，移动信息化开放平台应运而生。

而个人健康护理系统作为医院的移动信息化门户，信息的安全是首要的保障任务，系统承载了大量用户的信息，账户安全十分重要；同时，系统中运行的各应用流转了敏感业务数据，其中不乏涉及决策层的商业信息，信息的保密尤为重要；从移动信息化系统的特点来看，通信方式的安全同样至关重要。

6.2分类

系统的安全保密主要包括4个方面：

(1)物理安全。物理安全主要包括环境安全、设备安全、媒体安全等方面。处理秘密信息的系统中心机房应采用有效的技术防范措施，重要的系统还应配备警卫人员进行区域保护。

　　(2)运行安全。运行安全主要包括备份与恢复、病毒的检测与消除、电磁兼容等。涉密系统的主要设备、软件、数据、电源等应有备份，并具有在较短时间内恢复系统运行的能力。应采用国家有关主管部门批准的查毒杀毒软件适时查毒杀毒，包括服务器和客户端的查毒杀毒。

　　(3)信息安全。确保信息的保密性、完整性、可用性和抗抵赖性是信息安全保密的中心任务。

(4)安全保密管理。涉密计算机信息系统的安全保密管理包括各级管理组织机构、管理制度和管理技术三个方面。要通过组建完整的安全管理组织机构，设置安全保密管理人员，制定严格的安全保密管理制度，利用先进的安全保密管理技术对整个涉密计算机信息系统进行管理。

6.3设计

针对以上情况，选定可以附加增强安全手段的多层分布式架构来提供安全与保密保障的基础可能。根据架构特点，将安全保障方案分为物理层级和软件层级。在物理层级，可以通过私有云提供的隔离手段，将各层之间通过防火墙进行了物理隔离，并在DMZ中只保留了必须的接入服务器，以最大程度的在物理层次上降低安全风险。在物理层级提供了足够的安全保障之后，系统主要的安全性和保密性设计集中在了软件层级的设计上，下面，需要结合实际情况就软件方面所采取的防窃取、防破解、防泄露等技术手段进行详细说明：

第一，通过HTTPS、敏感数据加密、数据不落地的方式实现了通信数据的防窃取。平台作为移动信息化系统，决定了数据需要从内部网络流经移动互联网到达移动终端，在内部网络到外部网络部分，通过私有云提供的DMZ机制以及审计能力，可以提供足够的安全保障。但是数据需要在移动互联网上流转，这就要求数据流转的通道必须是安全的，同时敏感信息也必须是安全加密的。通道的安全，经过论证分析，最终需要采用HTTPS作为通信方式。HTTPS技术通过在HTTP协议附加SSL的方式实现，其非对称方式加密的特点既保证了通信数据的防窃取，又满足了使用和实现简单的要求。同时作为增强安全手段，在传输过程中，需要单独对密码等敏感数据进行了非对称加密，以达到更好的安全性和保密性。作为软件设计手段，在客户端的设计上采用数据不落地的形式，即所有客户端流经的数据，除了账号用于免输入以外，其他数据都不存储到客户端本地，终端的所有业务数据都从服务器获取，最大程度的避免了客户端被反编译和沙盒入侵所带来的安全风险。

第二，通过验证码、手势密码、锁定账户等手段防止系统入口的暴力破解。系统以移动APP形式提供服务，用户的必须登陆后才可以使用系统功能，密码的防暴力破解成为这方面的关键点。通过调查分析，单纯的使用账户、密码方式登陆系统，可能出现面对暴力破解时的泄露问题，为了解决这个问题，系统的认证环节需要引入验证码技术和手势密码技术。验证码技术可以提高登陆业务的复杂程度，加大针对密码的暴力破解的难度。而手势密码技术通过其生物识别技术特点，可以既保证使用的便捷，又满足安全的需要。同时，在系统中可以采取密码失败多次锁定账户一定时间的机制，具体为，用户密码或手势密码输入三次，系统自动锁定账户三十分钟，这三十分钟内，该账户无法登陆系统，这就进一步加大了破解账户密码的时间，基本上可以认为这些手段屏蔽了密码暴力破解的可能。最终可以选择的方式是将这三种技术手段根据场景结合使用，用户初次登陆系统时采用普通密码方式，登陆成功后，强制设置手势密码，并将密码存储于服务端，用户后续的登陆将只能使用手势密码登陆，密码三次错误锁定账号的机制则贯穿两种登陆方式，既满足了系统的易用性，又提高了登陆的安全性。

第三，使用增强的密码保存手段保障密码的保密性，降低密码的泄露风险。用户的密码或手势密码是存储在服务端的，这就要求在服务端，这些数据需要有足够的安全机制保障。在数据存储方面，需要将数据库的用户进行权限细分，管理账号不能远程登陆数据库管理系统，管理的维护只能在数据库所在机器本地进行，应用所使用的账号单独分配远程访问能力，并进行数据库、表的权限控制。在数据本身的存储安全方面，将采用加盐的信息摘要方式存储密码，信息摘要采用单向Hash方式在获取，既可以保证密码信息的可比较要求，又保证了存储入库的数据的不可逆要求，防止了数据库明文存储密码带来的一旦数据库被窃取密码随之丢失的问题。同时，因为普通的信息摘要技术对相同的密码会产生相同的摘要，为了避免多个账户使用同一个密码而造成的密码泄露，在摘要的生成上，采用了加盐的方式实现，将账号作为盐信息，将盐附加到原始密码，再进行实际的摘要生成，这样每个用户即使使用了相同的密码，也不会存储为同样的密码摘要。

但是在系统运行过程中，有时候也会出现技术手段存在的一些不足。首先是单纯的HTTPS通信并未将信道进行有效隔离，可以考虑增加VPN或VPDN的手段实现。其次是密码摘要的盐采用了用户账号，使得盐固化到了客户端，有一定的安全风险，可以采用客户端验密时先从服务端获取与账号不同的盐，再进行严验密的方式解决。这些问题都是后续系统开发过程中需要重点关注的问题。