2019年7月，我参与了某医疗信息系统有限公司移动护理项目的开发，担任项目技术负责人，负责系统整体架构设计及开发工作。该系统主要包含患者信息查对，医嘱执行，体征数据采集，护理文书管理等功能。本文以移动护理项目为例，介绍了系统安全架构设计在项目中的应用。在网络硬件方面通过设置状态检测防火墙及入侵检测系统，来保证内部网络的安全性；在数据存储方面通过数据加密及容灾备份机制，来保障数据保密性及抗突发风险的能力；在应用服务方面通过数据传输加密技术及登录认证策略，来保证数据传输及系统认证的安全性。通过以上技术方案的实现，我们完成了软件项目开发工作，保障了项目安全性和保密性。最终项目在某省三甲医院成功落地，而后也陆续收到其它医院的上线申请。

移动医疗时代的到来，为实现医疗无纸化，实现医嘱的全生命周期的跟踪，有效解决护士站到病房的＂最后１０米＂的信息延伸问题提供了更好的解决方案．最终达到改变医疗的存在方式，改善医疗业务流程，提升医疗服务质量，提高医疗安全性的目的．

2019年７月，某医疗信息系统有限公司启动了移动护理系统项目。此系统以电子病历系统ＥＭＲ和医嘱录入系统ＣＰＯＥ为平台，借助无线手持终端设备PDA进行信息的实时化传输和移动采集，实现患者信息查对，医嘱执行，体征数据采集，护理文书管理等功能．患者信息查对主要实现PDA扫描患者床头卡二维码或患者腕带条形码查询患者基本信息，核对患者身份；医嘱执行主要实现PDA扫描药品信息二维码，进行药品领取核对、记录护士医嘱执行过程，完成皮试药品双人核对，进行检验样本管扫码采集等功能。体征数据采集主要实现体征任务提醒，患者体征数据录入存库。护理文书管理主要实现患者量表，特护单，通用单，评估单等文档的编辑。我在项目中担任技术负责人，负责系统整体架构设计及开发工作，最终项目在某省著名三甲医院成功落地。

对医院而言，只有医疗系统的可靠安全才能为医疗服务提供安全保障。移动护理系统部署在医院较为复杂的软硬件环境中，可能面临来自内外网络的攻击；来自非法的数据访问和使用控制，未经审核的数据脚本等程序操作可能造成数据库中数据的丢失、篡改或泄露；系统中患者的医疗信息是严格保密的，这些敏感信息需要在网络中进行传输，在此过程中很可能被非法采集；移动护理的相关功能都是为专业护士提供，非法使用很可能造成医疗事故，所以必须确保系统登录认证的最高安全等级。

以上就是系统中可能面临的安全性和保密性问题，为了解决这些问题，我们采用了防火墙、入侵检测、加密解密、访问权限控制、主从复制、短信验证码等一系列安全防控策略。下面具体从网络硬件层面、数据库存储层面、应用服务层面分析所面临的问题以及对应的解决方案。

1、网络硬件层面

网络和硬件是整个系统运行的基础，一旦遭受网络的攻击会造成极大的破坏。为了确保系统拥有安全可靠的运行环境，需要采取相应的措施。首先对网络拓扑结构划分为三个部分，外部网络、DMZ和内部网络。外部网络主要提供对外的门户网站访问服务；DMZ部分主要部署WEB服务器、FTP服务器及内部管理器等；内部网络主要部署Oracle、分布式缓存Redis等服务器。通过在内部网络和外部网络之间设置硬件防火墙，抵御外部的恶意攻击，并且在内部网络中采用入侵检测系统，对越过防火墙的攻击行为以及来自网络内部的违规操作进行检测和响应。另外，在内部网络中增加Nginx反向代理，仅对外暴露代理服务器的虚拟IP，外部用户和系统无法直接访问目标服务器地址。通过上述网络部署和安全性策略极大提高了网络硬件的安全性。

2、数据存储层面

整个系统平台是以数据为核心，数据库中包含大量患者的隐私数据和医疗数据，必须要保障数据的安全性。在数据存储方面，患者的部分隐私数据受到保护，不能以明文的形式存储，在存储时进行加密处理。这样可以防止信息泄露，提高数据的安全性和保密性；在数据访问方面，不同模块对数据表有不同的操作权限，尽量最小化模块操作的访问权限，可以通过角色详细划分表的增、删、改、查权限。这样可以防止过大的数据库访问权限导致数据库遭到恶意破坏；在数据容灾方面，在不同的物理机上进行数据主从库备份，同时，每周进行一次全量备份，两次差量备份并且每天一次增量备份。这样系统遭遇故障和灾害时可以迅速切换到正常数据库服务，也能对数据的意外丢失和损坏进行快速恢复。通过以上数据库方面的举措大大提高了数据的安全性和保密性。

3、应用服务层面

系统应用对外提供服务的同时也向外暴露了系统的程序入口及数据的交互方式。一方面，系统需要与其它系统进行数据交互，比如说患者的护理文档，里面涉及患者隐私的病历信息，这些数据在传输过程中不能被非法采集和破坏。针对这个问题，我们采用信息摘要、数字签名、数字信封技术进行解决。护理文书一般数据量比较大，采用加密效率高的对称加密算法，对生成的随机密钥使用数字信封技术加密后发送给接收方，以确保密钥的分发安全。另外，为了确保接收到护理文书数据的完整性，保证数据是真实有效的，使用信息摘要算法对护理文档数据生成摘要信息。为了识别发送方的身份以及防止抵赖，要求发送方对摘要信息进行数字签名再进行发送。另一方面，护士登录系统时，除了输入用户名和密码，还需要输入短信验证码，以防密码被非法暴力破解，系统登录后，基于角色的权限分配，不同护士拥有不同的系统功能权限，只能使用有权限的功能，尽可能管控系统的功能权限，保证系统的使用安全。通过以上应用方面的安全技术，大大提高了系统的运行安全和使用安全。

基于系统安全架构设计，项目顺利开发完成，于2021年1月在某省三甲医院的成功上线。项目运行期间，各项安全性指标均达标，系统保持95%的使用率，获得患者，护士及医院领导的一致好评。可以说明系统安全架构设计在此项目中的运用是一次成功的实践．为我们提供了一套理论结合实践的成功经验。

尽管如此，在使用护理文书管理功能过程中，护士反馈打开护理文档查看时速度慢。这是由于系统接收的护理文档数据经过了加密，需要先解密然后验证数据完整性后才能展示，因此耗费了较长时间。在保证数据安全性的前提下，我们一方面选择效率更高的加密算法，另一方面分析护理文档信息，进行分块加密，只对必要信息加密，减少加密的数据量。从而在性能和安全性两方面达到较好的平衡。通过这次软件开发工作，让我认识到优秀的理论知识和实践相结合才能成就好的软件项目，这敦促我在工作中也不忘提升理论知识，最终成为一名优秀的软件架构师。