电子病历信息系统安全性分析与设计

21069100225 赵红玉

1.电子病历系统概况

1.1 电子病历系统介绍

电子病历(electronicmedicalrecords，EMR)也叫做计算机化的病案系统或者基于计算机的患者记录，它是采用计算机手段传输、存取、管理和重现数字化的患者医疗记录信息系统。

该系统能够为用户提供访问完整准确的数据、警示、提示和临床决策支持系统的能力。相对于纸质病历而言，电子病历能够为医护人员和患者提供完整、实时的数据；通过校验、警告、提示等手段提示医护人员有关处方可能出现的问题，降低医疗差错，提高医疗质量；同时，电子病历能够传输和共享患者的医疗记录信息，提高工作效率，也为医疗管理、科研医疗纠纷等提供数据源。

该系统具体结构如图 1.1 所示。

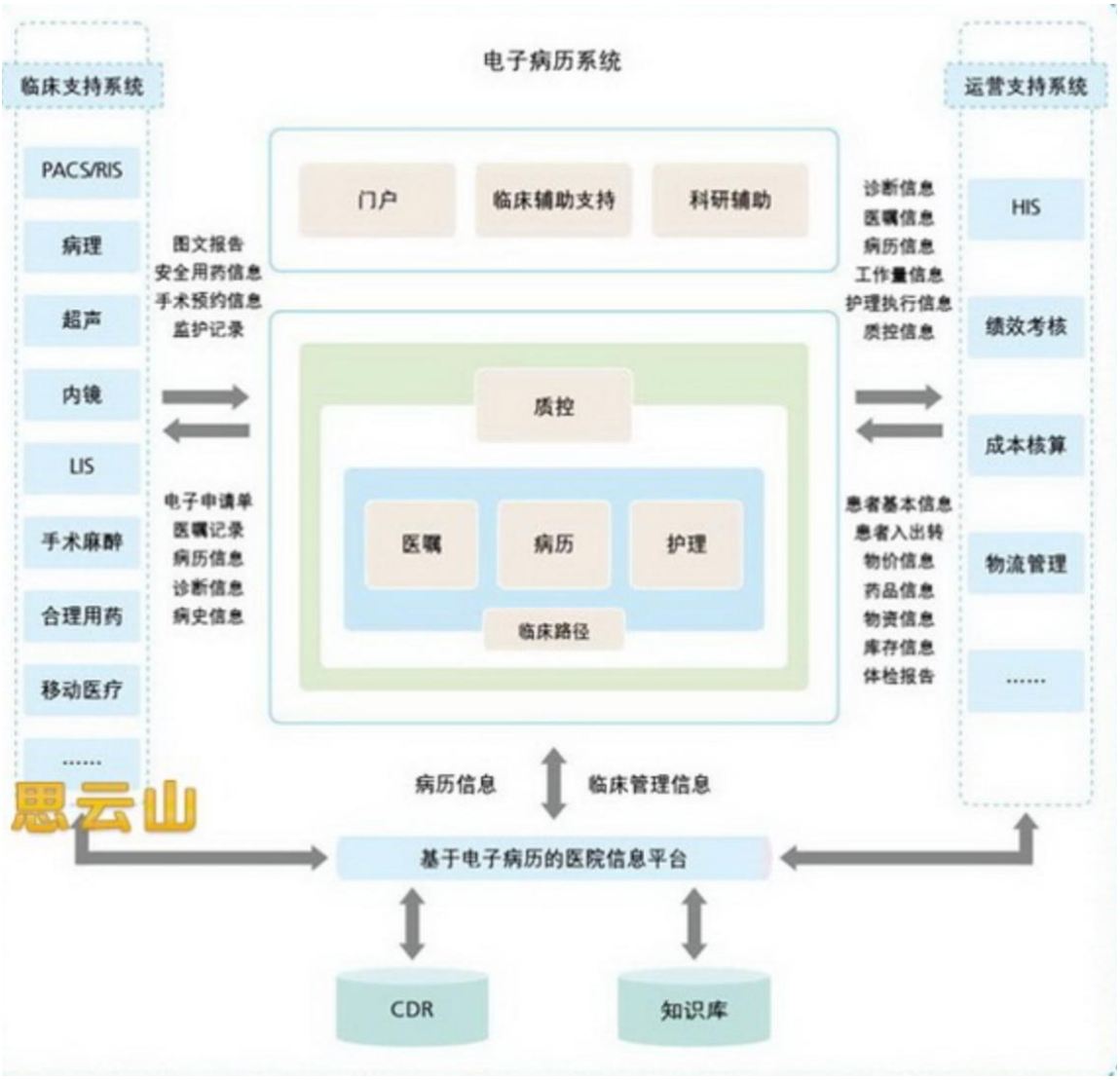

图1.1EMR 电子病历系统结构

1.2 电子病历系统基础功能

电子病历系统 EMR 具有用户授权与认证、使用审计、数据存储与管理、患者隐私保护和字典数据管理等基础功能，保障电子病历数据的安全性、可靠性和可用性。电子病历的管理以建立数据中心为基础，实现信息实时上传和自动备份到医院数据中心和第三方存储中心，在设定一定权限的基础上实现数据资源的共享，并保障数据安全。

包括：用户授权功能、用户认证功能、使用审计功能、数据存储与管理功能、患者隐私保护功能、字典数据管理功能。

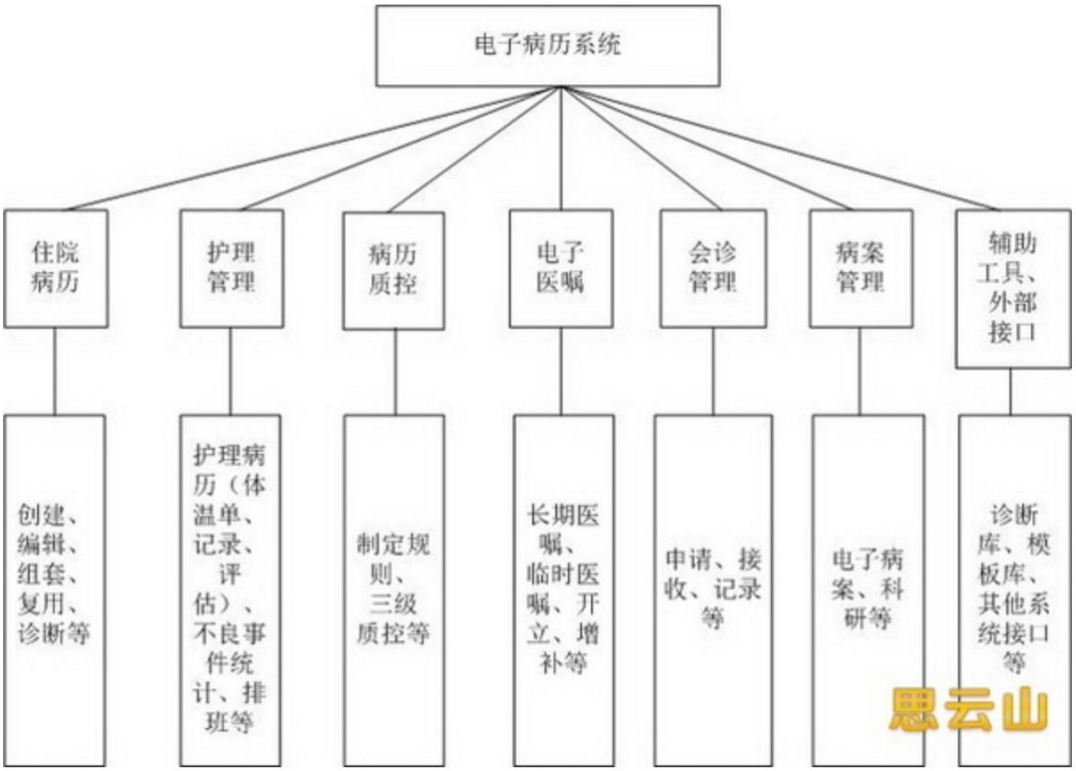

图1.2 电子病历系统基础功能

由此可知，电子病历能够有效、可靠地记载、传递、分析、共享患者的相关医疗信息，而这些信息对所有参与医疗保险提供服务系统的组织和个人都有不同的利害关系，尤其是涉及到医疗纠纷时，电子病历将扮演极其重要的角色。因此如何确保电子病案的安全使用是医院病案管理部门首先应该考虑的重要问题。

为了保障电子病历系统的安全，应该设计一个合理的认证技术和权限控制。

2.电子病历系统安全需求分析

电子病历所涉及的安全性方面主要有：

①电子病历包含患者的所有信息，涉及到个人的隐私，法律规定患者的信息不能随意被泄露，这要求电子病历的隐私性要得到保证；

②病历是作为医疗纠纷的法律依据，同时也是医疗诊断和治疗操作的依据，所以电子病历的完整性、不可否认性和可鉴别性都要得到保证。

就目前来讲，电子病历系统存在的安全隐患问题主要有：

电子病历系统如果遭遇病毒或黑客入侵，就会导致电子病历里的信息被修改；电子病历系统的授权用户滥用健康信息档案；政府或企业非法介入私人医疗保健问题等。

因此，主要从以下 4 个方面诠释电子病历的安全需求。

2.1 隐私性

电子病历的隐私安全保障是电子病历全面推广的前提。每个国家的公民都享有隐私权，我国也不例外。自电子病历引入我国医疗机构以来，患者的隐私权问题就逐渐引起了患者、相关部门以及学者的关注。随着医疗保险、远程医疗的不断推进，电子病历的信息共享更加频繁，这就要求信息在存取、传输的过程中要做好预防信息被非法截取或窃取的安全措施。本文通过用户认证和用于传输信息的密码技术来确保电子病历的隐私安全。

2.2 完整性

电子病历信息的完整性和真实性是电子病历应用的基础。要防止非法用户对电子病历的信息进行随意修改、删除，同时也要防止信息在传输过程中被篡改和丢失、重复等。本文通过数字签名的方式来实现信息的完整性。

2.3 不可否认性

电子病历是医疗纠纷、医疗理赔和事故鉴定的重要依据，那么如何保证医患双方的合法性是电子病历得以推广实施的关键。因此，要对数据和信息的来源进行严格的监控和检验，以保证信息是合法用户发出的，也要防止数据信息发送方发出信息后否认发送的内容，同时防止接受方接到信息后否认曾经接受过的信息或者篡改过数据信息，保证医务人员对病历信息的记录、修改及修改时间等具有不司否认性。

2.4 认证性

随着网络技术的快速发展，身份盗用、交易诈骗、网络钓鱼等事件也接踵而来。目前，大多数的临床信息系统都采用用户名和密码的方式登录系统，如果密码设置过于简单，就很容易被人盗取或破解，从而危害病历系统的安全性。通过有效的数字证书来认证用户登录电子病历系统可以进一步确保病历系统的安全。首先通过证书载体保护口令校验；然后通过随机数的签名和验证，防止重放供给；再认证用户证书的信任链以及有效期；接着通过 CRL 验证用户证书是否被吊

销；最后将证书的姆印与电子病历系统的用户账号对比，从而确定用户的身份和权限。

3.电子病历系统安全体系结构设计

根据上述分析，要实现电子病历的安全管理，就需要研究一套电子病历的安全管理体系。本文参照国内外网络管理模型，结合我国的实际情况及电子病历自身的特点设计了电子病历安全管理模型，如图2.1 所示。该系统结构采用了 c / s 的模式来实现，数据管理通过分布式的数据库来实现，与一般应用系统的不同之处在于该系统框架强调了病历的可操作性和信息的安全性。无论是电子病历的访问、修改、删除，还是网络上信息的传输，都是在电子证书认证的基础上进行的。通过电子认证可以保证信息的安全，从而避免非法人员恶意修改或伪造病历信息，同时也可保证医务人员否认曾经开过的处方(不可否认性)，为医疗纠纷提供坚实的法律依据。

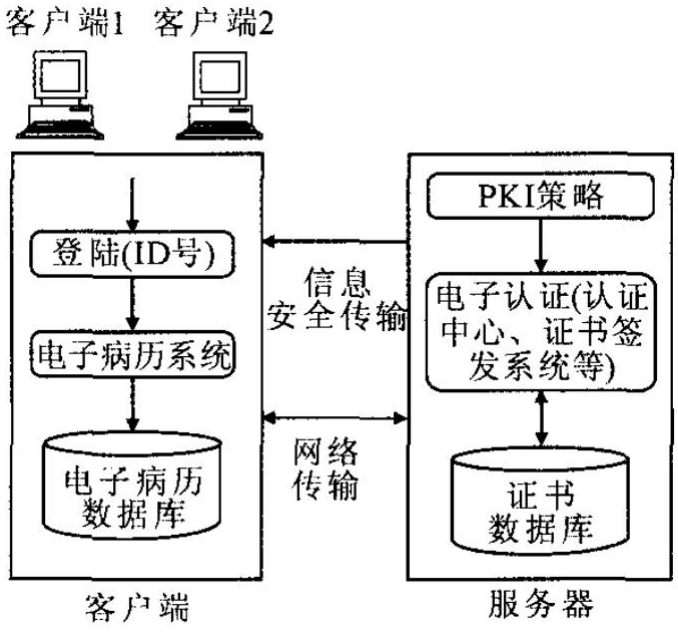

图3.1 电子病历安全管理模型

3.1 电子病历安全管理模型的客户端设计

客户端主要是由电子病历系统构成，电子病历主要包括患者的基本信息、医嘱、病程记录、检查检验结果、手术记录、护理记录等，其相关信息的存储需要数据库的支持。登录该系统的人员需要拥有正确的证书和口令以及验证码才能访问，这样既可以保证系统和相关信息的安全，也能保证医院工作人员实现合法的操作以及确保其身份的可信，同时能记录访问人员访问的时间、对病历的修改及修改时间和修改内容等。

3.2 电子病历安全管理模型的数据库安全设计

数据库安全和日志服务是两个相互关联的过程。数据库中数据的保护一方面通过应用程序的完整全面来避免系统维护人员和业务科室人员不直接操作数据库中的表，同时，通过日志一方面保证操作的可追踪性，另一方面保证操作的可逆性。

3.2.1 数据库权限控制

通过数据库提供的系统权限、对象权限(查询、修改、删除、插入等)来进行控制，并且利用权限角色将相应的权限分类，使得权限管理更加灵活。

3.2.2 数据库加密

对一些敏感的表进行加密，只有校验通过后，才能对这些表进行读写的操作，以免对这些表进行去操作或恶意的修改。

3.2.3 数据库日志

通过利用数据库软件提供的归档日志分析工具，可以分析数据库数据操作的全部过程，从中发现安全隐患，及时解决。

3.2.4 数据一致性维护

对数据进行严格的合理性校验，提高原始数据的可靠性；通过数据库本身的机制以及程序中的控制来保证数据的完整性和一致性。

3.2.5 数据库审计

通过安全审计记录和跟踪用户对数据库的操作，防止否认对数据库的安全责任。

3.3 电子病历安全管理模型的信息安全传输设计

为了保证信息传输的安全性，本系统在客户端和服务器之间建立一条安全通道(如图 3.3),并且是在公钥密码体制的基础上进行数字签名，即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一把仅为本人所掌握的私有密钥(私钥),可以用它进行解密和签名，同时拥有一把公共密钥(公钥)并可以对外公开，用于加密和验证签名。当发送信息时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样，信息就可以安全无误地到达目的地了，即使被

第三方截获，由于没有相应的私钥，也无法进行解密。通过数字签名的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。首先是客户端发送信息，经过数字签名，再将信息发送给服务器，服务器接到信息后进行完整性验证；然后对合法的信息进行处理，再向客户端反馈信息，在反馈的过程中，信息同样要进行加密解密的数字签名处理，这样可以保证信息的安全传输。

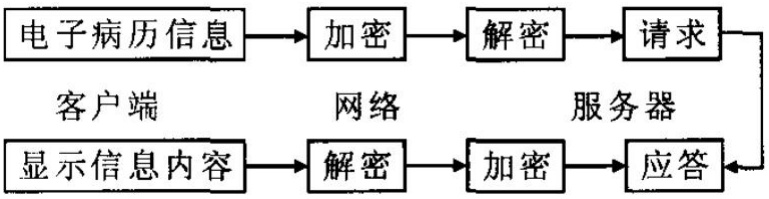

图3.3 信息安全传输过程

3.4 电子病历安全管理模型的服务器端设计

服务器端主要包括电子认证系统，该系统中包括认证中心、证书签发系统等，并且是在 PKI 的策略指导下进行的，同时也需要数据库的支持。其中，PKI(PublicKeyIn-frastructure)的全称是公钥基础结构，在20 世纪 80 年代基于公开密钥理论和技术的基础上发展起来的一种综合安全平台，能够为网络应用提供采用加密和数字签名的密码服务所需的密钥和证书管理，从而达到保证信息在网络上传输能够安全、真实、完整和不可否认的目的。PKI 主要由 PKI 策略、认证中心、证书签发系统和 PKI 应用等构成安全体系，其中，PKI 策略定义了信息安全的指导方针和密码系统的使用规则，具体内容包括 CA(CertificationAuthority)之间的信任关系、遵循的技术标准、安全策略、服务对象、管理框架、认证规则、运作制度、所涉及的法律关系

等。本系统的服务器端就借鉴了 PKI 技术，在 PKI 技术的指导下进行电子病历安全性、完整性、保密性等认证。具体的认证过程见图 3.4。

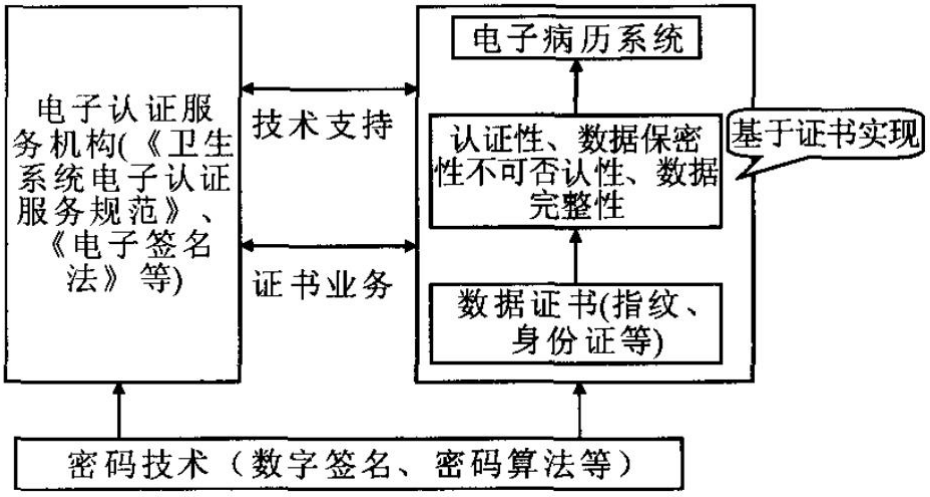

图3.4 电子认证过程

电子认证服务机构是经过国家主管部门授权经营的电子认证服务公司或是由卫生相关部门批发经营许可的 CA 认证机关，它签发的电子认证证书是最有权威性的。同时，政府主管部门通过法律统一的技术来规范电子认证的标准和程序，避免由于不同标准出现而造成电子认证无法实现而达不到网上认证安全性的目的。

该系统的密码技术主要包括密码算法、数字签名等。密码算法是指加密算法 E 和解密算法 D。加密算法是一组以加密密钥 Ke 为参数由明文变为密文的算法，可简写为 C=Eke(M),即将用户输人的密码在传送前变为密文，以密文的形式来传送可以防止密码被盗或修改；解密算法是一组以加密密钥 Kd 为参数由密文变为明文的算法，可简写为 M=Dkd(C)。数字签名又称电子签章，是以电子的形式存储在数据信息之中，可用于辨别数据签署人的身份，同时也表明签署人对数据信息中所包含信息的认可。首先，信息的发送者用自己的密钥对要发

送的信息进行编码运算，生成不能读取的密文；然后，将密文发送给信息接收方，接收方用发送方的密钥进行解码来核实签名。在传输的过程中，如果信息发生改变，数字签名的值也发生改变，这样可保证信息传输过程中的完整性、信息发送者身份的认证性、防止信息的发送者和接受者抵赖性。

数字证书是指标识网络用户身份的一系列数据，如指纹、身份证等，用来识别网络用户的身份，它是由权威的 CA 中心签发的，以加密技术为核心，对网络传输的信息进行加密、解密、数字签名、签名校验，以确保信息的机密性、完整性、用户身份的真实性以及签名信息的不可否认性，从而保障网络应用的安全。

4.电子病历系统安全性评价

针对上述进行了相关安全设计的电子病历系统，达到如图 4.1 形式，可以根据相关的指标进行安全性评价。以下是电子病历系统的安全性评价。

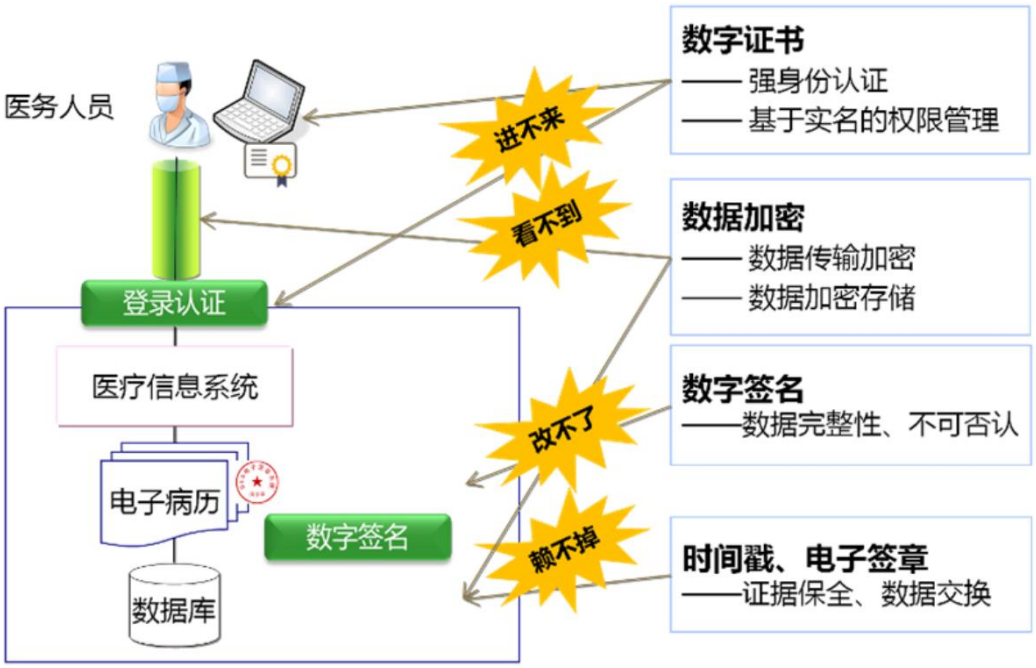

图4.1 经过安全设计的电子病历系统

4.1 访问控制

电子病历系统已经进行安全设计的客户端设计，包括身份认证和授权机制，确保了只有经过身份认证的用户可以访问系统，并减少未经授权访问的风险。

电子病历系统实施了基于角色的访问控制模型，限制用户对患者信息的访问权限。确保了用户只能访问其所需的信息，以减少误操作和滥用权限的可能性。

4.2 数据保护

电子病历系统的数据库安全设计，包括数据库权限控制、数据库加密和数据一致性维护等。实施了数据库权限控制机制，确保只有授权用户可以访问和操作数据库。并且使用适当的加密算法和技术对敏

感数据进行加密存储。实施了数据一致性维护措施，如数据校验和约束，以确保数据的准确性和完整性。

4.3 安全传输

电子病历系统的信息安全传输设计，使用了安全传输协议和安全套接字层来保护数据传输的安全性。而且使用数字证书和公钥基础设施（PKI）进行身份验证和数据完整性保护。

4.4.安全审计和监控

电子病历系统的安全审计和监控机制，进行了数据库日志记录、安全事件记录和异常检测等。并且数据库记录了所有的操作，包括读取、更新和删除等，以便追踪和审计数据库的访问和操作。电子病历系统具备入侵检测和防御系统，能够检测和阻止恶意攻击和安全威胁。

4.5 物理安全

电子病历系统服务器端设计，包括物理安全措施和设备保护。有适当的物理访问控制，如机房门禁、设备锁定等。有备份和灾难恢复计划，以应对意外数据丢失和系统故障。

5. 总结

通过全面的安全性分析与设计，电子病历信息系统能够在保护患者隐私和数据安全方面发挥重要作用。期待未来的系统能够不断提升

安全性能, 应对新的安全挑战, 并始终以患者隐私和数据安全为中心, 为医疗行业提供更安全可靠的电子病历管理解决方案。