基于等级保护的电子病历管理系统研究与设计*

苏金月 李建 陈积常

南宁学院信息工程学院，南宁，530200

摘 要 针对目前医院信息系统安全等级保护及电子病历系统建设中存在的问题，根据国家信息安全等级保护标准，设计了以电子病历等系统为计算环境的等级保护框架，从信息安全技术和信息安全管理两个维度构建医院信息系统安全防御体系。该电子病历可以实现可靠的电子病历系统身份验证、数据安全管理（采集、处理、传输、存储和利用）等功能，为降低病毒传播风险、电子取证、责任追踪和及时化解医患矛盾提供了解决方案。

关键字 医院信息系统, 等级保护, 电子病历数据库, 数字签名

Research and Design of Electronic Medical Record System Based on Hierarchical Protection

Su Jinyue Li Jian Chen Jichang

School of Information Engineering Nanning University
Nanning 530200,China;
943667593@qq.com

Abstract—Based on deep learning, image recognition and other technologies, a decision-making system and adaptive control system suitable for miniature intelligent vehicle control are designed and implemented by using Scikit_learn and OpenCV development tool. The system uses convolution neural network algorithm, vehicle control algorithm and image recognition algorithm to realize automatic driving, obstacle recognition and avoidance on micro road. The test results of data acquisition, system training and automatic driving test in the miniature intelligent vehicle show that the optimization method of neural network and its training can improve the effect and speed of machine learning. The designed and implemented miniature intelligent vehicle decision-making system can be better combined with vehicle control to realize automatic driving and obstacle avoidance in road environment.

Keyword—Hospital information system, Class protection, Electronic medical record database, Digital signature

1 引 言

突如其来的新型冠状病毒给世界各国人民的身体健康和生命安全带来了极大的威胁，特别是给现有的医疗体系造成了巨大的冲击，如何在提高医院病情诊断效率的同时，减小病毒对医护人员的二次感染风险，从而提高治愈率是摆在我们面前的重要研究课题。

医院信息系统是指利用计算机软硬件技术和网络通信技术等现代化手段，对医院及其所属各部门的人流、物流、财流进行综合管理，对在医疗活动各阶段产生的数据进行采集、存储、处理、提取、传输、汇总，加工形成各种信息，从而为医院的整体运行提供全面的自动化管理及各种服务的信息系统[1]。目前，各级医院都按照国家信息安全等级保护标准对医院信息系统实施了等级保护[2-4]。一些学者对医院信息系统等级保护问题进行了研究，但往往只停留在宏观的体系结构上，缺乏对具体的医疗业务系统实现的研究[4]。

目前，人们对医院电子病历系统进行了研究，提出了一些基于数字签名技术的电子病历方案。文献[5]提出了一套比较完整、高效的患者数字化签名解决方案，可以实现临床签名的真实、完整、可信。文献[6]探讨了使用移动电子病历实现在病床旁对患者进行数

*基金资助：本文得到 2017 年南宁学院校级重点专业（通信工程）（2017XJZDZY11)、广西民办重点专业建设（通信工程）（2021MBZDZY01)资助.

通讯作者：李建，教授，943667593@qq.com

据采集、医学诊疗、记录查房信息等操作的技术方案。文献[7] 采用基于数字证书认证的电子签名技术，提出了一种医院电子病历的安全运行机制。文献[8]和[9]对在医院信息系统数据库数据保护技术进行了研究。文献[10]-[12] 对电子签名技术在医院信息管理中的应用进行探讨。文献[13]设计实现了一个基于 CA 认证的可信电子病案系统。但是以上文献研究以及所提出的方案一是缺乏等级保护基础，二是没有真正实现电子病历功能。现有的电子病历系统仍存在着难以与原有的医院信息管理系统融合、等级保护和隐私保护不强、数据安全管理不到位等问题[14]。

针对上述存在的问题，论文提出了基于 PKI 技术的电子病历等系统等级保护架构，运用 Linux 操作系统、Shell 脚本编程、数据库 Mysql 等技术将数字签名与医院电子病历系统安全集成，实现可靠的电子病历系统身份验证、数据安全管理（采集、处理、传输、存储和利用）等功能，为降低病毒传播风险、电子取证、责任追踪和化解医患矛盾提供了一种解决方案。

2 医院信息系统等级保护安全体系设计

2.1 安全体系总体框架设计

本文以国家等级保护要求为原则，兼顾医院现有的信息技术与管理手段，设计医院信息系统安全体系总体框架如图 1 所示。

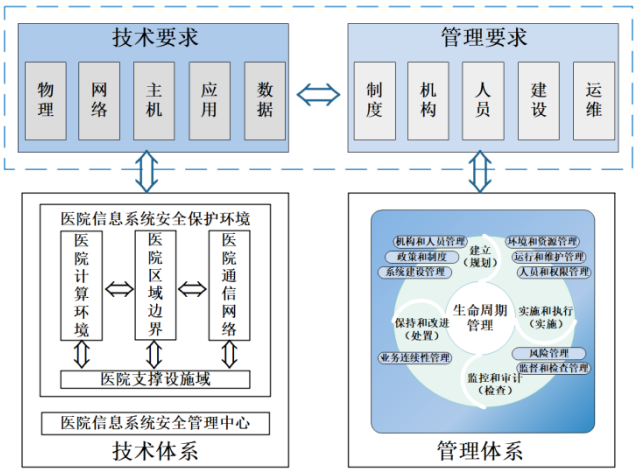

图 1 医生信息系统等级保护安全体系总体框架

在图 1 中，技术要求包括物理安全、网络安全、主机安全、应用安全、数据安全五方面要求，管理要求包括安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等五方面要求。技术体系和管理体系综合形成的两个保障体系，其中技术体系以“一个中心，三重防护”为核心理念。因此，综合来说，医院等级保护安全体系重构方案设计就是：二个体系（安全技术体系、安全管理体系）、一个中心（医院信息系统安全管理中心）、三重防护（医院安全计算环境、医院安全区域边界、医院安全通信网络）。

2.2 安全技术体系设计

本文参考国家颁布的《信息系统等级保护安全设计技术要求》的安全域模型，将安全域纵深防护、多层次立体防御 和信息安全等级保护等安全防御思想相结合，将医疗机构作为一个整体保护对象，建立医院信息系统等级保护网络安全体系架构如图 2 所示。

在图 2 架构的基础上，根据目前医院最高等级级别（三级）的组织结构、网络架构，设计医院信息系统等级保护安全体系技术框架（如图 3 所示）。三级安全域细分为计算环境域、区域边界、通信网络和支撑设施域，三级安全域内部又可以根据医院信息系统的不同组织对象划分为不同的三级安全子域。

(1) 计算环境是对医院信息系统的信息进行存储、处理及实施安全策略的相关部件。医院计算环境域防护主要针对医院信息系统的主机安全、应用安全及数据安全。它是通过医院业务终端（门诊、药房、住院部等部门终端）、医院内部网站维护终端、业务应用数据服务器（医院信息系统 HIS 、电子病历系统 EMR、影像归档 PACS、通信系统和检验科信息系统 LIS 等），以及安全设备（数据库审计系统）的安全机制与服务等，对用户行为的控制，有效防止非授权和授权用户非法访问，确保医院信息和信息系统的保密性和完整性，从而为医院应用业务处理全过程的安全、免受恶意破坏提供支撑和保障。

(2) 区域边界是对医院信息系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。区域边界防护主要针对医院信息系统的网络安全，其建设是通过双防火墙等安全产品实现，对进入和流出医院信息系统计算环境的信息流进行安全检查和访问控制，满足其安全控制措施的要求。

(3) 通信网络是对医院信息系统安全计算环境之间进行信息传输及实施安全策略的相关部件。医院通信网络防护主要针对信息系统的网络安全，其范围包

括互联网（联通、电信）、内联广域网等以及计算环境内部的交换域。通过通信网络设备对通信双方进行可信鉴别验证，建立安全通道，并实施数据传输保护，确保其在传输过程中不会被监听、篡改和破坏。

(4) 安全管理中心的支撑设施是对医院信息系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台，支撑设施的实施确保医院信息系统配置完整可信，明确用户操作权限，实施全程审计追踪。如图 2 所示，医院信息系统安全管理区细分为 CA 中心、终端管理系统、安全管理平台和网络审计管理中心等，看似独立存在，实则环环相扣，相互制约。其中电子病历系统应用 CA 数字证书是通过医院证书受理点获取用户数字证书，并实现医生登录身份验证、电子病历安全管理等。

2.3 安全管理体系设计

第一步根据医院信息化建设进程的实际需求，逐步建立起各项安全管理机构制度、医护人员安全管理，以及医院信息系统运维建设管理。第二步首先通过安全机构、医护人员对制度的执行，提高信息安全保障能力；其次根据执行结果检查各项制度存在的问题和缺陷；最后依据检查结果对制度进行改进。从而形成从建立，到实施和执行、再到监控和审计、最后进行保持和改进的不断循环过程，逐步形成完善的医院信息系统管理体系。安全管理体系架构如图 4 所示。

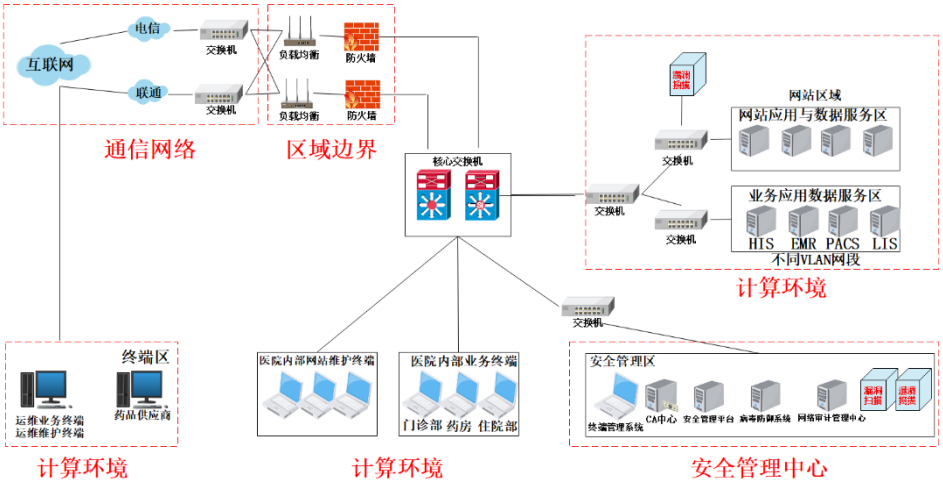

图 2 医院信息系统等级保护网络安全体系架构

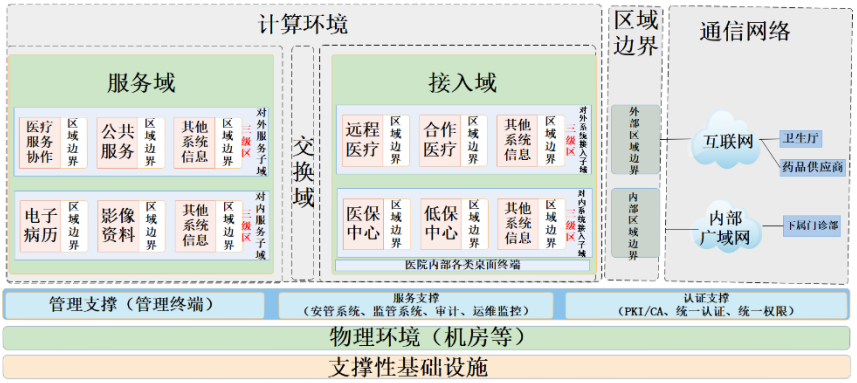

图 3 医院信息系统等级保护安全体系技术框架

3 电子病历系统设计与技术实现

3.1 电子病历系统概要设计

电子病历系统（EMR）是医学专用软件。医院通过电子病历以电子化方式记录患者就诊的信息，包括：首页、门诊医生站、护士工作站、病案管理、医嘱、手术记录、护理记录等，其中既有结构化信息，也有非结构化的自由文本，还有图形图像信息。

电子病历不仅指静态病历信息，还包括提供的相关服务。是以电子方式管理的有关个人终生健康状态和医疗保健行为的信息，涉及患者信息的采集、存储、传输、处理和利用的所有过程信息。

电子病历系统的功能需求包括医生登录身份鉴别、电子病历生成、电子病历数据数字签名、医生使用私钥对电子病历数据签名、数据库存取电子病历数据、数字签名验证、登录日志等。系统要求具有稳定性和安全性。稳定性是指：电子病历系统需要保证医生使用过程的正常稳定运行，在客户端的数据请求和访问操作下能够及时做出有效响应；安全性是指：防止医生登录信息进行暴露，还要对使用过程中产生的数据进行安全处理，更要防止个人信息的丢失。

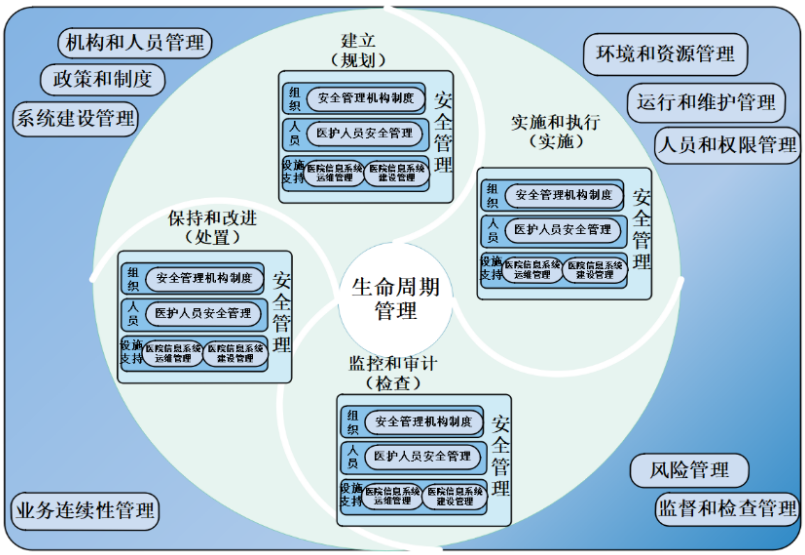

图 4 医院信息系统等级保护安全体系管理框架

本文的电子病历系统的技术架构图如图 5 所示，主要包括视图界面、业务逻辑处理和运行的环境。其中，视图界面层给医生提供可视化操作界面，包括医生登录操作，对电子病历各种操作等；业务逻辑层实现的是医生在数据请求和访问时的业务处理，不同界面之间的数据传递。数据的交互是通过不同的接口实现的，使用过程中医生会根据需要切换界面，当前界面的数据就需要进行本地保存和数据库存储，涉及了医生对电子病历数据的更新、查找，不断修改和保存；运行环境层是结合 Xshell 远程 VMware Workstation Pro 的 linux 操作系统环境以及 Shell 脚本编程技术实现。

3.2 电子病历系统的功能设计与技术实现

本文运用了 mysql 数据库管理技术、Xshell 远程、Shell 脚本编程、数字签名等技术，以及 OpenSSl 等安全工具，实现了终端对医生的身份鉴别功能、电子病历生成功能、电子病历数字签名功能、mysql 数据库系统存取电子病历数据功能、mysql 数据库系统加密电子病历数据功能、电子病历数字签名验证等功能。

(1) 医生的身份鉴别

登录界面要求首先后台管理员在 mysql 验证医生的数字签名，其次对比本地的用户文件，最后对比验证码，利用 echo 提示用户操作。具体的实现方式如下：

① 绘制电子病历的登录界面。使用的是应答协议 echo，通过它新的 AJAX 表现层引擎提供生动的用户界面，而且还提高了整体性能和实用性嵌套使用。

② 身份验证。医生验证身份时，首先使用自己 usbkey 中私钥(user.pri)对数字证书(user.crt)签名，其次把数字证书、签名数字证书(user.crt.sign)发送至 mysql，请求验证。后台 mysql 收到医生数字证书和签名数字证书后，使用医生数字证书中的公钥，对医生数字证书和签名数字证书进行比对，若确认是医生本人，允许登录进入下一步操作。反之则强制退出，并记录在本地登录日志中，供日后追踪。

③ 用户名验证。数字签名验证通过后，输入用户名，系统将检查本地用户信息文件，若用户存在，允许用户进入下一步操作，反之则强制退出。

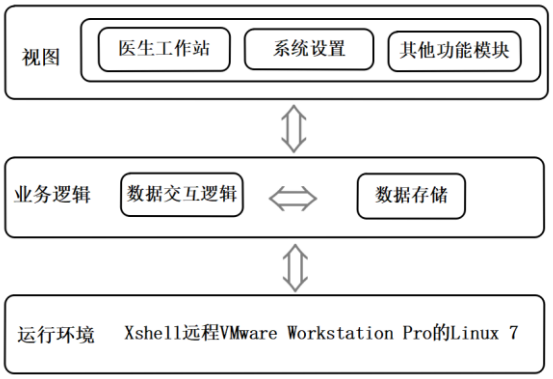

图 5 电子病历系统技术架构图

④ 验证码验证。用户审核通过后，输入验证码，实质是使用 Linux 操作系统 shuf、openssl 工具产生的随机数，包括数字字母。验证码验证的目的是区分用户是计算机还是人，防止恶意破解密码、刷页，有效防止网络攻击如黑客用特定程序暴力破解方式进行不断的登录尝试，达到系统确认医生身份效果。

(2) 电子病历生成并自动加密

电子病历首页包括患者个人信息和简要医疗信息。电子病历系统设置相应功能，实现患者再次看诊时个人信息在病历记录中的自动生成，以保证患者姓名、性别等信息不再重复录入，为医疗工作提供方便，节省时间；医生修改病历时，电子病历系统保存将每次修改痕迹、标记准确的修改时间和修改信息。最后电子病历数据采集完毕后，将自动加密电子病历数据。

技术实现时，使用 openssl（开放式安全套接层协议）以及 DES 算法自动加密电子病历数据，得到电子病历加密数据（电子病历数据.encry）。DES 算法为密码体制中的对称密码体制，又称为美国数据加密标准，是 1972 年美国 IBM 公司研制的对称密码体制加密算法，确保电子病历数据安全，保护患者隐私。

(3) 电子病历数据数字签名

数字签名机制作为保障网络信息安全的手段之一，可以解决伪造、抵赖、冒充和篡改问题，数字签名的目的之一就是在网络环境中代替传统的手工签字与印章，对医院传统手工病历发展电子病历趋势有相当重要的作用。

数字签名过程首先使用 openssl（开放式安全套接层协议），以及哈希函数又称散列算法 sha256，产生电子病历数据原文件摘要，再使用医生 usbkey 中的私钥(user.pri)对其摘要签名，结果产生电子病历数据签名文件(电子病历数据.sign)，过程如图 6 所示。

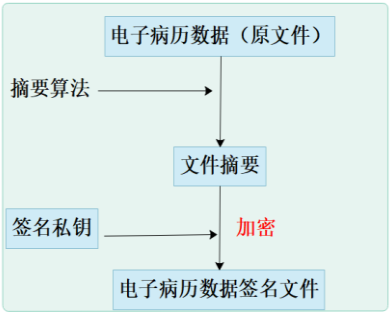

图 6 数字签名过程

(4) mysql 存取电子病历数据

具体的操作步骤如下：

① 医生把电子病历数据(电子病历数据.encry)、签名的电子病历(电子病历数据.sign)、医生数字证书(user.crt)送至数据库 mysql 本地后，医生在 mysql 本地使用数字证书的公钥验证电子病历数据在传输过程是否被篡改。

② 电子病历数据数字签名验证通过后，医生使用管理员身份进入数据库 mysql，在 mysql 中创建电子病历管理库，创建电子病历表格，表格如图 7 所示。

③ 医生进入电子病历管理库。使用电子病历表格存储电子病历数据时，医生只需要选择存在符合格式（字段数据之间用 tab 键隔开，null 值用\n 来代替）的文本数据文件（电子病历数据.encry）时，即可导入数据。从 mysql 电子病历表格导出电子病历数据时，医生只需要选择电子病历表格内容，保存 mysql 本地指定文件（电子病历 mysql 数据）即可。同时，导出数据与导入数据格式是一致的，以便后期数字签名的验证等，医生将电子病历数据导入导出 mysql 操作。

④ 医生从数据库 mysql 导出数据，保存至 mysql 本地后，并使用 gpg 工具加密导出数据。医生导出电子病历数据后，使用 gpg 对称密码加密导出数据。gpg 是 GNU 隐私保护(GnuPG)的 OpenPGP 部分，提供数字加密和使用 OpenPGP 标准签署服务、完整的密钥管理和所有附加功能。确保电子病历 mysql 数据加密后，保存至 mysql 本地时的相对安全，供医生需要时调用。

```
mysql> desc 电子病历;
+-----------------+-------------+------+-----+---------+-------+
| Field           | Type        | Null | Key | Default | Extra |
+-----------------+-------------+------+-----+---------+-------+
| 电子病历编号    | bigint(50)  | YES  | UNI | NULL    |       |
| 身份证号        | varchar(75) | YES  |     | NULL    |       |
| 姓名            | varchar(75) | YES  |     | NULL    |       |
| 性别            | varchar(75) | YES  |     | NULL    |       |
| 年龄            | varchar(75) | YES  |     | NULL    |       |
| 联系电话        | varchar(75) | YES  |     | NULL    |       |
| 既往史          | varchar(75) | YES  |     | NULL    |       |
| 过敏史          | varchar(75) | YES  |     | NULL    |       |
| 家族史          | varchar(75) | YES  |     | NULL    |       |
| 个人史          | varchar(75) | YES  |     | NULL    |       |
| 发病过程        | varchar(75) | YES  |     | NULL    |       |
| 病因推理        | varchar(75) | YES  |     | NULL    |       |
| 诊断意见        | varchar(75) | YES  |     | NULL    |       |
| 看诊日期        | varchar(75) | YES  |     | NULL    |       |
| 医生签名        | varchar(10) | YES  |     | NULL    |       |
| 家庭住址省份    | varchar(75) | YES  |     | NULL    |       |
| 家庭住址区      | varchar(75) | YES  |     | NULL    |       |
| 家庭详细地址    | varchar(75) | YES  |     | NULL    |       |
+-----------------+-------------+------+-----+---------+-------+
18 rows in set (0.00 sec)
```

图 7 mysql 电子病历表

(5) 电子病历数字签名验证

对应电子病历的数字签名，数字签名验证功能实现同时验证本地电子病历数据、调用的 mysql 数据。医生登录电子病历系统后，可同时验证本地电子病历数据以及从 mysql 导出的数据(电子病历 mysql 数据.encry)的数据完整性。医生使用数字证书的公钥解密签名电子病历数据，分别与电子病历数据，mysql 数据进行摘要比对。若两份数据比对结果都一致则证明本地电子病历数据以及收到的 mysql 数据都没被篡改，若任意一份比对不一致则证明本地的电子病历数据或收到的 mysql 数据有被篡改，应该重视，过程如图 8 所示。

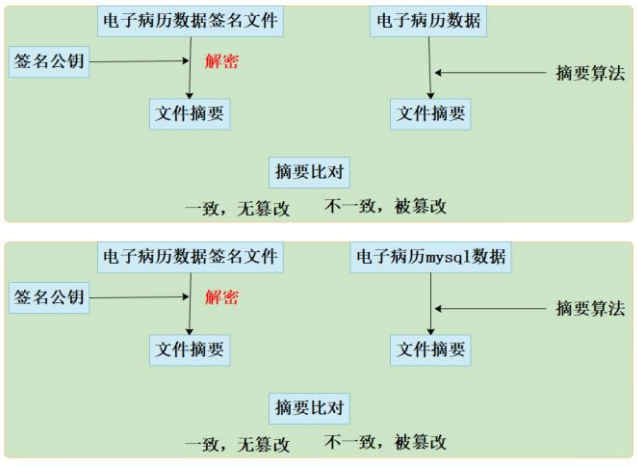

图 8 数字签名验证过程

(6) 登录日志生成并自动加密

医生登录电子病历系统过程，系统将检测医生数字证书、私钥信息以及用户信息，系统将自动记录登录时间、登录用户以及失败原因，记录后自动加密，供需要时使用。

本文系统使用 AES 算法密码分组链接模式（Cipher Block Chaining ，CBC)以及 128 位数据块为一组对电子病历系统登录日志进行加密，即 16 字节明文，对应 16 字节密文，明文加密时，如果数据不够 16 字节，则会将数据补全剩余字节。AES（Advanced Encryption Standard）是一种对称加密算法或称分组对称加密算法。使用 AES 算法加密电子病历登录日志（电子病历系统登录日志.encry）后不容易受主动攻击，符合 SSL、IPSec 的标准。

3.3 系统的性能测试与分析

具备数字签名的电子病历系统环境搭建主要是为系统提供数据加密、数字签名、数字签名验证、证书验证等功能。系统测试中，电子病历系统接收信息系统发送的签名服务请求，并返回签名或验证服务结果，利用可靠的数字签名技术、mysql 数据库技术、SSL 安全协议等，保证数据在产生、传输、 存储、再利用的整个生命周期过程的真实、完整、 准确，保证“数出有源”。

电子病历系统功能开发完毕后，我们通过用例测试，对相关的功能单元进行相关的单元测试，再利用测试结果分析优化代码、减少错误和提升用户的体验。测试的内容包括身份验证登录用例测试、电子病历自动加密用例测试、数字签名用例测试、mysql 存取数据用例测试、数字签名验证用例测试、登录日志生成与自动加密用例测试等。测试的结果表明，本文综合运用数据库、脚本技术和密码技术能够实现的电子病历管理系统能够提供可靠的电子病历系统身份验证、数据安全管理（采集、处理、传输、存储和利用）等功能，系统运行稳定、安全可靠。

4 结束语

本文从功能和非功能性两个方面分析了电子病历需求，运用 mysql 数据库管理技术、脚本设计技术、PGP 加密算法、密钥管理技术、数字签名技术对电子病历进行功能架构设计和技术架构设计。实现了终端对医生的身份鉴别功能、电子病历生成功能、电子病历数字签名功能、mysql 数据库系统存取电子病历数据功能、mysql 数据库系统加密电子病历数据功能、电子病历数字签名验证功能。通过搭建电子病历运行

环境，对电子病历系统进行了功能测试，结果表明综合运用数据库、计算机脚本技术和密码技术能够实现电子病历的管理功能，在保护医务工作者的身体健康和生命安全方面进行有益探索。

参 考 文 献

[1] 张益钊,朱卫国,孟晓阳,等.医院信息系统等级保护测评实践[J].医学信息学杂志,2015, 36 (10):14-18.

[2] 余兆明.医院信息系统信息安全等级保护的实施探讨[J].现代息科技,2019,3(03):150-151.

[3] 唐江波.基于医院信息安全等级保护的整改实践[J].中国数字医学,2018,13(11):83-86.

[4] 何强.应对关于医院信息系统数据安全问题的措施[J].计算机光盘软件与应用,2013,16(03):67+69.

[5] 陆松筠,刘昱,吴斌.住院患者数字化签名系统的探索与实践[J].医院管理论坛,2018,35(02):73-75+36.

[6] 刘迪,奚洋,沈锋,等.电子病历在移动医疗领域的研究与发展[J].无线互联科技,2018,15(23):156-157+166.

[7] 夏祺霖.数字签名技术在医院电子病历中的设计与应用[J].数字通信世界,2018(11):196.

[8] 吴吟.数据保护技术在医院信息系统数据库中的应用[J].数字技术与应用,2017(08):46-47.

[9] 杨燕红,刘长兴,蒋阅峰.数据保护技术在医院信息系统数据库中的应用[J].中国医疗设备,2015,30(09):96-98.

[10] 彭滢，石磊. 电子签名技术在医院信息管理中的应用[J].医疗卫生装备，2019，40(4):36-39，55.

[11] 李迎新，陈能太. 电子签名在医院电子病历中的实施[J].中国医学装备，2018，15(4):94-97.

[12] 王云军. 基于数字签名的电子病历及其研发思路探讨[J].医院管理论坛，2017，34(2):61-63.

[13] 崔志斌，崔宇璇，王腾飞. 基于 CA 认证的可信电子病案系统设计 [J].中国数字医学，2017，12(1):83-85.

[14] 李建梅.电子病历无纸化管理的优势与难点分析[J].信息与电脑(理论版),2016(22):60-62.