## 可维护性

落笔云烟的可修复性主要体现在下面几个方面：

1. 数据库的可恢复性：我们将使用另一台服务器作为数据库的备份，并且使用了cron的任务调度，每天会定时将数据库文件数据备份到另一台服务器。
2. 完善的日志系统：Flask轻量级框架可以实现完善的日志系统，落笔云烟利用了这一特性，会实时记录应用的运行日志，方便日后对于系统的维护。

## 例证：

**Cron:**

在Linux系统中，计划任务一般是由cron承担，我们可以把cron设置为开机时自动启动。cron启动后，它会读取它的所有配置文件（全局性配置文件/etc/crontab，以及每个用户的计划任务配置文件），然后cron会根据命令和执行时间来按时来调用度工作任务。cron 是一个可以用来根据时间、日期、月份、星期的组合来调度对重复任务的执行的守护进程。

cron 假定系统持续运行。如果当某任务被调度时系统不在运行，该任务就不会被执行。

根用户以外的用户可以使用 crontab 工具来配置 cron 任务。所有用户定义的 crontab 都被保存在/var/spool/cron 目录中，并使用创建它们的用户身份来执行。要以某用户身份创建一个 crontab 项目，登录为该用户，然后键入 crontab -e 命令，使用由 VISUAL 或 EDITOR 环境变量指定的编辑器来编辑该用户的 crontab。该文件使用的格式和 /etc/crontab 相同。当对 crontab 所做的改变被保存后，该 crontab 文件就会根据该用户名被保存，并写入文件 /var/spool/cron/username 中。

cron 守护进程每分钟都检查 /etc/crontab 文件、etc/cron.d/ 目录、以及 /var/spool/cron 目录中的改变。如果发现了改变，它们就会被载入内存。这样，当某个 crontab 文件改变后就不必重新启动守护进程了。

cron服务提供crontab命令来设定cron服务的。

以下是这个命令的一些**参数与说明**:

* crontab -u //设定某个用户的cron服务，一般root用户在执行这个命令的时候需要此参数
* crontab -l //列出某个用户cron服务的详细内容
* crontab -r //删除没个用户的cron服务
* crontab -e //编辑某个用户的cron服务
* crontab -u root -l // root查看自己的cron设置:
* crontab -u fred -r // root删除fred的cron设置

crontab文件的一些例子：

* 30 21 \* \* \* /usr/local/etc/rc.d/lighttpd restart

上面的例子表示每晚的21:30重启apache。

* 45 4 1,10,22 \* \* /usr/local/etc/rc.d/lighttpd restart

上面的例子表示每月1、10、22日的4 : 45重启apache。

* 10 1 \* \* 6,0 /usr/local/etc/rc.d/lighttpd restart

上面的例子表示每周六、周日的1 : 10重启apache。

* 0,30 18-23 \* \* \* /usr/local/etc/rc.d/lighttpd restart

上面的例子表示在每天18 : 00至23 : 00之间每隔30分钟重启apache。

* 0 23 \* \* 6 /usr/local/etc/rc.d/lighttpd restart

上面的例子表示每星期六的11 : 00 pm重启apache。

* \* \*/1 \* \* \* /usr/local/etc/rc.d/lighttpd restart

每一小时重启apache

* \* 23-7/1 \* \* \* /usr/local/etc/rc.d/lighttpd restart

晚上11点到早上7点之间，每隔一小时重启apache

* 0 11 4 \* mon-wed /usr/local/etc/rc.d/lighttpd restart

每月的4号与每周一到周三的11点重启apache

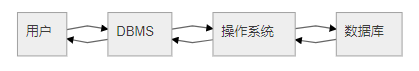
* 0 4 1 jan \* /usr/local/etc/rc.d/lighttpd restart

一月一号的4点重启apache

## 安全性

落笔云烟保护数据库以防止非法使用造成数据泄露，更改、或者破坏

### 例证:



1. 用户标识和鉴定

​ 数据库系统是不允许一个未经授权的用户对数据库进行操作的。

​ 用户标识和鉴定的方法有多种，为了获得安全性的保障，往往是多种方法并用。

（1）用一个用户名或者用户标识符来表明用户的身份，系统以此来鉴别用户的合法性。

（2）常采用用户名（username）和口令（password）相结合的方法，系统通过和对口令来判断用户身份的真伪。

（3）在鉴别用户的身份时，系统提供一个随机数，用户根据自己预先约定的计算过程或者函数来计算，系统根据计算结果来判断用户身份的合法性。

1. 用户存取权限的限制

​ 用户存取权限是不同的用户对于不同的数据对象允许操作的权限。在数据库系统中，每个用户只能访问他有权限访问的数据，并执行有权使用的操作。因此数据库系统必须预先定义用户的存取权限。

​ 存取权限由两部分构成

（1）数据对象

（2）操作类型

​ 在数据库的系统中，定义用户的存取权限称为授权。系统权限是由DBA授予用户的。对象权限是由DBA或者数据库的创建者授予。

1. 定义视图

​ 为不同的用户定义不同的视图，可以限制不同用户的访问范围。

通过视图机制将要保密的数据对无权限存取这些数据的用户隐藏起来，从而自动的实现对数据库的一定程度的安全性保护。

​ 但是，视图机制安全性保护不太精细，主要功能在于提供了数据的逻辑独立性

​ 在实际中，视图机制往往与授权机制相结合使用。

1. 数据加密

​ 防止数据在数据库中存储和传输中失密的有效手段。

​ 加密的基本思想是，根据一定的算法将原始数据加密成不可直接识别的格式，数据以米文德格式存储和传输。

加密的方法

（1）替换法。使用秘钥将明文中的每一个字符转换成密文中的字符。

（2）转换法。将明文种的字符按照不同的顺序重新排序。

1. 审计

​ 审计是一种监视功能，它更总记录有关数据的访问活动。

​ 使用审计功能将用户对数据库的所有操作自动的记录下来，存放在特殊的文件中，即审计日志。

​ 记录的内容一般有

（1）操作类型

（2）操作终端标识

（3）操作者标识

（4）操作时间和日期

（5）操作所涉及的相关数据

（6）数据的前象和后象

使用审计系统，会大大的增加系统的开销。

## 可改进性

落笔云烟的可改进性体现在以下几个方面：

1. 技术的可改进性：落笔云烟的主要功能（图像分割、字体打分等）结合了人工智能技术，人工智能相关技术的进步对于落笔云烟效果的提升具有很大帮助。

2. 功能的可改进性：落笔云烟的相关功能可以更具针对性地为某些独特的字体爱好者进行私人定制，大规模训练某一单一字体，以保证提供给意图练习该字体的用户更加有针对性的指导。