**隐私数据脱敏管理平台**

**需求分析报告**

**版本：<1.0>**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档编号： | 1 | 密 级： | 公开 |
| 编 写： | 陈思宇 | 编写日期： | 2024年8月19日 |
| 审 核： |  | 审核日期 | 2024年8月19日 |
| 批 准： |  | 批准日期： | 2024年8月19日 |

Copyright @, All right reserved

目录

[1 引言 2](#_Toc2712)

[1.1 编写目的 2](#_Toc1784)

[1.2 范围 2](#_Toc19552)

[1.3 定义 3](#_Toc23749)

[2 项目概述 3](#_Toc6446)

[2.1 产品描述 3](#_Toc11482)

[2.2 产品功能 3](#_Toc8724)

[2.3 用户特点 4](#_Toc20699)

[2.4 一般约束 4](#_Toc31635)

[2.5 假设和依据 5](#_Toc28402)

[3 具体需求 5](#_Toc12342)

[3.1 功能需求 5](#_Toc30834)

[3.1.1 用户管理 6](#_Toc8463)

[3.1.2 数据库管理 7](#_Toc29433)

[3.1.3 数据脱敏操作 8](#_Toc27373)

[3.1.4 UI界面设计 9](#_Toc1836)

[3.1.5 任务列表管理 10](#_Toc32397)

[3.1.6 记录操作日志 11](#_Toc27326)

[3.2 外部接口需求 11](#_Toc19225)

[3.2.1 用户接口 11](#_Toc10097)

[3.2.2 硬件接口 12](#_Toc5536)

[3.2.3 软件接口 12](#_Toc3868)

[3.2.4 通信接口 13](#_Toc11646)

[3.3 性能需求 13](#_Toc27913)

[3.4 设计约束 13](#_Toc27845)

[3.4.1 其他标准的约束 13](#_Toc18217)

[3.4.2 硬件的限制 13](#_Toc11556)

[3.5 属性 14](#_Toc21994)

[3.5.1 可用性 14](#_Toc23784)

[3.5.2 安全性 14](#_Toc20401)

[3.5.3 可维护性 14](#_Toc31997)

[3.5.4 并发性 14](#_Toc19790)

[3.5.5 可靠性 14](#_Toc22569)

[3.5.6 警告 15](#_Toc30435)

[3.6 其他需求 15](#_Toc1225)

[3.6.1 数据库 15](#_Toc25865)

[3.6.2 操作 16](#_Toc3551)

[3.6.3 场合适应性需求 16](#_Toc16457)

[4 附录 17](#_Toc17719)

1. 引言

编写目的

本文档旨在详细阐述隐私数据脱敏管理平台项目的需求，为项目经理、软件编写人员、软件测试人员等项目参与者提供一个明确的项目范围和程序设计的参考。该文档将作为项目开发过程中需求分析、设计、实现和测试的基础，预期的读者包括所有参与软件编写与测试的程序员、项目经理以及软件的用户。

范围

隐私数据脱敏管理平台是一款旨在保护个人隐私信息安全的软件系统。该系统通过脱敏技术处理敏感数据，确保在数据分析和应用过程中不会泄露个人隐私。平台提供用户友好的操作界面，支持多种脱敏方法，满足不同企业和用户的隐私保护需求。

隐私数据脱敏管理平台的功能如下：

1.用户管理：实现基于角色的访问控制，确保不同权限的用户只能访问对应的数据。

2.数据库管理：支持数据库文件的上传、下载、展示，以及数据的加密存储。

3.数据脱敏操作：自动识别隐私数据，采用多种脱敏方法对数据进行处理。

4.UI界面设计：提供直观、简洁的界面，便于用户操作和查看脱敏结果。

5.任务列表管理：跟踪任务执行进度，管理文件数据的上传、脱敏和展示。

6.记录操作日志：详细记录用户操作，便于审计和问题追踪。

L隐私数据脱敏管理平台可应用于多种场景，包括但不限于：

1）数据合规处理：用于企业在处理敏感数据时确保合规性，对数据进行脱敏处理，避免泄露个人隐私。

2）跨部门数据共享：作为企业数据共享平台的一部分，支持不同部门之间的安全数据交换，保障数据在流转过程中的安全性。

3）研究和开发：在研发过程中，允许使用脱敏后的数据集进行实验和模型训练，保护研究对象的信息不被泄露。

定义

涉众：与本项目有关的个体或组织，包括相关企业、维护人员和普通用户。

隐私数据：指个人身份信息、财务信息等敏感数据，需要通过脱敏手段保护。

脱敏：将隐私数据转换成不可识别或不敏感的形式，以保护个人隐私。

opengauss数据库：一种开源的关系数据库管理系统，用于存储和管理数据。

UI：用户界面，指系统的图形显示部分，用于用户与系统交互。

1. 项目概述

产品描述

隐私数据脱敏管理平台是一款综合性的数据安全解决方案，旨在帮助企业有效管理和保护敏感信息，防止数据泄露事件的发生。该平台融合了先进的数据识别、脱敏技术和用户权限管理机制。

产品功能

1）用户管理模块：本平台采用多层级权限管理机制，确保不同角色的用户能够根据其职责和需求访问相应的功能和数据。通过精细化的权限分配，我们保障了隐私数据的安全性，防止未授权访问，同时简化了权限管理流程，提高了管理效率。

2）数据库管理功能：平台提供了一站式的数据库文件处理服务，支持用户轻松上传、下载和在线展示数据库文件。特别针对隐私数据，我们实施了高级加密存储技术，确保数据在静态和传输过程中的安全，有效降低了数据泄露风险。

3）数据脱敏操作流程：系统自动检测数据中的隐私信息，对识别出的敏感数据进行专业的脱敏处理。我们不仅保留原始数据的完整性，还通过加密技术进行安全存储。用户可根据需要，对脱敏后的数据进行解密和导出，脱敏后的结果应不再包含敏感信息，即避免了隐私信息的暴露，但同时又能够保持其特征，确保数据处理过程的灵活性和安全性。

4）UI界面设计理念：我们致力于打造一个简洁明了、易于操作的界面，让用户能够直观地了解脱敏结构和流程。网页端的设计简洁而不失现代感，清晰展示任务执行结果，提升了用户体验。

5）任务列表管理功能：平台提供全面的任务管理功能，包括任务创建、执行、监控和进度展示。用户可以轻松管理文件数据的上传、脱敏和展示进度，通过进度条和任务列表实时掌握任务状态，提高工作效率。

6）操作日志记录系统：为了确保数据处理的透明度和可追溯性，平台详细记录了每个用户的操作信息。这些日志为维护人员提供了宝贵的审计资料，便于他们监控系统运行状态、排查问题并及时采取维护措施。

用户特点

最终用户的特点：

1）相关企业：关注数据安全和隐私保护，需调用脱敏后数据进行业务分析。

2）维护人员：负责系统运维，具备一定的技术背景，能处理突发问题。

3）普通用户：需注册、登录、上传数据、查看数据，对系统操作有一定了解。

一般约束

1）数据脱敏平台需要提供即时的信息收集情况反馈，这就要求系统在处理数据时具有很高的响应速度。

2）用户可能在不同的网络环境中使用即时通讯软件，软件必须能够适应不同的网络条件，确保在各种网络环境下都能正常运行。

3）要求多进程接收数据或者多线程接收文件。

4）编程语言：Java

5）操作系统：Windows 10及以上

6）数据库：opengauss数据库

7）用户的通讯内容和个人信息需要得到保护，因此平台必须实施加密，身份验证，权限控制等安全措施，以防止数据泄露和未经授权访问。

假设和依据

假设：

1）网络连接：假设用户处于具有稳定互联网连接的环境中，以保证数据上传、下载和脱敏操作的实时性和可靠性。

2）硬件资源：假设用户使用的设备具有足够的处理能力、内存和存储空间，以支持隐私数据脱敏管理平台的正常运行。

3）系统安全性：假设系统将在相对安全的环境中运行，所有敏感数据和用户操作都将受到严格的保护，防止未授权访问和数据泄露。

4）用户行为：假设用户会按照平台的预期方式操作，包括注册、登录、上传数据、执行脱敏任务等，并遵循平台的使用规范。

依据：

1. 用户需求：基于目标用户群体的具体需求，以及他们对隐私保护的关注点，作为平台功能设计的依据。
2. 技术可行性：依据当前硬件和软件技术的发展水平，以及opengauss数据库的技术特性，确保平台的技术实现可行性。
3. 法律法规：遵循国家关于数据保护、个人信息安全的相关法律法规，确保平台的设计和运营符合法律要求。
4. 安全标准：依据业界关于数据加密、传输和存储的安全标准和最佳实践，确保平台的安全性。

5）市场调研：基于市场调研结果，了解同类型产品的优势和不足，以及用户对数据脱敏服务的期望，作为产品定位和功能规划的依据。

1. 具体需求

功能需求

在当前的数据管理领域，隐私保护已成为公众关注的焦点。市场上的数据脱敏解决方案虽然多样，但往往存在操作复杂、效率低下的问题。针对这一现状，我们小组计划开发一款隐私数据脱敏平台，以高效、简洁、多功能为核心目标。该平台不仅能够满足用户在数据处理上的多样化需求，提升数据安全防护能力，还能确保用户隐私不被泄露，为用户提供一个安全、可靠的数据处理环境。

我们将功能分成了用户管理，数据库管理，数据脱敏操作，UI界面设计，任务列表管理，记录操作日志六个部分。

而对于每个功能将包括引言、输入、加工和输出部分，以确保对每个功能的目标、输入数据、操作和输出数据有清晰的理解。

用户管理

3.1.1.1引言

用户管理是隐私数据脱敏管理平台的核心功能之一，旨在确保只有经过授权的用户能够访问和操作敏感数据。此功能的目标是实现对不同用户角色的权限管理，保障隐私数据的安全。

3.1.1.2 输入

3.1.1.2.1 输入源

用户注册信息（用户名、密码、联系方式等）

用户角色信息（管理员、普通用户等）

用户权限配置信息

3.1.1.2.2 操作员控制细节的需求

用户需注册账户并登录后才能访问系统

管理员负责配置用户权限

用户权限变更需由管理员审核

3.1.1.3 加工

3.1.1.3.1 输入数据的有效性检查

系统需验证注册信息的完整性和合法性

系统需验证用户角色和权限配置的合法性

3.1.1.3.2 操作的顺序

用户提交注册信息

系统验证信息有效性

管理员配置用户权限

系统根据权限控制用户访问

3.1.1.3.3 响应

系统根据用户权限提供相应的功能访问

无权限用户尝试访问时，系统显示权限不足提示

3.1.1.3.4 输出数据的有效性检查

系统不直接生成输出数据，但确保用户权限配置正确

3.1.1.4 输出

3.1.1.4.1 输出目的地

用户权限配置结果直接影响用户的功能访问权限

3.1.1.4.2 有效输出的范围

用户权限配置成功或失败的消息

3.1.1.4.3 非法值的处理

若用户权限配置信息无效，系统拒绝配置并提示错误。

数据库管理

3.1.2.1 引言

数据库管理功能允许用户上传、下载和展示数据库文件，同时使用opengauss数据库对隐私数据进行加密处理，确保数据安全。

3.1.2.2 输入

3.1.2.2.1 输入源

用户上传的数据库文件（txt格式）

用户下载请求

3.1.2.2.2 操作员控制细节的需求

用户需上传txt格式的数据库文件

用户可下载已加密的数据库文件

3.1.2.3 加工

3.1.2.3.1 输入数据的有效性检查

系统验证上传文件的格式和大小

系统验证下载请求的合法性

3.1.2.3.2 操作的顺序

用户上传数据库文件

系统加密文件并存储

用户发起下载请求

系统处理下载请求

3.1.2.3.3 响应

上传成功后，系统显示文件列表更新

下载请求处理后，系统提供下载链接

3.1.2.3.4 输出数据的有效性检查

系统确保加密后的数据库文件可下载且安全

3.1.2.4 输出

3.1.2.4.1 输出目的地

加密后的数据库文件存储在服务器上

用户下载的文件

3.1.2.4.2 有效输出的范围

上传和下载操作的成功或失败消息

3.1.2.4.3 非法值的处理

若上传文件格式不正确，系统拒绝上传并提示错误

数据脱敏操作

3.1.3.1 引言

数据脱敏操作用于检查数据是否属于隐私数据，并在存储到数据库时进行加密处理，导出数据时进行解密和脱敏处理。

3.1.3.2 输入

3.1.3.2.1 输入源

存储在数据库中的隐私数据

3.1.3.2.2 操作员控制细节的需求

用户需要对隐私数据进行脱敏处理

3.1.3.3 加工

3.1.3.3.1 输入数据的有效性检查

系统验证数据是否属于隐私数据

3.1.3.3.2 操作的顺序

系统加密存储隐私数据

用户导出数据

系统解密并脱敏数据

3.1.3.3.3 响应

系统显示脱敏处理结果

3.1.3.3.4 输出数据的有效性检查

系统检查脱敏后的数据是否符合要求

3.1.3.4 输出

3.1.3.4.1 输出目的地

输出结果将直接影响隐私数据的安全性和脱敏效果

3.1.3.4.2 有效输出的范围

有效输出范围包括脱敏后的隐私数据和普通数据

3.1.3.4.3 非法值的处理

如果脱敏处理失败，系统将拒绝操作并显示错误消息

UI界面设计

3.1.4.1 引言

UI界面设计功能旨在实现简单易操作的用户界面，展示脱敏结构和任务执行结果。

3.1.4.2 输入

3.1.4.2.1 输入源

用户操作指令

3.1.4.2.2 操作员控制细节的需求

用户需要通过界面进行操作

3.1.4.3 加工

3.1.4.3.1 输入数据的有效性检查

系统验证用户操作指令的有效性

3.1.4.3.2 操作的顺序

用户发出操作指令

系统执行操作

系统展示结果

3.1.4.3.3 响应

系统显示简洁的网页端设计及任务执行结果

3.1.4.3.4 输出数据的有效性检查

系统检查界面展示的数据是否准确和完整

3.1.4.4 输出

3.1.4.4.1 输出目的地

输出结果将直接影响用户的操作体验和信息获取

3.1.4.4.2 有效输出的范围

有效输出范围包括用户界面展示的所有信息

3.1.4.4.3 非法值的处理

如果界面展示数据有误，系统应提供错误处理机制并通知用户

任务列表管理

3.1.3.5.1 引言

任务列表管理功能用于管理任务操作，显示任务进度条，任务执行列表，以及文件数据上传、脱敏、展示进度。

3.1.5.2 输入

3.1.5.2.1 输入源

用户创建的任务

系统执行的任务状态

3.1.5.2.2 操作员控制细节的需求

用户需要创建和管理任务

用户需要查看任务进度

3.1.5.3 加工

3.1.5.3.1 输入数据的有效性检查

系统验证任务创建参数的有效性

系统监控任务执行状态

3.1.5.3.2 操作的顺序

用户创建新任务

系统执行任务

系统更新任务状态和进度

3.1.5.3.3 响应

系统提供任务进度条和执行列表的实时更新

3.1.5.3.4 输出数据的有效性检查

系统检查任务进度和状态信息的准确性

3.1.5.4 输出

3.1.5.4.1 输出目的地

输出结果将直接影响用户对任务执行情况的了解和掌控

3.1.5.4.2 有效输出的范围

有效输出范围包括任务进度条、执行列表和文件处理状态

3.1.5.4.3 非法值的处理

如果任务执行出现异常，系统应记录异常信息并通知用户

记录操作日志

3.1.6.1 引言

记录操作日志功能用于记录每个用户的操作信息，以便于审计和监控。

3.1.6.2 输入

3.1.6.2.1 输入源

用户操作行为

3.1.6.2.2 操作员控制细节的需求

系统自动记录用户的所有操作

3.1.6.3 加工

3.1.6.3.1 输入数据的有效性检查

系统验证操作日志记录的完整性和准确性

3.1.6.3.2 操作的顺序

用户执行操作

系统记录操作行为

系统存储操作日志

3.1.6.3.3 响应

系统提供操作日志的查询和报告功能

3.1.6.3.4 输出数据的有效性检查

系统检查操作日志数据是否正确存储

3.1.6.4 输出

3.1.6.4.1 输出目的地

维护人员界面

3.1.6.4.2 有效输出的范围

有效输出范围包括所有用户操作日志记录

3.1.6.4.3 非法值的处理

如果操作日志记录出现错误，系统应采取相应的错误处理措施

外部接口需求

用户接口

3.2.1.1 对屏幕格式的要求：隐私数据脱敏平台的界面布局应清晰、简洁、直观，以便用户快速理解和操作系统的功能。显示屏幕需具备适当的分辨率和尺寸，确保信息的全面展示。字体大小、图标大小和样式应适宜，以便用户轻松获取信息和使用功能。支持多窗口操作，允许用户同时打开和管理多个窗口，以提高操作的灵活性和效率。

3.2.1.2 报表或菜单的页面打印格式和内容：打印内容的格式应清晰，布局合理，可根据用户需求调整页面占用大小，并包含所有必要信息。

3.2.1.3 输入输出的相对时间：系统应在用户发送数据后立即显示输出，以提供即时响应，确保操作的流畅性。减少加载和处理时间，并显示相关提示信息，让用户了解系统的当前状态和进度。

3.2.1.4 程序功能键的可用性：功能键应明确、简洁、直观，以便用户快速便捷地使用，并实现即时响应。

硬件接口

3.2.2.1网络接口：计算机需支持网络连接，并配置正确的网络参数，以实现数据传输。

3.2.2.2 IP地址设置接口：计算机需支持网络连接，并配置正确的网络参数，以确定数据发送的目标。

3.2.2.3文件传输接口：计算机需具备文件传输功能，并有足够的存储空间来存储传输的文件。

3.2.2.4界面接口：计算机需具备足够的处理能力和显示能力，以支持程序界面的展示和交互。

3.2.2.5硬件兼容性：若计算机系统连接其他硬件，需保证硬件设备的兼容性和正常运行。

软件接口

3.2.3.1 网络通信接口：

名称：Socket API

来源：Windows操作系统自带网络编程接口 用途：实现与其他计算机的数据通信，通过Socket API提供的函数进行网络连接、数据发送和接收。

3.2.3.2 用户界面接口：

名称：合适的前端框架（React或Vue.js）

来源：前端开发社区 用途：创建程序界面及相关功能按钮，通过前端框架提供的函数进行界面的创建、事件处理等操作。

3.2.3.3 文件传输接口：

名称：FTP协议 规格说明号：RFC 959

来源：Internet标准文档 用途：使用FTP协议进行文件的传输，通过实现FTP协议规定的命令和响应来实现文件的发送和接收。

通信接口

3.2.4.1TCP/IP协议

3.2.4.2Socket编程接口

3.2.4.3FTP协议

3.2.4.4JSON数据格式协议

性能需求

静态数值需求：

1) 支持500台终端

2) 支持50名用户并行操作

3) 可处理10万条文卷和记录数

4) 表和文卷的大小不超过10MB

动态数值需求：

1）正常情况下95％的事务必须在小于0.5s时间内处理完

2）峰值工作条件下95％的事务必须在小于1s时间内处理完

3）中断响应时间小于0.5s

4）任务切换时间小于0.1s

设计约束

设计约束受其他标准、硬件限制等方面的影响。

其他标准的约束

1. 编程语言的约束：必须使用Java。
2. 操作系统的约束：必须是Windows 10及以上版本。
3. 数据库的约束：必须使用opengauss数据库。

d. 网页开发的约束：必须使用合适的前端框架。

硬件的限制

1. 硬件配置的特点

必须要有一个网络接口卡（NIC），用于联网

根据需要，可添加数据库、文件服务器等设备接口

1. 内存储器容量：2GB以上
2. 辅助存储器的容量：128GB以上

属性

可用性

1. 用户界面设计应简单直观，易于新用户上手
2. 系统响应时间短，提供实时反馈，减少用户等待时间
3. 系统应提供帮助文档和操作指南，方便用户学习和使用

安全性

1. 利用可靠的加密技术保护数据传输和存储过程中的隐私数据
2. 掌握操作日志和审计跟踪，确保对数据访问和修改的记录
3. 为不同的用户角色和模块分配不同的权限，实现最小权限原则
4. 限制系统内部特定区域的通信，防止未授权的数据访问

可维护性

a． 软件采用低耦合高内聚的设计原则，模块间依赖关系清晰，便于维护

b． 软件结构应具有良好的可读性和可理解性，便于后续升级和扩展

c． 系统应提供有效的错误处理和日志记录，便于问题的诊断和修复

并发性

a.  系统应支持多用户同时操作，保持数据一致性和事务完整性。

b.  系统设计应考虑高并发场景，确保在高负载下的性能和稳定性

可靠性

a.  系统应具备高效的任务处理能力，确保服务的连续性和稳定性

b.  系统应能够快速恢复，即使在发生故障时也能迅速重新启动

警告

用规定的方法进行软件的使用和验证时需满足指定的属性

其他需求

在本节中，将描述隐私数据脱敏管理平台开发中的数据库、操作和场合适应性需求。

数据库

3.6.1.1信息类别

隐私数据脱敏管理平台的数据库需要存储以下信息类别：

用户账户信息，包括用户名、密码、权限等级。

数据库文件信息，包括文件名、上传时间、文件大小。

隐私数据信息，包括数据类型、加密状态、脱敏状态。

操作日志信息，包括用户操作、操作时间、操作结果。

3.6.1.2 使用频率

用户账户信息的读取和更新频率较低，通常在用户注册、登录和权限更改时进行。

数据库文件信息的读取和更新频率较高，因为用户频繁上传和下载文件。

隐私数据信息的读取和更新频率较高，以支持数据脱敏操作的实时性。

操作日志信息的读取频率较高，用于监控和审计。

3.6.1.3 存取能力

数据库应支持多用户同时访问，以满足企业内部多人协作的需求。

应实现适当的并发控制机制，以确保数据的一致性和完整性。

3.6.1.4 数据元素和文卷描述符

数据库中的数据元素应包括字段名称、数据类型和约束（如唯一性约束、外键约束等）。

文卷描述符应包括文件名称、大小、上传时间等信息。

3.6.1.5 数据元素、记录和文卷的关系

用户账户信息与数据库文件信息之间存在一对多的关系，一个用户可以上传多个文件。

隐私数据信息与数据库文件信息之间存在多对一的关系，一个文件可能包含多个隐私数据。

操作日志信息与用户账户信息之间存在一对多的关系，一个用户的操作会产生多条日志。

3.6.1.6 静态和动态的组织

数据库应静态地组织用户账户信息和数据库文件信息。

隐私数据信息和操作日志信息应动态地组织，以支持数据脱敏和监控需求。

3.6.1.7 数据保存要求

隐私数据信息应根据用户需求进行保存，允许用户查看脱敏后的数据。

数据库备份和恢复机制应定期执行，以确保数据的安全性和可用性。

操作

3.6.2.1用户组织内的各种操作

隐私数据脱敏管理平台应支持以下操作：

用户账户管理操作，包括注册、登录、注销、权限更改等。

数据库文件管理操作，包括上传、下载、展示等。

数据脱敏操作，包括检查隐私数据、加密存储、解密导出、脱敏处理等。

UI界面操作，包括展示脱敏结构、任务执行结果等。

任务列表管理操作，包括管理任务进度、执行列表等。

记录操作日志操作，包括记录用户操作信息等。

3.6.2.2 交互作用操作的周期和无人操作的周期

用户账户管理操作的周期较低，通常由用户触发。

数据库文件管理操作的周期较高，可以频繁执行。

数据脱敏操作的周期由用户需求决定。

UI界面操作和任务列表管理操作的周期较高，用于实时展示和监控。

记录操作日志操作的周期较高，用于实时记录。

3.6.2.3 数据处理运行功能

数据处理运行功能应包括：

身份验证功能，用于验证用户登录。

数据加密功能，用于保护隐私数据。

数据脱敏功能，用于实现脱敏处理。

日志记录功能，用于记录用户操作。

3.6.2.4 后援和恢复操作

平台应具备数据备份和恢复机制，以应对系统故障或数据丢失情况。

用户账户管理操作中应包括密码重置的后援和恢复操作，以确保用户账户的安全性。

场合适应性需求

3.6.3.1 对给定场合或相关任务或操作方式的需求

隐私数据脱敏管理平台应具备对不同场合的适应性，包括以下方面：

安全性需求：平台应支持不同安全级别的配置，以适应不同场合的安全要求。

配置需求：系统应允许管理员根据不同场合的需求配置脱敏规则和用户权限等。

3.6.3.2 指出场合或相关任务的特点

隐私数据脱敏管理平台应根据以下场合或相关任务的特点，提供可配置的选项：

数据敏感：平台应能够根据企业选择的脱敏方法做出正确响应。

灾难恢复：平台应具备灾难恢复能力，以适应紧急情况下的数据恢复需求。

1. 附录

暂无