福建水务营收系统-敏感数据加密方案

系统设计团队

2024年12月19日

1 用户敏感数据加密存储技术方案

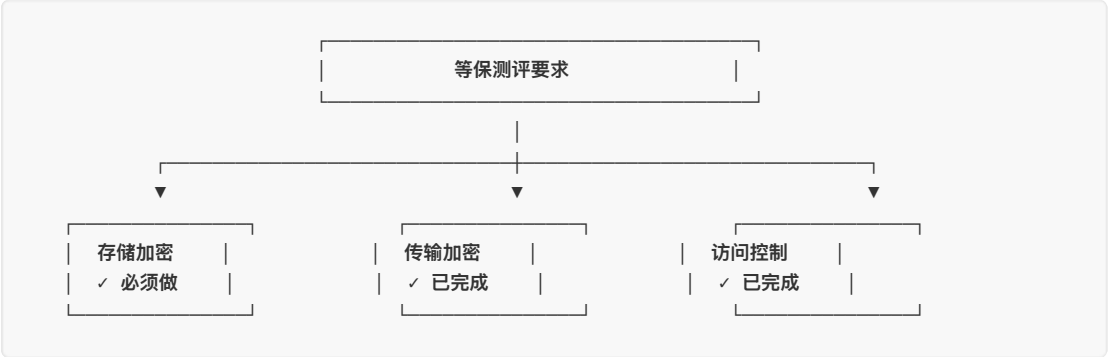
1.1 文档信息

项目信息	详情
项目名称	福建水务营收系统
文档类型	技术方案汇报
适用范围	用户个人信息加密存储与搜索
编写日期	2025年12月
文档版本	V1.0

1.2 一、方案背景

1.2.1 为什么要做加密?

根据等保测评要求，用户的敏感个人信息（身份证、手机号、银行卡等）必须加密存储，否则无法通过安全检查。



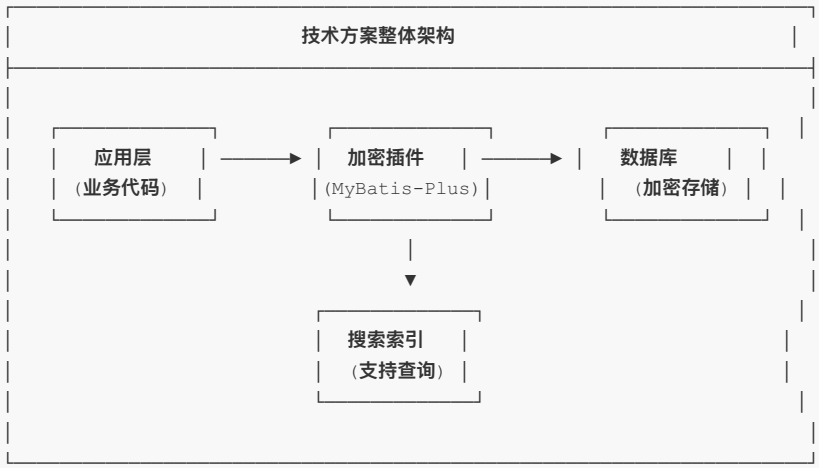
1.2.2 涉及哪些数据?

敏感数据类型	示例	加密要求
身份证号	350xxx19900101xxxx	必须加密
手机号	138xxxx8888	必须加密
银行卡号	6222xxxxxxxx1234	必须加密
邮箱地址	xxx@xxx.com	必须加密
真实姓名	张xx	必须加密

1.3 二、技术方案概述

1.3.1 核心思路

“先加密存储，再建立索引” —— 既保证安全，又保证能搜索



1.3.2 采用的技术

技术组件	说明	选择理由
MyBatis-Plus 加密插件	自动对数据进行加密和解密	框架自带功能，改造成本低
SM4 加密算法	国产加密算法，符合等保要求	安全等级高，符合等保要求
搜索索引技术	支持加密后的数据查询	保证业务搜索功能正常使用

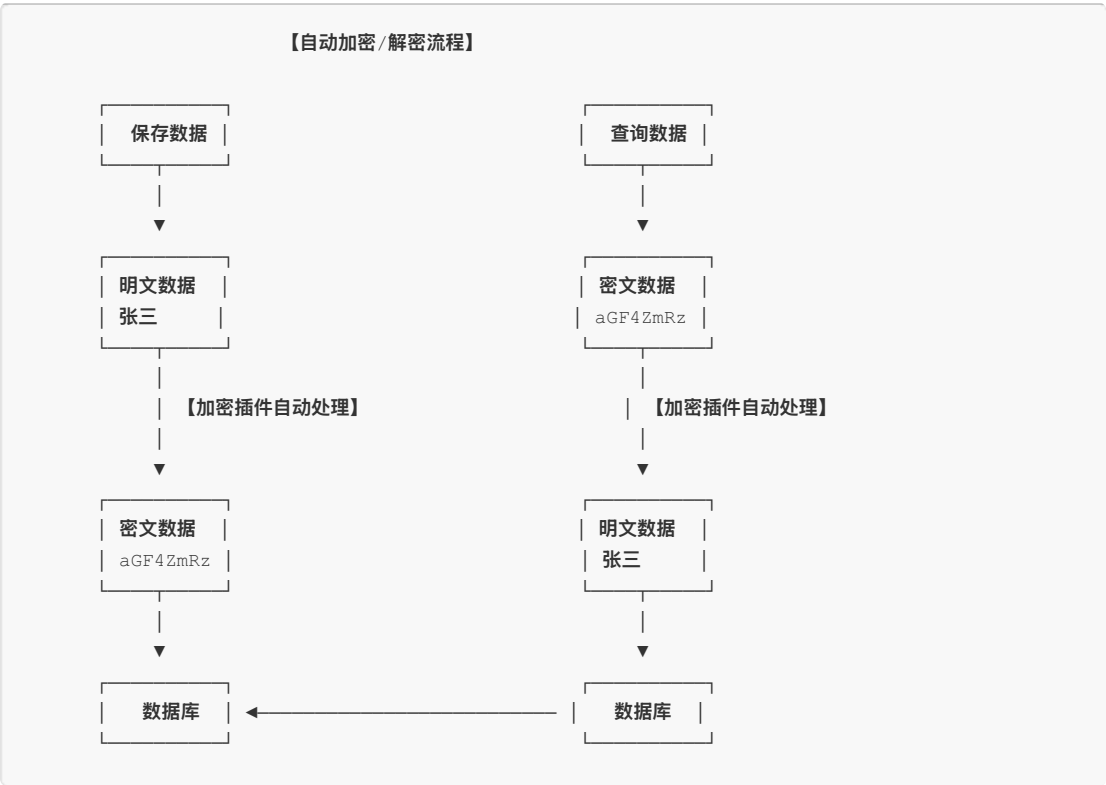
1.4 三、加密存储方案

1.4.1 加密前后对比

加密前（明文存储，不安全）： | id | real_name | id_card | phone | |—-|———|———|———-| | 1 | **张三** | 350102199001011234 | 13812345678 |

加密后（密文存储，安全）： | id | real_name | id_card | phone | |—-|———|———|———-| | 1 | aGF4ZmRz… | YmVydGlu… | c2VjdXJl… |

1.4.2 MyBatis-Plus 加密插件原理



优势说明： - **对业务代码透明** —— 开发人员无需修改业务逻辑 - **自动加密解密** —— 框架自动处理，不易出错 - **改造成本低** —— 只需添加配置和注解

1.5 四、搜索功能方案

1.5.1 为什么加密后还能搜索?

加密后的数据是乱码，无法直接用SQL的 `LIKE` 查询。我们的解决方案是：建立搜索索引。

1.5.2 支持的查询类型

查询类型	适用场景	实现方式
精确查询	身份证查用户	哈希索引（完全匹配）
前缀查询	手机号前几位	前缀索引（部分匹配）
模糊查询	姓名搜索	拼音索引（支持模糊）

1.5.3 查询流程示例

场景：根据身份证号查询用户

1.6 五、数据库表设计

1.6.1 表结构说明

1.6.2 字段对照表

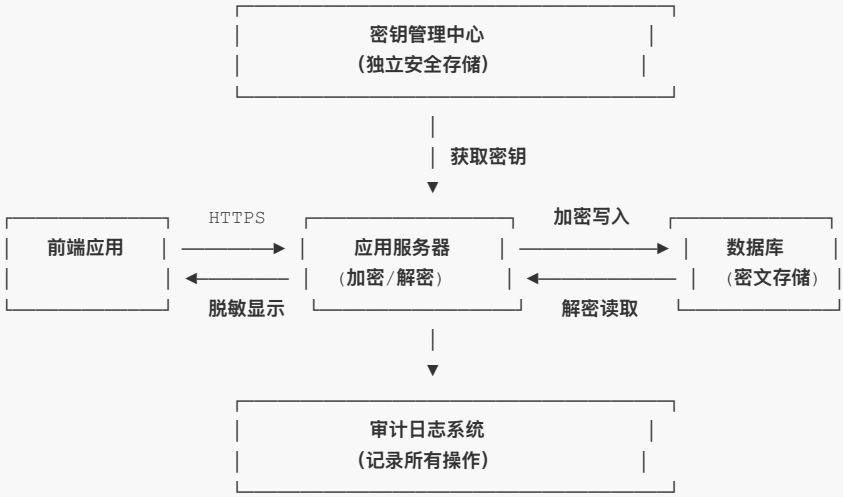
敏感字段	存储方式	对应索引字段	索引用途
id_card	SM4加密	id_card_hash	精确匹配
phone	SM4加密	phone_prefix	前缀查询
real_name	SM4加密	name_pinyin	模糊搜索
bank_card	SM4加密	bank_card_prefix	前缀查询
email	SM4加密	—	不支持搜索

1.7 六、等保符合性说明

1.7.1 安全控制措施对照

等保要求	我们的方案	符合性
个人信息加密存储	SM4算法加密	完全符合
数据传输安全	HTTPS + 加密字段	完全符合
访问权限控制	数据库权限 + 应用权限	完全符合
安全审计	操作日志 + 加解密审计	完全符合
密钥安全管理	配置加密 + 独立存储	完全符合

1.7.2 安全架构

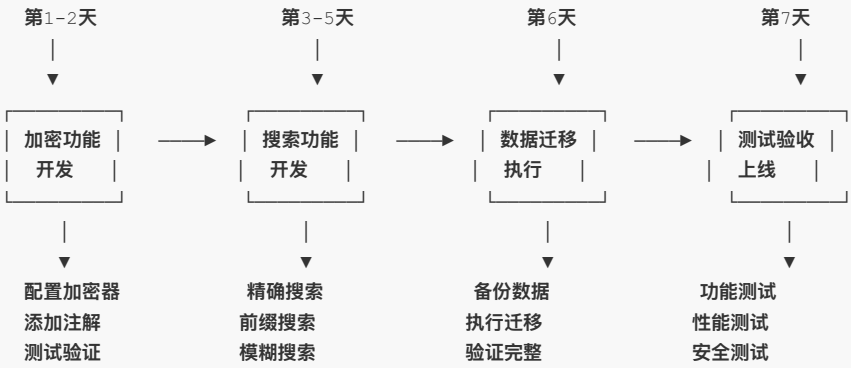


1.8 七、实施计划

1.8.1 实施时间表

阶段	工作内容	时间	负责人
第一阶段	基础加密功能开发	1-2天	开发团队
第二阶段	搜索索引功能开发	2-3天	开发团队
第三阶段	历史数据迁移加密	1天	运维 + 开发
第四阶段	测试与验收	1天	测试团队
合计	—	**5-7个工作日**	—

1.8.2 实施步骤

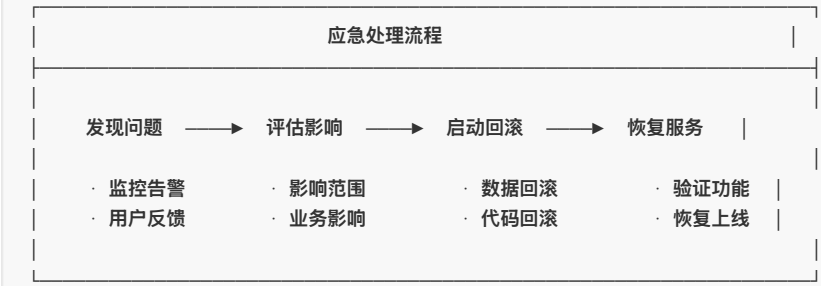


1.9 八、风险控制

1.9.1 风险识别与应对

风险类型	风险描述	应对措施
密钥泄露风险	加密密钥被窃取	密钥独立存储，定期轮换
数据迁移风险	迁移过程数据丢失	先备份后迁移，分批执行
性能影响风险	加解密影响系统性能	添加索引，使用缓存优化
功能影响风险	现有功能受影响	充分测试，灰度发布

1.9.2 应急预案



1.10 九、方案优势总结

1.10.1 核心优势

优势	说明
安全性高	采用SM4国产加密算法，符合等保要求
搜索能力强	加密后仍支持精确、前缀、模糊多种搜索
改造成本低	使用MyBatis-Plus插件，对业务代码侵入小
实施周期短	5-7个工作日可完成全部改造
运维友好	自动加解密，无需人工干预

1.10.2 投入产出分析

```
┌──────────────────────────────────────────────────────────────┐
│                        投入产出分析                          │
├──────────────────────────────────────────────────────────────┤
│                                                              │
│   【投入】                          【产出】                 │
│   ────                              ────                     │
│   · 开发工时：5-7个工作日           · 通过等保测评检查       │
│   · 测试工时：1-2个工作日           · 符合数据安全法规要求   │
│   · 运维工时：1个工作日             · 降低数据泄露风险       │
│                                     · 提升用户数据安全保障   │
│                                                              │
│   【总计：约7-10个工作日】          【价值：等保合规 + 安全保障】 │
│                                                              │
└──────────────────────────────────────────────────────────────┘
```

1.11 十、结论与建议

1.11.1 方案结论

本方案采用MyBatis-Plus加密插件 + 搜索索引的技术路线，能够：

1. **满足等保要求** —— 敏感数据全部加密存储
2. **保持业务功能** —— 加密后仍可正常搜索查询
3. **低成本实施** —— 对现有系统改动小，周期短
4. **安全可控** —— 密钥独立管理，审计可追溯

1.11.2 建议

建议事项	说明
1. 尽快启动	等保测评时间紧迫，建议尽快安排实施
2. 分阶段实施	先完成核心功能，再优化性能
3. 充分测试	上线前做好功能和性能测试
4. 保留回滚方案	确保出现问题可快速回滚

如有疑问，请随时沟通！