# 敏感数据处理

作者：88250
原文链接：https://ld246.com/article/1462956775250
来源网站：链滴

# 背景

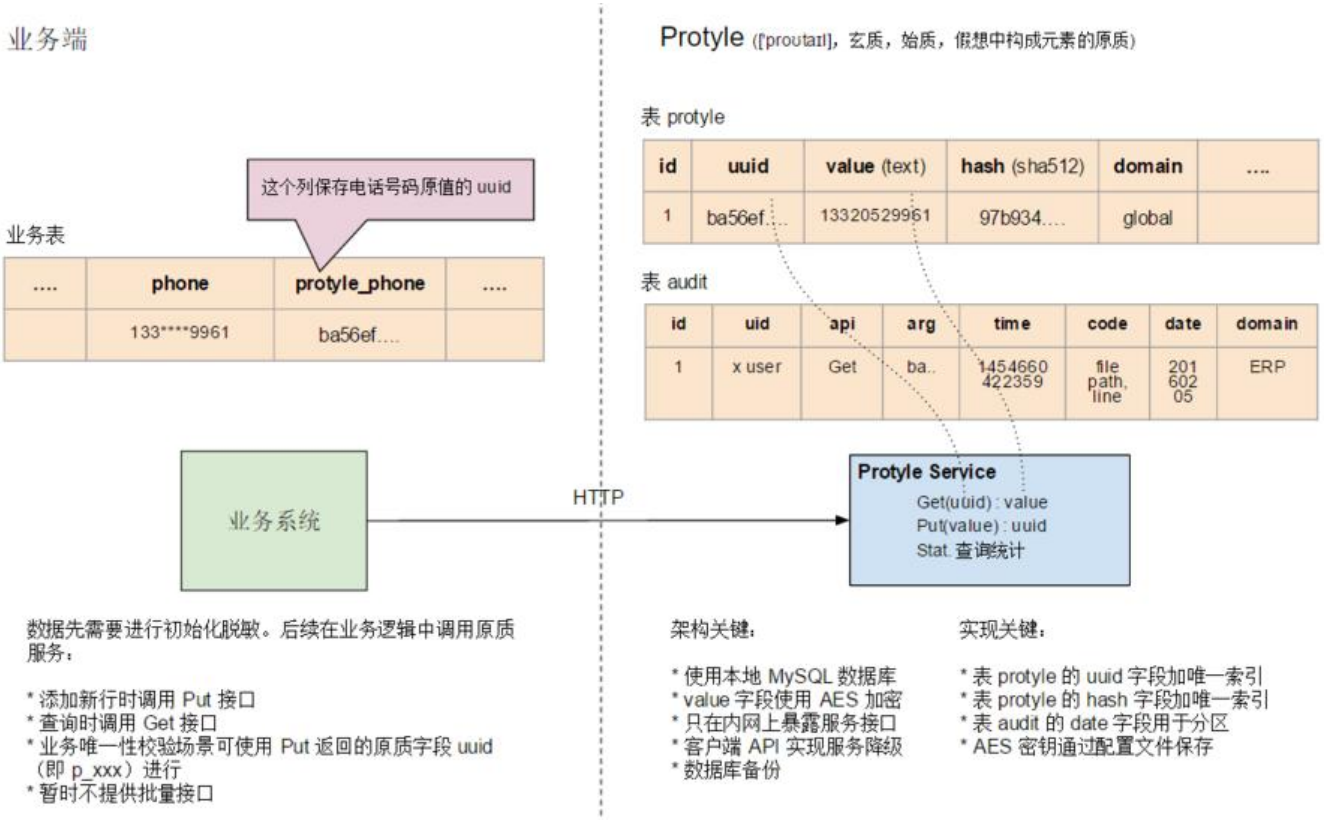
大多数应用或多或少都会涉及到敏感数据处理，比如用户的手机号、身份证号，甚至银行卡账号。作应用的开发者，如何 **安全地** 维护这些敏感数据呢？

这里讨论的安全不是指服务器如何保护，而是在数据库层面做敏感数据的分离：

- 业务库中不保存敏感数据，只保存混淆过的数据，比如电话字段保存的是 133****9961，在数据层就进行脱敏
- 敏感数据统一保存在另一个库中，有应用调用一个服务来建立原值和混淆值的映射关系
- 业务库中因为保存的是脱敏过的数据，通过只读复制镜像可以很方便地提供给其他服务使用，比如 LAP
- 除了技术开发上方便，运维上也方便了很多，降低了敏感数据被暴露到外部的可能性

# 技术设计

提供服务接口给应用存取敏感数据，本质上是一个 KV 存取服务。




一些细节：

- 表 protyle 的 domain 字段用于标识该记录的作用域，在一个作用域上相同的值要保证唯一
- 表 protyle 的 hash 字段值是 SHA-512(domain/value) 的结果，用于唯一性校验

---

大家有相关经验么？欢迎讨论~