# 服务器设计

## 需求分析

| 序号 | 数据接收方 | 实现功能 | 数据内容 | 数据类型 |
| --- | --- | --- | --- | --- |
| 1 | 服务器 | 注册 | 账户、密码、邮箱 | 字符串 |
| 2 | 客户端 | 注册 | 账户、邮箱是否重复 | 整型 |
| 3 | 服务器 | 登录 | 账户、密码 | 字符串 |
| 4 | 客户端 | 登录 | 账户、密码是否匹配 | 整型 |
| 5 | 服务器 | 建模 | 用户的声纹特征 | 2进制数据 |
| 6 | 客户端 | 建模 | 建模结果 | 整型 |
| 7 | 服务器 | 验证 | 用户的声纹特征 | 2进制数据 |
| 8 | 客户端 | 验证 | 验证结果 | 整型 |

## 安全性分析

问题1：数据包内容被篡改

解决方式：加入md5校验码。并计算校验码的RSA密文。

问题2：数据包重放攻击

攻击方式：攻击者截取用户发往服务器的验证数据包，通过重传该数据包欺骗服务器。

解决方式：在数据包内加入递增序列号，服务端检测序列号是否递增以判断是否为重放攻击。

## 数据包格式

表 3-4 网络传输服务消息详情表

| 参数名称 | 类型 | 说明 |
| --- | --- | --- |
| Intent.Action | String | com.soundInSight.action.message_send |
| Intent.Extra.sender | Int | 发送方，保留域 |
| Intent.Extra.receiver | Int | 目标接收方，保留域 |
| Intent.Extra.msgType | Int | 消息类型，便于服务器端使用正确的方法解释消息体 |
| Intent.Extra.jsonObj | String | 消息内容，使用 Json 方法串行化 |

表 3-5 用于网络间传输的数据封包列表

| 输入参数 | 加密前参数 | 签名后参数 | 加密后参数 | 类型 |
| --- | --- | --- | --- | --- |
| Intent.Action | | | | String |
| Intent.Extra.sender | sender | sender | sender | Int |
| Intent.Extra.receiver | receiver | receiver | receiver | Int |
| Intent.Extra.msgType | msgType | msgType | | Int |
| Intent.Extra.jsonObj | jsonObj | jsonObj | jsonObj | String |
| | packageIndex | packageIndex | | String |
| | | md5 | | String |
| | | | secPack | Byte[] |