任务书

为了解决现代预约挂号系统个人隐私泄露和安全漏洞问题,提出了一种具有隐私保护的在线预约挂号系统,它可以实现科室匹配和医生搜索功能。

1. 首先,患者使用可搜索加密（Searchable Encryption,SE）描述自己的症状,并将密文发送到云服务器。然后,电子健康记录（Electronic Health Record,EHR）云服务器匹配与类似症状相关的科室信息,并将科室密文发送给患者。
2. 此外,患者通过基于属性的关键词搜索加密将其需求发送到医生档案系统（Doctor's Profile System,DPS）服务器,该服务器可以在无需解密的情况下搜索与加密需求对应的适当医生,将医生的资料以密文的形式发送给搜索者。
3. 最后,搜索者可以在线预约预期的医生。

安全分析表明,该系统能够实现数据的保密性和完整性、相互认证、安全搜索、匿名性和陷门不可连接性。

数据库设计

科室表设计

1. 科室名称（主键）
2. 科室介绍
3. 科室keywords（主治）
4. 科室的医务人员

医生个人信息表设计

1. 医生姓名
2. 医生性别
3. 医生的主治病症
4. 所属科室（外键）
5. 医生职称
6. 医生介绍

索引表

1. 索引关键词（cph）
2. 文件列表

软件实现步骤

任务一

1. 患者填写信息，并用Search Encryption加密病历
2. 云服务器对通过科室的**keywords**对患者密文进行搜索，设置权重匹配最优科室，搜索过程中云端只能知道加密密文中可能包含的关键字
3. 返回加密的科室信息给病人，病人解密浏览科室信息

任务二

索引结构

```
public class Index {
    public String word;
    public String [] file;
    public Index(){

    }
    public Index(String word,String []file){
        this.word = word;
        this.file = file;
    }
}

```

1. 提前将医生个人信息表中的**医生主治，介绍**加密到随机命名的文件中，一个医生对应一份文件，得到f1，f2，……，fn
2. 用searchableEncryption对医生信息进行加密，加密后上传云服务器，云服务器不知道对应内容
3. 建立索引表：准备一些index.word，用他们在f1，f2，……，fn中搜索，建立起file的列表file[]={"f1","fx","fm"}，然后利用基于属性可搜索的加密方法加密index.word，此事索引就可上传索引表
4. 用户输入关键词，用msk，attrs等产生私钥，根据算法私钥产生令牌，用**令牌、公钥、index.word**的密文进行运算匹配，验证通过即可读取文件列表
5. 用户得到医生个人信息，进行解密，选取医生