1. 研究背景

近年来，随着网络不断发展，人们日常生活产生的数据越来越多，云存储技术随之兴起。同时为了保证数据安全和用户隐私，用户一些敏感数据通常需要先加密再以密文状态上传。这种方法在云端不完全可信的情况下可以对用户数据进行保密。但是加密存储的方法也让用户无法便捷的在云端对密文进行查询。

传统的密文存储服务中，由于云端没有相应的检索功能，不能根据用户的需求查找数据，只能将用户的所有密文数据全部返还给用户，让用户在本地进行解密操作后再进行检索操作。显然这种这种交互方式不仅占用了大量的网络开销，而且给用户带来了额外的计算开销。因此如何在用户提交检索需求时，云端借助自身强大的计算能力实现高效检索并准确的返回数据是当今云存储安全存储的重要需求。

2可搜索加密

可搜索加密SE（Searchable Encryption）是近年来发展起来的一种支持用户在密文上针对关键字进行查找的技术。它能够为用户节省大量的网络和计算开销，借助云端的强大计算能力准备的完成检索并返回结果。，而用户不会向云端暴露任何隐私。

可搜索加密的方案最早由Song等在2000年提出。可搜索加密的基本框架如图1.1，其主要过程分为四步。

1. 数据加密：数据所有者在本地对数据进行加密，然后将密文上传至云端。
2. 陷门生成：用户结合密钥和关键字生成对应的陷门，将陷门发送给云端。
3. 检索密文：云端借助用户提交的陷门和自身维持的索引表进行检索，返回包含陷门关键字的数据。
4. 文件解密：用户使用自身密钥对云端返回的数据进行解密。