**上 海 电 力 大 学**

**毕业设计（论文）任务书**

**课题名称**  云计算下加密数据查询关键技术的设计与实现

**院 （系）**  计算机科学与技术学院

**专 业**  信息安全

**班 级**  2019251班

**学生姓名** 陈思益

**学 号**  20191558

**设计地点**  上海电力大学

**指导老师签名**：

**教研室主任（系主任）签名**：

**学生签名**：

一、课题背景、目的、意义

|  |
| --- |
| 云计算是信息领域的一种新的技术变革，是在分布式计算、对等计算之后的一种新型计算模型。云计算具有强大的计算能力和海量的存储能力。它通过互联网平台将大量的资源连接在一起，为不同的用户提供云服务。而用户存储在第三方平台上的数据失去了用户对数据的控制权，而云提供云存储的第三方平台并非完全可信，因此云端数据面临着安全风险。为了解决这类问题，可搜索云加密技术应运而生。  可搜索加密技术使用户具有在密文域上进行关键词搜索的能力。数据以密文的方式存储在服务器上时，利用云服务器的检索能力进行关键词的检索。这项技术不但使得用户在云端的数据得到了有效保护，而且对于检索效率也可以在服务器的技术上得到大幅度的提升。  目前，云计算已经成为数字经济时代的算力中枢和数字底座，许多企业对云计算的态度愈加积极，特别是那些正在向云支付处理迈进的金融服务组织。一个安全的云计算平台和系统对云计算发展有着十分重要的意义。本项目的研究不仅具有重要的理论价值，而且具有巨大的实用价值。 |

1. 课题的主要内容及要求（要求详实、具体、准确）

|  |
| --- |
| 本课题的研究内容主要分为以下几个方面：   1. 查阅国内外文献，了解目前的可搜索加密技术以及加密数据查询技术 2. 通过现有的渠道，了解云平台的部署方式 3. 选择合适的加密算法，对客户端上传到云端的数据进行加密存储 4. 通过搜索关键字等方式对加密数据进行查询   本课题的主要要求   1. 实现云环境的部署 2. 对客户端上传到云端的信息进行加密，用户上传到云端的数据必须确保安全性 3. 对存储在云端的数据进行查找 |

1. 成品要求（包括课题主要目标及成果）

|  |
| --- |
| 1、建立云加密理论模型，对模型的可行性进行分析验证  2、选定加密方案并设计基于云计算下加密技术  3、实现从第三方向云端上传数据，并对数据进行正确搜索  4、尝试提高搜索算法性能，在大量云端数据中对信息进行搜索  5、尝试从系统模型、效率与安全性方面对算法性能进行探索和改进  6、交互界面功能齐全，美观 |

1. 课题计划进度

|  |  |
| --- | --- |
| **学生完成开题报告** | **1月18日** |
| **学生完成系统概要设计文档** | **2月12日** |
| **学生完成系统详细设计文档** | **2月19日** |
| **学生完成系统编码或仿真工作** | **3月12日** |
| **学生完成系统测试工作** | **3月17日** |
| **学生完成论文初稿** | **3月24日** |
| **中期检查** | **4月14日** |
| **预答辩** | **4月14日** |
| **完成论文定稿，并提交参与论文查重工作** | **4月18日** |
| **论文答辩** | **5月4日** |

1. 有关资料及参考书目

|  |
| --- |
| [1]王惠莅 杨建军 姚相振.云计算安全国家标准及云计算服务安全审查[N].信息技术标准化,2020-02-03  [2]李虹.可信云安全的关键技术与实现[M].北京:人民邮电出版社,2010  [3]丁一军.云计算:安全技术问题探讨[J].科技创新导报，2010，07(146),58-59  [4]房晶,吴昊.云计算安全研究综述[J].电信科学,2011,4(4),37-42  [5]余鹏飞.可信移动计算环境体系结构关键技术研究[D].华中科技大学,2010  [6]Vichael Perez Sanjeev Kumar.A quick survey on cloud computing and associated security[J].computer and communications.2017.12(12).80-95 |