**第十届中国大学生服务外包创新创业大赛**

****

**Ankh多方安全计算平台**

**概要介绍**

团队：1900156-我的队名不让你看

赛题：A11-多方数据安全计算平台的设计与实现

团队成员：丁峥元 赵大燕 黄怡 郭延鹏 向云帆

指导老师：杨柳 陈帆

二零一九年十二月——二零二零年五月

**目 录**

[一、 前言 1](#_Toc41415427)

[二、 创意描述 1](#_Toc41415428)

[三、 功能简介 1](#_Toc41415429)

[四、 特色综述 2](#_Toc41415430)

[五、 开发工具与技术 3](#_Toc41415431)

[六、 应用对象 3](#_Toc41415432)

[七、 应用环境 3](#_Toc41415433)

[八、 结语 4](#_Toc41415434)

# 前言

近些年来，随着网络技术不断提高，计算机在我们日常生活中普及度逐渐提高。而以云计算作为信息技术的新概念，已逐渐被广大的用户所接受，它的应用也涉及到社会经济和我们的个人生活。与我们的日常生活息息相关，在此背景下网络安全以及信息安全显得尤为重要。

传统用户隐私保护方案的实施过程为：先解密密文，再对解密后的数据进行相应数学运算，最后将结果加密，存在时空开销较大的不足，不能满足如今企业间数据高效、安全共享的需求。故我们在研究了同态加密和多方安全不同实现方法后，设计提出了一种支持多种风控模型的政企合作数据安全计算平台，使得在保护政府数据情况下对其进行有效利用。

# 创意描述

Ankh多方计算平台加密部分结合多种加密算法优势所在，使之能够适应多种形式的风控模型同态加密计算功能。此外针对密文比较，在保证安全性的其前提下，需要让中间结果解密并进行数据处理，再借助百万富翁问题模型进行两方比较计算。故我们将在政府数据平台添加一个辅助计算端（对于政府其为受信方）对比较计算的中间过程进行安全处理。

# 功能简介

1. 政府数据平台

构建数据库，存放用户数据信息。在收到数据请求后，验证请求方信息，若得到授权则按一定加密算法对相关数据进行加密，并将加密公钥公开。同时，政府端授权一受信方对部分中间结果进行加/解密及其他数据交互处理。此外，最终的数据结果，也经由该方交付。

1. Ankh多方安全计算平台

分为核心计算模块以及服务器模块。计算部分接入风控模型进行对密文的运算操作以及比较操作，得到计算申请结果。服务器模块完成平台其余各项数据交互以及对前端页面的支持。

1. 平台数据仓库

存放平台交互以及计算所需数据，用于支持平台注册、登录、身份认证以及贷款申请等功能。

1. 管理员平台

对平台数据使用情况进行实时监控，对各使用量进行可视化显示，以及查看模型历史数据，并可完成风控模型部署。

1. 用户平台

可实现用户注册登录。作为贷款申请用户可以提交贷款申请，查看贷款结果，提交反馈等操作。作为提供贷款的企业或银行可以管理产品，提交计算请求，提交申请审核结果以及提交反馈等操作。

架构示意图如图3-1所示

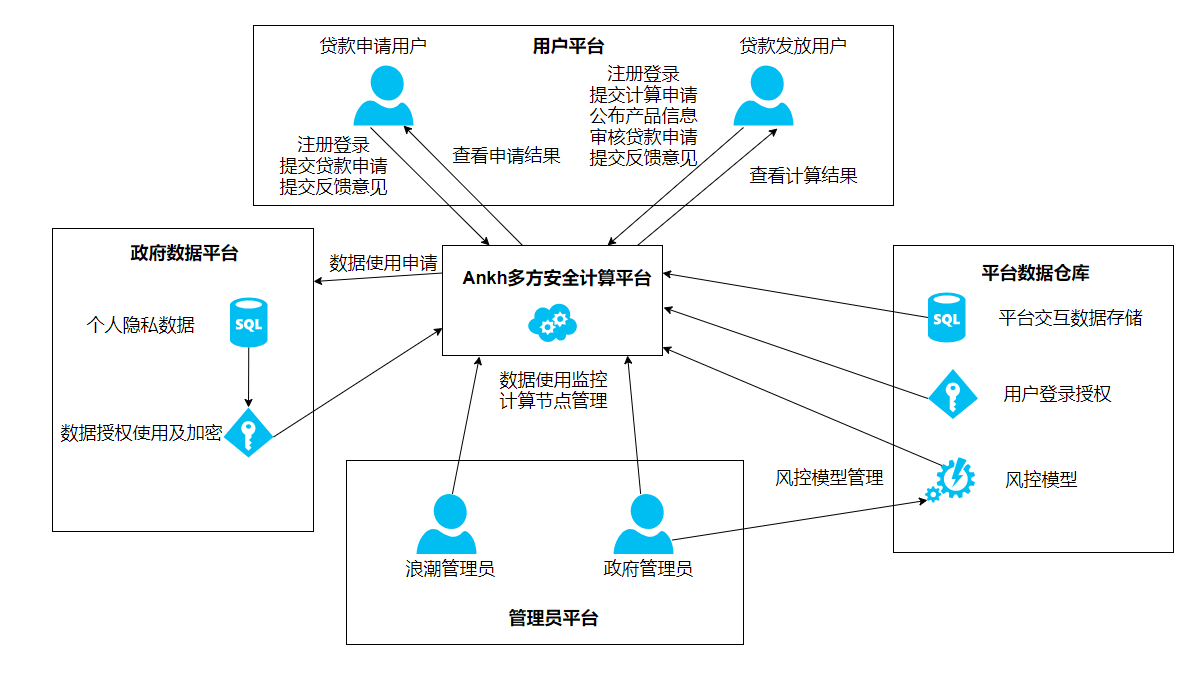


图3-1 Ankh多方安全计算平台功能架构

# 特色综述

* 1. 数据安全利用

使用基于RLWE和离散对数难题的加密方案，从而保证了加密数据的安全性，此外政府管理人员可以对数据加密情况进行监控，若出现加密密钥使用频率较高（多次使用统同一密钥将降低安全性）的情况则可申请重新加密。

* 1. 较强适应性的加密系统

采用多种同态加密算法，可以适应加法操作、乘法操作，多项式计算以及比较运算等多种计算功能的加密运算。企业方管理员可对风控模型进行修改，从而在计算过程调用对应封装完成的密文计算函数。

* 1. 公式的自动解析

对于新的风控模型公式，如果公式中没有复杂的数学函数，系统可自动识别并解析公式，进而构建加密流程。

* 1. 人性化的操作界面

平台主要以网页方式操作。网页的操作流程力求简洁直观，提升用户办事效率。不同角色的后台网页风格一致，但功能不一，突出体现了不同角色用户的需求。

* 1. 安全可靠的服务器

在SpringBoot框架中加入SpringSecurity组件，完善了用户认证过程并对各角色的访问权限进行了精细控制。此外SpringSecurity可支持对CSRF（跨站请求伪造）的防御，进一步提升了用户的账户及数据安全。

* 1. 良好的使用体验

Ankh平台与政府和各大金融机构合作，提供在线办理、快速审批的一站式贷款服务。贷款申请者无需经历复杂的申请流程，足不出户即可完成信息填写和材料提交流程。同时，平台提供的计算服务也减轻了放贷机构对申请者授信工作的负担。

# 开发工具与技术

1. 技术特色
2. 前端技术：Html5、Bootstrap
3. Web后台：MySQL、SSM框架、SpringBoot框架、SpringSecurity组件
4. 版本控制：git
5. 开发工具
6. 集成开发环境：IDEA、Visiual Studio 2019
7. 服务器：Tomcat
8. 数据库管理工具：MySQL
9. 浏览器：Chrome

# 应用对象

* 1. 放贷机构

面向各大金融机构以及小额贷款公司，平台将对机构资质进行审查，以保障用户使用安全。

* 1. 贷款用户

包括个人和企业，对于不同类型的贷款用户，平台将提供不同的产品筛选，以适应用户需求。

# 应用环境

1. 政府数据平台、计算平台、平台数据仓库环境：

a. 硬件环境：笔记本电脑, Core i5-8300H，16GB内存

b. 操作系统：Windows 10

1. 用户环境：

a. 操作系统：Windows

b. 浏览器：IE、Firefox、Chrome等主流浏览器

# 结语

希望Ankh多方安全计算平台可以提供贷款一站式服务，为企业、政府等组织给予安全、高效的计算支持，提高数据的利用率，促进企业间、政企间交流合作，提升企业的知名度，进而推动企业发展。同时也希望我们的产品能够激发技术人员对该方向研究热情，促进云计算、大数据行业的进一步的进步创新。