申报课题目录

申报课题

1、人工智能

1.1 图学习在时空情景化场景建模的探索

背景

随着支付宝从原来的金融支付平台升级为数字生活开放平台，越来越多数字生活服务接入到支付宝中。海量的用户和众多数字生活服务间的交互，构成了一个庞大的图。考虑到数字生活服务的本地化特性，这些图数据中除了附带有丰富的特征信息和复杂的拓扑关系外，每次交互还带有明显的时空情景化特性。这里的图不是一个静态的图，而是一个带有时间和空间信息的动态的图。把图机器学习技术应用到这样的场景进行建模，除了要回“what”的问题（为用户匹配哪种服务）外，还要回答“when”和“where”的问题（何时何地匹配哪种服务）。

目标

1. **时空图数据的表达、生成和推理。**如何对包含时间和空间信息的情景化图结构数据进行表达，如何给出下一个事件的发生时间和位置，或者在给定时间和位置上预测下一个事件发生的概率。
2. **时空图模型在数字生活场景的应用。**有了对时空图数据的表达能力后，如何结合数字生活场景内容跨多领域的特点，研发更高效的推荐搜索营销模型。
3. **基于图学习建模特征高阶交互。**对特征间的高阶交互进行建模，是个性化模型迭代升级的核心点之一。“图”可以很自然地描述高阶交互关系。因此，基于图学习来建模个性化模型中的特征交互关系，捕获高阶交互信息，是个性化模型继续升级的一个研究方向。

相关研究课题

1. 时空图机器学习；
2. 时序分析；
3. 推荐系统。

返回首页

1.2 基于图学习的跨模态推理及应用

背景

随着互联网的发展，网络中数据量越来越庞大，这些数据不仅来源于多个模态，它们之间还包含复杂的交互关系，蕴含丰富的信息。同时，随着蚂蚁业务的不断拓宽，场景与场景之间、数据与数据之间、数据和场景之间都存在着复杂的逻辑关系，在该背景下我们很多复杂的应用场景比如金融信贷风控、数字生活服务推荐等都需要挖掘数据中高层变量之间的关系来进行逻辑推理，更好地判断用户的意图，实现更为精确可控的风控和推荐。而图数据可以很自然地被用于建模各个模态数据之间的复杂关系，具备着捕捉数据之间可解释性、因果性、传递性的表达能力，可为现有学习任务增加逻辑推理或关系推理的能力。

目标

1. **跨模态推理能力**：蚂蚁现有的金融服务场景节点复杂多样，包含用户行为、文本、视觉、时空等不同感知模态，同时他们之间的关系复杂多样，如何融合跨模态的数据支持可推理的复杂系统是面临的第一个挑战。
2. **基于高阶关系和复杂结构的推理能力**：金融场景的复杂性和稳定性使得对模型的要求更多的从原来的“what”、“when”型的陈述事实性数据挖掘往“why”型的智能认知理解的方向发展，这就要求我们对模型如何挖掘更高阶的关联关系、更复杂的拓扑结构，提供具有可解释结果带来了要求和挑战。

3. **大规模图数据下的知识精炼**：图数据能够将不同模态的数据关联起来形成庞大的数据底盘，在此底盘下，如何精炼出对任务有关的知识是进行跨模态推理的又一挑战。

相关研究课题

1. 人工智能；
2. 图机器学习；
3. 跨模态推理。

返回首页

1.3 跨领域图学习及其应用

背景

随着阿里巴巴经济体服务日趋多样，这些服务背后沉淀出日渐丰富的图数据。这些基础图数据分属不同领域（domain）：交易、转账，社交和互动关系等。在该背景下，为了整合多个领域的知识学习有效的表示，来赋能蚂蚁的金融信贷风控、数字生活服务推荐等场景，我们面临着如下的挑战:

1. 如何利用多种领域的图数据，学习用户、内容服务的通用解耦图表征赋能下游业务。
2. 如何对跨领域图数据进行知识迁移来赋能特定的图学习任务，尤其是解决冷启动业务的建模问题。

目标

1. 针对跨领域图数据，通过无监督、自监督等方式，自适应学习多个领域的相关性，融合得到解耦图表达，可以有效地表达用户和内容服务，提升下游多个相关场景的学习性能。
2. 针对跨领域图数据，提取多个领域共性图表达，该表达可以有效帮助目标领域任务的

学习。

3. 针对历史积累的跨领域图数据，理解领域关系及演进，帮助目标领域在未来的冷启动业务上迅速拿到效果。

相关研究课题

1. 图机器学习；
2. 迁移学习；
3. 跨领域的图神经网络。

返回首页

1.4 复杂子图结构的深度表示学习

背景

随着互联网金融行业的迅速发展，各类互联网金融服务应用积累了大量的用户-用户、用户-商家的关系数据，蕴含着巨大的商业和研究价值。同时，图机器学习作为当前学术届和工业界的研究热点，被广泛应用于建模各类场景中的关系数据，在金融场景也有非常广阔的应用空间。过去几年里，图机器学习有很多研究围绕着如何表达节点而展开。然而，图数据中除了节点这一基本元素外，还有更复杂的图结构，如边、路径、子图等等，如何更好的对这些图结构进行表达学习，是图机器学习领域一个前沿的研究课题。

目标

1. 有效的边表达学习。综合考虑边特征、相关联的两个节点的特征，以及边所属的局部子图，甚至在全图上的作用等因素进行边的表达学习。可应用在链路预测，关系分类等等任务中。
2. 有效的子图表达学习。给定一个子图，结合子图中的所有节点和边，以及节点和边上

的特征，为子图产出嵌入表达，提高子图分类等下游任务的准确率。

3. 有效的图聚类学习。结合机器学习技术，在一个给定的图数据上进行节点聚类，挖掘出具有明显团伙性质的聚簇。

相关研究课题

1. 图表达学习；

2. 图聚类。

返回首页

1.5 金融序列数据建模

背景

随着机器学习技术的发展，越来越多的场景开始应用机器学习技术来提升业务效果，而效果提升一方面依赖于技术的进步，另外一方面也依赖于数据的极大丰富，合适的方法加上充足的数据可以对事物本身的描述更为深刻，从而提升最终的业务效果。在风控和营销领域对于数据的刻画越来越精细，其中非常重要的一点是在用户的动态行为的刻画越来越深入，但依然面临大量的问题，一方面序列数据天然的包含大量的噪声，用户在达到真实意图前可能会随机探索很多与目的无关的内容，这些随机的行为对理解用户的真实意图有非常大的影响，对后期的建模也有较大的影响，如何对高噪声的数据进行建模是我们面临的一个问题，另外一方面，在金融场景中，考虑到监管方面的问题，对使用的模型和特征方面都有非常高的可解释要求，这就造成大量的特征需要人工去加工，考虑到序列特征的复杂性，抽取序列性的模式一直耗时巨大，如何自动化的抽取序列化的特征也是我们面临的一个挑战。

目标

根据公司的实际需求，解决高噪声条件下的序列数据建模问题，对高噪声的数据进行有效的切分，自动化的抽取可解释的序列模式，对序列中的长期影响和短期影响，以及关键模式进行有效的区分并给出合理解释。

相关研究课题

1. 机器学习；
2. 可解释机器学习。

返回首页

1.6 面向金融场景的可解释机器学习

背景

人工智能近年来在图像、语音、自然语言处理等领域和相关产业取得的了丰硕的成果，但很多人工智能方法都是黑盒的，因此制约了人工智能在金融等高风险行业的应用。人工智能在金融场景的应用主要面临以下问题：（1）模型可靠性难以验证。（2）公众和政府日益重视数据安全，对人工智能做出的自动决策带来的公平、透明、问责制度要求越来越高。(3) 人类专家积累下来的经验无法有效地被人工智能利用。在合规监管大环境下，如何在控制人工智能引入的风险前提下，充分发挥数据和人工智能的价值，是金融可解释人工智能要解决的主要问题

目标

能解释黑盒模型，这些模型包括但不限于常见的 CV 和 NLP 领域的系列模型（如 CNN、RNN、BERT）以及图表示（graph embedding）相关的模型。或者能提出一些模型在能保持相当的性能的前提下，模型本身是可解释的。

相关研究课题

1. 因果推断；
2. 机器学习中的公平、透明、问责；
3. 特征可视化。

返回首页

1.7 面向金融风控的图学习算法研究

背景

随着数字金融的蓬勃发展，如何做好金融风控是持续稳定发展数字金融行业的核心问题。数字金融发展到现在，已经服务了超过十亿的用户和过亿的企业，同时也管理着数万亿的金融资产，而金融风控则是保障数字金融这一链路稳定可控的重要手段。随着图机器学习技术在各个应用领域的深入普及，图机器学习也给金融风控带来了极大的机会，同时也存在巨大挑战，主要表现如下：

1. **面向金融风控的图模型预训练任务。**设计合理的面向工业级图数据的预训练任务，为用户/企业等产出能刻画其风险水平的图嵌入表达，作为金融风控的底盘。可以将其应用于下游不同场景下的金融风险预测任务上，大大降低图模型训练成本的同时也对模型性能有相当程度的提升。
2. **风险的动态攻防。**金融风控需要不断的和黑产团伙进行攻防博弈，图模型应用于金融风控场景，需要更好地建模风险的动态性，迅速适应黑产团伙作案手法的变化。
3. **图模型的稳定性与鲁棒性。**金融风控，尤其是信用风控领域，由于大部分用户的风险水平都比较稳定，因此也要求图模型对风险的预测结果对于大部分用户也相对稳定。另一方面，为了更好地防御黑产团伙对模型进行攻击，也要求图模型具有较好的鲁棒性。

目标

1. 设计面向金融风控的图模型预训练任务，为用户/企业产出能够刻画其风险水平的图嵌入表达，并能应用于下游不同的金融风控场景。
2. 基于图学习建模实现金融风险的动态攻防，快速响应黑产团伙作案手法的变化。
3. 提高图模型的稳定性与鲁棒性，使得图模型对大部分风险水平稳定的用户也有稳定的预测输出，同时提高图模型应对黑产团伙攻击的能力。

相关研究课题

1. 图预训练学习；
2. 图对抗学习；
3. 图鲁棒学习。

返回首页

1.8 缺失与噪声环境下的行为序列鲁棒生成与学习技术

背景

在金融场景中，各参与方的信息多通过行为序列的方式留存，不仅直接反应了个体的偏好、意图等信息，也为整个系统或者群体的趋势提供了第一手的信息。由于这些数据往往在无法在一方进行集中记录，往往存在截断、缺失、模糊、小样本等痛点，无法被现有的机器学习模型进行充分利用。需要探索更为鲁棒的行为序列机器学习技术，具体包括：面向多方零散序列样本的协同机器学习、面向小样本序列的生成模型、以及复杂行为序列的缺失补全技术等。这些技术和工具将为后续的传统机器学习方法提供底层的低质行为序列预处理功能。

目标

探索和发展面向小样本序列的鲁棒生成模型，并能适应多个复杂分布的情形；探索和发展

多方零散序列样本的协同学习技术，在数据所有者信息安全的前提下，充分挖掘多方信息。

相关研究课题

1. 鲁棒机器学习。

返回首页

1.9 多方数据共享场景下的隐私保护图像建模

背景

大数据时代无论是金融授信风控或在线营销等都离不开数据。数据质量和数量已成为影响机器学习效果最重要的因素之一，通过数据共享扩充数据量以提升模型效果的需求也变得越来越强烈。但数据共享目前面临以下的问题：（1）数据安全风险。数据共享日益重要，但数据安全难以得到有效保障，出现了数据买卖、泄露和滥用等诸多问题；（2）公众和政府日益重视数据隐私保护，数据隐私保护的要求被提到了一个新的高度。欧盟通过的通用数据保护法案（GDPR），明确指出所有与个人相关的信息都是个人数据，数据的使用行为必须有明确授权。

在合规监管大环境下，如何在有效保护隐私同时让数据发挥真正的价值，共享智能正是基于这个问题提出并实践的。共享智能基于数据安全和隐私保护，在多个参与方之间通过共享加密数据或加密机制下的参数交换与优化，使用机器学习建立虚拟共享模型的平台。随着图像数据与人工智能的飞速发展，各种各样的图像处理应用蓬勃发展，已经在业界得到了广泛的使用。比如说人脸识别，刷脸支付技术的进步为用户带来了极大便利，蚂蚁金服提供的人脸识别功能已有数亿人使用。与此同时，针对用户图像数据中敏感信息的滥用所产生的安全问题也成为了人们关注的焦点。面对这些挑战，共享智能中的图像隐私是一个值得探索的方向，旨在保护用户数据隐私同时能提升系统的模型性能助力上述

金融图像场景。在图像隐私方向，两个方面的问题亟待解决：1）如何建立一种系统完善的人脸数据脱敏存储以及访问机制；2）如何在数据共享中保护模型训练以及预测时的隐私。

目标

此合作旨在研究以下图像相关隐私保护的问题：

1. 如何建立一种系统完善的图像数据脱敏存储，发布以及访问机制，最大限度地保护图像数据安全。
2. 如何在数据不出域合规的情况下，利用多方数据进行隐私保护联合建模，提升图像相关模型（例如，语义分割，人脸识别模型等）的性能。
3. 如何建立一套保证预测链路数据的隐私性和安全性算法及机制。
4. 对于已经训练好的图像相关模型，如何保护其模型本身被滥用，如何防止潜在的推理攻击也是一个潜在值得探索的方向。

合作期望交付：

1. 论文 2 篇（其中至少一篇 CCF A 类会议或者期刊）
2. 4 个相关专利提交

相关研究课题

1. 图像；
2. 隐私保护的机器学习。

返回首页

1.10 高精度高可靠面向大规模云计算环境下的智能运维算法研究

背景

为了确保蚂蚁各个业务和服务的稳定运行，运维在保障蚂蚁基础设施及其应用软件可靠性方面起到了一个重要的作用。随着基础设施、应用软件和业务的规模以及复杂度的急剧增长，基于人工的运维方法已经显得力不从心。当故障出现的时候，基于传统方法的运维人员只能被动式的响应，无法快速的进行人工干预，找到故障原因，并解决故障。另外，面对系统产生的海量运维数据，目前的主要工作在于对数据的收集和展示，如何利用已获取的历史运维数据，对其做智能化的分析还比较缺乏。而智能运维则侧重于利用机器学习和人工智能算法对海量监控数据进行不断学习，自动地发现故障，定位故障，甚至于预测故障可能出现的趋势，以辅助运维人员快速响应以及提早预防问题和风险的发生。

目标

在现有的机器学习和人工智能算法的基础上，研究高精度高可靠面向大规模云计算环境下的智能运维算法，以解决以下的六大技术问题：

1. 异常检测：包括单指标异常检测，日志智能分析，批处理任务异常检测。
2. 故障定位：包括调用链根因定位，多维异常定位，异常设备定位日志异常定位;
3. 故障预测：对时序指标进行预测，提早发现问题和风险（如业务量、磁盘空间、数据库表空间、网络流量）;
4. 报警降噪;
5. 容量预测;
6. 变更监控.

相关研究课题

1. 异常检测；
2. 故障定位；
3. 故障预测；

4. 报警降噪；

5. 容量预测；

6. 变更监控。

返回首页

1.11 机器学习模型安全

背景

自二十世纪 60 年代最初提出模拟人类智能的构想以来，人工智能受到了学术界和工业界的广泛关注和深入研究。在蚂蚁金服内部，人工智能技术也发挥着越来越重要的作用，目前已经成功应用于生物核身、车险定损、智能理赔等金融场景。尽管在有些任务重（图像识别、人脸识别），人工智能模型的识别准确率已经超越了人类，但它并没有达到人类的真正理解水平。在面对异常攻击样本时，人工智能模型无法正确输出结果，但是人类的理解能力却可以准确识别这个攻击样本。

目标

本项目拟从人工智能模型安全性本身出发，从理论上来证明模型的安全决策空间，并通过实验加以验证。

相关研究课题

1. 机器学习；

2. 安全与隐私。

返回首页

1.12 行为心理在财富管理的应用研究

背景

在整体经济增速放缓，流动性持续宽松，以房地产作为主的投资方式受到政策压制的大前提下，个人投资者对金融理财的需求正稳步提升。而业余投资者在面对复杂的金融产品选择、行情快速波动、账户盈亏的多重挑战时，心理状态也呈现对应的大幅波动。准确的捕捉这种心理波动，针对性的定制用户引导方案，将对精准营销、服务、陪伴等场景提供有力支撑。

早期的财富业务模式，主要是借鉴了阿里集团的商品推荐、服务策略设定方法，以及行业内第三方理财的业务形态。通过判定用户喜好，进行定向推荐，用户不满意再快速调换。前期的确起到了助推业务快速拓张的效果。随着场景进入深水区，投资理财的长链特性越来越突出。由于缺乏对理财产品风险的认知，用户在购买时或谨小慎微，或满仓博弈。而在经历涨跌的洗礼后，很容易流失。再次进行促活的成本也很高。

解决以上问题的方法是构建用户进阶体系，通过系统化的方法，引导用户逐步成为心智成熟的投资者。在这个过程中，需要对用户的恐惧、贪婪心理状态进行准确定位，构建对应的心理抚慰、引导方案，帮助用户在市场涨跌和账户盈亏中，逐步优化自身的投资行为，最终成为合格的个人投资者。这正与行为金融学所探讨的问题不谋而合，通过研究人的行为和心理相互的关系，来探讨优化人类选择的方法。

目标

1. 通过关键因子挖掘技术，找到影响用户金融行为心理状态的主要因子，并设计准确的心理状态估计方法
2. 通过蚂蚁现有用户交易行为数据的分析，对用户理财决策过程的主要心理状态进行划分，并制定相应的引导策略。
3. 根据用户心理状态设计对应引导策略，建立起用户投顾过程的心理状态迁移网络，并

应用到实际线上场景。

相关研究课题

1. 行为经济学；
2. 前景理论；
3. 行为序列的深度学习表征；
4. 用户心理迁移网络。

返回首页

2、安全

2.1 在 RISC-V 架构下的可信执行环境研究

背景

随着 5G、AIoT 等场景的迅速发展，RISC-V 架构的芯片未来正在受到越来越多的关注，将在智能物联网设备得到广泛的应用。可信执行环境（TEE: Trusted Execution Environment），是现代系统安全的重要支撑技术。在学术界，有不少研究团队关注于在 RISC-V 架构上，构建一个可信执行环境，其可以保证加载到该环境内部的代码和数据的安全性、机密性以及完整性。在工业界，也有越来越多的公司，正在研发支持 RISC-V 架构的处理器。

在实际业务场景中，AI 智能与数据安全共同面临一些挑战，例如人脸识别应用场景，如何满足人脸的特征计算、REE 与 TEE 的计算和存储资源分配、密钥存储派生和密文的数据流动路径设计、如何有效地降低安全环境的系统漏洞、以及微内核的形式化验证等等。前期设计阶段进行充分的验证与尝试，及时发现设计错误，降低全周期的设计的迭代

成本。

目标

期望申请人研究 RISC-V+TEE 的方案，可基于 FPGA 模拟，或理论分析，研究比较各种方案的性能和安全性，或提出新的 TEE 方案，或对 TEE OS 进行形式化验证研究。

相关研究课题

1. UC Berkeley 的 Keystone 项目(https://keystone-enclave.org/)
2. 上海交通大学的蓬莱项目(http://penglai-enclave.systems/)

返回首页

2.2 移动端小程序安全方案研究

背景

小程序是移动端近几年重要的技术创新，小程序新的技术架构同时也带来了新的安全风险和攻击面。目前业界有多款具有小程序功能的平台型 APP，但还没有形成统一的小程序安全技术架构方案，各自的方案存在一定的安全薄弱环节。为了保障小程序技术和业务未来的安全可靠发展，需要对市面上的小程序安全机制进行分析调研，并基于分析结果设计一套适合支付宝小程序的最优安全方案。

目标

完成对业界小程序的安全方案调研；产出适用于支付宝 APP 的小程序安全方案，相比现有方案的安全强度具有显著提升。

相关研究课题

1. 移动端 APP 架构安全。

返回首页

2.3 可信硬件与多方安全结合的下一代安全计算技术

背景

为了打破数据孤岛，将多种数据融合在一起，共同参与到分析与决策中，已经提出了多种安全计算方法，例如基于现代密码学的密态计算技术、基于可信硬件的隔离计算技术。目前，企业中应用的案例主要是轻量级的算法比如隐私保护集合求交。为了将多方安全计算从数据智能时代走向机器智能时代，需要引入机器学习、深度学习算法，实现多方间联合建模、联合预测。这其中既存在计算效率的问题，也有安全性的挑战。

对于密态计算技术，已有的机器学习框架，并没有从密码学上实现机器学习协议的可证安全。比如多方之间交互的梯度信息，会逆推出原始训练数据。此外，威胁模型建立在各方半诚实基础上，并没有对恶意参与方进行限制。

对于隔离计算技术，以 SGX 为例，其远程认证机制由 Intel 提供，安全性不完全自主可控。此外，目前也没有一个计算框架能兼容各种深度学习算法的训练和预测，实现对图片、文本等非结构化数据的训练和预测。

目标

本项目拟研究可以在企业中应用的下一代多方安全计算技术，实现常见机器学习、深度学习算法。相比已有研究，在提升模型训练和预测效率的基础上，做到机器学习算法协议的可证安全，并在一定程度上能抵御恶意参与方的攻击。

相关方向：

1. 多方安全计算；
2. 可信硬件；
3. 机器学习。

返回首页

2.4 针对分布式机器学习框架的安全性分析

背景

安全计算技术和分布式机器学习技术相结合能够帮助不同机构在满足用户隐私保护、数据安全和政府法规的要求下进行数据联合使用和建模，破解了数据孤岛，数据共享和隐私保护之间难以平衡的难题。目前，全球有很多相关的开源框架，但是这些框架的安心性还没有得到系统的分析。

目标

本项目拟系统化的研究分布式机器学习技术中的安全性问题，如 LR、XGboost、DNN 等经典机器学习方法在分布式机器学习场景下的安全性情况。

相关研究课题

1. 分布式机器学习

返回首页

3、生物识别&物联网

3.1 用户识别相关技术

背景

随着人工智能的不断发展，以人脸识别为代表的用户识别技术在支付宝刷脸支付、风控核身等业务中正在发挥着越来越重要的作用。由于人脸等用户识别技术用到的图像及特征数据涉及用户隐私，数据泄露或者滥用造成的后果难以想象，因此亟需加强对于用户识别特征 ID 的安全与保护相关技术研究。

目标

产出生物特征 ID 秘钥生成技术与加密空间共享学习技术，实现用户隐私保护前提下的分布式数据安全使用，探索成熟可应用的技术方案。

相关研究课题

1. 隐私保护技术；
2. 密钥生成技术；
3. 共享学习技术；

返回首页

3.2 基于 IoT 设备的用户感知与行为分析技术

背景

2018 年以来，支付宝刷脸支付技术与产品实现了从 0 到 1 的快速发展。目前，以刷脸为切入点，智能 IOT 设备网络也正在不断扩大铺设规模。从业务出发，我们一方面需要进一步增强对用户的识别能力，提升刷脸支付体验；另一方面，也需要赋予 IOT 设备场景数字化能力，实现对于人、货、场的智能感知，为商户提供更大价值。其中，基于 IoT 设备的用户感知与行为分析技术是关键技术能力，需要进行探索突破。

目标

产出生物特征强因子与行为数据弱因子的多变量建模技术，实现 IOT 设备多传感器下的用户感知和行为分析能力，并结合场景设计成熟可商业化的应用方案。

相关研究课题

1. 行人重识别；
2. 多传感器融合；

3. 行为分析；

4. 多模态识别。

返回首页

3.3 基于场景数据的助推理论在教育行业的应用

背景

“助推理论”（ Nudge Theory ）是 Richard Thaler 教授在针对人类行为学研究中提出的理论并因此获得了诺贝尔经济学奖。他的研究证明了小的提示对人们的行为有很大的影响。在 IT 工业界，“助推技术” （ Nudge Tech ）整合云计算、移动互联网、物联网、人工智能、大数据、社交分析等技术，助力机构及时地与用户进行个性化互动，影响场景用户个人行为。助推技术提供了实现大规模个性化的前瞻性解决方案。

在校园和线上教育场景，助推技术赋能学校、老师和培训机构，借助移动设备、智能穿戴设备，基于个人目标，及时提醒帮助学生用户建立良好的学习习惯，或推荐合适的学习资源和学习路径、或社会公益实践/兼职机会，这对于参与方在一个日益去边界化、个人化的教育生态系统中取得优势是非常关键的。

目标

“助推理论”在高校和 K12 教育场景落地算法模型，重点围绕习惯养成（学习习惯、理财观念等）、学习资源匹配和学习路径推荐、兼职/公益实践机会匹配/任务推荐这几个维度，基于但不限于人群和内容打标、推荐算法、行为跟踪、社交网络分析、人机交互、小程序、云计算、IoT 等领域技术，建设一个基础助推模型 PaaS 原型，能够孵化出面向学生和机构的移动小程序应用。

相关研究课题

1. 用户行为分析；
2. 智能推荐；
3. 定制化学习内容；
4. 数据安全管理；
5. 隐私保护的机器学习；
6. 社交网络分析。

返回首页

4、区块链

4.1 联盟链中安全高效的数据轨迹机制关键技术研究

背景

数据轨迹指的是跟踪和记录数据来源及其移动的过程，如今工业界和学术界纷纷对区块链系统中的数据轨迹投入越来越多的关注。当前的区块链系统仅支持粗粒度的数据轨迹，这对于许多不同的实际业务逻辑而言还不够。在区块链系统中，每笔交易都会使系统转移到新的状态。通过按区块重放所有交易，可以在离线分析过程中全面安全地重建区块链状态的演变历史（即数据或状态轨迹），例如数字资产状态轨迹。

通过重放所有交易，我们可以查询现有区块链中的数据历史记录，这仅适用于大规模离线分析。但是，它不适用于经常在业务活动中使用的联机事务处理（OLTP）。在智能合约执行期间，通常缺少可用于智能合约的安全的数据轨迹信息。目前智能合约编码业务逻辑的表达能力有限，主要是由于：1）缺乏数据轨迹的安全保障机制；2）缺乏运行时高效访问数据轨迹的机制。

目标

为联盟链构建安全且高效的数据轨迹系统，其主要研究内容如下：1）研究新型存储体系架构：用以解决当账户规模巨大的时候（达十亿级账户规模）不同数据的轨迹信息组合爆炸而带来海量数据存储问题；2）研究支持安全的海量数据轨迹查询处理机制：既要保证数据轨迹的安全又要支持海量数据轨迹的高效查询处理；3）研究数据轨迹访问框架：提供对开发者友好的接口，将数据的轨迹信息提供给业务智能合约，既降低智能合约的开发成本又减少访问区块链的存取开销；

相关研究课题

联盟链

智能合约

数据轨迹

查询处理

索引机制

返回首页

4.2 基于区块链的隐私数据多方协作方案

背景

区块链做为新经济的基础设施，必将改变现有商业行为和模式。如何在保护用户个人隐私及企业核心商业数据的前提下，实现安全，高效，且用户友好的多方（尤其是企业，机构等）协作，是个非常重要的课题。现有的解决方案，比如安全多方计算（MPC），零知识证明（ZKP）， 基于信道的数据隔离方案等，虽有效的保护了隐私，但是往往面临性能和通用性问题，且应用门槛很高，缺乏统一协议框架，给隐私数据流转带来了较高的技术成本。

目标

本课题向广大高校征集创新解决方案，包括但不限于如下方向：

1. 平台无关的，通用协作协议，有效的保护协作方的隐私数据安全；
2. 基于密码学的创新隐私保护方案；
3. 基于权限控制及数字身份的应用；
4. 区块链安全，如共识协议，智能合约，隐私保护协议的形式化验证等。

相关研究课题：

1. 区块链；
2. MPC；
3. ZKP；
4. 隐私保护；
5. 数据授权；
6. 形式化验证。

返回首页

4.3 融合区块链技术的新一代零信任网络安全架构

背景

目前，绝大多数企业都采用传统的网络分区和隔离的安全模型，用边界防护设备划分出企业内网和外网，并以此构建企业安全体系。然而，网络边界的安全防护一旦被突破，即使只有一台计算机被攻陷，攻击者就能够在安全区域内横向移动攻击。为解决网络边界建立信任的固有问题，基于零信任网络的安全架构诞生。零信任网络的核心思想是：从来不信任，始终在校验。任何访问主体（人/设备/应用），在访问时都不予信任，通过动态信

任评估机制，动态访问控制机制，进行持续的验证和授权。零信任网络的主要核心能力包括：统一的可信的身份识别能力，持续的动态的信任评估与授权机制，在授权后进行无边界的访问控制和预警，并且最终可以根据身份，授权，对访问进行可信审计。目前，在区块链平台上也诞生了与零信任网络相辅相成的技术，比如，分布式身份（DID），智能合约，隐私计算，密钥管理等技术与服务。因此，如何利用区块链技术帮助构建更强大的零信任网络安全架构，值得更深一步的研究。

目标

利用区块链技术构建更加强大的零信任网络安全架构，包括但不限于：利用区块链技术构建统一的可信身份识别系统，利用区块链技术构建可扩展的可审计的动态授权机制，利用区块链技术构建授权访问的可信审计与回溯。

相关研究课题

1. 利用区块链统一身份统一服务构建与零信任网络的可信身份识别框架；
2. 利用区块链技术构建可扩展的可审计的动态授权机制；
3. 利用区块链可根据身份对授权，访问进行可信的审计与回溯；
4. 零信任网络加持区块链后新的安全应用场景。

返回首页

5、软件工程

5.1 大规模软件系统下的模糊测试方法

背景

模糊测试（fuzzing）等程序动态分析技术是自动化挖掘软件可靠性缺陷和安全漏洞的

有效手段。业务部门的功能性测试和单元测试能够在一定程度上提升系统的可靠性、安全性和稳定性，但是需要大量的人力投入，且在研发效率和覆盖率等方面有一定的缺陷。随着业务种类和规模的发展，大规模的代码和复杂系统存在大量人工无法发现的缺陷，亟需新的解决方案。技术方面的挑战主要在于复杂程序的源代码或二进制分析与插桩，目标的高效运行，和缺陷检测工具的构建和完善，结合业务实际场景减轻对底层工具可扩展性的要求，以及业务层面相关检测环境的构建。

目标

程序动态分析可以用于蚂蚁、阿里的内部代码检测，包括但不局限于：**数据库、操作系统、中间件、服务端程序、手机应用、嵌入式等**代码的检测，及早发现问题、预防风险。

相关研究课题

1. 数据库 Fuzzing 算法：数据库是目前云计算系统的一个核心。数据库的可靠对整个云计算系统的可靠性至关重要。利用 Fuzzing 技术，可以发现数据库管理系统中的缺陷，防患于未然。
2. 程序动静态分析结合：程序静态分析可以获得较好的安全漏洞、可靠性缺陷等覆盖范围，但是精度不够，误报率高；而动态分析方法的覆盖率低，但是准确率高，所以动静态结合的程序分析方法，可以有效提高可靠性缺陷和安全漏洞挖掘的效率。
3. 大规模软件的动态分析：目前 fuzzing 更多集中在小型程序的检测或单元模块的测试。大规模程序的动态分析有很多技术难题亟需解决，如大规模插桩带来的性能问题、多线程带来的并行问题、全局状态带来的噪音问题、路径爆炸问题、测试预言（test oracle）等；而模块化的单元测试缺少一个对软件的整体评估，无法检测模块间的可靠性和安全性问题，难以达到全局最优。
4. 动态分析系统的自动化：目前模糊测试技术需要依据测试目标进行 fuzzer 的适配，即需要人工来定义 input 的格式，进而生成和变异，这导致需要大量的人力来把

fuzzer 适配到业务程序。如何自动化地针对目标程序构造输入用例，是有效解决 Fuzzer 的通用性问题的至关因素。

5. 动态分析的有效性与效率提升：动态分析的效率决定了测试的时间和计算资源的开销，而误报、漏报会对 fuzzing 的结果有极大的影响，因此如何增大被检测程序的路径或漏洞覆盖率、增快执行速度、降低误报率等，也是我们亟需解决的关键问题。

返回首页

5.2 高精度程序静态分析算法

背景

软件缺陷是在软件开发和维护中几乎无法避免的问题，软件缺陷可以导致系统失效以及安全漏洞。虽然在软件发布前已经经过了编码规则检测，代码评审，测试，灰度等多种手段避免软件软件缺陷，但是生产环境中因为软件缺陷导致的安全事故占到了企业总事故数的很大一部分。原因在于程序的输入空间巨大，可以认为是无穷的，有限的测试无法覆盖所有生产环境中出现的情况，而且软件越来越复杂，依靠人的经验的代码评审和规则检查只能减少却不能避免软件缺陷。基于静态分析的软件缺陷检测技术，可以在不运行程序的情况下，根据程序的源代码或者二进制代码，对程序行为进行近似，提取程序性质，自动发现程序的缺陷，提高蚂蚁的安全生产水平。

目标

对蚂蚁现有的软件和开发中的进行基于静态分析的缺陷检测，发现可能的软件缺陷，提高蚂蚁生产环境下软件的可靠性，减少因为软件缺陷导致的安全事故。同时，静态分析可以为动态分析提供指引，提高测试的覆盖率，也可以为技术蓝军提取目标系统的性质，提高攻击的效率。

相关研究课题

面向软件可靠性缺陷和安全漏洞的自动挖掘，深入研究以下几个题目：

1. 面向大规模、分布式软件的静态分析技术；
2. 混源代码静态分析技术；
3. 支持混合语言程序的静态分析技术；
4. 支持分析结果重用的增量式静态分析技术；
5. 对静态分析误报的消除技术；
6. 面向复杂数据结构和复杂性质的静态分析技术；
7. 支持高度可自定制规则的静态分析技术；
8. 支持多种分析技术配合的静态分析框架；
9. 面向二进制代码的静态分析技术。

返回首页

5.3 面向分布式系统的基于日志的智能排错方法

背景

日志被广泛应用于错误排查。然而基于日志排查分布式系统中的错误并不简单。排查过程可能涉及分析复杂的协议(如故障恢复，分布式 GC)、随机环境事件（节点宕机），计算语义错误，及特定的事件时序等因素，需要开发者对系统高度熟悉、且投入大量时间。随着业务规模的增大，错误诊断的成本和开销尤为凸显，保姆式的运维不再适用。如何高效地进行错误检测、定位、以及诊断是当前 Ray 团队的一个重要任务。

目标

希望通过模型检测、程序分析等手段建立起事件因果图，并结合日志达到自动诊断错误的目的。期望合作分成三个阶段。第一阶段：首先是合作方对分布式系统 Ray 进行建模，

并基于日志构建事件因果图。交付结果需具有自动诊断常见错误的能力，我方会提供一个小的 benchmark 供合作方进行开发和验证。该阶段主要目的在于构建基础能力，只需分析与日志及系统框架相关的事件，与应用层代码相关的排错能力放在第三阶段。第二阶段：可视化及在蚂蚁内部进行实际线上部署。第三阶段（可选）：在时间充足的情况下，结合对应用层的代码分析，丰富事件因果图，如某个任务对应的日志序列及程序状态。

相关研究课题

1. 程序分析；
2. 模型检测；
3. 人工智能。

返回首页

6、基础系统&数据库

6.1 自治化与智能数据库

背景

随着近年来机器学习和人工智能领域的发展，机器学习在数据库和系统软件领域的应用日渐成为一个热门领域，并产生了一些具有使用价值的成果。与此同时，数据库软件日益复杂，其自治化成为了现代云数据库的研究热点。华为高斯数据库提出了 AI-Native 数据库的口号，老牌数据库厂商（如 Oracle）在数十年积累之上也专门扩展了自治数据库产品线。自治数据库通过将机器学习技术引入到关系数据库，能够有效地降低运维成本，提升数据库性能和稳定性，具有极大的商业价值。

目标

1. 通过分析系统运行环境状态和日志数据信息，利用机器学习手段建模，来实现动态系统参数调整和系统优化，减少系统 DBA 的运维负担。
2. 在数据库系统查询与分析优化器的关键模块上运用这些技术可以实现从规则优化器和初级的性能优化器向高级的机器学习模型为主的高纬度查询优化器的演变。
3. 机器学习技术也可以帮助系统建立更加准确高效的在线预警与实时监测系统，来实现智能的 DBA 运维管控和资源调配。海量结构化，半结构化与非结构化数据的分析建模则提出了如何建立深度数据分析的智能数据库系统的科研问题。

相关研究课题

1. 自治数据库；
2. 系统参数的机器学习；
3. 智能诊断调优。

返回首页

6.2 金融级云原生操作系统研究

背景

以“Pay as you go”，“auto scaling”特性见长的 Serverless、FAAS 等新的计算形态，对操作系统提出了更高的要求。新操作系统需要具备极致的业务启动速度、极小的资源开销以及对资源按需申请/释放等功能。

金融业务涉及用户隐私数据、资金数据等重要敏感信息；金融数据的安全关系到国计民生。金融环境中的云原生技术必须以安全隔离为第一目标。

Linux 内核所提供的资源隔离和一定程度的安全隔离，难以满足上述两个要求。此外，Linux 内核自身的安全性不容乐观。

目标

针对金融行业在信息安全上的高要求与金融应用向云原生发展的趋势，研究并开发“金融级云原生操作系统”，满足金融级产品对安全与性能的高要求。具体目标如下：

1. **安全隔离** – 通过安全机制减少系统代码指针类型、整数类型、并发锁类型等 bug，增大漏洞利用难度，增大 DOS 攻击和逃逸的难度。
2. **灵活轻量** – 在内存利用做到灵活分配和释放，控制系统运行自身所需内存；运行于该操作系统之上的业务具备毫秒级的启动速度。
3. **性能优势** – 充分利用新架构，为业务性能优化提供可能。

相关研究课题

1. 安全强隔离技术；
2. 高效率资源调度系统；
3. 操作系统关键组件的热升级/热迁移技术。

返回首页

6.3 增强的 Go 语言 Runtime

背景

Go 语言是一门优秀的现代语言，随着这些年杀手级应用越来越多，在企业内使用也愈加广泛。Go 本身是一门有 runtime 的语言，但在企业使用过程中，runtime 的一些设计也渐渐暴露出了一些问题困扰着它的用户。例如 GC 导致用户程序延迟上升，GC 本身设计目标是低延迟而忽略了一部分更重视吞吐的用户需求。Go 提供了强大的 pprof 来帮助用户来定位内存泄露问题，但有些场景并不那么容易判断是哪里的“持有”逻辑最终导致了泄露等等问题，我们提出了下述一些目标。

目标

实现能够满足各种场景使用的 Go runtime，满足但不限于以下需求。

1. 内存管理及 GC：

低延时场景，希望能有分代 GC，降低 in_use 对象的扫描数量，以降低因为协助标记导致延迟上升。

高吞吐场景，希望能够在相同的 CPU 使用前提下，提供更高的吞吐量。也就是用户可以通过配置来选择优先吞吐还是优先延迟。

2. 内存使用追踪：

虽然 pprof 可以查看程序发生内存泄露时经过的代码路径，但是难以判断当前持有某块内存的具体持有对象。GC 扫描阶段从程序根对象(BSS，DATA 段等)开始启动扫描并遍历整棵对象树，希望能参考该流程实现内存对象的 dump。帮助诊断一些较难排查的内存泄露问题。

3. 堆外内存：

有些服务会有变化不频繁的大量常驻内存，而因为 Go 本身的 GC 机制导致这些内存在每次 GC 周期都会被扫描，希望能有类似// go:notinheap 的堆外内存使用机制，由用户决定何时分配、释放这些对象。

4. 调度器

支持非公平调度，当前 Go 的调度理论是有 work steal 的公平调度，因为“公平”所以导致一些网络事件处理协程也是以与 IO 协程相同的优先级进行调度，而导致极端情况下出现大时延。希望能够有特定的高优先级协程队列/ 执行机制，能够获得高优先级的执行权(类似内置的 netpoll)，以满足一些特定场景下的需求。

5. 热补丁

热补丁技术，在运行时对目标函数或者方法打补丁，对其进行热替换，实现对业务代码的检测和调试。

相关研究课题

1. 分代 GC；
2. 调度理论；
3. 堆外内存；
4. 热补丁；

返回首页

6.4 延迟网络下的高性能数据传输协议

背景

在全球化背景下，蚂蚁面临的网络背景从可靠网络演变成为延迟网络，而延迟网络的场景主要为：跨国通信，跨多ISP，并且由于境外的通信基础设施较差，弱网环境大量存在。在网络层面的具体表现为：长延时，丢包率高。而蚂蚁的业务场景对网络有着很高的要求。而不同的业务场景对于网络的特性又存在不同的需求，因此我们需要一种新的特性可配置的高性能延迟网络协议。下面介绍典型的两种网络特性诉求：

1. 高实时性要求的蚂蚁区块链网络：在允许一定的丢包场景下，保证数据的实时性，区块链传输的实时性有其特点，不同于音视频数据的传输可以实时调整码率改变发送端数据量；区块链的数据通信主要分为交易数据和共识数据，交易数据通信偏重完整性和全局数据交集最大化，而共识数据则偏重传输实时性、可基于实时性做一定数据取舍，甚至支持REMB (Receiver Estimated Maximum Bitrate)。蚂蚁区块链已经在构建自己的区块链传

输网络，在区块链传输方面，希望能够实时处理数据转发，以应用层路由为基础构建灵活的SD-RTN网络（software defined real-time network）。

2. 高可靠，高稳定性的蚂蚁数字生活网络：蚂蚁数字生活的场景需要在保证数据成功传输的前提下，尽可能的减少传输时延，并保障网络的稳定性。现有的解决方案典型如quic协议，缺乏流量调度的能力，并且在拥塞控制算法的层面能力相对单一，并不能满足我们的诉求。

目标

我们期望能定义并实现一种可扩展的，高性能传输协议。协议能满足以下能力：

1. 在使用层面：可以由应用层来决定当前网络需要满足哪些特性:比如实效性，稳定性，公平性，然后通过选择各种性能的权重配比，生成一个满足特性需求的网络。
2. 在流量调度层面：在端到端链路上区分更多的优先级，加入更多的业务属性，比如flow deadline等，从而在流的调度上基于这些属性做更多的特性支持，则可以提高整体的业务体验。
3. 在拥塞控制算法层面：针对不同的业务属性做拥塞控制算法的可协商、同时创新一些新的拥塞控制算法，包括AI+拥塞控制。
4. 在具体实现层面：可以基于(不限于)quic plugin，加入一种或多种创新的拥塞控制算法，并实现一种或多种智能流量调度策略，以保证较细粒度的网络特性模拟。

相关课题

1. 可变配多特性的高性能延迟网络设计及实现；
2. 延迟网络下的智能流量调度体系建设；
3. 延迟网络下的智能拥塞控制算法设计及实现。

返回首页