目录

2.2 面向企业级微服务的高精度软件分析

2.3 路径驱动的自动故障注入技术（混沌工程技术）

2.4 数据平台模糊测试

2.5 面向静态分析工具的模糊测试技术

2.6 面向 Maven 构建系统的依赖分析及优化研究

2.7 基于纯软件的高效且可扩展的正则表达式匹配算法研究

3. 区块链

3.1 大规模广域网联盟链的网络治理和自适应研究

3.2 智能合约编程语言关键技术研究

3.3 隐私应用安全审计

3.4 零知识证明及其在区块链领域中应用的关键技术研究

3.5 区块链结构化数据可验证查询关键技术研究

4. 基础系统&数据库

4.1 智能实时数据平台相关研究

4.2 代码自动分布式化方法研究

4.3 面向隐私合规的信息流分析和控制技术研究

4.4 自适应统一传输层技术研究

4.5 基于 RDMA 的高效分布式事务处理机制的研究

4.6 基于 FPGA/GPU 的存储引擎加速研究

4.7 面向 HTAP 数据库的工作负载隔离机制的研究

4.8 面向 HTAP 数据库的的新型存储引擎的研究

4.9 数据库存储成本优化研究

4.10 单机多级调度系统的研究

4.11 应用镜像加载、存储和传输技术研究

4.12 分布式动态决策调度系统研究

5. 安全

5.1 移动端数据隐私保护技术研究

5.2 更为鲁棒的设备身份篡改识别方案

5.3 JAVA 开放式动态反序列化 Gadget Chains 自动化挖掘

5.4 基于轻量级隐私保护方案进行横纵向联邦、联邦迁移学习及隐私计算

5.5 基于大规模图计算的异常识别检测和风险挖掘

5.6 CV 模型安全性研究

5.7 高精度鲁棒相机指纹技术研究

5.8 深度学习模型隐私安全技术研究

5.9 基于人工智能的恶意通信识别

申报课题

1、人工智能

1.1 在风控决策中的样本偏差与因果推断问题研究

背景

在信用及交易风控决策场景中，所有的观测标签都受到风控决策策略的影响，从而存在的选择偏差（曝光偏差）问题。同时我们希望通过研发因果分析算法，自动发现黑样本或者违约背后的真实原因，以便更好的提升模型的稳定性，准确性。

目标

1. 如何从因果推断的角度量化样本的偏差程度；
2. 如何从有偏的观测数据中去除偏差的影响，从而进行无偏的决策模型训练；
3. 该技术应用于投资理财背后的归因分析；

相关研究课题

1. 因果分析
2. 模型稳定性

返回目录

1.2 特征算法结果可解释性研究

背景

在反洗钱，交互式风控，信用场景中，我们使用的模型需要一定的解释，有助于用户更容易理解我们的决策逻辑，同时提升我们模型的鲁棒性，对用户风险行为的进行判断，并给出带有逻辑性的可解释文本/富文本结论。可行的方向包括将业务专家知识以知识图

谱的形式保存，并融入算法中，以 Generation+Retrieval 的方式生成。

目标

1. 知识图谱与文本生成算法的融合，例如Graph-embedding融入生成算法，或将现有算法升级成Generation+Retrieval+Knowledge的算法等；

2. 小样本场景下的文本生成算法；

3. 从文本生成算法升级到包括图像、表格在内的富文本生成算法

相关研究课题

1. 模型可解释

2. 知识图谱

3. 密码学

返回目录

1.3 AI 攻防智能与 AI 可信

背景

当前的学习系统容易受到规避攻击（如对抗性例子）的攻击，本课题旨在：保证深度学习系统可以在新的环境中运行，并且仍然能够安全可靠地抵御对抗性干扰等攻击；测试和验证深度学习系统所需的安全性并提供可证明的保证；探索针对现实世界机器学习模型的实用新型攻击策略，并开发强大的学习算法，以应对强大的自适应攻击者；

目标

1. 将博弈论和对抗学习算法与团伙挖掘算法相融合，挖掘团伙变化中的潜在模式，提升团伙模型在风险对抗中的鲁棒性；

2. 对黑产与风控系统的动态博弈行为进行建模，并研究相应算法（包括经典深度学习模

型，序列模型和图模型）

相关研究课题

1. 对抗学习

2. 博弈论

3. 模型鲁棒性

返回目录

1.4 AI与经济学结合及多智能体的研究

背景

人工智能正在从单个智能体向多智能体发展。多智能体比如研究营销环境下多个商家和个体之间的关系和行为，比如，投资如何设计好的策略，这里包含多方机构、个人和投资者。这种情况下，我们如何把人工智能、深度学习、经济学、机制设计，博弈论等技术结合起来，从一个系统的角度来分析智能的作用、演化和对系统本身的影响。

目标

探索应用于包括智能投顾，智能投研、市场营销和用户忠诚度上等方面的方法，并且研究探讨算法公平性问题。

相关研究课题

1. 机制设计与博弈论

2. 多智能体

返回目录

1.5 多源数据融合的高可靠智能运维算法研究

背景

金融云的智能运维系统面临着如下问题：

1. 高度复杂的多源数据关系，多种数据包括日志、链路图、告警文本、链路图等之间的关系极其复杂，哪一些是和业务任务相关的非常不清晰；

2. 高度依赖于人工参与，大量异常情况都是人工规则在处理，系统自动化程度较低；

3. 数据量巨大且多数没有标注，有监督学习已经不能适应实际需求，导致算法精度严重不够；

4. 应急即时处理的需求，对算法的复杂度和系统的要求极高。

另外一方面，智能运维系统强烈依赖于有效的、结构化的数据输入，但是目前金融云的智能运维系统，数据层存在着两大问题：

1. 数据资产不够完善，大量的事中和事后数据，严重缺乏事前程序分析的数据，特别是涉及程序变更影响面、资产影响面的数据；

2. 大量孤立的数据资产，缺乏结构化的组织，缺乏互相之间关系的挖掘，导致具体任务需要哪一些指标是不清晰的。

目标

本课题从以下几个方面（包括但是不限于）研究构建高可靠、高自动化、高精确的智能运维系统：

1. 从多源融合学习、图关系学习、半监督/自监督学习等角度探索智能运维中的一些关键问题，如全系统级别的异常检测和根因定位；

2. 探索构建结构化的事前、事中、事后数据资产，事前数据从程序分析获取，事中和事后数据从日志、DB、链路还有各种告警和处理文本获取，同时探索各类数据之间隐藏的关联关系，构建风险知识图谱，最终驱动应急决策。

预期产出：

（1）1篇CCF-A类会议论文投稿；

（2）1+篇专利；

相关研究课题

1. 故障知识图谱；

2．全链路智能关系学习；

3. 半监督、自监督异常检测

返回目录

1.6 云原生系统的自动化调优和智能化降本提效

背景

云原生系统中托管着大量的对象，包括docker，JVM，中间件，数据库等等，这些对象通常有大量的配置参数，针对不同微服务、应用，这些托管参数的配置不能千篇一律，不然会来带各种问题，包括但不限于：

1. 资源利用率不高的问题；

2. 性能达不到最优的问题；

3. 请求处理吞吐量不高的问题；

4. 负载不均衡的问题。这些问题不仅可能会耗费人力来支持维护，同时可能会引起可靠性问题。

特别的，金融云系统由于支付量巨大，每秒钟产生的日志、告警、DB等数据以TB来计算，大量关键数据我们需要保存一段不短的时间，从而给存储系统带来巨大负担。传统的流式压缩技术，将产生的数据压缩存储到外部存储器，需要使用的时候解压缩到内存使用。

为了确保处理的实时性，普遍采用的流式分块压缩技术压缩比很有限，给整个系统带来巨大的存储开销。

目标

本课题从以下几个方面（包括但是不限于）探索自动化降本提效的可能性：

1．探索基于强化学习、黑盒优化，自动调节相关参数，实现诸如资源消耗最优、性能最优、吞吐量最优、负载均衡等目标，最终实现这些配置参数的自动托管处理，不用人力参与，从而大量节约云原生系统的成本还有人力成本。

2. 综合运用算法（包括但不限于基于深度学习的压缩算法）甚至硬件加速技术，构建高压缩比、高速的流式压缩、解压缩算法；

预期产出：

（1）1篇CCF-A类会议论文投稿；

（2）1+篇专利；

相关研究课题

1. 强化学习的自动调参；

2．黑盒优化的自动调参；

3. 深度学习的无损压缩技术

返回目录

1.7 面向版权保护的视频多模态侵权检测算法研究

背景

传统的版权保护行业存在着费时费力成本高，海量内容难以全量保护，内容分发难以掌控传播的安全问题。区块链技术具有不可篡改、追根溯源、分布式共识等特点，和数字

版权保护具有天然契合之处，将区块链技术与 AI 多媒体侵权检测技术相结合，能够极大降低版权维权成本，提升版权保护的效率，同时也为网络版权的存证、交易、维权提供了新的途径。但是目前针对版权侵权检测，尤其是视频侵权这一领域在帧空间域和时间域上的定义尚不清晰，业界的数据集和评测标准尚不明确，在此基础上的算法研究更是相对较少。目前已有的业界的算法大多无法同时实现高鲁棒性、低延时以及侵权时间轴定位的能力，整体行业缺乏高效率、准确和实用的多媒体侵权比对和检测技术手段。**目标**

1）将视频侵权检测的客观指标（数学定义）与主观指标（实际观感）统一定义，实现客观指标在人工打标数据集上的统一验证，完善相关定义和评测标准。

2）对已有的其他相关任务（包括但不限于视频分类、动作识别等）的视频特征提取算法进行有效改进，可以利用但不限于图学习、信息检索等相关技术方案，在视频侵权比对算法上得到比较高的指标。

3）根据1）视频侵权的统一定义，将需要比对的视频对的帧在时间段上进行匹配定位，完成类似视频动作识别的时域对齐，实现实际版权保护业务中视频侵权片段的有效指向。

4）利用视频的多模态信息（视频画面、音频、标题等）进一步提高视频侵权检测算法的准确率和召回率。

相关研究课题

1. 视频检索
2. 多模态语义关联
3. 视频理解
4. 向量检索

返回目录

1.8 结合专家经验的对话策略模型

背景

对话系统是人工智能的重要方向，广泛应用于智能客服机器人、理财顾问机器人、电话销售机器人等产品，支持了蚂蚁内部的多个重要业务。为了持续提升对话系统的能力，使其逐渐接近真人，蚂蚁智能服务团队自研了一套基于强化学习的对话模型，通过引入长期奖励来优化对话决策过程。然而，基于强化学习的对话模型并不能很好地结合专家经验，缺乏可解释性与可控性，真正在线上使用时会遇到较多阻碍。针对这一问题，我们希望深入研究结合专家经验的对话策略模型，进一步提升对话效果的同时保证对话的关键流程可控，更加接近真人的对话效果。

目标

1. 持续在强化学习方向探索更智能的对话策略模型，应用学术前沿的强化学习方法，提升模型的可控性与业务转化率；

2. 结合问答、文档、数据表、知识图谱等数据，在在线学习、对抗学习、图学习、自动学习等多个方向进行探索，发现新一代对话模型实现方案；

3. 充分考虑运营端与用户端的使用体验，研究更易用的平台产品，提升产品智能化水平，提升运营效率和用户体验。

相关研究课题

1. 端到端对话系统；

2．深度强化学习结合知识

返回目录

1.9 基于自然语言指示的嵌套对话模型

背景

对话系统是人工智能的重要方向，广泛应用于智能客服机器人、理财顾问机器人、电话销售机器人等产品，支持了蚂蚁内部的多个重要业务。然而对话系统也经常产生错误决策，影响用户体验，部分原因包括泛化性不足以及缺乏常识等原因。如果引入人在泛化性，常识等方面的能力，则可以弥补当前对话系统的不足。近年学术界在 natural language instructions 方面的研究有可能对该方向的研究提供帮助。通过嵌套决策的方法，首先生成 instructions，再联合原始特征和生成的指示共同决策，相当于引入外部知识，提升泛化性和常识，增强可控性和可解释性。

目标

1. 探索在knowledge grounded dialog的基础上，增加基于natural language instructions生成的嵌套决策方案，融合instruction和原特征嵌套决策，缓解泛化性不足和缺乏常识的问题；

2. 充分考虑在训练阶段的人工提供instructions的低成本和高泛化性，在预测阶段，支持采用自然语言的方式提供instruction进行预测修正；

相关研究课题

1. knowledge grounded dialog；

2. learning from instructions

返回目录

1.10 异构图神经网络自动机器学习技术研究

背景

异构图（heterogeneous graphs）常用来描述具有多种结点类型和多种连边类型的复杂网络数据。在蚂蚁集团，支付网络和数字生活交互网络属于典型的异构图。同时，反欺诈、信用评估、信贷风控等场景也都依赖于异构图数据分析能力。近年来，越来越多基于异构图的深度学习模型被提出来解决异构图数据上的分类预测和异常检测等问题。但是，这些模型都高度依赖手工选择特征和调整网络结构参数，耗费大量人力，模型开发效率相当低。本研究尝试回答下面这个具有挑战性的问题：给定一个异构图数据集，如何自动寻找最优的图神经网络模型？在实践中，自动机器学习（AutoML）已经被用于深度学习神经网络建模，典型地包括自动特征选择与生成、卷积神经网络和传统同构图神经网络结构搜索等。但是，如何针对异构图神经网络来进行 AutoML 的研究还不充分。

目标

该研究尝试解决以下新的技术挑战：

1. 如何自动选择或者生成点/边特征；

2. 如何设计针对异构图神经网络的搜索空间；

3. 如何针对异构图设计高效的增强学习搜索算法；

4. 如何针对复杂应用场景，比如监督、半监督和非监督学习场景评估搜索算法的性能；

5. 如何在算力、搜索时间、图规模、预测延迟和吞吐等多目标约束下通过算法和图学习系统联合优化尽可能逼近最优解。

针对这些挑战，本研究拟以阿里和蚂蚁集团真实业务场景中的异构图学习问题作为样板，构建一套大规模异构图神经网络自动机器学习的解决方案，并产出CCF-A类论文3篇以上。

相关研究课题

1. 异构图神经网络；

2. 自动机器学习；

3. 超大规模分布式图学习；

4. 分布式图计算

返回目录

1.11 知识驱动的对话图生成

背景

目前我们的智能保顾系统的数据及推理模型建构于 graph based 结构之上，其数据结构的构建，算法的构建都极其复杂，落地成本很高。在建构的过程中遇到了几个启发性问题，他们的解决可以帮助我们一切 graph based 的应用成本和泛化能力。

目标

落地：

1． 图网络对边的理解依然局限于拓扑的关系， 而如果这些边含有了复杂世界的因果关系呢？ 是否网络可以学习？

2． 图网络方法目前更多局限于静态的图， 而显示世界的图更多是动态的， 变化的。 那么如果有一个机器学习模型可以不停的适应这种动态变化的图， 需要什么样的表示？

3． 说到底， 图网络结构是产生在我们的大脑里。 当婴儿探索世界的时候， 他的大脑里没有图的概念， 而是片段的序列信息， 那么这个图的结构是如何从这种片段序列信息里面整合出来的， 这个过程是怎么通过大脑神经网络构建起来的？

能解决这个问题，我们就可以将支付宝域内大量零散的序列化数据进行构图，使其进行关联从而衍生出无限可能的用户服务推理能力

学术：CCF A/B 类2 篇

相关研究课题

1. 图神经网络

2. Graph Mining

3. 序列建模

返回目录

1.12 用户在金融场景下的决策行为与心理

背景

金融场景中，用户长期稳定的兴趣及短期的情绪波动，对于用户金融需求、决策有关键影响作用。尤其是非理性决策时，需要对用户进行精准识别并进行适时干预。这其中的核心难点在于从稀疏的数据中，提取可信的信息，并通过端智能来保障数据隐私情况下，仍然能够对用户决策进行辅助和适时引导。

目标

结合行为金融学、决策心理学、数据算法建模工具，构建一套能够实时辅助用户进行合理决策归因体系，同时可以对现有理论进行丰富优化，完成具有学术价值的突破。

学术：

CCF类论文2篇

相关研究课题

1. 因果推断

2. 决策心理学

3. 内容生成

4. 端智能

返回目录

1.13 社交网络增强的个性化建模

背景

支付宝数字生活场景存在数据大而薄的特点，具体来说，支付宝用户量大，但用户在支付宝端停留时间短、行为稀疏、且部分行为与待推荐的内容关联性较弱，导致很难进行精准的个性化建模。为了缓解这一问题，可以引入社交网络，基于社交关系近的用户兴趣相近的基本假设，增强薄数据用户的表征，从而提高各类个性化场景（营销、推荐、搜索、广告等）的效果。此外，支付宝上存在大量基于社交玩法设计的营销活动（如人传人红包、组队瓜分等），此类营销活动的 ROI 优化问题也需要考虑社交网络的影响，如何结合用户社交关系对持续优化 ROI，是提高支付宝营销效率的关键课题之一。

目标

1. 探索如何基于社交关系增强用户表征，为支付宝用户（尤其是中低活用户）提供精准的个性化服务；

2. 研究营销活动中的社交效应，提高支付宝内营销活动的ROI；

3. 针对上述两类问题，完成并发表两篇CCF A/B类文章，并提交两个专利。

相关研究课题

1. 个性化推荐

2. 图学习

3. ROI优化

返回目录

1.14 融合对话情景的深服务主动对话智能机器人研究

背景

在智能服务战场 ，深服务转型升级已经到了一个关键时点，目前我们已经在选品服务域验证了深服务式主动对话在转化率和 GMV 上已经超过了短频快的营销式服务。作为实现深服务核心的主动对话引擎，通过深度强化学习解决服务和投顾策略编排和串联、对话话题转移等一系列对话智能关键问题，在提升用户理财体验的同时实现复访、gmv 等业务价值。

目标

本课题的目标：

1）在现有业务上已落地基础上进行framework方法论升级、引入新机制提升指标，深入探索强化学习提升复访、转化率和GMV的天花板

2）探索主动对话形态，并落地业务。

3）CCF A/B类文章二篇。

相关研究课题

1. 对话式推荐系统

2. 智能决策/深度强化学习

返回目录

1.15 安全对抗与意愿交互技术研究

背景

面向各种行业与环境下的刷脸支付场景，以及各种身份与角色下的恶意攻击与测试行为，在基于 IOT 的主动防御与对抗、未知攻击检测、非配合式意图识别与确认等方向展开新

思路新方法的技术探索与攻坚，支持产品与服务的不断升级。

目标

1. 在完成学术界论文检索与产业界解决方案研究的基础上，完成调研报告与技术路线选型。

2. 完成技术预研POC并在指定测试数据集达到state-of-the-art性能；

3. 完成相关专利申请与学术论文发表。

相关研究课题

1. 计算机视觉；

2. 生物识别

3. 情感计算

返回目录

1.16 多模态视频内容理解

背景

随着支付宝数字生活平台化建设的深入，越来越多的多媒体内容（图像、短视频）出现在支付宝各种业务场景中。内容数据的结构化理解不仅要面对海量数据的挑战，考虑到内容产生和消费的时间、空间、个性化、服务场景等关联因素，模态的多样性和统一特征表达的难度给这个任务带来了极大的挑战。把多模态数据分析应用到场景内容理解上，除了要考虑视觉、语音等媒体数据外，还要挖掘场景背后的业务关联属性。

目标

1. 更加泛化的特征表达方式，如何在网络中更好的融合视觉、文本、语音、离散场景数据，或者显示学习到关联属性。

2. 多模态在业务场景中的应用，例如如何指导内容创作、个性化素材或者服务推荐、内容和业务关系性学习等。

相关研究课题

1. 视频内容理解；

2. 时空多模态分析；

3. 个性化内容推荐。

返回目录

1.17 深度学习模型与物理模型的底层结合以及在农业监测中的应用

背景

该研究的主题，深度学习模型与物理模型的结合，是机器学习领域和多学科交叉应用领域最近几年呈现爆发态势的热门课题。在很多行业中，长年累积的专家知识储存在各类定量物理/机理模型中，而将这类模型中宝贵的知识和先进的深度学习方法结合，是提升纯数据驱动方法的潜在机会，体现在几个方面：1. 有助于让训练出的深度模型具备可解释性，且这种可解释性与已有的传统科学领域完全兼容；2. 利用物理模型中的领域知识替代标注数据，可以大量减少训练深度模型的数据量需求，也更接近人类智能利用已有知识快速学习新领域的过程。该研究将会尝试一系列模型结合的技术，例如物理约束的损失函数、物理模型转化为神经元连接等等，难度和实用度有所不同，保证既有基本产出也有钻研的空间。

在应用场景方面，将以农业监测为切入点，将筛选的农业机理模型和深度神经网络模块融合成一个端对端的可训练框架，创造模型数据同化的全新方法，提高模型预测结果的可靠性特别是物理上的合理性。一方面在当前的应用上，可以获得高效率的农地监测方

法，和农业金融紧密结合，服务于农作物制图、长势评估、灾害定损等一系列场景，在实地标注数据稀缺的情况下也能快速迭代出可靠的结果。另一方面在技术上，可以实验物理驱动的深度学习这一全新课题，为其它领域的机理模型和领域知识的利用积累经验。

目标

预期产出：

1. 高效农作物监测模型，通过物理模型与深度学习模型的结合，具备可解释性并且对标注数据需求较低，用于大范围产量和灾害监测

2. 该方法将是农业模型的全新突破，预计发表遥感学界顶尖期刊至少一篇（中科院SCI一区）

相关研究课题

1. 知识驱动的机器学习

2. 农业遥感

返回目录

1.18 视频检索中的特征量化聚合研究

背景

视频检索目前存在很多难点，在安全、推荐分发、版权业务中表现为消耗机器资源大、人工审核成本高、检索速度慢。原因在于为保证检索精度，模型提取的多帧、高维特征会直接导致运算量剧增、高时延检索。在多源业务场景下，丰富多样的视频内容对特征的抗干扰性也提出了更高的要求。视频特征量化（如深度哈希学习，深度乘积量化等）能够大幅度降低特征维度，有助于构建更加高效的轻量化视频检索模型，以及提升特征的学习和表达能力。视频特征聚合能够降低特征数量，增强时序信息的表达能力。另一

方面，视频特征度量学习通常能够拉近嵌入空间中的相似特征，提高检索准确性。通过在嵌入空间中学习特征的邻域结构信息， 进一步增强特征的鲁棒性和泛化性。

目标

本项目拟解决的技术问题主要从：1）如何进行合理的特征量化；2）如何利用时序信息进行特征聚合；3）如何学习邻域结构信息增强特征度量三个方面进行。从而实现低资源消耗的高精快速检索，以提降低成本，提升盈利能力。

预期产出：(1)1篇CCFA类文章(2)2个算法demo

相关研究课题

1. 视频检索

2. 紧凑特征

返回目录

2、软件工程

2.1 基于抽象解释的程序逻辑分析

背景

由于企业软件的功能性质普遍缺乏严格数学定义，往往依赖于人对代码和文档的理解，因此在开发，评审，测试中，都容易造成对功能性质的误解，考虑不全等安全隐患。另外，即使人对功能性质的理解完成正确，由于程序的状态空间巨大，可以认为是无穷的，也无法通过测试完全避免功能性缺陷。抽象解释，是把程序的具体语义，映射到开发人员关心的抽象语义上，把无穷的程序具体空间压缩为有穷的抽象空间，并提取出开发人员关心的性质。

目标

本课题从以下几个方面（包括但是不限于）探索抽象解释在程序逻辑分析的应用。

1.通过抽象解释，可以自动提取程序的重要逻辑关系，如所有资金相关的逻辑关系，从而帮助开发测试人员理解程序，提高其测试开发效率；

2.发现逻辑关系分母，指导其编写全量防御（攻击）规则；

3.对于简单逻辑关系，抽象解释可以自动生成防御规则，揭示风险。

相关研究课题

1. 抽象解释

2．形式化验证

返回目录

2.2 面向企业级微服务的高精度软件分析

背景

微服务系统由原来的单一系统演变为诸多子系统的联合，随着企业业务的日益庞杂，跨应用的服务调用链路也变得日益复杂和冗长。隐式调用、异步事件等微服务特性，也使得软件缺陷的定位和排查变得更加困难。因此迫切需要高精度的软件分析能力，将微服务系统白盒化。软件静态分析是在不运行软件的基础之上分析软件可能的行为，其优点是简单和全面，缺点是不精确。软件动态分析则是通过运行程序来观察和分析程序的行为，其优点是精确，但缺点是分析结果不全面。

目标

本课题从以下几个方面（包括但是不限于）探索面向企业级微服务的软件分析，动静结合技术，一方面保障分析可以尽可能的全面，保障软件缺陷能在研发态时尽早发现；另

一方面保障分析尽可能的精确，特别是在运行态时的故障定位更加精准，减少运维人力成本。**相关研究课题**

1. 程序分析

2．代码扫描

返回目录

2.3 路径驱动的自动故障注入技术（混沌工程技术）

背景

在微服务架构中，故障场景组合是非常多的。攻防体系下，详尽地检查每一种故障场景，其所需执行的故障注入测试次数，会随着故障种类和服务个数的增加，呈现几何级数增长。因此，需要自动获取并计算一套系统的无故障状态(稳态)，然后试图去回答“系统是如何达到稳态”，以及“整套逻辑链路中，能导致系统发生故障的穿透性故障点”。逻辑链条中的错误会将整个完整的防御链条击穿打破，导致系统无法到达最终稳态而发生故障；推演系统达到稳态的各种逻辑链条，组成图（graph）帮助找到那些最有价值的故障场景。

目标

本课题从以下几个方面（包括但是不限于）探索混沌工程在工业界的应用，

1．计算一套系统的无故障状态(稳态)，及构造逻辑关系图。

2．推演系统达到稳态的各种逻辑链条，帮助找到那些最有价值的故障场景

相关研究课题

1. 混沌工程

2．代码注入

返回目录

2.4 数据平台模糊测试

背景

实时数据平台是蚂蚁数据计算的基础设施，其系统可靠性与安全性至关重要。传统的数据库测试方法（面对单一系统）无法满足该平台的测试需求。比如传统方法自动化能力不足，测试效率低，代码覆盖率不足；面对实时数据平台复杂的数据链路和研发过程，传统方法缺乏对故障的定位能力。综上，实时数据平台需要新的可靠性保障技术解决上述问题。

目标

本课题目标：

1. 建立数据平台的模糊测试能力；
2. 提高系统的测试覆盖率；
3. 可定制SQL pattern的随机测试能力；
4. 实现故障分析定位。

相关研究课题

1. 数据库测试；
2. 模糊测试

返回目录

2.5 面向静态分析工具的模糊测试技术

背景

静态分析技术已在蚂蚁集团及阿里集团内部广泛使用于软件漏洞检测，防止软件漏洞在软件发布后带来的严重损失。然而，静态分析工具本身作为软件，其软件质量直接影响了其在软件漏洞检测中的能力，质量低的静态分析漏洞技术可能带来大量的误报和漏报。大量的误报导致软件工程师拒绝使用静态分析系统以及忽略隐藏在大量报告中的真实软件漏洞，大量的漏报则直接导致开发者忽略软件中的漏洞，带来软件安全隐患。测试静态分析技术是一项有挑战的工作，其主要困难有两点：（1）测试预言缺失，（2）测试程序多样性不足。为了充分保证静态分析系统在集团内的稳定、高效运行，从而保障软件质量、减小软件线上故障，因此申报该课题。

目标

本课题从以下两项技术展开研究

1. 基于数据流分析的程序随机生成技术。生成程序需要满足多方面的特征：首先，种子程序必须具有复杂性，以反映静态分析工具在复杂程序上的分析效果。其次，种子程序必须具有结构、语义多样性，保证静态分析工具的充分测试。最后，在保证程序复杂性、多样性的前提下，还要保证种子程序没有缺陷，以避免遗留缺陷对测试预言的干扰。

2. 基于符号执行的软件缺陷注入技术。缺陷注入需要满足多个条件：注入缺陷的有效性是制约生成的测试用例集质量的关键。缺陷注入位置是影响变异数据有效性的重要原因。首先，注入缺陷都应该能够被至少一个输入触发（反之，该用例无法有效评估静态分析工具的检测效果）；其次，注入缺陷应当不易被检测到（反之，该用例不具有挑战性）；最后，注入位置必须满足缺陷触发的各种先置条件（如依赖条件等）。

相关研究课题

1. 模糊测试

2．正确性验证

返回目录

2.6 面向Maven构建系统的依赖分析及优化研究

背景

蚂蚁的软件大量使用 Java 语言编写，并依赖 Maven 构建系统生成最终的产品。Java 项目通常依赖大量的第三方库，当版本冲突的相同第三方库出现在 classpath 中时，构建系统将选择加载其中之一并抛弃其他版本冲突的第三方库。当加载的第三方库无法覆盖项目所有需求时，依赖冲突问题将显现出来，导致项目运行失败、带来经济损失。不幸的是，目前 Maven 等构建工具只能检测非常简单的依赖冲突问题，一些没有检测出的依赖冲突问题由于不会导致运行时错误而经常被程序员忽略，成为项目在未来开发中的定时炸弹。为了减少软件构建导致的潜在漏洞，从而减少软件线上故障，因此申报该课题。

目标

1. 探索较为深入的Maven项目依赖冲突问题，提出系统化的解决方案，实现自动扫描工具
2. 提出自动化的修复方案，帮助开发者避免依赖冲突带来的编译时及运行时错误，提高研发效能

相关研究课题

1. 软件冲突解析

2. 构建自动化

返回目录

2.7 基于纯软件的高效且可扩展的正则表达式匹配算法研究

背景

互联网高速发展带给人们巨大便利的同时，网络空间安全也面临前所未有的挑战。非法数据流和恶意软件层出不穷，深度数据包检测是维护网络安全的有效手段，广泛用于路由器、网路入侵检测和防御、防火墙、7 层交换等各种设备上，用于恶意软件检测、攻击检测、流量监测、以及应用协议识别等。正则表达式由于其强大的表达能力、高效性，以及对攻击和恶意软件特征描述的灵活性，已经成为实现深度数据包检测最典型的实现方式。纯软件的实现方式更有利于正则表达式匹配算法的部署。如何实现基于纯软件的、高效的、且可扩展的正则表达式匹配算法是网络空间安全急需解决的问题。

目标

正则表达式有两种标准的实现方式：确定性有限状态自动机（DFA）和非确定性有限状态自动机（NFA），这两种实现方式各有优缺点，DFA效率高，但存在空间爆炸问题；NFA空间效率好，但对每一个输入字符需要进行多次查找，因此效率较低。本项目需要实现以下几个目标：

1. 算法时间的高效性：对输入数据包匹配实现在线性时间内完成，即达到DFA匹配效率。

2．算法空间的高效性：对给定的正则表达式实现仅采用与之规模成多项式的存储空间进行存储，使得正则表达式可以存储在SRAM中，实现高速处理。

3. 自动构建和自动构建的可扩展性：实现对给定的正则表达式集在存储器中的自动构建，使得正则表达式匹配在实际环境中更加容易部署。同时，正则表达式集的自动构建算法需要具备可扩展性，使得所设计的正则表达式匹配方案能应用与大规模正则表达式集上。

预期产出：

（1）1篇CCF-A类会议论文投稿；

（2）1+篇专利；

相关研究课题

1. 自动机；

2. 深度数据包检测。

返回目录

3、区块链

3.1 大规模广域网联盟链的网络治理和自适应研究

背景

大规模广域网的联盟链（大于 1000 节点）中，节点之间无法全部通过 p2p 的形式直连，一般会借助链上节点的应用层转发如 gossip 协议。在联盟链中还可以借助于链下基础设施如路由、网关等进行通信。在一个分布式、松散管理的网络中，需要解决节点连通性问题、消息可靠传输问题、时延问题、节点负载均衡问题等，并且随着链上节点的变更，网络拓扑结构也需要相应地调整和自适应。

目标

设计一种大规模广域网上的联盟链的网络自动治理协议，契合区块链共识算法的运行特性和要求。每个节点在不了解网络全局拓扑结构的情况下，能够自动组成区块链网络，消息能够高效地被全网广播，并且在有限节点故障的情况下保证可靠性传播。在节点组成变化的情况下，该协议能快速完成网络结构自动调整。

需要在专业领域发表 CCF-A 类或 B 类论文 1 篇，申请国内外专利 5 项。

相关研究课题

1. 网络协议

2. 共识算法

3. 分布式系统

返回目录

3.2 智能合约编程语言关键技术研究

背景

随着区块链安全事件的不断爆发，智能合约安全已经成为重灾区，设计一门智能合约语言，能够保证编写的智能合约保证资产的安全，将能够从根本上解决智能合约的资产安全问题。

目标

智能合约语言具有安全性，从根源上保证智能合约的资产安全；智能合约语言具有可用性，开发者能够方便使用合约编写安全的智能合约；智能合约语言具有可验证性，能够在方便的进行形式化验证，智能合约语言具有抽象性，能够很方便的表示各种数字资产，智能合约语言具有可扩展性，能够轻巧的迁移到不同的区块链平台，智能合约编程语言应当具备自动代码生成的能力，减少开发者需要编写的重复代码。需在相关专业领域发表CCF-A类论文一篇，申请国内外专利5件，以及相关研究成果具备落地到蚂蚁链的能力。

相关研究课题

1. 编程语言设计

2. 编译器

3. WebAssembly

返回目录

3.3 隐私应用安全审计

背景

开发者可以通过 TEE 等技术改造实现隐私计算算法与应用，在保护数据隐私前提下发挥数据价值。

但是在隐私计算的场景中，往往有多个参与方，会对第三方应用的隐私安全性存在担忧：应用本身是否存在漏洞或者恶意行为，进而会泄漏机密数据。比如应用中可能有隐藏的代码将数据通过 HTTPS 接口发送出去，达到窃取数据的目的。

目标

引入自动化审计的方法，结合静态扫描，模糊测试，形式化验证等技术，对应用的隐私安全性进行审计。需在相关专业领域发表CCF-A类论文一篇，申请国内外专利5件，以及相关研究成果具备落地到隐私计算平台的能力。

相关研究课题

1. 隐私安全
2. 代码安全

返回目录

3.4 零知识证明及其在区块链领域中应用的关键技术研究

背景

零知识证明(Zero Knowledge Proof，简称 ZKP)作为近年来的热点研究方向，与区块链技术领域有着高度紧密的联系。ZKP 结合区块链系统可以实现增强数据隐私保护能力，提升吞吐效率，降低存储成本等。从 DSL（Domain-Specific Language，简称 DSL）语言到底层证明系统的“电路”编译技术，到高效的、去除可信设置前置条件的证明系

统理论的演进，学术界和工业界进行了充分的研究，并不断有创新的技术和理论出现。

目标

本课题的目标：

1）理论方面优化、改进现有证明系统，提升证明和验证效率，最小化前置可信依赖。

2)基于ZKP基础理论和能力构建更加完善的应用体系，能够在隐私计算、可验证计算等领域有所创新和突破。

3)要求申请国内外专利5篇并满足以下条件之一：a)基础理论创新方面相关专业领域CCFA类论文一篇b)应用技术创新CCFA类论文1篇以及以及本课题相关研究成果具备落地至蚂蚁链的能力。

相关研究课题

1. 零知识证明

2. 隐私计算

返回目录

3.5 区块链结构化数据可验证查询关键技术研究

背景

区块链业务场景和规模持续增长，传统的拉块数据离线分析模式无法满足实时性要求，未来会逐步将分析迁移到链上进行。而链上提供结构化查询服务的节点不一定部署在各联盟参与方本地，对于各方访问必须提供有效的正确性和完备性证明。区别于传统可验证场景，中立的结构化查询节点、联盟参与方节点均为数据共同拥有者，一份数据能支持同时被多方独立验证。同时链本身可作为受信媒介，容许存放少量验证信息，以加速证明和校验过程。

目标

结合当下可验证查询领域成果，设计新的可验证数据结构，支持对各种常用SQL操作进行验证，能在较短的时间内完成初始化、生成证明，不引入太多额外的存储空间。需在相关专业领域发表CCF-A类论文一篇，申请国内外专利5件，以及相关研究成果具备落地到蚂蚁链的能力。

相关研究课题

1.可验证查询

返回目录

4、基础系统&数据库

4.1 智能实时数据平台相关研究

背景

实时数据平台（即虚拟化数仓）是蚂蚁实时计算的重要基础设施，承载蚂蚁重要业务的实时数据存储和计算任务。这一定位要求该系统满足高性能，高可用等要求。我们希望开展如下研究课题，包含但不限于：

1. 智能数据存储：利用机器学习相关技术，通过学习数据存储、访问的模式、优化大规模实时存储系统的性能和成本。

2. 智能物化发现：利用机器学习相关方法，通过分析大量复杂业务 SQL，高效发现物化视图，提高物化识别命中率，节省计算资源。

3. 智能计算优化：利用机器学习方法对分布式计算进行持续调度优化以及其他执行计划的调优。

4. 智能测试诊断：通过分析分布式计算存储系统中大量复杂调用链路中产生的日志和系统指标，自动化分析诊断链路中的问题，对线上查询进行自动化验证测试，

目标

针对上述一个或多个课题，结合最新研究成果，提出解决方案并落地（算法，工具，学术论文等），例如（但不限于）：

1. 探索建立基于数据的模式学习模型，设计相应的算法和数据结构以及索引方式，从而优化内存或者非易失性内存上的数据读写性能。

2. 设计机器学习的方法能在物化识别前，根据SQL和物化视图的特征进行物化视图筛选，以及设计算法预测SQL执行所需的计算、存储资源。

相关研究课题

1. 机器学习与数据仓库；

2．实时存储；

3. 性能优化

返回目录

4.2 代码自动分布式化方法研究

背景

公司的业务系统里有很多业务检测、条件判断的单机串行脚本程序，随着业务系统的发展，这些脚本的规模越来越大，处理的数据量也越来越大，早已经突破了单机所能承担的容量上限，执行的速度越来越慢，成了影响业务的 bottleneck。

目标

本课题是想通过找到一种通用的解决方法，能把单机的程序自动化的转化成分布式的形

式去执行。

1. 如何把一个单机系统通过静态、动态的分析自动的转化成一个分布式系统，达到执行时长或者吞吐上优化。

2. 如何把大量的单机脚本程序通过一定的统筹、编排方法达到执行时长或者吞吐上的优化，可以通过单线程、多线程、多机的优化。

相关研究课题

1. 分布式系统

2. 返回目录

4.3 面向隐私合规的信息流分析和控制技术研究

背景

近几年出台的隐私保护法规越来越多、越来越严，对隐私数据处理平台提出了极高的要求。具体地，我们需要确保隐私信息及其变换形态在平台的流动中不会直接或间接地泄露隐私，而且能检查并切断数据滥用。

目标

本课题探索针对隐私数据流的静态/动态分析和控制技术，具体目标是：

1. 确保数据在使用过程中都是经过授权的

2. 确保数据及其变换形态不会直接或间接地泄露出去

3. 研发工具原型，该工具能够针对给定系统生成用于说明该系统隐私合规性的分析和诊断报告

4. 针对具体系统（比如TEE中的数据处理软件）作为给定系统，来验证工具的适用性

5. 1+篇CCF-A论文

相关研究课题

1. 程序分析
2. 安全
3. 隐私保护
4. 数据滥用
5. 数据所有权

返回目录

4.4 自适应统一传输层技术研究

背景

随着蚂蚁集团的业务种类越多越多，包括：支付、保险、基金、股票、小游戏，区块链等，面临的网络环境也越来越复杂：从国内到海外，从一线城市到农村，从有线到无线，从 LTE 到 Wifi 等。不同的业务场景对传输有不同的诉求，比如股票的行情信息需要低时延、流媒体播放则更侧重高吞吐，不同的网络条件对传输也有不同的适应能力，比如无线场景有适用的传输控制算法，长肥网络也有自己最优的传输控制策略。然而，当前我们的传输层是一视同仁的，无法提供差异化的体验和服务，所以如何在蚂蚁多业务场景、复杂网络条件下提供统一的自适应最优传输能力是我们关注的问题。当前 QUIC 将传输层从内核态提到用户态，使得我们有机会提供一套统一的传输层来实现这个能力，然而其中如何对不同环境和业务进行建模，如何对算法进行抽象和挑选，都极具挑战，需要我们与学术界的一起进行研究。

目标

落地：

1. 一套基于 QUIC 的自适应传输控制框架，并在蚂蚁的接入层 spanner 上利用起来

2. 从传输层角度对底层网络、业务类型的感知、归类、抽象建模的方法

3. 一套针对业务、网路进行传输算法匹配的策略

学术：

1. CCF 优秀B类及以上相关会议论文一篇

2. IETF 草案一篇

3. 专利一项

相关研究课题

1. QUIC 协议

2. 拥塞控制算法

返回目录

4.5 基于RDMA的高效分布式事务处理机制的研究

背景

无共享（shared nothing）数据库采用两阶段提交协议实现跨机分布式事务，每次事务涉及多次网络交互，一种可能的思路是采用 RDMA 技术来降低分布式事务的延迟、提升吞吐。

目标

本研究的目标是基于RDMA技术优化跨机分布式事务的性能。研究成果包括：

1. demo系统；

2. CCF-A或CCF-B类论文一篇

相关研究课题

1. 新硬件

2. 分布式系统

返回目录

4.6 基于FPGA/GPU的存储引擎加速研究

背景

LSM 存储引擎执行 Compaction 操作时性能大幅下降，并引起系统抖动。可以通过 FPGA/GPU 等新硬件解决 LSM 存储引擎 Compaction 性能瓶颈，提升性价比。

目标

本研究的目标是通过新硬件对存储引擎加速 ，并探索如何解决LSM引擎持续平滑写入的技术难题。

研究成果包括：

1. demo系统；

2. CCF-A或CCF-B类论文一篇

相关研究课题

1. 新硬件

2. 存储系统

返回目录

4.7 面向HTAP数据库的工作负载隔离机制的研究

背景

HTAP 数据库在同一套引擎同时处理 OLTP 和 OLAP 混合负载，一个必然面临的问题是

OLTP 和 OLAP 工作负载的隔离，避免 OLAP 大查询影响 OLTP 小查询。这就涉及到在数据库内部实现 OLTP 和 OLAP 的资源隔离，包括 CPU、IO、网络，等等。

目标

本研究的目标是探索数据库内部实现不同查询请求资源隔离的方案。

研究成果包括：

1. demo系统

2. CCF-A或CCF-B类论文一篇

相关研究课题

1. 资源隔离

2. OLAP

返回目录

4.8 面向HTAP数据库的的新型存储引擎的研究

背景

HTAP 数据库在同一套引擎同时处理 OLTP 和 OLAP 混合负载，OLTP 往往采用行式存储，OLTP 采用列式存储。为了实现 HTAP 混合负载处理，需要设计新型存储引擎，能够兼顾 OLTP 和 OLAP 两种工作负载，并尽可能降低存储成本。

目标

本研究的目标是探索采用同一套引擎处理HTAP混合负载的新型存储引擎技术方案。

研究成果包括：

1. demo系统

2. CCF-A或CCF-B类论文一篇

相关研究课题

1. 资源隔离

2. 存储系统

返回目录

4.9 数据库存储成本优化研究

背景

蚂蚁集团的全部业务底层都采用 OceanBase 数据库，服务器数量较多，存储成本较高。

期望能够结合业务的特性，降低数据存储成本，包括提升数据压缩比、冷热数据分离、

更加合理的存储层调度策略等等。

目标

本研究的目标是降低蚂蚁OceanBase数据库存储成本。

研究成果包括：

1. demo系统

2. CCF-A或CCF-B类论文一篇

相关研究课题

1. 机器学习

2. 存储系统

返回目录

4.10 单机多级调度系统的研究

背景

目前，单机系统里面通常涉及多级任务调度，1、以 Linux　CFS 作为第一级调度；2、许多编程语言（类似 Go、Rust、Kotlin 等）都提供了协程调度器；3、在云计算背景下，通常中间还有一层 guest　kernel 引入的调度（比如 Linux 虚拟机的 CFS）。从性能和资源效率的角度，我们需要在繁忙时尽可能多地利用 multi-core 资源，又必须在闲暇时尽快让出 CPU 让其它混布应用来运行。除此之外，如何兼顾各种应用的特点、考虑各种硬件架构特性，提出更加定制化的、轻量的调度系统设计，是一项重要且有意义的研究。

目标

通过本研究预计产出：

1）设计并开发适合云原生场景的协同调度系统，要求在整体利用率和时延上都优于现有系统；

2）产出1篇CCF-A论文。

相关研究课题

1. 调度优化

2. 性能优化

返回目录

4.11 应用镜像加载、存储和传输技术研究

背景

容器镜像是云原生技术栈不可变基础设施的重要组成部分，传统的镜像格式存在诸多问题，不可按需加载，不可重建等，传统的镜像中心需要应付大规模并发启动的问题。目前我们已经实现了一套新的镜像格式来帮助容器快速启动并可以按需加载，同时我们通过 p2p 来实现规模分发。　但是缺少对这些镜像数据的合理使用，比如如何挖掘镜像之

间的数据关联，冷热程度，进而进一步优化全局的镜像存储，镜像预热，镜像瘦身等。

我们还需要针对特定的 runtime，e.g.　JVM，来探索优化应用启动加载镜像里面软件包，类库的方案。最后，我们还需要探索自适应的 p2p 分发算法，从而适应不同的业务场景

目标

通过本研究预计产出：

(一) 落地上：

1. 蚂蚁生产的镜像数据统计，以及针对典型应用的预热和加载优化

2. JVM对镜像中jar包的加载优化

(二)影响力上：

1. CCF 优秀B类及以上相关会议论文一篇

2. 专利两项

相关研究课题

1. 基于镜像统计数据的镜像加载和镜像存储优化

2. 更优的p2p分发算法

3. 针对JVM的jar包加载的优化

返回目录

4.12 分布式动态决策调度系统研究

背景

目前蚂蚁数据中心调度系统是中心化调度架构，即所有资源分配和业务编排都通过一个中心调度组件进行决策，而随着单数据中心规模越来越大以及大量 serverless 特征业务被统一调度，中心决策在高并发下性能吞吐和调度延迟已无法满足业务需求。同时，随

着数据中心利用率越来越高，中心调度器需要对整个数据中心动态运行数据进行实时加工用作决策参考，由于数据计算量大和中心组件算力瓶颈，导致调度质量下降而引发业务运行稳定性问题。

通过建设分布式调度决策算法和系统架构，将部分调度决策下移至节点组件与中心决策形成互补，可有效地解决单一中心调度决策瓶颈问题，吞吐性能会有成倍增长，调度质量也会明显提升。而引入分布式调度决策则会引起一致性问题导致调度成功率下降，另外，如何将大量动态数据有效地应用于分布式调度系统，做到数据中心成本、性能、稳定三者的平衡，都将是本研究课题的难点和挑战。如何研究出一套适用于蚂蚁大规模数据中心的分布式动态决策调度系统是当前亟需且有意义的一项研究。

目标

通过本研究预计产出：

1）一套适用于蚂蚁生产级别的分布式决策调度系统，吞吐性能做到10k/s以上，相较于当前中心决策提升50倍；调度质量优于现有k8s调度系统。

2）一套毫秒级的中心快速决策搜索算法；一套分布式节点调度决策算法和调度优先级体系。

3）产出1篇CCF-A论文。

相关研究课题

1. 大规模数据中心调度系统
2. 分布式调度决策算法
3. 调度系统性能优化

返回目录

5、安全

5.1 移动端数据隐私保护技术研究

背景

随着互联网银行业务的高速发展，越来越多的业务场景需要将数据、模型、算法等放到移动端使用，越来越多的重要业务操作也会由端侧发起，这给端安全带来了巨大的挑战，如何保证端数据可信，防范被篡改或劫持等风险，成为十分重要的安全诉求。本项目旨在设计并实现一套完善的移动端安全解决方案，包括但不限于端侧的数据采集防护、模型保护算法、篡改或劫持等威胁的感知能力等。

目标

主要两个目标：

1）根据研究的算法场景，给出满足要求的实现代码以及技术白皮书

2）一篇CCF-A类会议

相关研究课题

1.隐私保护

2.机器学习

返回目录

5.2 更为鲁棒的设备身份篡改识别方案

背景

目前我们面临：

1）设备身份的攻防研究/设备稳定性研究还存在提升空间；

2）灰产对设备持续攻击篡改，风险较为严峻；

3）数据隐私大背景下，终端数据采集趋于最小化。

借助本课题研究，希望能：在数据最小化的情况下，借助攻防技术，建设更为鲁棒的设备身份篡改识别方案。

目标

1. 建设更为鲁棒的设备身份篡改识别方案，稳定性提升；在作弊、赌博等违规违禁场景的风险识别有明显增益；

2. 学术产出：发表高质量学术论文、产出相关专利等。

相关研究课题

1. 隐私保护下的攻防研究

返回目录

5.3 JAVA 开放式动态反序列化Gadget Chains自动化挖掘

背景

ODD（开放式动态反序列化）概念由蚂蚁基础安全负责人岚刻提出，是近年来在 JAVA 领域非常流行的一种设计模式，这种设计存在天然的重大缺陷，通常情况下，攻击者只需要几行代码，即可低门槛攻击并完全控制一台使用 ODD 设计的机器，进一步盗取企业和用户的敏感数据如囊中取物。因此，我们希望通过程序分析和 AI 等综合技术运用，构建高准确度和高覆盖率的 JAVA 开放式反序列化 Gadget Chains 自动化挖掘技术，更好地帮助提升 JAVA 基础设施安全性，如果实践效果好，还进一步通过开源技术能力，赋能全社会。

目标

1．JAVA反序列化Gadget Chains自动化挖掘技术和程序分析技术；

2．发表高质量学术论文、产出相关专利或检测工具引擎等。

相关研究课题

1. 程序分析技术

2. 漏洞自动化挖掘技术

返回目录

5.4 基于轻量级隐私保护方案进行横纵向联邦、联邦迁移学习及隐私计算

背景

随着《中华人民共和国数据安全法》出台，个人和企业数据权益、安全、及合理利用等问题的关注度空前提高。国际上对数据隐私的保护在 2018 年欧盟《通用数据保护条例》出台后也日趋严谨。打造数据与知识驱动的智能风控引擎保护用户和商户免受安全风险、推动国内、国际生态合作伙伴对风控联防联控的同时，隐私保护是我们首要的关注点。现有的一些隐私保护解决方案是通过密码学技术（同态加密或安全多方计算）实现，因大量的带宽和计算开销在大规模实际应用中广泛部署比较困难；业务的发展推进了蚂蚁安全对横切纵切同时存在的联邦迁移学习的需求。如何打破数据孤岛，满足数据不出域的情况下进行合作建模和实时本地预测，以及在合作中解决公平性和可解释性等开放性问题，是本课题亟需解决的问题。

目标

1. 理论研究：通过本项目的研究，将系统地发展横纵向联邦，和联邦迁移学习中关于安全和隐私的理论和方法;

2. 项目落地：应用于蚂蚁大安全丰富的横纵向联邦，联邦迁移场景和有隐私计算需求的

场景；

3. 学术产出：发表高质量学术论文、产出相关专利等。

相关研究课题

1. 隐私计算

2. 联邦学习

返回目录

5.5 基于大规模图计算的异常识别检测和风险挖掘

背景

当前风险攻防从显性风险，转向更加隐蔽、复杂、结构性的社会生态的风险（如洗钱、赌博、营销作弊、泛欺诈等），给对整个数字生活生态带来巨大危害的同时，也对风控算法能力提出了更高的要求。

借助本研究项目，我们希望能：

（1）进一步提升风控基于复杂网络的异常识别检测能力，打造异常资金流预警、异常行为挖掘等能力，直接助力反洗钱、反赌博、反欺诈、营销反作弊等多个场景。

（2）针对没有标签反馈的场景，研发新的算法方案储备。

目标

1. 沉淀相应算法组件；

2. 发表高质量学术论文、产出相关专利等；

3. 产生业务级价值增益；

4. 提出符合业务需要的更优方案算法。

相关研究课题

1. 图计算
2. 全图风控
3. 风险挖掘

返回目录

5.6 CV模型安全性研究

背景

近几年，CV 模型大放异彩，已经被广泛应用在娱乐、安防、金融等领域，现代的 CV 模型主要基于深度学习，而深度学习本身的脆弱性也为 CV 模型带来了不同于传统软件的安全问题。具体而言，深度学习面临着对抗样本、模型窃取、数据投毒等的威胁，对预测结果也总是给出不实际的置信度，本项目主要是研究 CV 模型的上述安全问题的可操作可落地的测试、攻击和防御方法。

目标

一篇CCF-A类会议

相关研究课题

1. deepfake攻防
2. 对抗机器学习
3. 对抗样本攻防
4. 模型窃取攻防

返回目录

5.7 高精度鲁棒相机指纹技术研究

背景

图像指纹指的是照片在成像时会保留相机的硬件噪声（传感器的固定偏差、随机白噪声等）以及图像处理软件带入的软件处理噪声（可以理解为某种滤波器），传统的图像指纹技术包括基于 PRNU 和度量学习的图像指纹提取，这些技术都存在精度问题，难以非常精确的区分某个特定硬件拍拍摄的图像。本项目目标研究一种高精度的摄像头硬件指纹提取方法，可以实现相机指纹识别准确率 95%+。

目标

一篇CCF-A类会议

相关研究课题

1. 图像噪声

2. PS检测

3. deepfake伪造检测

返回目录

5.8 深度学习模型隐私安全技术研究

背景

深度学习隐私安全考虑的是模型训练、预测过程中涉及到的数据隐私安全以及模型本身的 IP 资产安全，本项目希望研究 NLP 模型的隐私安全问题，包括：1）NLP 模型训练过程中的成员推断攻击&防御；以及 2）NLP 模型输出 Embedding 的逆向攻击&防御。

目标

一篇CCF-A类会议

相关研究课题

1. 联邦机器学习

2. 隐私保护机器学习

3. 成员推断攻击&防御

返回目录

5.9 基于人工智能的恶意通信识别

背景

随着全球数字化发展，恶意软件（包括但不限于挖矿、勒索、DDOS、间谍木马等）获利的方式越来越便捷，其种类和数量也愈发庞大。在网络安全领域里，识别恶意软件有多种途径，其中在网络流量下进行检测发现，是一个便捷高效的方式。传统方法主要基于流量的统计特性和以及特殊通信协议的典型特征，难以发现未知的恶意软件类型。

目标

本课题的目标：在网络流量和进程行为数据下，以恶意软件通信为视角，研究其通信模型，实现通用识别恶意软件通信的模型算法。

相关研究课题

1. 网络威胁识别

2. 入侵检测算法

返回目录