

## 技术发明奖公示信息

一、项目名称：智能物联网数据安全处理关键技术及应用

### 二、提名者及提名意见

提名者：陕西省教育厅

提名意见：推进数据资源安全融合与应用，实现数据要素价值的有效释放，是建设数字中国的重要目标。面向广域分布的海量物联数据资源，亟需开展数据安全整合能力建设，构建开放物联环境下数据安全融合与应用技术体系，提升数据要素价值发现与高效利用能力，为推进国家大数据战略发展提供有力支撑。

该项目攻克了开放物联环境下数据融合与应用系统的“可信融合-安全服务-高效跨域”多个公认难题，形成了多源物联数据的按需保护与可信融合技术、差异化平台服务模型的安全高效应用技术、密态数据的高效跨域流转与安全管控技术等完全自主知识产权的创新成果。

该项目选题新颖，研究起点高，对技术进步和产业发展有重要的引领作用，符合陕西省技术发明奖等奖提名条件。

提名该项目为陕西省技术发明奖二等奖。

### 三、项目简介

针对开放物联环境下数据融合与应用存在的数据安全问题，本项目聚焦开放物联环境下数据安全共享与服务的核心问题，在多源物联数据的按需保护与可信融合、差异化平台服务模型的安全高效应用、密态数据的高效跨域流转与安全管控等方面取得原

始创新，构建了开放物联环境下数据安全融合与应用理论的技术体系，在海康威视、百度、海信、华为等企业开展了大规模应用，为开放物联数据的价值发现与释放提供重要的技术保障。

本项目的创新集中在以下三个方面。

### （1）多源物联数据的按需保护与可信融合

本项目提出了机器学习隐私泄露量化模型和分布式数据安全聚合框架，发明了隐私量化的回归模型定制加扰、参数特性驱动的神经网络裁剪训练、基于运算归约的非交互协作训练、融合对抗样本的鲁棒强化集构建等方法，解决了密态物联数据安全融合效能下降、毒化样本影响下模型鲁棒性降低等问题，实现了开放物联环境下多源数据的安全可信融合。

### （2）差异化平台服务模型的安全高效应用

本项目提出了开放物联环境下机器学习模型的可靠部署和资源受限场景下模型服务的高效提供框架，发明了安全算法自适应的模型传输、抗模型提取攻击的动态模型响应加扰方法，设计了双向安全的快速医疗诊断、可信模块辅助的轻量级生物特征识别方案，解决了资源受限的物联场景下设备易遭受物理攻击、模型服务资源消耗高的问题，实现了差异化服务平台中安全高效模型服务的提供。

### （3）密态数据的高效跨域流转和安全管控

本项目提出了国家商用密码算法的通用优化机制与跨域密钥管理框架。发明了多层协作的 SM4 算法自适应优化方法和高

吞吐数据动态切分的大数模逆计算优化方法，设计了跨域密钥一致性校验与安全同步方案，解决了低时延、高并发场景下国密算法实现的性能优化和跨域密钥管理等问题，实现了开放物联环境下敏感数据安全流转和加密密钥安全管控。

#### 四、客观评价

(1) 本项目依托的科技创新 2030-“新一代人工智能”重大项目“视频感知新一代人工智能开放创新平台”通过科技部高技术中心组织的专家组现场验收，验收意见指出“项目构建了从数据服务、算法训练、模型管理、云边部署、开源开放到行业应用的一站式视频感知开放平台，开放了一批 AI 能力，服务了大量中小微企业，满足了传统产业面向复杂场景识别、检测、认知等视频感知的需求”。

(2) 本项目依托的陕西省重点研发计划项目“面向互联网服务的隐私保护关键技术”通过陕西省科技厅组织的专家组现场验收，验收意见指出“提出了隐私计算框架，构建了涵盖典型互联网服务的实用化隐私保护技术体系，研发了数据计算和发布隐私保护工具集，完成技术验证和示范应用”。

#### 五、应用情况和效益

本项目的研究成果应用于海康威视、百度公司、海信集团、陕西航信、交大一附院等单位的系列产品中，支撑智慧安防、语音助手、智慧家居、税务信息化、智慧医疗等领域中的数据安全融合、处理与流转，推动开放物联环境下数据安全处理相关技术

的发展与应用，服务数字中国建设。

本项目经成果转化，支撑研发了海康威视国家新一代人工智能开放创新平台、视维数据人工智能安全生产监控系统和天特信实时 **Geo-IP** 库查询平台等模型安全训练与服务产品，累积生产模型超过 8 万个，服务超过 2 万家企业；支撑研制了海康威视 **DS-SCS** 系列密码机、**HikHSM-P** 系列密码卡、**HSCM300-GS/S** 密码模块等二十余款国家密码产品二级认证产品，作为海康威视智慧安防系统的核心组成部分，服务全国三十余个省、市、自治区、特别行政区的公共安全和平安城市建设。取得了显著的社会经济效益。

六、主要知识产权目录

序号	知识产权类别	知识产权具体名称	国家（地区）	授权号	权利人	发明人
1	发明专利	一种并行环境下高吞吐量的模逆计算方法及系统	中国	ZL202110090167.1	西安电子科技大学	朱辉；黄煜坤；李晖；刘兴东；李临风
2	发明专利	一种深度神经网络的虚拟对抗训练方法、装置及设备	中国	ZL202110352167.4	杭州海康威视数字技术股份有限公司	王滨；王星；张峰；万里；周少鹏；钱亚冠
3	发明专利	面向物联网服务隐私保护声纹识别方法及系统、移动终端	中国	ZL201910267624.2	西安电子科技大学	朱辉；李祁；寇笑语；李晖；张紫铃；杨晓鹏
4	发明专利	一种安全高效的分布式 k-d 树构建方法	中国	ZL202311437767.6	西安电子科技大学	郑艳冬；王枫为；张松年；朱辉

5	发明专利	一种隐私保护的神经网络多方协作无损训练方法及系统	中国	ZL202110560355.6	西安电子科技大学;中移(苏州)软件技术有限公司	朱辉; 赵家奇; 胡国靖; 王枫为; 季琰; 徐奇
6	发明专利	一种模型数据的处理方法、装置及设备	中国	ZL202010268456.1	杭州海康威视数字技术股份有限公司	王滨; 陈学明
7	发明专利	多因子通用可组合认证及服务授权方法、通信服务系统	中国	ZL201910060302.0	西安电子科技大学	曹进; 罗玓榕; 李晖; 赵兴文
8	发明专利	一种基于 GPU 的高吞吐量 SM2 数字签名计算系统及方法	中国	ZL202110866751.1	西安电子科技大学	朱辉; 黄煜坤; 李晖; 刘兴东; 王枫为; 李临风
9	发明专利	基于 FPGA 的高速 SM4 密码模组实现方法及装置	中国	ZL202310721393.4	杭州海康威视数字技术股份有限公司	王滨; 吴程涛; 陈加栋; 王星
10	发明专利	一种基于 GPU 的 Paillier 同态加解密计算方法及系统	中国	ZL202211017789.2	西安电子科技大学	朱辉; 李临风; 郑艳冬; 王枫为; 李晖; 薛行策; 黄煜坤

## 七、主要完成人情况

完成人	工作单位
朱辉	西安电子科技大学
王滨	杭州海康威视数字技术股份有限公司
王枫为	西安电子科技大学
郑艳冬	西安电子科技大学

张松年	西安电子科技大学
曹进	西安电子科技大学

## 八、主要完成单位情况

第一完成单位：西安电子科技大学

第二完成单位：杭州海康威视数字技术股份有限公司

## 九、完成人合作关系说明

朱辉、郑艳冬、张松年、王枫为合作发表论文“PGSim: Efficient and Privacy-Preserving Graph Similarity Query Over Encrypted Data in Cloud”;

朱辉、郑艳冬、张松年、王枫为合作完成发明专利《一种安全高效的分布式 k-d 树构建方法》

朱辉、王滨合作完成成果应用“开放物联环境下数据安全融合关键技术及应用”;

朱辉、曹进合作发表论文“Information dissemination model for social media with constant updates”。