浙江工业大学“青年英才支持计划”
申 请 表

所 在 部 门：计 算 机 科 学 与 技 术 学 院
（盖章）

申 报 人：朱添田

申报类别：☐A 类　　☑B 类

填表日期　　2023 年 1 月　10　日

一、申请人简况

基本情况	姓　　名	朱添田	性别	男	出生年月	1992.01
	专业技术职务	副教授	最终学位及授予学校			博士 浙江大学
	所在学科、团队	软件工程、网络空间安全科研团队			联系电话	17858610074
	研究方向	网络空间安全			电子邮箱	ttzhu@zjut.edu.cn

二、申请理由：

2.1 对照“青年英才支持计划”申报条件所提出的申请理由：

☑正常申报　　☐单独推荐　　☐单列计划

申请单独推荐，需列出团队完成本聘期学校重大（重点）发展目标的内容和时间及申请人对团队贡献；单列计划和正常申报需列出符合申报条件的具体条目内容、时间、排名等成果信息。

作为第一（通讯）作者发表高水平学术论文：

[1] **Tiantian Zhu**, Zhengqiu Weng, Qijie Song, Yuan Chen, Qiang Liu, Yan Chen, Tieming Chen*. ESPIALCOG: General, Efficient and Robust Mobile User Implicit Authentication in Noisy Environment[J]. *IEEE Transactions on Mobile Computing*, 21(2), 2022: 555-572. (**CCF A**)

[2] **Tiantian Zhu**, Lei Fu, Qiang Liu, Zi Lin, Yan Chen*, Tieming Chen. One Cycle Attack: Fool Sensor-based Personal Gait Authentication with Clustering[J]. *IEEE Transactions on Information Forensics & Security*, 16, 2020: 553-568. (**CCF A**)

[3] **Tiantian Zhu***, Zhengyang Qu, Haitao Xu, Jingsi Zhang, Zhengyue Shao, Yan Chen, Sandeep Prabhakar, Jianfeng Yang. RiskCog: Unobtrusive Real-time User Authentication on Mobile Devices in the Wild[J]. *IEEE Transactions on Mobile Computing*, 19(2), 2019: 466-483. (**CCF A**)

[4] **Tiantian Zhu**, Zhengqiu Weng, Guolang Chen*, Lei Fu. A Hybrid Deep Learning System for Real-world Mobile User Authentication Using Motion Sensors[J]. *Sensors*, 20(14), 2020: 3879.

[5] **Tiantian Zhu**, Jiayu Wang, Linqi Ruan, Chunlin Xiong, Jinkai Yu, Yaosheng Li, Yan Chen, Mingqi Lv, Tieming Chen*. General, Efficient, and Real-time Data Compaction Strategy for APT Forensic Analysis[J]. *IEEE Transactions on Information Forensics and Security*, 16, 2021: 3312-3325. (**CCF A**)

[6] **Tiantian Zhu**, Hongyu Gao, Yi Yang, Kai Bu, Yan Chen*, Doug Downey, Kathy Lee, Alok N. Choudhary. Beating the Artificial Chaos: Fighting OSN Spam using Its Own Templates[J]. *IEEE/ACM Transactions on Networking*, 24(6), 2016: 3856-3869. (**CCF A**)

[7] **Tiantian Zhu**, Zhengqiu Weng*, Lei Fu, Linqi Ruan. A Web Shell Detection Method Based on Multiview Feature Fusion. *Applied Sciences*, 10(18), 2020: 6274.

[8] Lei Fu, Ke Yan, **Tiantian Zhu***. PowerCog: A Practical Method for Recognizing Power Quality Disturbances Accurately in a Noisy Environment[J]. *IEEE Transactions on Industrial Informatics*, 18 (5), 2021: 3105-3113.

[9] Lei Fu, **Tiantian Zhu***, Kai Zhu, Yiling Yang. Condition Monitoring for the Roller Bearings of Wind Turbines under Variable Working Conditions Based on the Fisher Score and Permutation Entropy[J]. *Energies*, 12(16), 2019: 3085.

[10] Lei Fu, Yiling Yang, Xiaolong Yao, Xufen Jiao and **Tiantian Zhu***. A Regional Photovoltaic Output Prediction Method Based on Hierarchical Clustering and the mRMR Criterion[J]. *Energies*, 12(20), 2019: 3817.

[11] LeiFu, **Tiantian Zhu***, Guobing Pan, Sihan Chen, Qi Zhong and Yanding Wei. Power Quality Disturbance Recognition Using VMD-Based Feature Extraction and Heuristic Feature Selection[J]. *Applied Sciences*, 9(22), 2019: 4901.

主持Ⅴ类（理工科）及以上纵向科研项目：

1.面向 APT 智能检测的攻击链数据建模与分析关键技术研究（62002324），国家自然科学基金项目-青年/纵向/V 类，2021.01-2023.12，排名：1/1

2.2 近 5 年主要教书育人业绩、学术成绩、创新成果及其社会效益（限 800 字）

1.在教书育人方面，本人参与浙江省委宣传部科学思维拍摄，将科学思维与网络安全结合提高学生主动发现与解决问题的能力；指导网络空间安全学生实验室获得浙江工业大学最美实验室；通过讲座的方式提高本科生对高等数学的重视程度，通过实际案例激发学生对数学的热爱；指导本科生参与科研项目并撰写发明专利；帮助学生树立正确的就业观，通过各种渠道准确地向用人单位推荐学生，已帮助学生成功就业 5 人。此外，为深入学习贯彻习近平总书记总体国家安全观，落实党中央关于加强大中小学国家安全教育文件精神，本人积极参与学校《国家安全》课程建设。承担“网络安全”模块课程教学大纲的制定与修订、课程教学内容研讨、课程思政案例的研讨以及整个课程教学的组织与实施。此外，作为学校“青说青听”青年科学家理论宣讲团成员进行宣讲，对学生进行思政教育，传播正能量。

2.在科研学术方面，**共发表论文 20 余篇，其中第一作者 5 篇，通讯作者 4 篇**；作为**第一主编和第一副主编出版网络安全相关教材共 2 部**。

其中，标志性成果的创新性、科学价值或社会经济意义如下：

（1）**移动设备用户动态认证研究**。

探索继第一代移动设备用户认证技术（基于密码、图案等知识的用户认证）与第二代移动设备用户认证技术（基于指纹、人脸的静态生物认证）之后，新一代移动设备用户认证技术（基于用户动态行为）。实现零信任、无感知的场景下准确高效的用户认证，并进行移动设备用户认证鲁棒性研究。已有研究工作在上千数量级的用户测试中达到 95%以上的精度。发表 CCF A 类期刊三篇，相关**研究得到了国家自然科学基金面上项目的资助**。**北京大学信息科学技术学院王平教授**在发表的论文中对本人所研究的针对不同步态模型的攻击进行了分析与肯定，表明隐私信息的泄露以及学习模型的脆弱性都将会导致严重的后果。韩国科学技术院 **KAIST** 的 **UICHIN LEE** 教授在发表的论文中论述了申请人所使用的基于上下文系统传感数据、以及用户交互数据的用户身份认证系统的先进性，并突出了此类隐式无感、用户体验友好的移动设备用户认证技术具有重要的研究价值与现实意义。**上述相关研究成果已被应用集成到腾讯手机管家、支付宝风险大脑作为关键的风险控制因素之一**。

（2）**终端高级持续威胁检测研究**。

对云网边端存在的高级持续性威胁进行动态分析与监控，研究多源异构数据的高效采集、重构和压缩方法，针对持久化、欺诈、敏感文件/库的读取和逃避等可疑行为与特征建立相应的检测点，研究面向 APT 智能检测的攻击链上下文信息聚合框架，并且尽可能地检测未知攻击，提高攻击的门槛和成本，从而降低 APT 攻击的危害和造成的损失。发表 CCF A 类期刊两篇，相关**研究得到了国家自然科学基金重点项目及青年项目、浙江省自然科学基金探索项目的资助**。上述成果对应的相关数据采集及压缩系统在美国国家网络空间靶场进行了四次大规模数据采集。靶场环境由专门团队负责搭建，模拟了真实的 APT 攻击环境，包括正常网络流量、正常用户行为、以及部分 ATT&CK 模型

中的攻击技术。成果对应的检测框架成功在靶场实战中检测到所有的攻击，**效果优于 Endgame**。在靶场实战时，为了模拟真实的攻击场景，攻击方的攻击时间、攻击技术及手段是防御方事先未知的。相关数据采集及检测系统**已在网商银行、浙江能源集团有限公司、中国联通温州分公司等企业应用**。
3.在科研项目方面，共主持纵向 2 项，横向 11 项；**主持项目到校总经费 280 万元**。

2.3 近 5 年主要教学工作

学年	讲授主要课程	授课对象及人数	本人承担内容
2019/2020（2）	网络攻防技术	2017 网络工程等，26 人	主讲
2020/2021（1）	信息安全基础	2018 计算机科学与技术等，41 人	主讲
2020/2021（1）	信息与网络安全基础	2018 数据科学与大数据技术等，5 人	主讲
2020/2021（2）	计算机安全基础	2018 软件工程(中外合作办学)，4 人	主讲
2021/2022（1）	物联网信息安全技术	2019 物联网工程，37 人	主讲

2.4 近 5 年主要科研项目（5 项以内）

序号	项 目 名 称（项目编号）	经费(万元)	起止年月	负责或参加	项目来源
1	面向APT智能检测的攻击链数据建模与分析关键技术研究（62002324）	27.96	2021.01-2023.12	负责	国家自然科学基金项目-青年
2	面向高级网络攻击的样本增强及智能分析方法研究（LQ21F020016）	10	2021.01-2023.12	负责	浙江省自然科学基金项目-探索项目
3	安全生产区块链关键技术研究及应用-能源安全生产区块链关键技术研究及应用平台研制（2021C01117）	234	2021.01-2023.12	参加	浙江省科技计划项目-重点研发
4	面向APT网络攻击链的智能检测与溯源方法及关键技术研究（U1936215）	45	2020.01-2023.12	参加	国家自然科学基金项

					目-联合重点子课题
5	防跌落安全带野外救援监测硬件装置（SH1190210165）	30	2021.03-2023.03	负责	金华捷科工具有限公司

2.5 近 5 年以第一作者/通讯作者发表的论文（5 篇以内）

序号	论文题目	刊物名称	发表时间	简要评价（创新点、贡献性及意义）
1	One Cycle Attack: Fool Sensor-Based Personal Gait Authentication With Clustering（第一作者）	IEEE Transactions on Information Forensics and Security, ISSN:1556-6013, 16	2020.08	针对现有的步态生物认证模型，构建了一种新型攻击方法，即“单周期”攻击来绕过大部分市面上已有的步态认证模型。同时，提出了一种基于模态的上下文行为语义分析方法来增强模型的鲁棒性，从而来对抗此类攻击。
2	General, Efficient, and Real-Time Data Compaction Strategy for APT Forensic Analysis（第一作者）	IEEE Transactions on Information Forensics and Security, ISSN:1556-6013, 16	2021.04	针对现有 APT 攻击中的存在数据爆炸问题，提出了一种多源异构数据的高效采集和重构方法，为后续 APT 攻击智能检测提供轻量且完整有效的数据内容。
3	EspialCog: General, Efficient and Robust Mobile User Implicit Authentication in Noisy Environment(第一作者）	IEEE Transactions on Mobile Computing, ISSN: 1536-1233, 21 (2)	2022.02	探索继第一代移动设备用户认证技术（基于密码、图案等知识的用户认证）与第二代移动设备用户认证技术（基于指纹、人脸的静态生物认证）之后，新一代移动设备用户认证技术（基于用户动态行为）。实现零信任、无感知的场景下准确高效的用户认证。
4	A Web Shell Detection Method Based on Multiview Feature Fusion（第一作者）	APPLIED SCIENCES-BASEL, ISSN: 2076-3417, 10 (18)	2020.09	以 Web Shell 为入口的攻击愈发广泛，提出了一种多视角融合的 Web Shell 检测方法，同时满足高精度与高效率的要求。
5	A Hybrid Deep Learning System for Real-World Mobile User Authentication Using Motion	SENSORS, ISSN:1424-8220, 20(14)	2020.07	针对现有运动传感器存在的但是现有的方法存在着噪音处理能力差、可用性不足、特征提取覆盖率低等一系列问题，提出了一个适用于真实复杂环境的混合深度学习系统进行移动用户认证。

	Sensors（第一作者）					

2.6 近 5 年主要出版著作情况（5 项以内）

序号	著作题目	作者排序	出版社	出版时间	书号	类别（教材、专著、译著）
1	Web 应用安全与防护	1/4，主编	电子工业出版社	2022.04.01	ISBN: 9787121432316	教材
2	数据安全	3/6，第一副主编	电子工业出版社	2021.04.01	ISBN: 9787121409776	教材

2.7 近 5 年授权发明专利（5 项以内）

序号	专利名称	专利类别	专利号	授权时间	授权国家（地区）	转化情况
1	一种基于生成对抗网络的恶意文件智能分析方法	发明专利	ZL202110339736.1	2022.06.28	中国	5 万
2	一种基于 Snort 和 OpenFlow 启发式诱导 APT 攻击引入蜜罐的方法	发明专利	ZL202110577612.7	2022.06.24	中国	无
3	一种基于系统审计日志与打分机制的 webshell 实时检测方法	发明专利	ZL202011454037.3	2022.06.28	中国	无
4	一种基于元学习的远程访问木马智能分析方法	发明专利	ZL202110379282.0	2022.06.28	中国	无
5	一种跨平台多主机联合日志压缩方法	发明专利	ZL202010903265.8	2022.06.28	中国	无

2.8 近 5 年获奖情况（5 项以内）

序号	获奖项目名称	奖励类别	等级	授予单位	获奖时间	本人排名
1	ACM 杭州新星奖	地市级	地市级	ACM 杭州分会	2021.09	1/1

三、支持期内工作任务规划

要求计划具体，目标明确（至少新增一项标志性任务，具体参照《浙江工业大学“青年英才支持计划”实施办法》第四章目标与考核第八条，限一页）

3.1 标志性任务

人才：冲击省青拔、省杰青等D类及以上人才培养计划/项目（入选或上会）

项目：理工科：主持IV类及以上纵向科研项目1项。

3.2 工作任务

学科建设：
积极参加网络工程、软件工程学科平台建设。

科学研究：
主持国家自然科学基金面上项目1项，主持浙江省杰出青年科学基金项目1项，冲击国家优青和国家重点研发计划青年科学家项目。年均发表CCF A类以上高水平论文2篇，冲击网络安全四大顶会，在网络攻击智能检测领域发表ESI高被引有影响力的根论文，年均申请发明专利20项，授权发明专利转化2项。

平台建设：
利用当前平台（包括复杂网络攻击智能检测浙江省工程研究中心、浙江省网络空间安全创新研究中心）对外交流研讨，组织学会会议。

团队建设：
依托复杂网络攻击智能检测浙江省工程研究中心完善“人机物融合空间的云网边端协同安全创新试验场”的建设。

人才培养：
主编出版网络空间安全教材1本，培养研究生20人，指导学生“互联网+”竞赛并获金/银奖。

其他：
积极完成学校学院布置的任务。

四、资格审核

本人承诺：本人提出“青年英才支持计划”申请，愿意遵守相关政策规定。本表内所填内容属实，所提供的材料客观真实。 本人签字： 日期：　　年　　月　　日
所在单位师德考察意见
（包括申请人的思想政治表现、师德师风等情况。） 所在单位党委（总支）书记签字： （加盖党委公章） 日期：　　年　　月　　日
所在单位资格审查意见
经审核，上述材料均内容真实，与证明材料原件相符。 审核人签字：　　所在单位负责人签字： （加盖单位公章） 日期：　　年　　月　　日
学校意见
负责人签章： （加盖学校公章） 日期：　　年　　月　　日