计算机学院科研团队情况介绍表

团队名称	ZJU NESA Lab（https://nesa.zju.edu.cn/）			团队负责人	纪守领
联 系 人	张旭鸿	Email	xuhongnever@gmail.com	电话	0571-87951819

团队致力于人工智能与安全、数据驱动安全、软件与系统安全、计算机视觉、大数据挖掘与分析、多媒体理解研究与应用。

浙江大学网络系统安全与隐私实验室（Network SystEm Security & PrivAcy Lab，NESA Lab）立足于信息安全、人工智能、数据分析与网络系统的交叉科学领域，致力于研究相关基础理论、关键技术与应用系统。实验室负责人为国家级人才计划入选者纪守领研究员，现有教授/研究员 8 人、研究助理 2 人，博士生 12 人，硕士生 12 人，本科生 8 人，**当前主要研究方向包括：人工智能安全、数据驱动安全、软件与系统安全、计算机视觉、大数据挖掘与分析、多媒体理解**，在 ACM/IEEE Trans. ToN、TISSEC、TDSC、TIFS 和 IEEE S&P、ACM CCS、USENIX Security、NDSS、CVPR、KDD、ICDE、AAAI、IJCAI 等权威期刊和会议上发表论文 150 余篇，包括 CCF A 类论文 100 余篇，获最佳论文奖 10 项。

实验室承担多项国家和省部级科研项目，包括国家自然科学基金重点项目和面上项目、国家重点研发计划项目（课题）、国家预研重点项目、国家创新特区项目、浙江省杰青项目、浙江省重点研发计划项目等。实验室与多家企业公司具有深入良好合作关系，包括阿里巴巴、蚂蚁金服、腾讯、华为、绿盟、启明星辰，研发的多个系统在大型商业平台上获得应用。

实验室具有优良的国际合作关系，与普林斯顿大学、佐治亚理工学院、伊利诺伊大学——香槟分校、弗吉尼亚大学、宾夕法尼亚州立大学、悉尼大学、IBM T. J. Watson 研究中心的多位教授/研究员具有长期稳定的合作关系，实验室每年有多位同学被选派至上述学校继续深造、访学研究。

实验室具有丰富的竞赛经验，曾荣获 2014、2015、2016、2018 年世界大学生超级计算机竞赛总决赛一等奖及 2016 年高性能计算冠军奖、ACM Multimedia (MM) 2016 最佳挑战奖（Grand Challenge Award）、2015 年微软 Bing 图像检索挑战赛第一名、2016 年微软视频到语言挑战赛第四名、NIST TRECVID 2016 视频与文本匹配任务第一名、NIST TRECVID 2017 视频与文本匹配任务第一名、ICCV LSMDC 2017 电影检索/标注比赛第二名、2018 HULU

视频推荐竞赛第一名、2018 全球迅雷区块链应用开发大赛第一名等。

团队主要成员

纪守领研究员获美国佐治亚理工学院电子与计算机工程博士学位、佐治亚州立大学计算机科学博士学位，现任浙江大学“百人计划”研究员、博士生导师、浙江大学滨江研究院国产信创中心副主任，兼任佐治亚理工学院 Research Faculty，入选多个国家和省部级人才工程。先后主持国家自然科学基金重点项目和面上项目、国家重点研发计划项目（课题）、国家预研重点项目、创新特区项目、浙江省杰青项目、浙江省重点研发计划项目、阿里巴巴科研基金、蚂蚁金服科研基金、华为科研基金、CCF-腾讯“犀牛鸟”科研基金、CCF-绿盟“鲲鹏”科研基金、CCF-启明星辰“鸿雁”科研基金等多项，作为技术负责人或项目骨干，参加美国 NSF 项目 8 项。发表论文 100 余篇，包括 IEEE S&P, ACM CCS, USENIX Security, KDD 等 CCF A 类论文 60 余篇，出版英文专编著 4 部。申请专利 30 余项，研制了深度学习模型安全与评估系统 DeepSec、大数据驱动的反欺诈系统 ATF、新型对抗性验证码生成系统 aCAPTCHA (advCAPTCHA)、自适应知识驱动的模糊测试系统 MOPT、模糊测试评估平台 UNIFUZZ、物联网固件漏洞挖掘系统 iFIZZ 等多个系统。其中，多个系统已被部署应用于拥有千万用户级以上的商业大平台，相关成果被 CCTV、人民网、新华网、凤凰网等二十余家媒体报道，产生了较大经济和社会效益。MOPT 在 Google 模糊测试公开评测平台上位列第一名(截至 2021 年 1 月);相关漏洞挖掘系统在实际系统和软件中发现漏洞 400 余个，包括工业 PLC 漏洞数十个，IoT 设备固件漏洞 100 余个，IoT 协议漏洞（缺陷）100 余个，已获得 CVE 100 余个，形成了较大影响力。曾获美国著名高校弗吉尼亚理工学院（Virginia Tech)、凯斯西储大学(Case Western Reserve University)、里海大学(Lehigh University)、佐治亚大学（University of Georgia）终身教职系列（Tenure-Track）助理教授职位，获中国国家优秀自费留学生奖（中国海外留学生最高奖)、8 项最佳/优秀论文奖、GSU 杰出研究奖、ELSEVIER 高引论文奖、《计算机研究与发展》高引论文奖、浙江大学先进工作者、“个推”青年创新奖等。

张旭鸿研究员，于 2017 年获美国中佛罗里达大学计算机工程博士学位，浙江大学滨江研究院“百人计划”研究员、服务安全与可靠性研究中心主任。长期致力于分布式大数据系统以及分析，人工智能系统以及算法的研究，博士期间作为项目技术骨干，参与了 4

个美国NSF项目的申请与研发工作。目前已发表国际高水平论文10余篇(如VLDB，ICDE，TPDS IEEE Transactions on Big Data，HPDC，IPDPS，JPDC等)。在LinkedIn任职期间，作为团队核心成员，成功领导研发了LinkedIn新一代端到端大规模自动化分布式机器学习平台，得到公司各部门（包括朋友推荐，工作推荐，人才搜索，广告推荐等组）的广泛采用，使公司内部机器学习的生产效率提高一倍。同时负责公司内部深度学习平台的设计与研发工作，成功让公司多项产品由深度学习模型驱动，为公司带来巨大收益。提出的亿级ID表征学习算法，成功应用于LinkedIn工作推荐服务，在不损失精度的情况下，比上一代模型体积减少近100倍，消耗的训练资源减少近100倍。相关成果申请3项美国专利，并开源一套人工智能数据处理系统。

陈建海副教授，获浙江大学计算机科学与技术博士学位，2018全球区块链专利创新人才百人榜，浙江大学智能计算与系统实验室Incas-lab区块链负责人，云象区块链首席技术官（CTO），浙江大学超算队负责人。澳大利亚斯威本科技大学访问学者。IEEE、ACM、CCF会员，CCF区块链专委会委员。研究领域涉及云计算超算、区块链应用、人工智能，擅长区块链应用安全，高性能计算与并行应用优化，云计算调度与优化，近似算法与博弈论运用，以及数据挖掘等。区块链方面，智能合约设计器Designer项目获2018全球迅雷区块链应用开发大赛第一名（全球500多支参赛队）。智能合约在线服务平台SCOSER项目获2018区块链Hackathon大赛第二名。Tako智能合约在线服务平台获得2019建行杯大学生互联网+创新创业大赛银奖。高性能计算方面，率领浙大超算队2014~2016年与2018年四次冲入ASC世界大学生超级计算机竞赛总决赛获一等奖，获2019ASC世界大学生超算竞赛二等奖，获2016世界最高Linpack计算性能冠军奖，以12.03TFlops的成绩打破并创下新的最高计算性能世界纪录。负责区块链、高性能计算方面的重点研发项目子课题2项，浙江省重点研发计划项目子课题1项，参与完成多项云计算虚拟化相关的国家科技部支撑计划、国家基金以及企业合作项目超过10项。累计发表SCI/EI论文20+篇，申请授权专利超过40项。

Raheem Beyah教授（合作研究）. Dr. Raheem Beyah serves as Georgia Tech's Vice President for Interdisciplinary Research, Executive Director of the Online Masters of Cybersecurity program (OMS Cybersecurity), and is the Motorola Foundation Professor in School of Electrical and Computer Engineering. He has held several other leadership roles including chairing ECE's Computer Systems and Software

Technical Interest Group (2015-2017), serving as ECE's Associate Chair for Strategic Initiatives and Innovation (2016-2018), and serving as the Interim Steve W. Chaddick ECE School Chair during the 2018-2019 academic year. He leads the Communications Assurance and Performance Group (CAP) and is affiliated with the Institute for Information Security & Privacy (IISP). He is also the Co-Founder of Fortiphyd Logic, Inc. His research interests include Network security and monitoring, Cyber-physical Systems Security, Network traffic characterization and performance, and Critical infrastructure security. He received the National Science Foundation CAREER award in 2009 and was selected for DARPA's Computer Science Study Panel in 2010. He is a member of AAAS, ASEE, and a lifetime member of NSBE, a senior member of IEEE, and an ACM Distinguished Scientist.

董建锋教授（合作研究），于 2018 年获得浙江大学计算机科学与技术专业博士学位，浙江大学-悉尼大学计算机学院联合培养博士。董博士现任浙江工商大学计算机与信息工程学院研究员，浙江大学 NESA 实验室研究员，阿里巴巴-浙江大学前沿技术联合研究中心访问学者。研究方向包括多媒体理解，计算机视觉。曾获 2013 年浙江省优秀本科毕业生、2018 年浙江大学优秀博士毕业生等奖项。目前已发表国际高水平论文 30 余篇，其中以第一作者/通讯作者在计算机学会 CCF A 类期刊/会议 TKDE、CVPR、AAAI、ACM Multimedia、SIGIR 等发表论文 10 篇。其成果获得国际同行认可，近五年所发表的论文累计被引用 480 余次，一篇一作论文被引超过 100 次，两篇一作论文引用超过 50 次；曾获得多媒体领域顶级会议 ACM Multimedia 2016 Grand Challenge Award， CSS 2019 最佳论文奖。董博士目前是 IEEE TPAMI，IEEE TNNLS，IEEE TMM， ACM TOMM，Elsevier Neurocomputing，Multimedia System，AAAI，ACM Multimedia 等国际重要期刊和会议论文的审稿人。董博士主持国家级和省部级项目共计 4 项，包括国家重点研发计划项目子课题，国家自然科学基金青年项目，浙江省自然科学基金青年项目等；作为技术负责人参与国家级和省部级项目共计 4 项。

林昶廷研究员，2018 年毕业于浙江大学计算机科学与技术学院并获工学博士学位，现为浙江大学滨江研究院“百人计划”研究员。以项目主持人身份承担国家和省部级项目 3 项。博士期间曾参与 973 国家重大基础课题、863 国家重大项目课题以及国家重点研发计划重点项目等。研究方向包括网络空间安全，人工智能，软件定义网络，物联网以及区块

链技术，以第一作者或通信作者已发表国际高水平论文 10 余篇。林昶廷研究员是 IEEE Transactions on Industrial Informatics (TII)、Cybersecurity 等国际重要期刊和会议论文的审稿人。

承担的主要项目

项目名称	项目性质及来源
面向攻击链的 APT 智能检测与溯源方法及关键技术研究	国家自然科学基金重点项目
***技术	重点项目
***研究	重点项目
人工智能安全与鲁棒性	国家重点项目
物联网固件漏洞挖掘与隐私防护技术研究	中央高校基础研究基金
可信人工智能模型与关键技术	华为科研项目
人工智能驱动的模糊测试技术研究	中央高校基础研究基金
海量多源异构数据的使用授权与鉴权体系研究	国家自然科学基金重点项目
机器学习安全与隐私保护研究	浙江省杰青项目
人工智能安全研究	国家重点研发计划项目-课题
基于电商大数据的反作弊对抗学习理论与关键技术	国家自然科学基金面上项目
区块链关键技术研究与技术交易应用	浙江省科技计划项目
工控拟态安全网关研发与应用-工控网关拟态防御技术研究	浙江省科技计划项目
深度神经网络的模型可解释性研究项目	华为科研项目
高维稀疏数据对抗学习	蚂蚁金服科研项目
终端系统安全证明验证测试服务	中科院软件所
基于模糊测试的智能化漏洞挖掘技术研究	CCF-绿盟“鲲鹏”科研基金项目
基于增量学习的异常行为检测理论与关键技术研究	CCF-启明星辰“鸿雁”科研基金
基于大规模图挖掘的对抗学习理论与关键技术研究	阿里巴巴集团研究项目
社交反欺诈模型研究	拍拍贷

社交大数据隐私保护理论与技术	CCF-腾讯“犀牛鸟”科研基金

主要研究成果：

请见： https://nesa.zju.edu.cn/