

同行专家业内评价意见书编号： 20250854450

附件1

浙江工程师学院（浙江大学工程师学院） 同行专家业内评价意见书

姓名： 肖昌斌

学号： 22260717

申报工程师职称专业类别（领域）： 电子信息

浙江工程师学院（浙江大学工程师学院）制

2025年06月04日

填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位+申报工程师职称专业类别(领域)4位+流水号3位，共11位。

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1. 对本专业基础理论知识和专业技术知识掌握情况(不少于200字)

本人肖昌斌，目前就职于某金融单位，长期从事网络安全相关研发工作，具备扎实的计算机科学与网络信息安全专业背景。近年来，我专注于基于深度学习的恶意流量检测技术研究，致力于将人工智能方法应用于金融行业中的网络安全威胁识别与防御领域，提升金融信息系统在面对新型攻击手段时的安全防护能力。

在此过程中，我系统掌握了以下基础理论知识和专业技术知识：

一、基础及专业知识

1.1

数学基础：深入理解概率论、统计学、线性代数等数学基础知识，为深度学习算法提供坚实支撑。

1.2

计算机科学与技术：具备扎实的数据结构、算法分析能力，熟悉操作系统原理、网络协议及其工作方式，特别是TCP/IP协议栈、网络拓扑结构等，为理解和开发恶意流量检测系统提供技术支持。

1.3

机器学习与深度学习：精通监督学习、无监督学习以及强化学习的基本理论和方法；深入了解各种神经网络架构（如CNNs, RNNs, LSTMs等），并能灵活应用于恶意流量特征提取和分类任务中。

1.4

网络攻防技术：熟练掌握常见的网络攻击手法（如DDoS攻击、SQL注入、跨站脚本攻击、中间人攻击、0day漏洞利用等）及其防御策略，具备实战化攻防对抗经验。

1.5

恶意流量防护：深入了解恶意流量的特点与行为模式，包括但不限于僵尸网络、钓鱼网站、恶意软件传播、C2通信、加密隧道攻击等，并掌握相应的检测与防护技术，能够通过流量特征建模进行精准识别。

1.6

网络空间安全：对网络空间安全的整体框架有深刻的理解，包括网络安全政策法规、风险评估、应急响应机制等，能够从宏观角度规划和实施网络安全策略。

1.7

网络流量分析技术：熟悉主流网络流量采集与分析工具（如Wireshark、tcpdump、Zeek/Bro、ELK等），具备基于原始流量包（PCAP）进行深度解析与异常行为建模的能力。

1.8

安全防护体系构建：掌握防火墙、IDS/IPS、WAF、SIEM、EDR等典型安全设备或系统的部署

与联动机制，具备构建纵深防御体系的技术能力。

1.9

高级持续性威胁（APT）检测：了解APT攻击生命周期与战术行为（TTPs），能够结合日志分析、流量特征与威胁情报实现高级攻击的发现与溯源。

1.10

人文社科知识：了解网络安全相关的法律法规、政策制度，以及数据隐私保护原则，确保研究成果合法合规。

二、行业知识

2.1

新技术应用：紧跟行业动态，关注最新的深度学习模型和技术在网络安全领域的应用进展，如使用生成对抗网络（GANs）生成训练样本以增强模型泛化能力，特别关注其在网络空间安全中的具体应用场景。

2.2 行业标准与规范：熟悉国际国内关于网络安全的技术标准和规范，如ISO/IEC 27001信息安全管理标准，NIST网络安全框架，《网络安全法》《数据安全法》等相关法律法规，并能结合实际需求进行灵活应用。

2.3

先进技术前沿：持续跟踪全球范围内恶意流量检测技术的发展趋势，包括但不限于新型攻击手法、防御策略及解决方案，特别是在网络空间安全领域的新发展，如量子加密技术在网络通信中的应用。

2.4

攻防演练与红蓝对抗经验：参与过多次真实环境下的攻防演练与渗透测试项目，具备模拟攻击者行为进行系统脆弱性验证的能力，同时也能构建有效的防御策略以提升整体安全水位。

2.5

成本开销：在设计和实施恶意流量检测系统时，充分考虑硬件采购、软件授权、运维管理等方面的成本开销，优化资源配置，降低总体拥有成本（TCO）。

2.6

方法可行性：针对不同规模和需求的金融单位，选择合适的深度学习模型和技术方案，确保其在实际环境中具有良好的可行性和可操作性。

2.7

能耗与效率：考虑到数据中心的能耗问题，采用高效的计算资源分配策略，优化GPU/CPU利用率，减少不必要的能源消耗。

2.8

高可用性与冗余性：设计高可用性的系统架构，通过负载均衡、故障转移、数据备份等机制提高系统的可靠性和稳定性，确保业务连续性。

2.9

硬件国产化与替代性：探索使用国产化的硬件设备（如CPU、GPU），保证供应链的安全性和自主可控性，同时评估不同品牌硬件之间的兼容性和性能差异，确保系统的稳定运行。

2.10 显卡交火与多卡配置：根据实际需求配置多块显卡（如NVIDIA SLI或AMD CrossFire），以提高计算能力和处理速度，满足大规模数据分析和实时检测的需求。

三、跨专业领域知识

面对日益复杂的网络安全威胁，为满足金融信息系统对安全防护的高标准要求，通过融合人工智能、网络安全、硬件工程与金融业务四大领域的知识，构建了适用于金融场景的恶意流量检测与防御系统。在基于深度学习的恶意流量检测技术研究过程中，深入掌握了人工智能算法模型的设计与优化方法，并结合网络安全领域的攻击特征分析与防御机制，构建了高度适应性的智能检测系统。具体而言，利用监督学习、无监督学习以及强化学习等技术，实现了对各类恶意流量的精准识别与分类。与此同时，在模型部署与实际应用中充分考虑了硬件层面的因素，包括但不限于GPU加速计算、国产化芯片替代方案、显卡交火配置及资源调度优化，确保所开发的检测系统能够在生产环境中高效运行并具备良好的扩展性。例如，通过采用国产化CPU和GPU解决方案，不仅提升了系统的自主可控性，还有效降低了整体拥有成本（TCO）。此外，根据金融行业的特性和需求，将金融系统的业务逻辑、数据特性与网络行为模式纳入模型设计考量之中，增强了检测系统的针对性与实用性。通过与安恒信息的战略合作，结合前沿的网络安全技术与金融行业特有的合规性、稳定性要求，共同研发了面向金融场景的恶意流量识别模型，并在真实网络环境中进行了测试与验证，证明该模型在高并发、低延迟、强安全等多重约束条件下具有卓越的性能表现。这种跨人工智能、网络安全、硬件工程与金融业务的深度融合，不仅显著提升了在复杂工程问题解决中的综合能力，也为金融行业在网络空间安全建设方面提供了创新的技术路径和发展思路。

此外，在研究生阶段，我的实践考核成绩评定为“优秀”，并荣获“2024年度优秀研究生”称号。硕士论文经三位评审专家评议，获得两个A级评价、一个B级评价（修改后答辩），顺利通过学位论文答辩，体现了我在科研与工程实践方面的综合能力与学术水平。

2. 工程实践的经历(不少于200字)

项目实践1. 基于深度学习的恶意流量与加密流量检测系统

合作单位：安恒信息

时间：2022.11-2024.01

角色：安全研发工程师

关键技术：

基于LSTM与ResNet-18的混合深度学习模型设计

针对加密流量检测中传统方法难以获取有效特征的问题，提出一种融合时序行为分析与协议语义建模的新型混合神经网络架构。该模型采用LSTM提取网络流量的时序行为特征，结合ResNet-

18对TLS握手过程中的协议字段进行图像化语义建模，实现对加密流量（如HTTPS隐蔽隧道）的多维度特征融合识别，显著提升在无明文内容场景下的检测准确率。

项目实践2. 基于类增量学习的恶意流量动态检测系统

合作单位：安恒信息

时间：2023.06-2024.08

角色：安全研发工程师

关键技术：

针对恶意流量检测场景中新型攻击类型持续演进、传统静态模型难以适应的问题，提出一种基于双分支网络结构的类增量学习框架。该框架采用特征共享与分类解耦相结合的设计思路，主干网络提取通用流量表征特征，两个独立分类分支分别处理已知类别与新出现类别，实现模型在不遗忘历史知识的前提下，逐步学习新增恶意流量类型的识别能力。

项目实践3. 基于信创UOS国产操作系统与华为国产GPU的恶意流量检测系统

时间：2024.10-2025.01

角色：安全研发工程师

关键技术：

针对金融行业对系统安全性与自主可控性的高要求，基于统信UOS（UnionTech OS）国产操作系统平台完成恶意流量检测系统的部署与加固。通过内核模块裁剪、SELinux策略定制、服务最小化配置等方式，构建低依赖、高隔离、强审计的安全运行环境，保障检测系统在国产操作系统上的稳定性和合规性。

华为昇腾GPU异构计算加速与模型移植优化在国产硬件适配方面，完成了深度学习模型从主流NVIDIA

GPU向华为昇腾系列AI加速卡的迁移与性能调优。采用华为CANN异构计算架构和MindSpore深度学习框架，重构原有检测模型的算子实现方式，并结合混合精度训练、模型量化等手段提升推理效率，实现在国产GPU平台下的高性能运行。进一步地，结合UOS系统特性与昇腾GPU的异构计算优势，开展软硬一体化性能调优工作，包括内存管理机制优化、线程调度策略改进、数据流并行化处理等，显著提升恶意流量检测模型的吞吐量与响应速度，在满足金融级实时检测需求的同时，兼顾能效比与资源利用率。

3. 在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字）

在金融科技与网络安全深度融合的数字化浪潮中，金融基础设施面临前所未有的安全挑战。传统恶意流量检测系统普遍依赖静态模型与集中式部署，难以适应新型攻击手段快速迭代、加密流量占比持续上升、边缘设备资源受限等现实问题。特别是在金融行业的核心业务边缘节点，如支付网关、API服务接口、交易前置机等场景中，网络环境复杂多变，且对系统的实时性、稳定性、资源占用率均有严苛要求。在此背景下，如何构建一种具备动态学习能力、轻量化部署架构、高效推理性能并符合国家信创标准的智能检测体系，成为亟待解决的关键工程难题。

本项目积极响应国家“信息技术应用创新”发展战略，围绕“资源约束下的持续学习”这一核心命题，融合计算机网络、人工智能、电子信息与金融支付等多学科知识，构建了一套面向金融边缘计算环境的恶意流量动态检测系统。该系统不仅实现了对新类型攻击行为的快速响应，更有效缓解了模型更新滞后、灾难性遗忘严重、部署成本高昂等传统方案中的瓶颈问题，同时全面适配国产化软硬件生态，具备良好的可推广性与行业示范意义。

面对金融边缘节点普遍采用低功耗嵌入式CPU架构的实际限制，项目团队设计并实现了一套端到端的轻量化类增量学习解决方案。系统底层模型基于ResNet-18结构构建，具备强大的特征提取能力，在保留其优秀表征能力的基础上，通过通道剪枝、参数压缩与INT8量化等优化手段，将模型参数量控制在合理范围（约9.6MB），并在部署阶

段进一步压缩至2.1MB以内。整个训练与推理过程均运行于国产化算力平台之上，包括但不限于华为昇腾AI加速卡（Atlas系列）、鲲鹏CPU（如Hi1710）等，充分满足金融行业对核心软硬件自主可控的要求。

操作系统层面，项目全面适配统信UOS V2.0及后续版本，完成了从开发环境搭建、中间件配置、模型部署到服务运行的全栈国产化迁移。所有模块均通过兼容性测试，运行稳定，性能表现良好，为未来在更大范围内替代国外操作系统奠定了坚实基础。此外，系统还集成了国产密码算法SM2/SM4/SM9等，用于数据传输加密、身份认证与完整性校验，确保在流量采集、样本上传、模型下发等各环节的数据安全性与合规性，全面满足《商用密码管理条例》和金融监管机构对信息安全的强制要求。

在模型架构层面，项目创新性地提出了双分支类增量学习框架：主干网络负责通用特征提取，两个独立分类头分别用于已知类别识别与新增类别学习，解耦模型更新路径，使单次训练时间由传统全量训练的3小时缩短至40分钟，极大提升了模型迭代效率。此外，系统集成了知识蒸馏机制与原型记忆回放策略，通过保留旧模型输出的概率分布作为软标签，引导新模型在学习新类别的过程中保持对历史类别的识别一致性，将旧类知识保持率提升至98%以上，同时将存储开销压缩70%，有效解决了灾难性遗忘问题与样本存储压力之间的矛盾。

针对边缘计算场景下算力资源受限的实际情况，项目进一步开展了模型轻量化与推理优化工作。结合TensorFlow Lite-Micro推理引擎进行部署优化，成功实现在无GPU支持的CPU设备上单核运行时平均推理延迟低于10ms，内存峰值占用控制在4.8GB以内，完全满足金融业务场景中对毫秒级响应与低资源消耗的双重需求。特别值得注意的是，在高并发场景下，通过优化后的模型能够在确保高精度的同时，提供稳定的实时响应，极大地提高了系统的可用性和可靠性。

为了实现系统的持续演进与智能化管理，项目还构建了一套完整的自动化增量训练流水线。该流程打通了从“可疑流量捕获—主动学习标注—增量训练—OTA热更新”的闭环链条，形成一套具备自我进化能力的智能安全防护体系。各边缘节点通过HTTPS加密通道上传可疑样本至中心平台，经校验与归一化处理后进入训练流程。系统结合不确定性采样机制与人工审核平台，优先对置信度较低的样本进行标注，大幅降低人工成本达90%以上；同时引入SHA-256完整性校验与一键回滚机制，确保模型更新过程的安全性可控性，服务中断时间控制在500ms以内，保障了关键业务的连续性。此外，系统还配备了详细的日志记录与监控机制，便于运维人员及时发现并解决问题，进一步增强了系统的健壮性。

系统已在某金融单位测试环境中的多个边缘网关设备完成部署验证，覆盖银行交易、支付接口、API服务等多个高敏感业务场景。实测数据显示，系统检测准确率（AUC）由原有全量训练模型的0.972提升至0.985，对加密流量的检测性能较传统载荷分析方法提升36%，推理延迟稳定控制在10ms以内，充分满足金融监管机构对安全系统“高精度、低延迟、强鲁棒”的严格要求。更重要的是，系统在国产芯片、操作系统、密码算法等方面均实现了深度适配与稳定运行，标志着我国在金融安全领域自主可控能力建设方面取得了实质性进展。

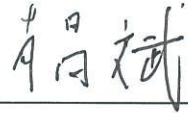
综上所述，本项目通过跨领域技术融合与工程实践创新，成功构建了一套具备持续学习能力的轻量化恶意流量检测系统，有效解决了金融边缘节点资源受限、模型更新滞后、灾难性遗忘严重等关键技术难题。其在实际应用中展现出良好的性能表现与部署可行性，不仅为金融行业提供了可靠的安全保障方案，也为物联网、工业互联网等资源受限场景下的动态安全防护提供了可复用的技术范式 and 工程参考。项目的实施体现了人工智能、边缘计算与业务场景深度融合的巨大潜力，彰显了多技术领域协同创新在解决复杂工程问题中的核心价值，具有广泛的应用前景与推广意义。特别是在国家大力推进信息技术应用创新战略的背景下，本项目在国产软硬件适配、国密算法应用、安全可控体系建设等方面所取得的成果，具有重要的示范作用和社会价值。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】

1. 公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
Adaptive and Lightweight Intrusive Traffic Detection Method Based on Deep Learning under Evolving Network Threats	会议论文	2025年01月23日	2024 IEEE International Conference on Electronics and Information Technology (EIT)	1/3	EI会议收录

2. 其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

(三) 在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 82 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 10 年（要求1年及以上） 考核成绩： 88 分
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！	
申报人签名： 	

二、日常表现考核评价及申报材料审核公示结果

日常表现 考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： <input checked="" type="checkbox"/> 优秀 <input type="checkbox"/> 良好 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 德育导师/定向生所在工作单位分管领导签字（公章）：2025年6月4日
申报材料 审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： <input type="checkbox"/> 通过 <input type="checkbox"/> 不通过（具体原因： 工程师学院教学管理办公室审核签字（公章）：

浙江 大学 研究生 院
攻读非全日制硕士学位研究生成绩表

学号：22260717	姓名：肖昌斌	性别：男	学院：工程师学院	专业：电子信息	学制：2.5年						
毕业时最低应获：24.0学分		已获得：24.0学分		入学年月：2022-09	毕业年月：						
学位证书号：			毕业证书号：		授予学位：						
学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2022-2023学年秋冬学期	工程伦理		2.0	80	公共学位课	2022-2023学年秋冬学期	自然辩证法概论		1.0	88	公共学位课
2022-2023学年冬季学期	通信网络		2.0	79	跨专业课	2022-2023学年春夏学期	移动互联网智能设备应用设计与实践		3.0	84	专业学位课
2022-2023学年冬季学期	通信与网络安全		2.0	87	跨专业课	2022-2023学年春夏学期	现代集成电路工艺前沿技术		2.0	88	专业学位课
2022-2023学年秋冬学期	信息安全前沿技术与研究方法论		2.0	82	跨专业课	2022-2023学年春夏学期	研究生英语		2.0	61	公共学位课
2022-2023学年秋冬学期	电子与信息工程技术管理		2.0	85	专业学位课	2022-2023学年春夏学期	新时代中国特色社会主义思想理论与实践		2.0	88	公共学位课
2022-2023学年秋冬学期	标准与知识产权		2.0	87	专业选修课	2022-2023学年春夏学期	科技写作		2.0	74	专业学位课

说明：1. 研究生课程按课种统计学分，不区分必修、选修。

说明：1. 研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2. 备注中“*”表示重修课程。

学院成绩校核章：
成绩校核人：张梦依
打印日期：2025-06-03 (60) HFF
成绩校核章

检索证明文件

《Ei Compendex》收录证明

经检索“Engineering Village”，下述论文被《Ei Compendex》收录。（检索时间：2025年1月23日）。

<RECORD 1>
Accession number:20250217660489
Title:Adaptive and Lightweight Intrusive Traffic Detection Method Based on Deep Learning under Evolving Network Threats
Authors:Xiao, Changbin (1); Xie, Lei (2); Chen, Huifang (2)
Author affiliation:(1) Zhejiang University, College of Engineering, Hangzhou, China; (2) Zhejiang University, College of Information Science and Electronic Engineering, Hangzhou, China
Corresponding author:Xie, Lei(xiel@zju.edu.cn)
Source title:2024 3rd International Conference on Electronics and Information Technology, EIT 2024
Abbreviated source title:Int. Conf. Electron. Inf. Technol., EIT
Part number:1 of 1
Issue title:2024 3rd International Conference on Electronics and Information Technology, EIT 2024
Issue date:2024
Publication year:2024
Pages:794-799
Language:English
ISBN-13:9798350369151
Document type:Conference article (CA)
Conference name:3rd International Conference on Electronics and Information Technology, EIT 2024
Conference date:September 20, 2024 - September 22, 2024
Conference location:Hybrid, Chengdu, China
Conference code:204574
Sponsor:IEEE
Publisher:Institute of Electrical and Electronics Engineers Inc.
Number of references:0
Main heading:Contrastive Learning
Controlled terms:Adversarial machine learning - Deep learning - Federated learning
Uncontrolled terms:Class incremental training - Detection methods - Features fusions - Incremental learning - Incremental learning framework - Incremental training - Intrusive traffic detection - Learning frameworks - Prototype extraction - Traffic detection
Classification code:1101.2 - 1101.2.1
DOI:10.1109/EIT63098.2024.10762098
Funding text:The work presented here was partially funded by Anheng Information Co., Ltd. We gratefully acknowledge the support and guidance provided by Professor Lei Xie and Professor Huifang Chen of Zhejiang University.
Database:Compendex

- 注：
- 1. 以上检索结果来自 CALIS 查收查引系统。
 - 2. 以上检索结果均得到委托人及被检索作者的确认。



检索地址

https://www.engineeringvillage.com/app/doc/?docid=cpx_5a27f2c119474b77dc8M673510178165208&pageSize=25&index=1&searchId=3307bf56488345659fb0b36e5f9c390c&resultsCount=53&usageZone=resultslist&usageOrigin=searchresults&searchType=Quick

← → ↺ 🏠

engineeringvillage.com/app/doc/?docid=cpx_5a27f2c119474b77dc8M673510178165208&pageSize=25&index=1&searchId=3307bf56488345659fb0b36e5f9c390c&resultsCount=53&usageZone=resultslist&usageOrigin=searchresults&searchType=Quick

☆

+

🔍

📄

📁

🔒

完成更新

Engineering VillageSearch

Search history

Alerts

Selected records

More

🔍

🏠

Create account

A

< Back to results

Link to Full Text

Share

Export

Print

Cite

Folders

< Record 1 of 53 >

Abstract

Indexing

Metrics

Conference Information

Funding

Bibliographic Information

☐ Compendex • Conference article (CA)

Adaptive and Lightweight Intrusive Traffic Detection Method Based on Deep Learning under Evolving Network Threats

2024 3rd International Conference on Electronics and Information Technology, EIT 2024, Pages 794-799, 2024

Xiao, Changbin^[1]✉; Xie, Lei^[2]✉; Chen, Huifang^[2]✉

Corresponding author: Xie, Lei✉

Author affiliations:
[1] Zhejiang University, College of Engineering, Hangzhou, China

Accession number

20250217660489

Publisher

Institute of Electrical and Electronics Engineers Inc.

ISBN-13

9798350369151

DOI

10.1109/EIT63098.2024.10762098

The 3rd International Conference on Electronic Information Technology

09/20/2024 – 09/22/2024 Chengdu • China

Acceptance Letter

Dear Author(s):

Congratulations! Your manuscript has passed the peer review (the reviewers' comments are available in the attached file on AIS) and has been accepted by the The 3rd International Conference on Electronic Information Technology. The conference will be held in Chengdu • China from 09/20/2024 – 09/22/2024. We are glad to invite you to attend the conference and make an oral report.

Manuscript No.: VYEE MN IJPN

Author name(s): Changbin Xiao, Lei Xie, Huifang Chen

Manuscript title: Adaptive and Lightweight Deep Learning Solution for Intrusive Traffic Detection in Evolving Cyber Threat Landscapes

Your manuscript, after presented in the oral report or poster in the conference, will be published on IEEE (ISBN: 979-8-3503-6915-1), after which it will be submitted for index in IEEE Xplore, EI, Scopus.

The 3rd International Conference on Electronic Information Technology

AEIC Academic Exchange Information Center

08-22-2024

Notices:

1. Authors need to revise the manuscript as per the reviewers' comments before re-uploading the final version (in Word or PDF) to the AIS system.
2. Authors need to ensure that the submitted manuscript is an original paper with a similarity lower than 20%. Once the manuscript is submitted to AIS, the authors are not allowed to re-submit it to other journals for publication.
3. Authors need to confirm their attendance one week before the conference is held. If the authors are not able to be present on the conference after agreeing to attend the conference, the authors need to reach the conference secretary for re-arrangement.

Again, congratulations and we look forward to meeting you in Chengdu • China

The 3rd International Conference on Electronic Information Technology

09/20/2024 – 09/22/2024 Chengdu • China

Notice for Registration

Dear Author(s):

Congratulations! Your manuscript has been accepted by The 3rd International Conference on Electronic Information Technology. To proceed to publication, you need to check the following information and follow the guidelines for registration.

Manuscript No.: VYEEMNIJPN

Author name(s): Changbin Xiao, Lei Xie, Huifang Chen

Manuscript title: Adaptive and Lightweight Deep Learning Solution for Intrusive Traffic Detection in Evolving Cyber Threat Landscapes

Charges: The registration fee is 3800 RMB/manuscript, and manuscripts exceeding the prescribed number of pages (4 pages) will be charged an extra fee of 400 RMB/page.

Deadline: Authors need to complete registration and make payment 7 work days after receiving this notice.

Payment receiver: The conference organizer has entrusted Guangzhou KEO Information Technology Co., Ltd. to collect the fees for registration and publication from authors. KEO is also entrusted to provide invoices for these payments to authors. (Beneficiary Bank Name: Industrial and Commercial Bank of China, Guangdong Provincial Branch, Guangzhou Tianhe Sub-BR, Account Name: Guangzhou KEO Information Technology Co., Ltd., Account Number: 3602879819100299208)

Registration flow: Log in AiScholar → My AIS → Order center → Conference paper → Orders awaiting confirmation/orders awaiting payment/Copyright transfer & invoice → Agree to contract /awaiting payment → Provide invoicing information → Make payment

About the invoice:

E-invoice: Authors who make payments online via Alipay, WeChat or Paypal can obtain an e-invoice from the AIS system promptly after the payment is completed; authors making payments via bank transfer will receive an invoice after the invoicing information is confirmed by the AIS system.

The 3rd International Conference on Electronic Information Technology

AEIC Academic Exchange Information Center

08-22-2024



CERTIFICATE

OF ORAL PRESENTATION



This certificate is presented to

Changbin Xiao

From Zhejiang University

Who had participated in The 3rd International Conference on Electronic Information Technology

(EIT 2024) on September 20-22, 2024 as an oral presenter. The report title is Adaptive and

Lightweight Intrusive Traffic Detection Method Based on Deep Learning under Evolving

Network Threats.

EIT

September 21, 2024

DATE

