技 术 服 务 合 同

合同编号（甲方）：

合同编号（乙方）：

项目名称： 国网客服中心2021年基于人工智能的互联网安全技术支持服务

委托方（甲方）： 国家电网有限公司客户服务中心

受托方（乙方）： 天津大学

签订时间 ： 2021.8.31

签订地点： 天津

有效期限： 自合同签订日起至2021年12月31日

技术服务合同

委托方（甲方）：国家电网有限公司客户服务中心
受托方（乙方）：天津大学

鉴于本合同为甲方委托乙方就国网客服中心2021年基于人工智能的互联网安全技术支持服务项目进行的专项技术服务，并支付相应的技术服务报酬。为明确各自的权利和义务，双方经过平等协商，根据《中华人民共和国合同法》等有关法律法规的规定，订立本合同。

1. 技术服务项目概要

1.1 技术服务的目标：落实公司网络安全工作要求，进一步加强新技术应用对网络安全攻防水平的强力支撑，开展网络安全创新技术研究应用，确保95598系统及网上国网系统安全可靠。

1.2 技术服务的内容：

（1）为中心移动端安全隐私保护提供技术服务。

工作内容：针对移动端应用的安全隐私问题，通过隐私保护政策语义识别方法、自然语言处理技术以及数据流分析技术，实现隐私保护政策内容语义完整性检测，有效识别软件代码中的数据收集行为，解决软件代码与隐私保护政策的语义鸿沟问题，实现数据收集行为的一致性检测。

成果：移动端安全隐私保护技术应用于网上国网、企业微信等安卓应用（脱壳apk），通过该技术检测的安卓应用符合国际或国家隐私合规标准。

（2）为中心二进制文件漏洞挖掘提供技术服务。

工作内容：基于二进制1和0的底层原始数据，构建二进制字节数据模型，分析二进制文件中的漏洞函数特性，采用二进制函数语义匹配技术扫描二进制文件中的潜在漏洞，生成被测二进制文件的漏洞

报告，给出详细的漏洞信息，比如：漏洞函数、漏洞类型、漏洞描述、整改方法等。

成果：二进制文件漏洞挖掘技术应用于中心范围所有 jar 文件，对于指定已知漏洞类型和测试文件集，相较于传统哈希匹配方法准确率具有较为明显提升。

（3）为中心 web 端应用自动化漏洞挖掘提供技术服务。

工作内容：基于 AI 自动化渗透技术和 web 端应用渗透测试知识以及测试人员行为抽象等技术，根据渗透测试需求开展定点、定项（特定时间、特定漏洞类型）自动化 web 应用漏洞扫描与挖掘，对已知及新发现漏洞开展关联交互分析，完成衍生漏洞研究，生成自动化漏洞报告，给出详细的漏洞信息，比如：漏洞函数、漏洞类型、漏洞描述、整改方法等。

成果：自动化漏洞挖掘技术应用于中心各类 web 应用，对于指定攻击类型，例如，针对 OWASP TOP10 网页安全漏洞类型，检测出现有工具 OpenVAS 和 Nessus Essentials 检测不到的漏洞。

（4）互联网安全自主创新能力提升。

工作内容：在研发过程中与国网客服中心研发团队协同工作进行技术攻关，总结科研成果，发表至少三篇核心论文（至少一篇 EI 或 SCI 论文）和申请两篇发明专利，合作期间新产生的算法、模型、源码等核心技术资料归双方共同享有。

成果：发表至少三篇核心论文（至少一篇 EI 或 SCI 论文）和申请两篇发明专利。

1.3 技术服务的方式：现场实施和远程支持。

2. 技术服务具体要求

2.1 技术服务地点：国家电网有限公司客户服务中心。

2.2 技术服务期限：合同签订之日起至 2021 年 12 月 31 日。

2.3 技术服务进度：自合同签订之日起 1 个月内完成工作方案编制并通过审核；自方案审核通过后 6 个月内开展项目技术现场服

附件二：

技术服务人员表

姓 名		单 位	性 别	出生年月	职称或职务	专 业	承担的主要工作	投入时间
负责人	[redacted]					计算机科学与技术	项目管理，统筹	3 个月
	陈森	天津大学智能与计算学部	男	1990	副教授	计算机	算法设计与指导	3 个月
主要技术服务人	[redacted]					计算机	算法设计与指导	3 个月
						计算机	相关工作调研，算法设计与研发	6 个月
						计算机科学与技术	可行性分析，算法设计与研发	6 个月
						计算机技术	系统研发与部署	6 个月