FUJIAN TELECOMMUNICATIONS TECHNOLOGY

福建通信科技

二〇二〇年
增刊

国家网络安全宣传周
China Cybersecurity Week

福建省2020年国家网络安全宣传周网络空间安全治理优秀论文及解决方案

获奖论文及解决方案专辑

2020年增刊
闽内资准字K第111号
内部资料　免费交流

福建省2020年国家网络安全宣传周
网络空间安全治理优秀论文及解决方案

获|奖|名|单

*排名不分先后

类别	论文题目	公司	作者
优秀论文	电信运营商网络与信息安全体系架构的研究	中电福富信息科技有限公司	江承兴
优秀论文	基于深度学习的操作系统补丁自动安装方法	国网福建省电力有限公司 漳州供电公司	张坤三、陈智、 傅仕琛
优秀论文	基于OCR技术的网页篡改检测研究	泉州师范学院 网络中心	吴伟斌
优秀论文	大数据业务场景下的零信任体系架构	厦门市美亚柏科 信息股份有限公司	朱熹、程硕
优秀论文	基于复杂异常值的 DDOS异常网络流量检测技术	三明学院网络中心	余建 、林志兴
优秀论文	基于人工免疫系统的安全运营中台	中电福富信息科技有限公司	林文伟
优秀论文	基于网络流量解析的敏感信息发现	福建省海峡信息技术有限公司	阮陈强
优秀论文	浅谈主机安全防护技术在 金融机构网络空间安全的应用	兴业银行总行信息科技部	郑鹏飞
优秀论文	泉州港口发展中心网络信息安全形式与对策研究	福建省泉州港口发展中心	黄韵玲
优秀论文	网络安全AI工具箱的探索及实践	中国移动通信集团 福建有限公司网络部	俞捷
优秀论文	新一代“智慧海洋”建设的网络安全框架	福建省海洋预报台	林竹明、张彦
优秀论文	云存储环境下基于矢量量化的图像伪装加密方法	福建农林大学 计算机与信息学院 网络空间安全系	柳晓龙、郑思飞、 纪祥敏、陈日清
优秀解决方案	5G时代数据安全保护的属地化推进	中国移动通信集团 福建有限公司莆田分公司	龚晓波
优秀解决方案	风电场网络信息安全风险辨识探讨	福建省三川海上风电有限公司	林晋洪
优秀解决方案	福建移动互联网 电视平台安全防护整体解决方案	中国移动通信集团福建有限公司	上官涛、吴篁、 林伟、董健业
优秀解决方案	互联网医院网络安全风险闭环管理体系	福建中信网安信息科技有限公司	林锴、赵贤
优秀解决方案	基于智慧中台 打造新入网用户一站式风险防控运营体系	中国移动通信集团 福建有限公司厦门分公司	崔文迪
优秀解决方案	基于智能协同的主动防御体系模型研究与实践	福建省海峡信息技术有限公司	赖建华、唐敏
优秀解决方案	使用深度学习对网络攻击行为识别的研究	中电福富信息科技有限公司	郑炎
优秀解决方案	未来网络安全流量分析解决方案	中国移动通信集团福建有限公司	邹芳

2020年增刊
总第144期
1983年创办　2020年9月编印

福建通信科技

FUJIAN TELECOMMUNICATIONS TECHNOLOGY

目　录 CONTENTS

优秀论文

《福建通信科技》
与时俱进!

福建通信科技

FUJIAN TELECOMMUNICATIONS TECHNOLOGY

主管单位：福建省通信管理局

主办单位：福建省通信学会

福建省互联网协会

福建省信息通信行业协会

福建省邮电规划设计院有限公司

总　编：陈星耀

副总编：邵　冲

主　编：林　炜

责任编辑：赖蔚萍　赛　波

编　　印：福建省邮电规划设计院有限公司

《福建通信科技》编辑部

通信地址：福州市五四路111号宜发大厦9楼

电子信箱：laiwp@fjpdi.com

网　　址：www.icfj.cn

电话号码：(0591)87879622

邮政编码：350003

闽内资准字K第111号

（内部资料　免费交流）

目　录 CONTENTS

优秀解决方案

序　言

为深入贯彻落实习近平总书记关于网络强国的重要思想，围绕党的十九大以来网络空间安全领域的科研成果，分享有关网络与信息安全研究成果和应用经验，广泛探讨网络空间安全所面临的风险挑战问题。在省网信办、省公安厅共同指导下，由福建省网络与信息安全产业发展促进会、福建省互联网协会、福建省信息协会、福建省计算机学会、福建省高校教育信息化学会、福建省信息通信行业协会、福建省通信学会等单位共同主办，福建师范大学、福建中信网安信息科技有限公司冠名共同承办，于 7 月 27 日起面向福建省内企事业单位、省内高校（含高职）公开征集福建省 2020 年国家网络安全宣传周第二届“华安星杯”网络空间安全治理优秀论文及解决方案作品。

活动期间，共收到省内高校、运营商、广电、金融、电力、税务、机场、港口、海洋、水利、医疗等行业以及政府部门、网络安全企业的投稿作品 68 篇，其中论文作品 42 篇，解决方案作品 26 篇。由七家主办协会联合福建省互联网网络与信息安全专家委员会成立了由 16 名专家成员组成的作品评审专家组，采用分组盲评方式，从征集作品的学术水平、创新性、推广价值等方面进行评审，9 月 2 日上午在盲评基础上再经过现场分组讨论、综合评议讨论后优选出 20 篇优秀作品（优秀论文 12 篇、优秀解决方案 8 篇），于 9 月 14 日下午举办的网络空间安全技术论坛上进行颁奖，获奖优秀作品由期刊《福建通信科技》（闽内资准字 K 第 111 号）发行增刊刊登。

在此特别感谢积极参与此次征集活动的投稿作者，同时也对评审专家、《福建通信科技》编委会、指导单位、主办单位、冠名承办等工作人员的辛勤付出表示衷心的感谢！

以下刊登文章排名不分先后。

福建省网络与信息安全产业发展促进会
福建省互联网协会
福建省信息协会
福建省计算机学会
福建省高校教育信息化学会
福建省信息通信行业协会
福建省通信学会

关于征集福建省2020年国家网络安全宣传周网络空间安全治理优秀论文及解决方案活动的通知

为深入贯彻落实习近平总书记关于网络强国的重要思想，围绕党十九大以来网络空间安全领域的科研成果，分享有关网络与信息安全研究成果和应用经验，广泛探讨网络空间安全所面临的风险挑战问题，在省网信办、省公安厅共同指导下，由福建省网络与信息安全产业发展促进会、福建省互联网协会、福建省信息协会、福建省计算机学会、福建省高校教育信息化学会、福建省信息通信行业协会、福建省通信学会等单位共同主办，福建师范大学、福建中信网安信息科技有限公司冠名共同承办，面向福建省内企事业单位、省

内高校（含高职）公开征集第二届“华安星杯”网络空间安全治理优秀论文及解决方案作品。

一、评选范围

在活动期间内，涉及网络空间安全领域的基础理论、热点研究的学术论文和面向各行业的网络安全、信息安全示范应用等解决方案，未在国内外正式期刊公开发表的作品均可参加本次征集评选。

二、评选要求

作品主题突出、论据充分、文字精炼、数据可靠，有较高的专业学术水平和实际推广应用价值，对我省网络空间安全领域发展有学术推动和产业升级作用，篇幅(含摘要、图、表、参考文献等)不超过5000字。

三、评选原则

优秀作品评选聚焦于论文质量和实际应用情况，遵循“公平、公正、公开”的原则，福建省网络与信息安全产业发展促进会等主办单位组织信息安全专家评审组按照参赛作品提出的创新点、写作的规范性、研究的先进性、结论的可信度以及推广示范应用价值等方面进行评选，入选优秀作品将在福建省2020年网络安全宣传周开幕式上进行颁奖。

四、评选程序

1.作品投稿。作品征集活动设立专用邮箱收集，作者可以将参评作品直接发至电子信箱：　893867377@qq.com，投稿方向注明是优秀解决方案或优秀论文，**投稿截止日**

期：2020年8月24日。

2.作品格式及字数要求

正文标题：黑体、2号、加黑、居中，凝练、概括、有启发性。

作者基本信息：宋体、5号、居中，包含单位（院系）、姓名、手机等联系方式等信息。

摘要：楷体、5号、两端对齐、首行缩进2个字符，“摘要”和“关键词”两词用黑体、5号、加黑，文章各部分核心内容的连缀，150字左右为宜，关键词：文章涉及的核心概念，可供检索，3－5个为宜。

正文：宋体、5号、首行缩进2个字符。

3.作品评审。征文截止后，由信息安全专家评审组进行优秀作品遴选评审，最终评选出10篇行业优秀解决方案以及15篇优秀论文（获奖作品比例不超过投稿作品的20%）；优秀作品将由期刊《福建通信科技》（闽内资准字K第111号）发行增刊发放；代表性优秀作品在2020年福建省网络安全宣传周技术论坛做分享交流。

4.奖金发放。入选优秀论文或优秀行业解决方案的作品将授予获奖证书及奖金；冠名承办单位福建中信网安信息科技有限公司将根据第一作者提供的有效身份证号和个人汇款账号于2020年10月31日前发放奖金。

（联系人：何晓玲　18250489875　0591-83175068）

福建省网络与信息安全产业发展促进会

福建省互联网协会

福建省信息协会

福建省计算机学会

福建省高校教育信息化学会

福建省信息通信行业协会

福建省通信学会

2020 年 7 月 27 日

优 秀 论 文

电信运营商网络与信息安全体系架构的研究

江承兴

中电福富信息科技有限公司　福州　350001

摘　要：本文主要针对电信运营商网络与信息安全体系架构进行研究，文中总结了近些年电信运营商对网络与信息安全体系架构优化的实践成果，从管理、运营及技术三个维度分别分析了电信运营商网络与信息安全体系的构成要素，给出了整体架构模型，展望了未来的优化方向。

关键字：网络安全、信息安全、体系、架构、最佳实践

一、引言

近些年来，网络与信息安全威胁已成为全球各国在网络空间方面最为关注的课题之一。各国纷纷出台保护关键信息基础设施的战略和政策。早在 20 世纪 90 年代，美国就开展了相关保护工作，自 2001 年“911”事件后，其对安全保护的相关工作提速，出台了一系列法令、政策、标准，加强对关键基础设施的网络安全保护。在我国，2016 年 4 月，习总书记在国家网络安全和信息化工作座谈会上，强调“网络安全是整体的而不是割裂的，网络安全是动态的而不是静态的”等理念。在 2018 年 4 月，全国网络安全和信息化工作会上，习总书记强调“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障，要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设”等。由此可见，当前我国网络与信息安全建设要从体系化的角度出发，综合研究管理体系、运营体系及技术体系等各方面建设要求，形成自顶而下的、体系化的解决方案。

二、电信运营商加强网络与信息安全体系建设正当其时

我国信息安全建设始于 20 世纪 90 年代后期，随着各行各业信息化和网络建设的发展，网络安全的理念得以逐步普及。同时期，也是我国通信业高速发展时期，电信运营商注重对通信网络的保护，从通信节点的选址、通信线缆的保护，到通信系统的运维保障、应急响应、数据灾备，到人员的安全教育、技能培训，乃至机房管理制度等，涉及了通信网络安全保障的各方面，初步形成了体系化保护的理念。

在国家层面，1994 年 2 月 18 日国务院签发的第 147 号令《中华人民共和国计算机信息系统安全保护条例》，明确提出对计算机信息系统进行安全防护，以促进计算机的应用和发展。2003 年中办签发的 27 号文《国家信息化领导小组关于加强信息安全保障工作的意见》的出台，标志着我国信息安全保障工作有了总体纲领。2017 年，随着我国《网络安全法》的正式颁布，我国对网络空间安全的重视程度达到新高度。

在行业层面，自 1999 年我国发布第一部国家强制标准《计算机信息系统安全等级保护划分准则》（GB17859），我国对网络和信息安全领域相关标准规范的研究步伐加快，二十年多年来，相关部门紧跟业界前沿技术和理论，先后发布了一百多部关于网络和信息安全的标准规范，对安全体系建设起到很好的指导作用。

在经济层面，进入 21 世纪以来，我国日渐成为全球经济增长的发动机，近些年更随着“互联网 +”产业政策的贯彻实施，我国的数字经济增长势头良好，支撑数字经济发展的关键基础设施建设也迎来巨大机会，其中就包括 5G 通信和云计算等新兴技术。5G 通信及物联网所代表的连接技术与云计算乃至边缘计算、超级计算、人工智能等计算技术的有机结合，再加上丰富的行业应用，必将为我国数字经济带来新的增长动力，而电信运营商作为国家央企，必可凭借自身在网络和信息技术方面的深厚积淀，成为数字经济重要助力者、领军者。

有鉴于此，站在新时代的起点上，电信运营商应从国家战略角度，审视自身网络与信息安全的体系架构，结合网络空间安全前沿理论和技术、法律法规、标准规范以及业界最佳实践，对自身网络与信息安全体系架构加以完善，开展网络与信息安全的体系化建设，朝着成为“信息基础设施安全的保卫者、清朗网络空间的守护者、智能安全服务的提供者以及网络安全生态的建设者”的方向迈进。

三、电信运营商网络与信息安全体系优化实践的分析

经过多年发展，电信运营商构建了相对完整的网络与信息安全的体系，近些年更在制度和能力建设、基础网络安全以及云的安全服务体系建设优化等方面，开展了积极有效的优化工作。

首先，在制度和能力建设方面，电信运营商在组织体系、队伍建设、能力体系、规章制度等方面进行了调整优化。例如中国电信 2019 年对组织体系进行了调整，成立了集团的网络和信息安全领导小组，并由集团主要领导亲自挂帅，组建了集团和省两级的网络和信息安全的部门，作为管理单位；成立了集团、省级两级操作中心以及不良信息处理中心等保障单元；在队伍建设方面，建立了集团网络信息人才选拔基地，在集团和省级层面，已拥有网络安全专家及专业人才近千人，以确保网络和信息安全体系的保障举措执行落地到位。在能力体系方面，通过构建安全运营中心（SOC）及信息安全管理平台等，确保网络和信息安全的防护措施落实到位。在规章制度方面，制定了完善的管理办法、规范开展安全管理和考核，包括网络和信息安全的基础信息管理、风险处置预案和风险网络安全事件闭环管理等内容，通过这一系列的安全制度和能力建设，保障中国电信的网络安全、信息安全的管控到位。同一时期，中国移动 2019 年中也提出，要全面落实网络强国战略和网络安全工作责任制要求，贯彻执行“力量大厦”的总体思路，全面对接集团“十三五”安全规划，统筹考虑“大网安”工作的各项内容，面向“央企前列、世界一流”的工作目标，更新完善中国移动网络安全工作体系和整

体框架，打造安全保障体系化能力，深化区块链等技术应用，强化全方位网络安全态势感知和集中管控，提供数据、应用、主机防护等超 50 项安全保障服务等。

其次，在基础网络安全方面，电信运营商已具备提供“国家队”水准的网络安全基础服务能力。如中国电信的云堤服务，依托其自身运营的国内最大的互联网接入骨干网络，拥有着国内最大规模的攻击防护能力，通过全球部署的 36 个分布式清洗中心，实现对目的地及近源地清洗，针对高流量攻击提供高级防护服务，并将攻击流量引流，从而确保客户的业务持续性。

第三，在体系架构方面，电信运营商构建了包括管理体系、技术体系、运营体系的完整架构，可对外提供电信级的安全服务能力。例如中国电信，在管理方面，优化了集团和省级的组织体系、管理策略；在运营方面，凭借其在通信网络运营维护方面的丰富经验，可提供高可靠的、电信级的运维能力；在技术方面，围绕着业务能力和管理能力的解耦，针对企业内部及外部核心网络，分别设计资源池的资源架构，划分多个服务区，实现了不同功能及安全级别的架构优化，可以提供计算资源独享、计算存储资源独享、计算存储网络资源独享的三大服务能力。

第四，在网络与信息安全生态圈方面，电信运营商注重打造合作共赢的安全生态圈。例如中国电信通过天翼云、云市场，引入了各个行业的网络安全专家、信息安全专家，共同为客户提供整合的网络空间安全服务能力。

四、电信运营商网络和信息安全体系的整体架构分析

综上所述，不难看出电信运营商的网络和信息安全体系架构优化，是从纵向和横向两个维度展开，并精准施策、细化形成一套层次分明、相对合理的体系架构模型。

4.1 纵向维度方面的体系优化

在纵向维度上，根据国家网络空间安全战略要求，基于纵深防御和分析管理思路，分别对网络安全、信息安全的技术体系进行了梳理和优化。

1）在网络安全体系上，基于 ISO/OSI 七层模型，从应用层、表示层、会话层、传输层、网络层、链路层、物理层等方面，针对内外部的网络安全环境的新变化，结合业界相关前沿技术和理论，进行安全域划分、隔离等防护措施的加固建设。具体如下图所示。

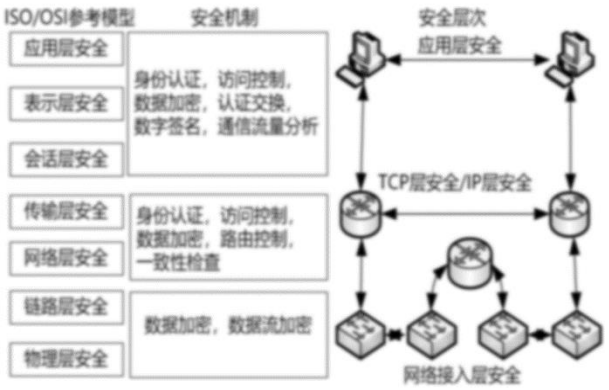


图 1　网络安全体系模型

在具体目标或场景上，侧重开展如下方面的技术研究：

①数据加密与数字签名

②CA 数字证书

③边缘计算安全(SA)

④NFV 隔离与访问控制(SA)

⑤网络切片安全(SA)

⑥身份认证、访问控制

⑦异常通信流量分析

⑧安全域划分、隔离

2）在信息安全体系方面，基于信息的保密性、完整性、可用性、真实性、可控性和可审查性等要素，以信息安全的全生命周期为主线，实现从被动防御向主动防护演进、从基础合规向价值能力输出演进；通过打造事先化的基准安全、主动化的核心管控、自动化的智慧安全的三大信息安全管理能力，实现向新技术新兴业务输出核心信息安全监管能力，打造从人防到技防的技术体系。具体如下图所示。

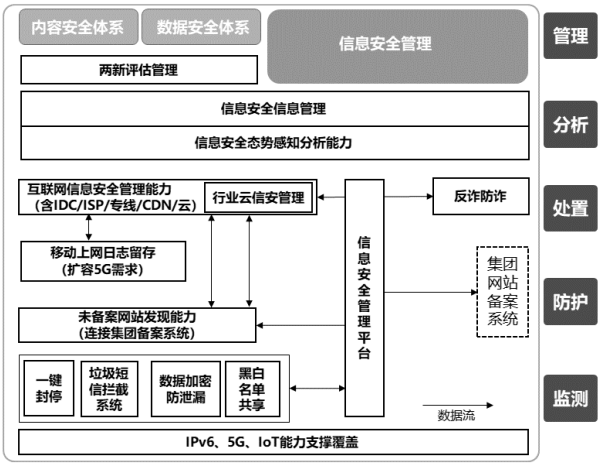


图 2　信息安全体系模型

在具体目标或场景上，侧重开展如下几方面的体系优化：

①在双新评估中嵌入业务全流程、实现信息化、自动化评估

②信息安全的态势分析、一键封停、黑名单共享能力建设

③敏感数据保护，实现数据资产管理、身份认证、访问控制、数据加密能力

④信息安全能力覆盖 5G、IoT 等技术及领域

⑤信息安全信息化管理，在线指挥调度，以及考核、人员、制度等基础在线作业管理

4.2 横向维度方面的体系优化

在横向维度上，电信运营商结合自身企业特点，分别从组织建设、制度规章、队伍建设入手，梳理决策层、管理层、执行层的各层级职责要求；研究人员能力、管理能力、合规能力、运营能力、技术能力等全方位能力提升手段；打造感知体系、管控体系、溯源体系、分析体系等多层次体系，形成网络与信息安全保障体系的整体框架。具体如下图所示：

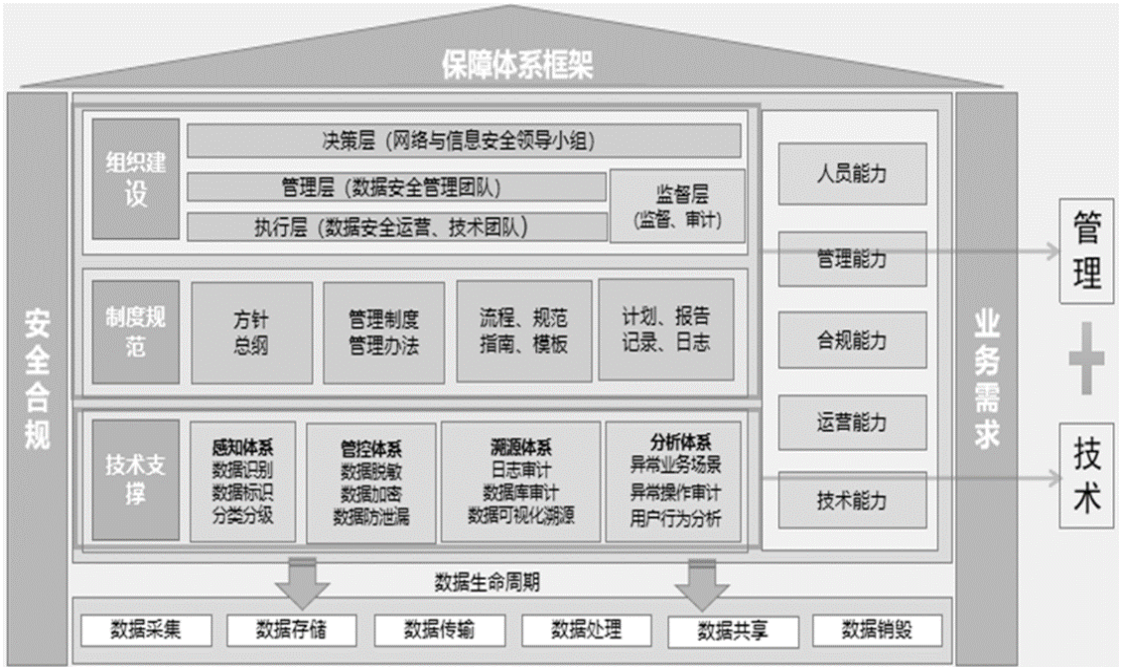


图 3　网络和信息安全保障体系整体框架

在这个保障体系框架中，在管理体系优化的目标上，电信运营商一方面围绕自身企业在网络与信息安全体系的设计、实施、监视、保持和改进等过程管理的特点，持续完善相关配套制度，厘清责任部门的分工及安全职责，形成统筹管理、归口管理、协作管理的分工明确、整体协作的管理机制；另一方面，针对网络和信息安全的最新形势，梳理完善网络和信息安全关键岗位的动态需求，采取内部培

养和市场化招聘相结合的用人模式，定期开展网络与信息安全的通识教育、任职资格和专业资格认证等教育培训活动，打造一支责任明晰、保障有力的网络与信息安全人才队伍。

在运营体系的优化措施上，电信运营商一方面根据国家法律法规，贯彻国安委、网信办等部委文件精神，结合行业标准规范、部省两级监管单位等指示要求，提炼形成安全运营任务清单，对每个任务执行全过程闭环管理，健全安全运营管控机制、应急响应机制和攻防演练机制等措施；另一方面，电信运营商还将自身具备的安全服务能力，在条件成熟的省分公司中，试点开展面向行业客户的、差异化的、可运营的安全服务，将内在安全运营能力转变为实际收入。

4.3 电信运营商网络和信息安全体系的整体架构模型

综述所述，经过多年深耕，电信运营商在网络和信息安全体系建设方面，积淀了丰富的实践经验和较强的防护能力，形成了一套基础理论与最佳实践相结合的网络与信息安全体系架构，如下图所示：

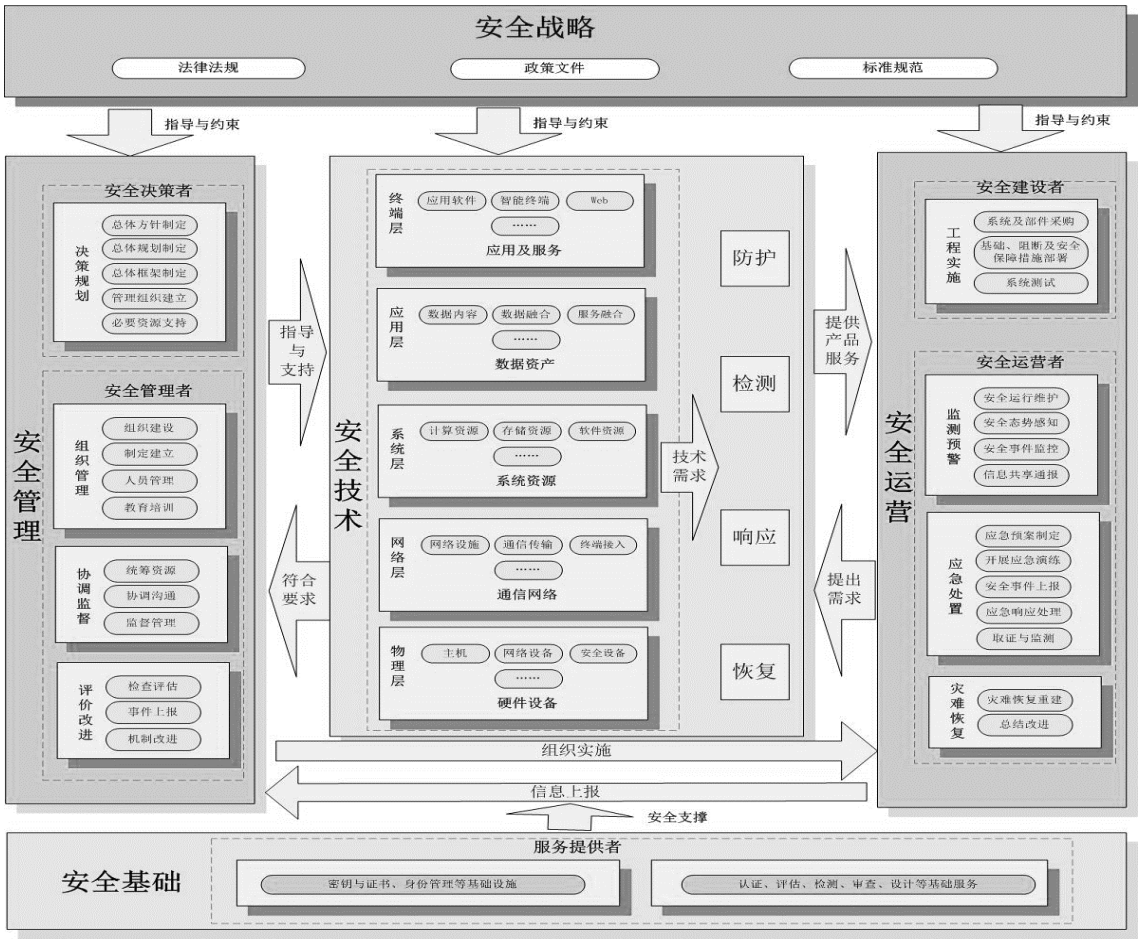


图 4：电信运营商网络和信息安全体系总体架构

当下，由于国际形势变化，我国将迈入“国内大循环为主体、国内国际双循环”相互促进的新发展格局，未来面临的网络与信息安全形势仍然复杂严峻，电信运营商作为我国信息化建设主力军，仍需本着纵深防御、动态防御、持续优化的理念，侧重加强 5G 安全、密码技术等方面研究，持续提升网络和信息安全体系保障能力，为政府、金融、能源、交通等行业发展赋能，为我国数字经济发展贡

献更大力量。

五、结束语

我司身为电信运营商体系的组成单元，近些年积极投身于中国电信、中国移动的网络和信息安全体系优化的建设实践，面向集团及省分公司提供网络和信息安全规划咨询、项目建设等支撑服务，目前已有多个项目落地实施，并陆续取得了良好的建设成果。

参考文献

[1]中国电信.5G 网络安全重点工作指南(S).中国电信企业标准.2020.6

[2]中国移动.5G 网络与业务安全基准测评规范(S).中国移动企业标准.2019.8

[3]刘鹏等.美国网络空间安全体系建设分析与思考[J].网络空间安全.2017.9

[4]袁小明.电信运营商如何构建新一代网络与信息安全体系(N).人民邮电.2016.12

[5]侯芳等.分阶层、多维度、全周期的网络与信息安全综合管理体系建设[J].电信技术.2011.5

[6]吴岳强.构建信息安全体系保障企业持续运营[J].电信技术.2008.7

[7]孙强等.信息安全管理:全球最佳实务与实施指南(M).北京:清华大学出版社.2004

[8]沈昌祥.关于加强信息安全保障体系的思考(J).信息安全与通信保密.2002.12

基于深度学习的操作系统补丁自动安装方法

张坤三　陈智　傅仕琛

（国网福建省电力有限公司漳州供电公司　福建漳州　363000）

摘要：为了提高信息系统的安全性和可靠性，降低漏洞入侵和攻击的风险，提出一种基于深度学习的操作系统补丁自动安装方法，该方法通过提出一种补丁检测可视化系统，并且通过系统版本信息以及补丁安装返回值判断补丁安装情况，如若安装成功则返回系统基本信息状态在可视化服务端上。如若安装失败，则建议手动升级并且显示在补丁检测可视化服务端上。通过实际运用统计分析，统计结果表明所提方法明显优于原始以及传统安装方法，能够有效避免客户端重复下载问题，并且极大地提升了补丁自动升级的成功率。有效地节约了升级成本问题，同时保证了信息系统的安全性和可靠性。

关键词：深度学习；操作系统补丁；补丁检测可视化

一、引言

当前，国际网络安全形势日益严峻，网络空间已成为国家继陆、海、空、天四个疆域之后的第五疆域，网络攻击集团化、国家化的趋势日益明显。电力作为关乎国计民生的重要基础设施，一直以来都是网络攻击的重点目标。乌克兰停电事件[1]、以色列网络攻击[2]、勒索病毒(WannaCry)[3]和委内瑞拉大面积停电[4]等多种事件表明，操作系统漏洞入侵[5]是黑客攻击电力等大型企业的一种重要的手段。

目前绝大多数政府机构、企事业单位都建立了自己的内部信息网络[6]，信息内网作为一个独立局域网，不与外界互联网连通，导致信息内网所有计算机的操作系统无法及时更新补丁，操作系统的漏

洞未能得到及时有效的修补，一旦其中一台终端感染蠕虫类等传染性极强的计算机病毒，整个局域网就会受到严重的威胁，有时甚至会导致整个信息内网的瘫痪[7]。

为了解决上述存在的问题，本文提出一种基于深度学习的自动操作系统补丁安装方法，能够实现信息内网的操作系统补丁自动化安装，实时监控补丁安装情况以及可视化安装过程，并进行相应的分类统计，根据补丁安装情况进行相应的处理，有效解决了内外网隔离的内网客户端进行操作系统补丁安装的安全性和安装成本问题，使得内网客户端操作系统安装可以做到及时性，迅速性和便捷性，节约了大量人力物力和安装成本，同时也保证了信息系统的安全性和可靠性。

二、现有的操作系统补丁安装方法

补丁安装主要包括两种方式：手动安装和自动安装。

手动安装需要专业的运维人员接入内网逐一地进行安装操作，电力信息内网桌面终端数量庞大，且系统分布在不同地区[8]，这使得补丁安装升级需要耗费大量的人力物力，而且也会使得补丁安装升级的周期大大延长，对于某些需要及时和频繁升级的系统来说，补丁安装所需投入的时间就会增加很多，而且补丁安装的速度变得不太理想。

自动安装通常采用客户端/服务器的形式，通过内网操作系统补丁安装服务器将所需安装补丁分发安装到每台内网客户端上，有效解决了电力信息内网操作系统补丁安装工作量过大的问题[9-11]。但是现有自动安装方法在实际运用过程中暴露出一些问题：

1. 现有的操作系统版本种类繁多，例如 windows、linux 和 mac 等系统，其中尤其又以 windows 系统安装补丁多而著称。如果补丁安装服务器批量推送工作量大而且较为耗时，用户需等待较长时间直至下载完成或者下载失败，导致更新程序长时间占用客户端系统资源或网络带宽。

2. 在同一局域网内多台客户端安装相同升级补丁时，需要对多台客户端分别进行升级，将会严重占用局域网与广域网之间的连接带宽。

3. 补丁安装升级是一个复杂的过程，即使补丁推送下载成功，由于操作系统版本和环境变量配置问题，使得补丁安装失败的概率仍然变大，有些操作系统需要预先安装多个前置补丁。

4.数量众多的计算机操作系统补丁是否已被正确安装，也不便知晓。导致已成功安装的客户端重复下载升级补丁，未能成功安装的一直处在安装失败状态。

三、基于深度学习的操作系统补丁自动安装系统及方法

基于上节分析的自动安装方法存在占用客户端系统资源或网络带宽、补丁安装成功率低等问题，为实现上述目的，本文提供如下技术方案：基于深度学习的操作系统补丁自动安装系统及方法，具体流程图如图 1 所示，包括下列步骤：

1. 建立一个内网操作系统补丁升级服务器；

2. 研制一款补丁检测可视化系统，包括：补丁检测客户端和补丁检测可视化服务端；

3. 通过内网操作系统补丁升级服务器将补丁检测客户端分别安装到各个内网客户端上；

4. 通过补丁检测客户端根据自身操作系统版本向内网操作系统补丁升级服务器下载安装对应的补丁，并通过操作系统版本信息，系统补丁安装返回值判断操作系统补丁安装情况，并做相应处理；

5.如果判断系统补丁安装返回值为补丁安装失败，且系统补丁安装次数不大于三次，则返回至步骤 3。如果判断系统补丁安装返回值为补丁安装失败，且系统补丁安装次数大于三次，则判定该主机无法成功安装该系统补丁，建议手动升级。并将操作系统 IP、操作系统使用人信息、操作系统版本信息，系统补丁安装次数、系统补丁安装情况和处置建议实时显示在补丁检测可视化服务端上；

6. 如果判断系统补丁安装返回值为补丁安装成功，则将操作系统 IP、操作系统使用人信息、操作系统版本信息，系统补丁安装次数、系统补丁安装情况实时显示在补丁检测可视化服务端上；

7. 如果判断系统补丁安装返回值为需要预先安装前置补丁，则通过所述补丁检测客户端向内网操作系统补丁升级服务器下载安装所需前置补丁，补丁检测客户端通过操作系统版本信息，前置补丁安装返回值判断操作系统前置补丁安装情况，并做

相应处理；

8. 如果判断前置补丁安装返回值为补丁安装成功，且补丁安装次数不大于三次，则返回步骤 3。如果判断前置补丁安装返回值为补丁安装成功且补丁安装次数大于三次，则判定该主机无法成功安装该系统补丁，建议手动升级。并将操作系统 IP、操作系统使用人信息、操作系统版本信息，系统补丁安装次数、系统补丁安装情况和处置建议实时显示在补丁检测可视化系服务端上；

9.如果判断前置补丁安装返回值为补丁安装失败，则判定该主机无法成功安装该系统补丁，建议手动升级。并将操作系统 IP、操作系统使用人信息、操作系统版本信息，系统补丁安装次数、系统补丁安装情况和处置建议实时显示在补丁检测可视化系服务端上。

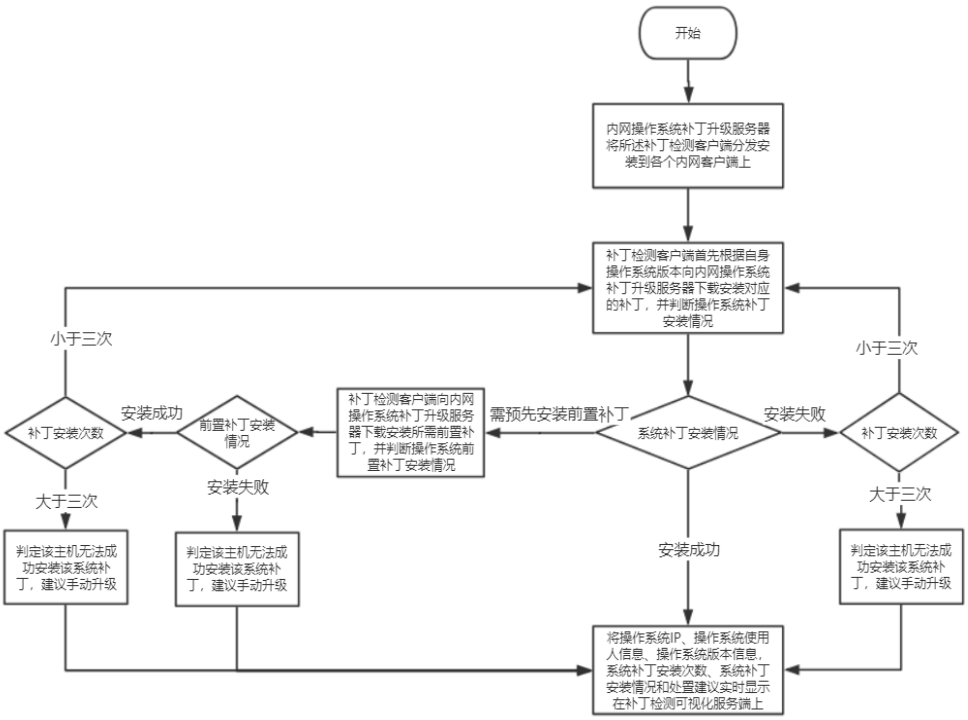


图 1 基于深度学习的操作系统补丁自动安装系统流程图

内网客户端与所述内网操作系统补丁升级服务器同处于一个内部局域网；内网操作系统补丁升级服务器用于保存操作系统补丁文件和前置补丁文件，并提供升级补丁的下载服务。其中，前置补丁是为系统补丁更新做准备，为了与后面的补丁升级所适应。

补丁检测客户端可根据自身操作系统版本向内网操作系统补丁升级服务器下载安装对应的补丁，并通过操作系统版本信息，系统补丁安装返回值判断操作系统补丁安装情况，补丁检测客户端可将系统 IP、系统使用人信息、系统版本信息，系统补丁安装次数、系统补丁安装情况和处理建议发送至补丁检测可视化系服务端。

补丁检测可视化系服务端用于将操作系统 IP 系统使用人信息、系统版本信息，系统补丁安装次数、系统补丁安装情况和处置建议可视化显示，并进行分类统计。

四、实验测试分析

为了验证所提方法的有效性和可靠性，我们通过对不同类型的方法对 18 种常见的漏洞补丁进行实际安装对比，参与比较的方法包括原始安装方法、传统安装方法以及所提自动安装方法[12]，将得到的安装结果呈现在图 2 中。

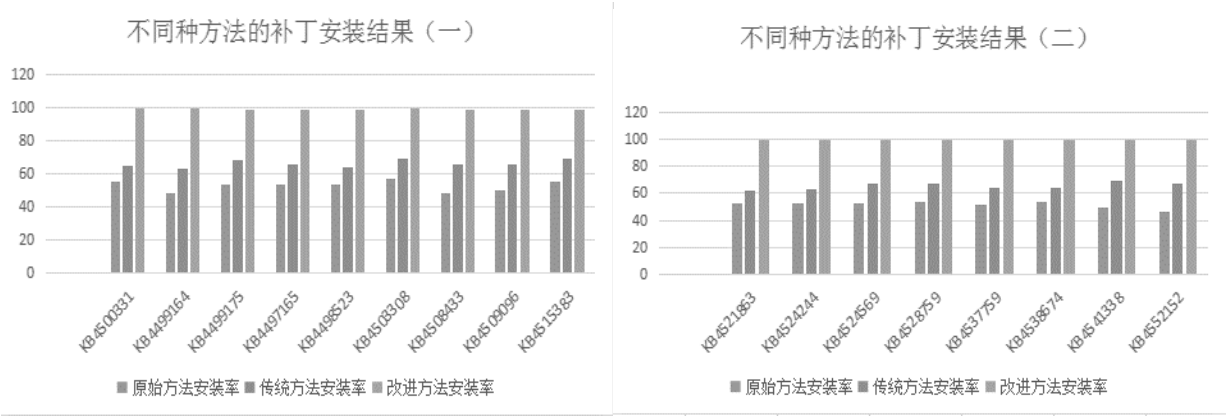


图 2 不同安装方法的对比结果图

表 1 在不同单位实际应用的统计结果

补丁号	补丁安装率	各单位补丁安装率（%）									
		漳州本部	龙海	长泰	漳浦	平和	诏安	南靖	华安	东山	常山
KB4500331	99.31	99.72	99.08	98.77	99.31	98.73	99.69	99.74	99.12	99.28	99.69
KB4499164	99.25	99.55	98.96	98.73	99.79	99.07	99.41	99.59	99.38	99.94	98.05
KB4499175	98.95	99.77	98.47	98.55	98.01	99.05	99.75	98.84	99.22	99.72	98.09
KB4497165	98.79	99.80	98.77	98.70	98.10	98.34	99.19	98.37	98.14	98.55	99.98
KB4498523	98.83	99.46	99.12	98.46	98.10	98.28	98.59	98.16	99.05	99.75	99.34
KB4503308	99.38	99.84	99.07	99.82	99.61	99.90	99.69	99.25	99.73	98.80	98.15
KB4508433	99.22	99.72	98.55	99.73	99.16	99.35	99.18	99.97	98.87	98.32	99.34
KB4509096	99.00	99.85	98.25	98.89	98.22	98.55	99.48	99.61	98.76	99.19	99.20
KB4515383	98.95	99.69	98.59	99.57	98.75	98.43	98.91	98.62	99.03	98.76	99.12
KB4516115	99.29	99.87	98.91	100.00	99.95	99.09	98.62	99.47	99.34	99.55	98.11
KB4521863	98.79	99.13	99.65	98.92	98.40	98.87	98.23	98.45	98.33	99.92	98.00
KB4524244	99.05	99.43	99.12	98.42	99.76	99.37	98.59	98.72	99.46	98.56	99.12
KB4524569	99.20	99.55	98.78	99.51	99.20	98.24	99.67	99.49	99.78	98.33	99.45
KB4528759	99.01	99.49	98.20	98.67	98.80	99.52	99.71	99.17	99.29	98.20	99.03
KB4537759	99.01	99.98	98.26	98.41	99.46	99.79	99.08	98.18	98.24	99.76	98.90
KB4538674	98.90	99.11	98.19	98.35	98.93	99.66	99.71	98.35	98.08	98.73	99.85
KB4541338	99.05	99.75	98.94	98.31	99.74	98.60	99.91	98.28	99.54	98.98	98.40
KB4552152	98.87	99.31	99.76	98.29	98.25	98.90	98.50	98.80	98.42	99.37	99.07

由图 2 和表 1 可以看出，采用所提安装方法的实际应用效果要明显优于原始安装方法和传统安装方法，并且在 18 种补丁上的安装率均在 98%以上。由此可知，所提方法能够实现较好的安装效率，通过多层判断学习能够有效提升补丁的安装成功率。对于未能被成功安装的补丁则建议采用手动升级，并且将基本系统信息发送至可视化系服务端便于后续的升级安装。

六、结论

经过上述实验验证分析，并且与多种现有的方法对比，所提的方法具有如下的优势：

1. 所提的补丁检测可视化系统可根据自身操作系统版本向内网操作系统补丁升级服务器下载安装对应的补丁，补丁安装的针对性较强，能够有效防止客户端重复下载升级补丁，节省网络流量和带宽。

2. 所提的可视化操作系统补丁自动安装系统及方法能实时监控补丁安装情况，并根据补丁安装情况进行相应的处理，极大地提升了补丁自动升级的成功率。

3. 所提的可视化补丁自动安装系统及方法能将详细的补丁安装信息可视化显示，并进行分类统计，有效地解决了内外网隔离的内网客户端进行操作系统升级的安全性和升级成本问题，使得内网客户端操作系统升级可以做到及时性，迅速性和便捷性，有效地节约了人力物力以及升级成本问题，同时保证了信息系统的安全性和可靠性。

参考文献

[1]童晓阳，王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化, 2016, v.40;No.581(07):150−154.

[2]王超. 加强关键信息基础设施网络安全保障刻不容缓[J]. 网络空间安全, 2018, 9(06):54−59.

[3]胡国强. 从勒索病毒看网络信息安全的隐患与对策[J]. 信息安全与技术, 2018, 009(001):5−7,20.

[4]龚郁安. 关于委内瑞拉大停电事故的情况分析和关键基础设施的安全防护建议[J]. 信息技术与网络安全, 2019.

[5]张爱侠，施金龙，王滢,等. 电力监控系统安全防护要素[J]. 建筑工程技术与设计，2018, 000(002):1020.

[6]杨浩，付艳芳. 企业局域网安全综述[J]. 电脑知识与技术, 2013(21):63−64.

[7]杨军. 计算机蠕虫病毒的解析与防范[J]. 电脑知识与技术, 2005, 000(010):32−34.

[8]周澎洋，宋岸峰，李宏伟. 多措并举提升电力信息内网安全准入管理水平[C]// 中国电机工程学会年会. 2016.

[9]郭文，周路捷，张洁. 物理隔离环境下操作系统补丁更新方案[J]. 计算机安全, 2013(8):65−70.

[10]孟强龙，周冬青，邵俊. 信息内网计算机操作系统补丁更新研究[J]. 信息化建设，2015, No.206(10):81.

[11]李宇宏. 关于 WSUS 操作系统补丁分发系统部署以及注意事项[J]. 科技与企业，2015, 000(022):69.

[12]余超. 补丁管理系统数据库研究与实现[D]. 四川师范大学, 2012.

基于 OCR 技术的网页篡改检测研究

吴伟斌

（泉州师范学院网络中心　泉州 362000）

摘要：当前网站受到各种安全的威胁态势并未减弱,网站被篡改事件还在增长，除了加强防范外，网页被篡改检测也是重要一环。本文提出基于 OCR(Optical Character Recognition)技术的网页篡改检测模型，利用自然场景文字识别技术对网页截图进行文字识字，经敏感词检测判断网页是否被篡改。经对网页篡改检测模型进行实验，该模型在实验的数据集上准确率较高。

关键词：OCR 网页 篡改检测 场景文字识别

在信息时代，互联网已成为生活一部分，网站成为人们获取信息重要来源，已成为信息传播、电子商务、电子政务等的重要载体。虽然现网站已采取不少的安全防范措施，但由于系统漏洞问题会长期存在，病毒、木马和恶意代码肆虐，网站的被植入后门、被篡改等事件态势并未减弱。网站被篡改事件迅猛增长，已经成为危害比较严重的网络安全问题，截至 2019 年 12 月，国家计算机网络应急技术处理协调中心监测发现我国境内被篡改网站 185573 个，较 2018 年底（7049 个）增长较大[1]。

网络安全问题严重影响网站建设单位的形象,可能造成一定的经济损失和不良社会影响，需构建一个完善的网络安全体系。网站的前置各种软硬件防火墙、Web 应用防护系统、入侵检测系统等安全产品也在不断发展进步，网站系统本身也建立各种防篡改的防护，但篡改事件持续发生。为减少网站被篡改所带来的影响，除了建立有效的防止网页篡改措施，还需继续研究如何在网站被篡改后及时检测识别等工作。

一、相关工作

常见的防网页篡改技术主要有外挂轮巡技术、核心内嵌技术、事件触发技术[2]。三种方法中核心内嵌技术、事件触发技术适用于网络管理员在操作系统、服务器上进行主动部署、主动防御；而外挂轮巡技术即可应用于服务器侧，也可以应用于第三方检测。[3]外挂轮巡技术主要是网页与其基线进行比较来判断完整性，但其对动态网页进行检测、其对网页图片篡改类的识别效果很差，有一定的局限性。为弥补该技术的短板，引进图像识别技术来解决此类问题[3]。文献[3]是用角点检测技术用已知样本图片对网页篡改截图进行有效识别标记。文献[4]利用图像处理中两种特征点检测的方式获取图像中的特征点信息从而起到检测网页是否被篡改的作用。

网页篡改按照攻击手段来分类，有显式篡改和隐式篡改两种方式。[5]本文主要研究显式篡改检测识别，通过网页截图对网页篡改检测进行识别，利用 OCR 文字识别后综合判断检测网页是否被篡改。不少人将 OCR 技术定义为广义的所有图像文字检测和识别技术(简称图文识别技术)，即包括传统的 OCR 识别技术，又包括自然场景文字识别技术[6-7],本文所用 OCR 指的是广义 OCR 技术，将利用自然场景文字识别技术。PaddleOCR 旨在打造一套丰富、领先、且实用的 OCR 工具库[8]，供多种文字检测训练算法和多种文字识别训练算法,本文使用 PaddleOCR 提供的中文 OCR 模型完成文本检测以及文本识别串联任务，对网页截图进行文字识别，对识别后的文本进行敏感词检测判断网页是否被

篡改。

二、篡改检测模型

1. 篡改检测模型实现

具体检测模型实现步骤如下：（1）模拟访问待检测网站，抓取网页并截图保存；（2）OCR 识别截图中的文字生成文本；（3）对生成文本进行敏感词检测。后续若是检测被篡改发送报警到管理员，非文重点讨论不再不再赘述。网页的篡改检测流程如图 1 所示 。

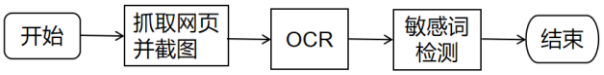


图 1

2. OCR 文字识别

自然场景文字识别技术主要包括两个步骤：文本检测和文本识别，流程如图 2 所示。文字检测上找出文字位置和范围；文本识别对文本检测定位的文本区域进行识别，输出结果：文本信息。

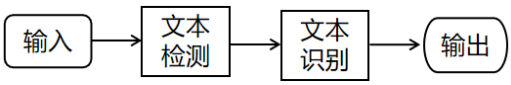


图 2

文字识别是将图片中的文字序列识别的过程。文字识别时输入的是含有文字的候选框,输出是该检测框中的文字序列[9]。PaddleOCR 在文本检测和文本识别分别提供多种算法，下文实验文本检测采用文本检测模型 DB(Differentiable Binarization)[10]算法，文本识别采用 CRNN(Convolutional Recurrent Neural Network)[11]算法。

DB 是一个检测任意形状的场景文本检测网络，利用可微分二值化的方法，可在分割网络自适应地设定二值化阈值。可微分二值化不仅有助于把文字区域与背景区分开，而且还能把相近的实例分离开来。[12]在 ICDAR2015 文本检测公开数据集上，算法效果精度 83.79%[8]。

CRNN 网络是一个端到端的识别网络，包括特征提取、序列分析、序列解码三个部分。该网络首先利用 CNN(Convolutional Neural Networks)提取文本图像的特征，使用双向 LSTM(Long Short-Term Memory)[13]提取上下文特征得到每列特征的概率分布，将语音识别领域的 CTC(Connectionist Temporal Classification)[14]引入图像处理不定长序列对齐问题，对输入的单个词的切分和序列的整合工作。DB 和 CRNN 两个模型串联使用，分别实现文本检测和文本识别。

三、实验与分析

通过工具采集了正常 99 个网站首页的截图及网上收集篡改网页（包含敏感词）截图 11 张图片；对正常 99 个网页的截图模拟网页被篡改操作，通过图片处理技术加入敏感词，然后对图片随机仿射、加噪点等处理，共计产生内含敏感词的图片 246 张；总计获得实验数据 356 张图片，其中正常网页图片 99 张，被篡改网页图片 257 张。

实验硬件环境为虚拟机：Xeon CPU E5-2650 v4、内存 48G，软件环境 CentOS 8、python 3.7。实验采用 PaddleOCR 作为文字识别模型，使用通用中文 OCR 模型(简称为 DB_CRNN)和支持空格的通用中文 OCR 模型(简称为 DB_CRNN_EN)[8]两个模型进行 OCR 文字识别，其中文本检测采用 DB 算法、文本识别采用 CRNN 算法。两个模型分别对图片进行 OCR 文字识别并生成对应的文本，对生成文本进行敏感词检测。

结果评价采用准确率和二值分类器常见的两个指标假正率(False Positive Rate，FPR)、假负率(False Negative Rate，FNR)。FPR 和 FNR 在这里定义如下:

FPR = 被认为正常的篡改页面数/篡改页面总数

FNR = 被认为异常的正常页面数/正常页面总数[15]

表 1 两个模型的 FPR、FNR 和平均值运行时间

模型	准确率/%	FPR/%	FNR/%	平均运行时间/s
DB_CRNN	99.16	1.17	0	48.06
DB_CRNN_EN	99.72	0.39	0	48.76

两个模型的运行时间只计算 OCR 文字识别的运行时间，敏感词检测时间短忽略不计。表 1 所示，通过 OCR 识别网页截图的篡改检测结果，DB_CRNN_EN 模型虽然运行平均时间比 DB_CRNN 模型略长，但假正率较低，检测准确率都高；假负率都为零，说明 OCR 识别网页截图的文本出现敏感词的异常概率接近零，也要选择好敏感词以免正常网页误判为异常。

网页截图进行 OCR 文字识别后的文本进行敏感词检测为最后步骤。如图 3 所示，横坐标为敏感词代码，共计十三个词，纵坐标为检测出敏感词的总数。被篡改网页的图片都包括有两个敏感词，其代码为分别 S01 和 S02，图 3 显示两个模型都未能全部检测出来，经检查主要原因还是图片在加入敏感词的处理时包含两个敏感词的文字都不全，但配合其他敏感词判断准确率接近 100%。同样的数据，对两个模型检测出敏感词的总数统计显示 DB_CRNN_EN 模型较优。

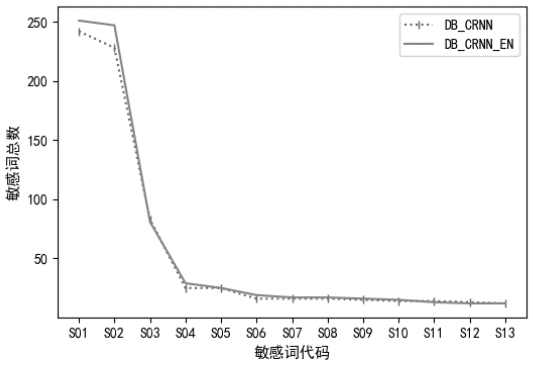


图 3

四、结论

OCR 技术的发展，特别是自然场景文字识别技术快速迭代，为网页截图文字识字提供了可能。本文提出利用 OCR 技术的网页篡改检测模型，采用PaddleOCR 框架和文本检测DB算法与文本识别 CRNN 算法对网页截图进行文字识字，对 DB_CRNN 和 DB_CRNN_EN 模型进行实验，两个模型都有较优的效果、准确率高。该模型也存在不足之处:1)无法识别隐式篡改；2)依赖敏感词，文字之外其他异常信息尚待研究。

参考文献:

[1]中国互联网络信息中心.第 45 次中国互联网络发展状况统计报告(2020−04−28)[EB/OL],[2020−08−08],
http://www.cac.gov.cn/2020−04/27/c_1589535470378587.htm.

[2]盖玲.防网页篡改技术比较分析[J].图书与情报.2007(01)

[3]韩钢.国家互联网应急中心图像处理技术在网页篡改识别上的应用[J].通信管理与技术.2017(03)

[4]颜于凤,沈勇.基于图像处理的网页篡改检测[J].计算机与数字工程.2020(6):1479−1482, 1518

[5]王闻祎.网页篡改检测系统设计与实现[D].西南交通大学 2019

[6]牛小明,毕可骏,唐军.图文识别技术综述[J].中国体视学与图像分析 2019(24):241−256

[7]SIGAI.自然场景文本检测识别技术综述(2018−06−30)[EB/OL],[2020−08−08], https://blog.csdn.net/SIGAICSDN/article/details/80858565

[8]Paddle,PaddleOCR(2020−08−08)[EB/OL][2020−08−08].https://github.com/PaddlePaddle/PaddleOCR

[9]白翔,杨明锟,石葆光,等.基于深度学习的场景文字检测与识别[J].中国科学:信息科学,2018,48(5):531−544.

[10]LiaoMinghui, Wan Zhaoyi, Yao Cong, et al. Real−time Scene Text Detection with Differentiable Binarization[C].National Conference on Artificial Intelligence,
2020.

[11]Shi B, Bai X, Yao C. An end−to−end trainable neural network for image−based sequence recognition and its application to scene text recognition[J]. IEEE transactions on pattern analysis and

machine intelligence,2016,39(11):2298−2304

[12] 墨殇浅尘.场景文本检测(Differentiable Binarization)−DB (2020−07−03)[EB/OL], [2020−08−08],https://www.cnblogs.com/monologues mw/p/13223314.html

[13]Alex Graves,J ü rgenSchmidhuber.Framewise phoneme classification with bidirectional LSTM and other neural network architectures[J].Neural Networks,2005 (5)

[14]Graves A, Fern á ndez S, Gomez F, et al. Connectionist temporal classification: labelling unsegmented sequence data with recurrent neural networks[C]. Proceedings of the 23rd international conference on Machine learning.New York:ACM,2006: 369−376.

[15]魏文晗,邓一贵.基于局部变化性的网页篡改识别模型及方法[J].计算机应用.2013,33(2):430−433

大数据业务场景下的零信任体系架构

朱 熹　程 硕

厦门市美亚柏科信息股份有限公司

摘要：随着大数据的迅速发展，现有大量数据被共享，从分散到云化进行集中管理，从而导致数据滥用风险逐步凸显。基于以上问题本文提出了大数据业务场景下的零信任体系架构，在不可信的网络中构建通过动态安全防护、动态信任管控、动态审批监管、主动风险发现、主动预警响应，来打造一套以“安全”加 “可信”加“合规”为目标的大数据纵深防御体系。

关键字：大数据；零信任；网络安全；

一、引言

如今，大数据、人工智能、5G 和区块链等数字技术发展迅速，其中大数据是信息化发展的新阶段，它不仅能够推动大数据技术产业的创新发展，还能运用大数据提升国家治理现代化水平、促进保障和改善民生。在享受大数据下科技成果给我们带来的美好甘甜之余，也不能忽视大数据治理过程中产生的网络边界模糊等重要问题。数据治理过程中的隐私保护、数据安全与数据共享利用效率之间尚存在明显矛盾，成为制约大数据发展的重要短板。

一方面，数据共享开放的需求十分迫切；另一方面，数据的无序流通与共享，又可能引发隐私保护和数据安全方面的重大风险，必须对其加以规范和限制。大数据业务场景下的安全防护大多数是基于单点或单面防护，对数据整体框架结构安全的防护考虑还不足[1]。因此，我们需要提出一种以防护数据为核心的安全思维方式，在不影响数据资源共享的同时，解决内部人员数据滥用、外部窃取的风险控制问题。

二、传统网络安全模型

1. 传统“边界”网络安全模型

传统的安全模型是以边界模型为基础而逐步完善的，其核心思想是分区、分层，通过划分边界提升网络防御能力。所谓边界就是划分信任和不可信任的设备或网络环境，并在这两者之间建立边界防护服务，从而保证不可信的设备或网络环境无法

在携带威胁信息的情况下，访问到可信的设备或网络环境信息。

随着边界防护技术的发展，越来越多的威胁信息都可以被边界防护直接拦截，这使得边界信任模型看起来完美无缺。但是，边界化网络安全模型存在不可忽视的致命弱点。该模型将所有的“防护”都孤注一掷地依赖于防火墙等边界防护设备，一旦有新的威胁形式超出防护范围，那么这些边界防护设备就形同虚设。譬如攻击者进入内网，内网区域的所有信息将暴露无余。同时传统网络安全往往只顾按部就班地防守，当新的威胁形式来临后才采取应对措施。但新形式安全威胁的发展一定快于防范手段，因此，不能毫无防备的等待危险的降临。

我们不应该一味地防范“坏人”，很多安全威胁事件都是“好人”变坏或是对所谓的“好人”过度信任导致的，信任才是安全最大的漏洞，如图 1 所示。因此，安全思维和安全架构急需进化，构建全新的零信任身份安全架构来重新评估和审视传统边界安全的架构思想。要做到知白守黑，去刻画“好人”的特征，只有符合“好人”的标准才能为其敞开信任的大门。

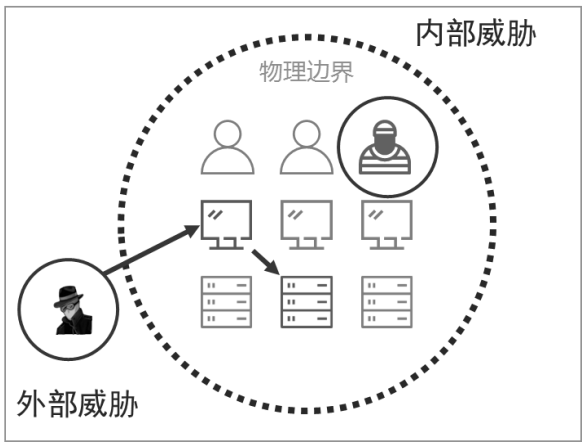


图 1　信任是安全最大的漏洞

2. 传统零信任网络安全模型

2004 年 Jericho Forum 耶利哥论坛起草了“反边界化”的 IT 安全策略，这种策略对公司网络上所有的数据进行加密，让终端使用者只能通过即时授权才能访问公司网络上特定的加密数据。2010 年 Forrester Research 的约翰·金德瓦格（John Kindervag）提出“零信任”的概念。2014 年发表了 BeyondCorp 系列研究论文，成为零信任大规模实施的典范[2]。中国的零信任市场目前仍在导入期，渗透率极低。2019 年，腾讯制定了全球首个零信任行业标准，零信任安全首次被工信部列入网络安全需要突破的关键技术，得到政策认可。

零信任不仅是一个安全术语，更是一种企业资源管理的理念和战略。零信任是基于用户行为的安全模型，其核心理念就是弱化“边界”的概念，不以边界来判定访问用户是否可信[3]。假设所有人事物都是不怀好意的，没有任何主体以及主体的请求是可信的，没有任何资源是可信的，没有任何网络连接是可信的。将资源缩小到单个或更小的资源组，所有资源按需授权，将授权颗粒度最小化。所有用户的每一个访问请求都会被持续、动态的分析评估，只有合法和必要的请求才会被授权，达到“按需授权”和降低不确定性的目的。消除对数据和服务的非授权访问，使访问执行的授权尽可能精细化。重点是通过身份认证、合法授权和最小化隐含信任区域，同时最小化认证机制中的时间延迟来实现。

除非网络明确知道接入者的身份，否则任谁都无法接入到网络。用户的访问权限将不会受到网络位置的限制，不同用户将通过自身被授予的权限拥有不同的访问资源。零信任对访问控制进行了范式上的颠覆，引导安全体系架构从“网络中心化”走向“身份中心化”，其本质诉求是以身份为中心进行访问控制。

零信任架构是对企业级网络发展趋势的回应，企业级网络开始包含远程用户和位于企业网络边界的基于云的资产。为了确保企业能够按照既定预期顺利转型，零信任的发展方向应该更加贴合数字化信息时代的发展趋势。其中，大数据业务场景下的网络安全正面临着巨大挑战，本文着力于构建一款基于零信任安全模型的用来解决当前形势下以数据为中心的安全问题。

三、大数据时代的特点

大数据时代已经真正到来，大量、高速、多样、

价值是人们赋予它的标签。具体来讲就是数据量巨大，数据的爆发性增长迫切的需要智能的算法、强大的数据处理平台和新的数据处理技术，来统计、分析、预测和实时处理如此大规模的数据；数据类型繁多，广泛的数据来源决定了大数据形式的多样性；价值密度低，现实世界所产生的数据中，有价值的数据所占比例很小；数据分析处理速度快，主要通过互联网传输。数据量或数据的多样性，也关系到数据的安全性和隐私性[4]。

再此之前，我们一贯按照一个应用对应一类数据这种独立的模式进行数据安全治理。而大数据的核心优势就是通过数据融合的方式，将数据价值最大化。那么在大数据模式下，多个应用共同使用一个数据中心的情况会普遍存在，如图 2 所示。而这种模式伴随着越来越多的数据共享将导致高敏感、低敏感数据融合导致权限混杂，大量的数据共享势必造成非授权用户访问，数据滥用风险增大，将被动抬高整体风险。

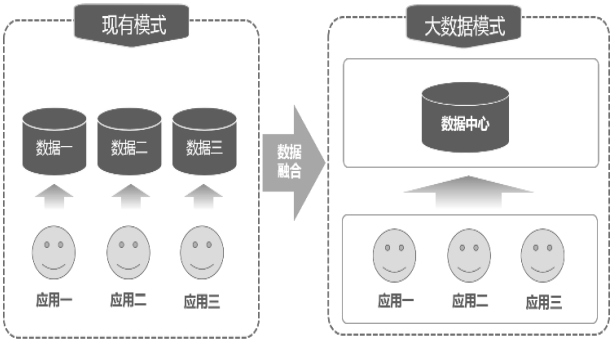


图 2　大数据模式的数据资源分配

数据中心承载着海量数据的集中存储和处理，其安全性和稳定性可能会直接或间接地影响社会安定。数据安全正受到前所未有的挑战，该问题已成为企业资产安全性、个人隐私安全性、国家和社会安全的核心问题[5]。因此，我们急需一种新的安全思维，再次引导安全体系架构从“身份中心化”走向“数据中心化”。

四、大数据业务场景下的零信任体系架构设计

1. 大数据业务场景下的零信任总体思想

大数据业务场景下，我们依然需要具备传统零信任 “安全”的思想，要保障大数据融合后的数据访问安全，还要使用一些可能提前让风险暴露的能力，例如：考虑身份和操作环境是否“可信”，以及用户操作和使用流程是否“合规”等问题，不能等到资源“不安全”才采取措施弥补。因此，大数据零信任需要依托“安全”加“可信”加“合规”的设计理念，隔离一切不可信的访问身份，排除一切不合规的操作手段，打造适用大数据业务场景的零信任体系。

大数据业务场景下零信任的技术本质是：以数据为中心，构建业务安全、可信、合规的动态访问控制机制。它不仅继承了传统意义上零信任“永不信任，始终验证”的理念，还被灌注了其独特的、能有效解决大数据环境下网络安全问题的全新思想。大数据零信任的核心思想主要为：以“防护数据”为中心，将用户、设备、应用和服务、任务等身份统一抽象成主体身份，通过主体身份的属性进行动态认证和鉴权；采用督办监督体系规范数据使用流程；利用业务安全审计发现潜在风险。最终实现对数据“可用可见、可用不可见、不可用不可见”，让数据访问更“安全”，身份认证更“可信”，操作流程更“合规”。

大数据场景下零信任体系的防护目标为，打造一套“安全”加“可信”加“合规”的网络安全模型，具体防护内容有：

1）多维度的身份认证，动态可信的访问控制，实时度量的环境感知，实现持续动态的“可信”传递。

2）细粒度的权限管理。利用权限最小化机制，主要防护数据，通过数据分级分类来控制知悉范围，让有限的人员看到有限的数据，打造“安全”的防护体系。

3）职能角色和任务驱动的审批。使每个独立的事物信息化、流程化和规范化，实现任务的上传下达、

工作督办监督体系和规范数据查询审批流程。

4）全面的业务安全审计。负责发现用户违规

使用的问题，使风险处理更及时，制定完备的“合规”使用标准。

2. 大数据业务场景下零信任体系的核心能力

大数据业务场景下零信任体系的核心能力主要包括：认证能力、环境感知能力、权限管理能力、业务审批能力、业务审计能力、策略控制能力，如图 3 所示。

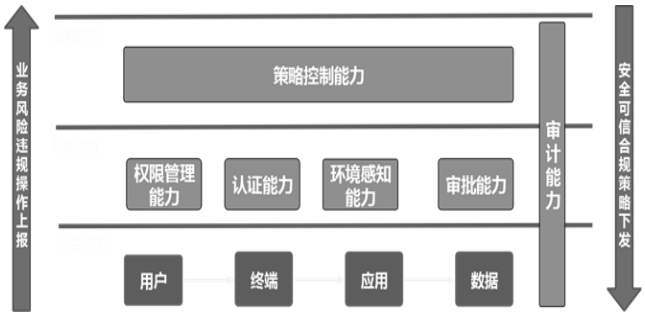


图 3　大数据业务场景下零信任体系的核心能力

其中，认证能力解决“你是谁”的身份可信问题。将用户、设备、应用和服务等的身份均统一抽象成主体身份，负责统一的主体身份管理和身份认证，通过主体身份的属性进行持续动态认证和鉴权，确保主体身份是“可信”的，才能继续访问。

环境感知能力负责发现“环境怎么样”的环境可信问题。对终端身份进行不可仿冒标识，对终端环境进行感知和度量，协助完成终端的安全环境核查，确保操作环境是“可信”的，从而实现动态访问控制的目的。

权限管理能力解决“你能干什么”的访问安全问题。它负责对权限进行维护，并对访问资源的请求进行鉴权，作为第三方为业务应用提供精细化的权限管理，通过将数据权限控制到数据表、数据项以及数据元等级别实现细粒度的权限控制。权限授予、访问控制动态化以及权限最小化是权限管理的核心准则，确保大数据业务场景下零信任体系的访问控制是“安全”的。

审批能力解决“工作任务从哪里来”的流程合规问题。审批工作的信息化、流程化和规范化，实现工作任务的上传下达、工作督办监督体系、规范数据查询流程，确保数据的使用流程是“合规”的。

审计能力负责“发现违规使用”的操作合规问题，贯穿了各大能力。它能够接收零信任体系以及应用系统的业务日志，对用户访问敏感数据、执行关键操作行为等各类业务日志进行真实、全面的记录；对各类业务行为进行审计，并提供异常行为分析、发现、告警和处置的能力，确保用户操作是“合规”的。

策略控制能力决定了整个大数据零信任体系的安全控制流转。负责安全方面的风险汇聚、信任评估、联动通报、安全指令下发。策略控制能力对用户的访问进行综合信任评估，产生安全指令并下发，确保访问过程中风险能够及时发现、及时决策、及时处置，确保整个大数据业务场景下的零信任体系是实时“安全”的。

3. 零信任体系“信任”的传递方式

零信任本质并不是“不信任”，它是通过可信令牌来实现“信任”传递的。大数据业务场景下的零信任安全模型设计了两类令牌，实时为资源信息的安全保驾护航。这里所说的令牌包括用户令牌和应用令牌。

用户令牌是访问者在通过认证时生成的，令牌内容涵盖了用户信息以及环境信息，认证能力可携带令用户牌向其他能力传递“可信”请求。每次认证有且仅有一个用户令牌，当用户退出登录、令牌到期或强制下线时用户令牌失效。

应用令牌是在访问者确定访问应用时生成的，应用令牌不仅包含了用户令牌中承载的用户信息和环境信息，还另外含有确定访问的应用信息，业务应用可携带应用令牌以及相应的请求信息完成信任传递与鉴权。跟用户令牌不同的是，应用令牌不仅仅只有一个，它的个数取决于访问应用的个数。当用户退出登录、令牌到期、强制下线或用户令牌下线时应用令牌失效。

令牌是访问大数据业务的入口和敲门砖，没有安全的令牌就不可能访问到系统内的任何信息以及任何资源，因此，令牌是获得大数据零信任体系信任的第一步。

4. 风险管控办法

尽管大数据业务场景下的零信任体系有动态的身份认证和访问控制等安全防护措施的全方位把控，但也难免会有防护体系外的安全事件以及违规操作等现象的发生。这些现象在本文统称为“风险”。既有风险，就需要罗列出可能存在的风险有哪些，这样就可以提前制定策略，控制风险的发生。

因此，将风险管控办法分为定义、发现、决策、处置以及统计 5 个模块。零信任体系风险管理流程，如图 4 所示。

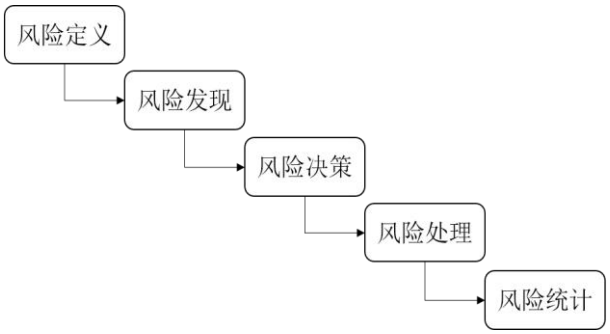


图 4　零信任体系风险管理流程

我们首先做的是定义风险，制定风险识别策略，评估风险等级，给出怎样的风险应对措施，都需要事前定义好。根据这一系列定义好的风险策略，进而发现风险并做出相应决策，通过指令下发、指令执行的方式进行风险处置，给出告警。大数据业务场景下的零信任体系对于发生过的每个风险都有针对性的统计分析，根据统计结果对系统进行实时性的安全评估。风险管理流程，如图 5 所示。

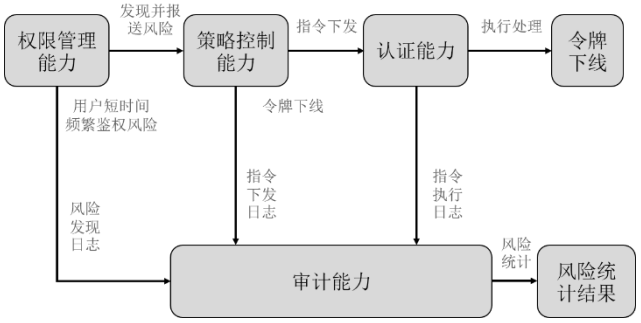


图 5　风险管理流程

一般地，常见的风险是从权限、认证、审批、环境感知等能力在业务处理过程中发现的，这种风险也就是 “违规操作”触发的风险，如表 4-1 所示。

表 4-1 违规操作触发的风险

认证能力	权限能力	审批能力	环境感知能力
频繁身份认证	短时间频繁鉴权	审批内容命中白名单	环境变化
非活体身份认证	短时间频繁白名单命中	提交人与审批人重复	–
多人脸身份认证	鉴权必要条件不完整	一次审批中单人连续审批	–
–	用户持续越权访问	–	–

另外，大数据业务场景下的零信任安全体系还会在日志对账、日志分析的过程中发现风险，这种风险类型属于潜在的安全事件。全方位定义风险点，提前发现、暴露问题，做到及时决策、及时处置，控制发生不可挽回的风险。

大数据业务场景下零信任体系完备的风险管控办法，有着风险及时发现、及时处理的优点，处置方式一般包含令牌下线或权限冻结。风险管控是零信任网络安全架构的最后一道防线，在大数据业务场景中尤为重要。

五、结束语

传统零信任引导安全体系架构从“网络中心化”走向“身份中心化”，使得用户的访问权限将不再受到地理位置的影响。在多样性的大数据业务场景下，为了避免数据融合导致的数据滥用风险，本文提出了大数据业务场景下的零信任体系架构，再次让安全体系架构从“身份中心化”向“数据中心化”过度。

大数据业务场景下的零信任依托传统零信任“安全”的思想，提出六个控制数据中心访问安全的核心能力，其中，权限管理能力和策略控制能力负责访问控制的“安全”，认证能力和环境感知能力为了保障访问资源主体身份的“可信”，审批能力、审计能力确保操作流程的“合规”。大数据业

务场景下的零信任构建 “安全”加“可信”加“合规”的安全防御体系，实现对大数据业务场景下的数据访问行为进行精细化访问控制，为大数据中心的整体安全架构提供技术支撑。

参考文献

[1]薛朝晖,向敏.零信任安全模型下的数据中心安全防护研究［J］.通信技术，2017（6）：1294.

[2]Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security.

[3]吕波.以零信任技术为指导的数据安全体系研究[J].现代信息科技,2020,4(12):126-130+133.

[4]Moreno, J., Serrano, M. A., & Fern á ndez-Medina, E. (2016). Main issues in big data security. *Future Internet*, *8*(3), 44.

[5]Toshniwal, R., Dastidar, K. G., & Nath, A. (2015). Big data security issues and challenges. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, *2*(2).

基于复杂异常值的 DDOS 异常网络流量检测技术

余建　林志兴

（三明学院网络中心　福建三明　365004）

摘　要：为保障网络信息安全，结合在局域网出口环境下的网络流量情况，通过基于时间序列的附加异常值和新息异常值检测方技术，利用迭代方法的异常值检验方法对网络出口的流量变化进行监控，以及时地检测出流量的异常。然后利用端口异常流量检测算法对异常流量特征进行提取和过滤，进而进一步检测出异常网络数据包。最后实验结果表明该方法在在检测网络的 DDOS 攻击方面时，能较好的取得检测效果，并对该算的优劣性进行了分析。

关键词：局域网；时间序列；复杂异常值；DDOS；网络流量

中图分类号：TP393　　标识码：A　　文章编号:

1 引言

分布式拒绝服务（通常缩写为 DDOS）[1-3]是一种因电影和互联网而臭名昭着的网络攻击。简而言之，这是一种拒绝任何类型服务的情况。DOS 仅代表拒绝服务。这项服务可以是任何类型的传统的异常流量攻击，对于计算机和计算机网络，或在道德黑客攻击期间，拒绝服务可以采取以下形式：劫持网络服务器使用请求重载端口使其无法使用拒绝无线认证拒绝在 Internet 上提供的任何类型的服务可以从单个机器执行这种意图的攻击[4]。虽然单机攻击更容易执行和监控，但它们也易于检测和缓解。为了解决这个问题，可以从遍布广泛区域的多个设备执行攻击。这不仅难以阻止攻击，而且几乎不可能指出主要罪魁祸首。此类攻击称为分布式拒绝服务或 DDOS 攻击。分布式拒绝服务攻击，会产生大量的垃圾数据包来堵塞网，从而导致网络大面积瘫痪。

2 相关研究

2.1 DDOS 流量统计特征分析

DDOS 攻击中，其流量还是有一定的特征可寻的[5]，毕竟大部份 DDOS 攻击由人为编写的恶意攻击程序而发起的[6]。非专业的黑客一般会使用相关的黑客工具发起 DOS/DDOS 攻击，因为隐蔽性和专业性不强，一般都可以根据 IP 来追踪其踪迹。DOS/DDOS 攻击中，所产生的数据包由于产生的速度和时间都比较快，如果攻击数据包都使用不同生成方法的话，必须会使发包的速度变慢，影响攻击的效果。由于受到攻击的所有内容实际上都是在计算机上运行，因此如果可以降低计算机上的性能，则可以使服务不可用。这是DOS和DDOS的基础。一些 DOS 攻击是通过使用连接请求泛滥服务器来执行的，直到服务器过载并被认为是无用的。其他通过将未分段的数据包发送到服务器来执行，而服务器无法处理。这些方法在由僵尸网络执行时，会以指数方式增加他们正在进行的破坏程度，并且难以减轻突飞猛进的增加。

异常行为[7]的流量中一般包括异常行为过程中的各个会话数据,包括源 IP,源端口,源掩码,目标 IP,目标端口,目标掩码,协议类型,TCP/Flag,源设备接口,目标设备接口,流量大小，数据包数，数据包大小等详细信息。系统能够在全网中发生异常事件或行为时，实时记录异常明细数据,包括异常行为过程中的各个会话数据, 包括源 IP,源端口,源掩码,目标IP,目标端口,目标掩码,协议类型,TCP/Flag,源设备接口,目标设备接口,流量大小，数据包数，数据包大小等详细信息。

2.2 相关文献研究

在 DDOS 异常网络流量检测的研究工作中，刘纪伟等[8]提出了一种综合考虑网络流量双向特征、固定特征和统计特征,采用增量式神经网络算法的 DDoS 攻击检测方法。根据 DDoS 攻击流量的特点提取流量特征,组成流量八元组联合特征,然后利用增量式 GHSOM 神经网络算法进行异常流量分析。而高一为等[9]利用小波分解网络流量的方法，提出了一种基于数据预处理的分布式拒绝服务 DDoS 攻击检测算法。通过对小尺度流量数据进行预处理，使得短相关的网络流量体现出长相关性并保持小尺度模型的时间敏感度，满足了 Hurst 指数刻画多分形模型的条件，解决了现有小尺度网络异常实时检测方法的缺陷。宋宇波等[10]提出由触发检测和深度检测相结合的 DDOS 联合检测方案,将低开销、粗粒度的触发检测算法与高精度、细粒度的深度检测算法相结合,在保障高检测精度的前提下降低了系统的复杂度；同时,在 Mininet 平台上实现了基于 SDN 的 DDoS 攻击检测系统。

本文针对 DDOS 攻击以及恶意扫描时通过的异常流量攻击检测，过基于时间序列的附加异常值和新息异常值检测方技术，利用迭代方法的异常值检验方法对网络出口的流量变化进行监控，，提出一种基于复杂异常值的的 DDOS 异常网络流量检测。

3 基于复杂异常值的 DDOS 异常网络流量检测模型及算法

基于复杂异常值的 DDOS 异常网络流量检测模型主要包括如下两部分。

1) DDOS 流量特征提取:首先采集网络中的流数据，然后对 DDOS 的流量进行特征分析，最后进行数据采样。

2) 检测过程:首先对出口的端口流量进行统计，通过基于复杂异常值的流量检测算法（附加异常值和新息异常值）进行流量检测，最后对端口流量异常值进行检测，最后输出检测结果。

基于复杂异常值的 DDOS 异常网络流量检测模型如图 1 所示。

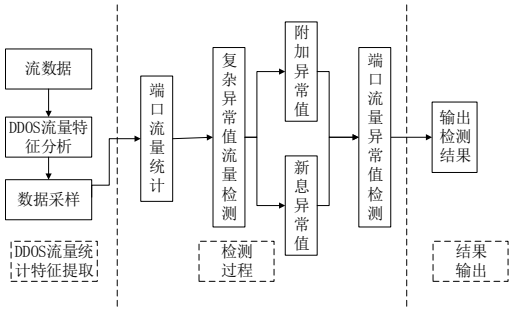


图 1 基于复杂异常值的 DDOS 异常网络流量检测模型

3.1 附加异常值和新息异常值

为了不失一般性，考虑一个零均值的平稳过程[11]。令 Z_t 是观测序列，X_t 无异常值的序列。假定 $\{X_t\}$ 适合一个普通的 ARMA（p,q）模型：

$$\phi(B)X_t=\theta(B)a_t \tag{1}$$

其中，$\phi(B)=1-\phi_1B-\mathrm{L}\ -\phi_pB^p$，$\theta(B)=1-\theta_1B-\mathrm{L}\ -\theta_qB^q$，是没有公共因子的平稳和可逆算子，$\{a_t\}$ 是相互独立、具有相同分布 N（0，σ_a^2）的白噪声序列，附加异常值（AO）模型定义为：

$$Z_t=\begin{cases}X_t, & t\neq T\\ X_t+\omega, & t=T\end{cases} \tag{2}$$

$$=X_t+\omega I_t^{(T)} \tag{3}$$

$$=\frac{\theta(B)}{\phi(B)}a_t+\omega I_t^{(T)} \tag{4}$$

其中

$$I_t^{(T)}=\begin{cases}1, & t=T\\ 0, & t\neq T\end{cases}$$

是描述在时刻 T 时异常值是否存在的示性函数。新息异常值（IO）模型定义为：

$$Z_t=X_t+\frac{\theta(B)}{\phi(B)}\omega I_t^{(T)} \tag{5}$$

$$=\frac{\theta(B)}{\phi(B)}\left(a_t+\omega I_t^{(T)}\right) \tag{6}$$

因此，附加异常值只影响第 T 个观测值 Z_T，而新息异常值通过由 $\theta(B)/\phi(B)$ 描述的系统记忆影响 $t=T$ 时刻之后的所有观测值 Z_T,Z_{T+1},L 。

更一般地，一个时间序列可以包含若干个（如 k 个）不同类型的异常值，我们有下面的一般异常值模型：

$$Z_t=\sum_{j=1}^{k}\omega_j\nu_j(B)I_t^{(T)}+X_t \tag{7}$$

其中，对于 $X_t=\frac{\theta(B)}{\phi(B)}a_t$，$\nu_j(B)=1$；而对于 1O 在时刻 $t=T_j$ 有 $\nu_j(B)=\frac{\theta(B)}{\phi(B)}$。

3.2 当发生时刻已知时异常值影响的估计

为了引出 AO 和 IO 的检验方法，我们考虑 T 和式（1）中所有参数都为已知的简单情形。令

$$\pi(B)=\frac{\theta(B)}{\phi(B)}=\left(1-\pi_1B-\pi_2B^2-\mathrm{L}\ \right) \tag{8}$$

定义

$$e_t=\pi(B)Z_t \tag{9}$$

由式（4）和式（6）可得：

AO：$e_t=\omega\pi(B)I_t^{(T)}+a_t$ （10）

和

IO：$e_t=\omega I_t^{(T)}+a_t$（11）

对于 n 个有效的观测值，式（10）的 AO 模型可写为：

$$\begin{bmatrix}e_1\\ \mathrm{M}\\ e_{t-1}\\ e_T\\ e_{T+1}\\ e_{T+2}\\ \mathrm{M}\\ e_n\end{bmatrix}=\omega\begin{bmatrix}0\\ \mathrm{M}\\ 0\\ 1\\ -\pi_1\\ -\pi_2\\ \mathrm{M}\\ -\pi_{n-T}\end{bmatrix}+\begin{bmatrix}a_1\\ \mathrm{M}\\ a_{T-1}\\ a_T\\ a_{T+1}\\ a_{T+2}\\ \mathrm{M}\\ a_n\end{bmatrix} \tag{12}$$

令 $\hat{\omega}_{AT}$ 是对 AO 模型中 ω 的最小二乘估计。由于 $\{a_t\}$ 是白噪声序列，由最小二乘理论有：

$$\text{AO：}\ \hat{\omega}_{AT}=\frac{e_T-\sum_{j=1}^{n-T}\pi_j e_{T+j}}{\sum_{j=0}^{n-T}\pi_j^2}=\frac{\pi^*(F)e_T}{\tau^2} \quad (13)$$

其中，$\pi^*(F)=\left(1-\pi_1F-\pi_2F^2-\mathrm{L}\ -\pi_{n-T}F^{n-T}\right)$，$F$ 是前移算子，有 $Fe_t=e_{t+1}$，$\tau^2=\sum_{j=0}^{n-T}\pi_j^2$。估计的方差为：

$$\begin{aligned}\mathrm{Var}\left(\hat{\omega}_{AT}\right)&=\mathrm{Var}\left(\frac{\pi^*(F)e_T}{\tau^2}\right)\\&=\frac{1}{\tau^4}\mathrm{Var}\left[\pi^*(F)a_T\right]\\&=\frac{\sigma_a^2}{\tau^2}\end{aligned} \quad (14)$$

类似地，令 $\hat{\omega}_{IT}$ 是 IO 模型 ω 的最小二乘估计，可得

$$\text{IO：}\ \hat{\omega}_{IT}=e_T \quad (15)$$

及

$$\begin{aligned}\mathrm{Var}\left(\hat{\omega}_{IT}\right)&=\mathrm{Var}\left(e_T\right)=\mathrm{Var}\left(\omega I_t^{(T)}+a_T\right)\\&=\sigma_a^2\end{aligned} \quad (16)$$

因此，在时刻 T 的 IO 影响的最好估计是残差 e_T，而 AO 影响的最好估计是残差 $e_T,e_{T+1},\mathrm{L}\ ,e_n$ 的线性组合，其权数依赖于时间序列的结构。容易看出，$\mathrm{Var}\left(\hat{\omega}_{AT}\right)\le\mathrm{Var}\left(\hat{\omega}_{IT}\right)=\sigma_a^2$，且在某些场合 $\mathrm{Var}\left(\hat{\omega}_{AT}\right)$ 可能比 a_a^2 小得多。

可以实施各种假设检验：

H_0：Z_T 既不是 AO 也不是 IO

H_1：Z_T 是 AO

H_2：Z_T 是 IO

对于 AO 或 IO 的似然比检验为：

$$H_1\ \text{vs.}\ H_0:\ \lambda_{1,T}=\frac{\tau\hat{\omega}_{AT}}{\sigma_a} \quad (17)$$

和

$$H_2\ \text{vs.}\ H_0:\ \lambda_{2,T}=\frac{\hat{\omega}_{IT}}{\sigma_a} \quad (18)$$

在原假设 H_0 条件下，$\lambda_{1,T}$ 和 $\lambda_{2,T}$ 都满足 $N(0,1)$ 分布。

3.3 异常值迭代检验

如果 T 是未知的，而时间序列的参数是已知的，那么我们可以对于 $t=1,2,\cdots,n$ 着手计算 $\lambda_{1,T}$ 和 $\lambda_{2,T}$，然后基于前述样本结果作出判断。但是，事实上时间序列的参数 ϕ_j,θ_j,π_j 和 σ_a^2 通常是未知的，必须去估计。众所周知，异常值的存在将使参数估计产生严重偏差。特别是如前所述，σ_a^2 常被估计过高。Chang 和 Tiao（1983）提出了迭代检验方法，用来处理 AO 或 IO 存在的个数为未知的情形。

Step 1　假设网络流量序列值正常，对序列 Z_t 建模，并由所估计的模型计算残差，即

$$\begin{aligned}e_t&=\hat{\pi}(B)Z_t\\&=\frac{\hat{\phi}(B)}{\hat{\theta}(B)}Z_t\end{aligned} \quad (19)$$

其中，$\hat{\phi}(B)=\left(1-\hat{\phi}_1B-\mathrm{L}\ -\hat{\phi}_pB^p\right)$，$\hat{\theta}(B)=\left(1-\hat{\theta}_1B-\mathrm{L}\ -\hat{\theta}_qB^q\right)$，令

$$\hat{\sigma}_a^2=\frac{1}{n}\sum_{t=1}^{n}e_t^2$$

这是 σ_a^2 的初始估计。

Step 2　利用已估计的模型，对 $t=1,2,\cdots,n$，计算 $\hat{\lambda}_{1,t}$ 和 $\hat{\lambda}_{2,t}$。定义

$$\hat{\lambda}_T=\max_t\max_i\left\{\left|\hat{\lambda}_{i,t}\right|\right\} \quad (20)$$

这里 T 记为最大值发生的时刻。如果 $\hat{\lambda}_T = \left|\hat{\lambda}_{1,T}\right| > C$，其中 C 是预先确定的正常数，通常取 3 和 4 之间的某值，于是在时刻 T 有一个 AO，其影响用 $\hat{\omega}_{AT}$ 来记。我们可以用式（4）修正数据如下：

$$Z_t^{(1)} = Z_t - \hat{\omega}_{AT} I_t^{(T)} \tag{21}$$

并由式（10）定义新的残差：

$$e_t^{(1)} = \hat{e}_t - \hat{\omega}_{AT}\hat{\pi}(B) I_t^{(T)} \tag{22}$$

如果 $\hat{\lambda}_T = \left|\hat{\lambda}_2, \tau\right| > C$，那么在时刻 T 存在影响为 $\hat{\omega}_{IT}$ 的 IO。利用式（5）修正数据，IO 的影响可以消除，即

$$Z_t^{(2)} = Z_t - \frac{\hat{\theta}(B)}{\hat{\phi}(B)} \hat{\omega}_{IT} I_i^{(T)} \tag{23}$$

由式（11）定义新的残差序列：

$$e_t^{(2)} = \hat{e}_t - \hat{\omega}_{IT} I_t^{(T)} \tag{24}$$

由此，可以从修正后的残差计算新的估计 σ_e^2。

Step 3　在修正后残差和 σ_e^2 的基础上再次计算 $\hat{\lambda}_{1,t}$ 和 $\hat{\lambda}_{2,t}$，并重复 Step 2，直到所有的异常值都被识别出来。$\pi(B)$ 中的初始估计仍保持不变。

Step 4　假设 Step 3 结束后，有 k 个异常值在时刻 T_1，T_2，…，T_k 被试探识别出。将这些时刻当作已知值来处理，估计异常值参数 ω_1，ω_1,L ω_k，并同时估计时间序列参数，这需要用到下述模型：

$$Z_t = \sum_{j=1}^{k} \omega_j v_j(B) I_j^{(T_j)} + \frac{\theta(B)}{\phi(B)} a_t \tag{25}$$

其中，在时刻 $t = T_j$，若对应 AO，$v_j(B) = 1$；若对应 IO，$v_j(B) = \theta(B)/\phi(B)$。由此便导致了新的残差：

$$\hat{e}_t^{(1)} = \hat{\pi}^{(1)}(B)\left[Z_t - \sum_{j=1}^{k} \omega_j \hat{v}_j(B) I_t^{(T_j)}\right] \tag{26}$$

于是 σ_a^2 的修正估计就可以计算出来。

重复 Step 2 到 Step 4，直到所有的异常流量值都被检测出，并同时估计出它们的攻击影响。这样，我们就得到下面拟合复杂异常值的模型：

$$Z_t = \sum_{j=1}^{k} \hat{\omega}_j \hat{v}_j(B) I_i^{(T_j)} + \frac{\hat{\theta}(B)}{\hat{\phi}(B)} a_t \tag{27}$$

其中，$\hat{\omega}_j, \hat{\phi}(B) = \left(1 - \hat{\phi}_1 B - \text{L} - \hat{\phi}_p B^p\right)$ 和 $\hat{\theta}(B) = \left(1 - \hat{\theta}_1 B - \ldots - \hat{\theta}_q B^q\right)$ 是在最后一次迭代中得到的。

3.4 异常值流量的统计算法

我们知道基于大型局域网的网络环境，用户的流量都是通过路由器进出，在多出口环境下，本文针对了对多个端口的不同目的 IP 流同时进行检测，运用矩阵的方法对每个路由器特定端口的特定目的 IP 流设定统计数值。再通过附加异常值和新息异常值算法来判断其异常流量。

首先记 $\{x_{n,m}\}$ 为在第 n 个时间段，第 m 个流入某端口的统计量，则有

$$\delta_{n,m} = (1-\beta) \times \delta_{n-1,m} + \beta \times x_{n,m}, \delta_{0,m} = x_{0,m} \tag{28}$$

$$Z_{n,m} = x_{n,m} - \delta_{n,m} - d \tag{29}$$

$$S_{n,m} = \sum_{i=0}^{n} Z_{i,m}, S_{0,m} = 0 \tag{30}$$

$$Y_{n,m} = S_{n,m} - \min_{1 \le k \le n} S_{k,m} \tag{31}$$

其中 $\delta_{n,\text{m}}$ 为第 m 个端口统计序列 $\{x_{n,m}, n = 1,2,3,\text{L}\}$ 的均值，β 为 EWMA

（Exponentially Weighted Moving Average）系数。通常情况下取 β=0.01~0.03，d 为使统计量 $E(Z_{n,m})$ 在正常情况下小于 0 的偏移。

定义 2：在 $n\times m$ 的随机矩阵中，对于第 m 列序列的统计量，如果在 $t-1$ 时间段内没有检测出异常，那么在 t 时刻检测出异常当且仅当（其中 h 为门限）

$$Y_{n,n}\le h,\quad n=1,2,3,\mathrm{L}\ ,t-1$$

$$Y_{t,m}>h$$

根据以上定义得：

$$Y_{n,m}-Y_{n-1,m}=Z_{n,m}-\min\left\{0,S_{n,m}-\min_{1\le k\le n-1}S_{k,m}\right\}=\max\left\{Z_{n,m},Z_{n,m}-S_{n,m}+\min_{1\le k\le n-1}S_{k,m}\right\}$$
$$=\max\left\{Z_{n,m},\min_{1\le k\le n-1}S_{k,m}-S_{n-1,m}\right\}=\max\left\{0,-Y_{n-1,m}\right\}$$

即：

$$Y_{n,m}=\left(Y_{n-1,m}+Z_{n,m}\right)^{*},\qquad Y_{0,m}=0 \tag{32}$$

其中 X^{*} 定义为：

$$X^{*}=\begin{cases}x & x>0\\ 0 & x\le 0\end{cases} \tag{33}$$

$Y_{n,m}$ 值越大，则遭到的 DDOS 攻击性就越强。

3.5 基于端口的复杂异常值流量检测

3.5.1 端口网络流量分析

在文献[11]中，提出了一种端口流量检测算法，先通过观察网络出口的流量变化，然后再统计出其端口输入输出的统计特征，再设定阀值判断异常流量的变化，最后获得异常流量值的。其算法如下：

（1）网络正常时的出口网络流量值（输出和输入值）：

$$C_{out}(n)\sim C_{in}(n)\quad 0\le E\left(\frac{|C_{in}(n)-C_{out}(n)|}{C_{out}(n)+C_{in}(n)}\right)<t<1 \tag{34}$$

（2）异常流量下 DDOS 攻击的网络端口网络流量值：

$$C_{out}(n)=C_{in}(n)\text{或}C_{in}(n)=C_{out}(n),\quad 1>E\left(\frac{|C_{in}(n)-C_{out}(n)|}{C_{ant}(n)+C_{in}(n)}\right)>t \tag{35}$$

我们把式中 C_{in} 表示为校园网输入的网络流量，C_{out} 为输出的网络流量，t 表示正常网络流量阀值上限，当然不同的网络情况下，t 值也不一样：

$$t=\max\left\{E\left(\frac{|C_{in}(n)-C_{out}(n)|}{C_{out}(n)+C_{\mathrm{in}}(n)}\right),\quad n=1,2,3,\mathrm{L}\right\} \tag{36}$$

3.5.2 基于端口的异常值流量检测

根据文献[12] 我们定义网络出口端口为 m，那么其在第 n 时间段的网络流量为：

$$x_{n,m}=\frac{|C_{in}(n,m)-C_{out}(n,m)|}{C_{out}(n,m)+C_{in}(n,m)},\quad n=1,2,3,\mathrm{L} \tag{37}$$

设 $Z_{n,m}$ 为网络流量的检测变量，由于网络的流量值一直是一个动态的不断变化的的数值[11]，因此 $Z_{n,m}$ 也会随着流量的变化而变化。在非 DDOS 攻击的情况下 $x_{n,m}\in(0,t)$，$t<1$，$Z_{n,m}=x_{n,m}-\delta_{n,m}-d$（$\delta_{n,m}$，$d>0$），由此检测变量 $Z_{n,m}$ 将符合上述两个必要条件。

我们定义检测时间为 T_a，攻击反应时间 ρ_n：

$$T_a=\inf\{n:Y_n>h\} \tag{38}$$

$$\rho_n=T_n-T_a \tag{39}$$

其中 T_a 为 DDOS 攻击的初始时间。

根据一般情况下攻击对 $x_{n,m}$ 产生的流量抖动情况，可以设定以下参数：

$$d = \mu \times \delta_n \quad \mu \in (0.05, 0.25) \tag{40}$$

$$h = \lambda \times \delta_n \quad \lambda \in (10, 20) \tag{41}$$

其中 μ 为偏移比率，λ 为门限倍数，端口均值 $\delta_n = \sum_{i=1}^{m} \delta_{n,i}$。

由式（36）、式（37）和式（39）得：

$$\rho = \inf\left\{k : \sum_{i=0}^{k} \left(x_{n,m} - \delta_m - d\right) > h\right\} \tag{42}$$

4 测试与分析

4.1 测试准备

为了验证复杂异常值的 DDOS 检测技术，我们采集了某高校 2020 年某 3 个月的校园网中相关出口设备流量的数据，按照网络安全结构的需求，本文实验网络拓扑如图 3，出口流量值为 1GB。在测试检测时，先收集校园网中的较为稳定流量的基数，再根据式（28）计算出较稳定的 δ_n，设定 $\mu \in$（0.05,0.25）和 $\lambda \in$（3.5,7.5）。最后由式（40）和式（41）计算出所需要的门限 h 和零值偏移 d，最后再对其网络进行流量值检测。

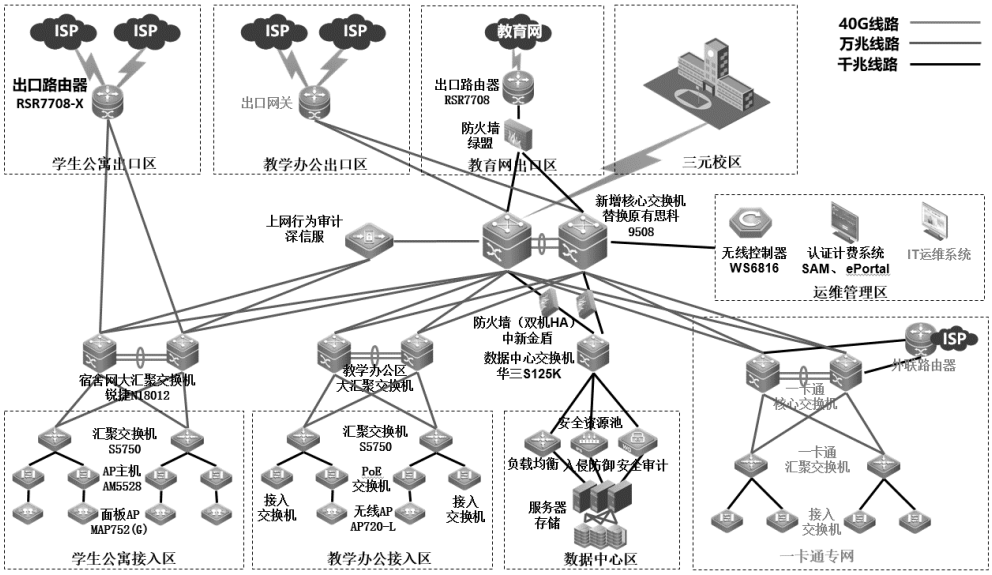


图 2 某高校安全网络系统拓扑下的测试环境

4.2 功能测试

我们知道，当一个局域网遭攻击时，可以通过异常流量指数、系统脆弱性指数、APT 攻击指数、网站安全指数、网络攻击指数[13-16]等因素来判断其攻击的严重性，其严重性可由不同攻击的指数来确定。我们以某高校一周的出口流量为例（如图 3），可以观测到，除周日外，日常流量都较为稳定。我们利用异常值检测法来检测其是否遭受 DDOS 攻击，并来判断网络是否正常。

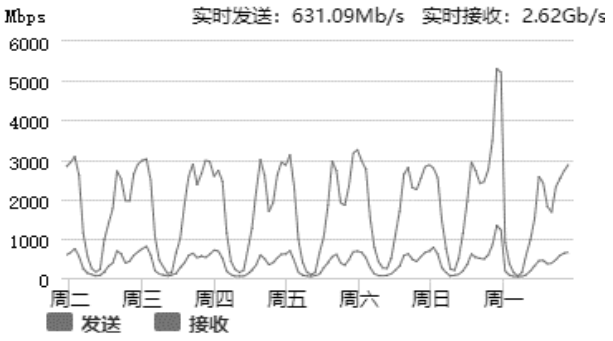


图 3 某高校出口网络实际流量监控图

为了验证该算法的可操作性，我们抽取了该大学 2019 年 12 月某天 $T_0 \to T_5$（取值为 7:00−12:00）时间段的运行服务情况，每个时间段分别以 1 小时为单位，现假设观察了 8:00−12:00 期间 5 个时间点的异常流量值，观测基准值为 500MB，根据式（27），可得 $T_0 \to T_4$ 时间段内复杂异常流量值情况表，如

图 1 所示：

表 1　网络端口流量值检测

$T(n)$	$X_{n,m}$	$Z_{n,m}$	复杂异常流量值（MB）
T_0	0.12	0.11	59.25
T_1	0.21	0.23	231.19
T_2	0.29	0.31	298.94
T_3	0.14	0.16	199.56
T_4	0.92	0.93	983.25
T_5	0.82	0.81	883.28

实验数据表明，当网络在正常情况和在较高强度的的 DDOS 攻击下，对端口 m 的统计数据 $X_{n,m}$ 和 $Z_{n,m}$ 的波动均值小于 1，复杂异常流量值检测在 T_4 和 T_5 时段的流量值为 983.25MB 和 883.28MB，处于出口端口流量值的极限制范围之内，而 $X_{n,m}$ 和 $Z_{n,m}$ 也分别达到 0.92、0.93 和 0.82、0.81，符合当时异常值的检测要求。

接着，在测试实验中，我们利用 Namp 以速率分别为 145MB/ 秒和 912MB/ 秒发起混合（UDP+ICMP+TCP）、UDP Flooding、ICMP Flooding、TCP SYN Flooding 等攻击，如表 2 所示。可以看到在 ICMP FLooding 和 UDP FLooding 攻击中，攻击开销 μ 值都较大，由此可以检测到复杂异常值流量。

表 2 网络端口攻击检测结果

攻击方式	偏移比率 μ (s/pkt)	存活的端口数	未建立流的比 U（%）
混合（UDP+ICMP+TCP）	0.3521	21	21.12
UDP FLooding	0.5042	8	31.28
ICMP FLooding	0.3427	22	56.25
TCP SYN FLooding	0.1264	56	98.3
正常状态	0.0032	212	13.17

图 4 是 53413 攻击端口在网络出口设备的数据。图 5 是复杂异常值算法对原始数据检测结果。由图 4 和图 5 可以分析出两者流量检测结果基本一致，本检测方法可行性较高。

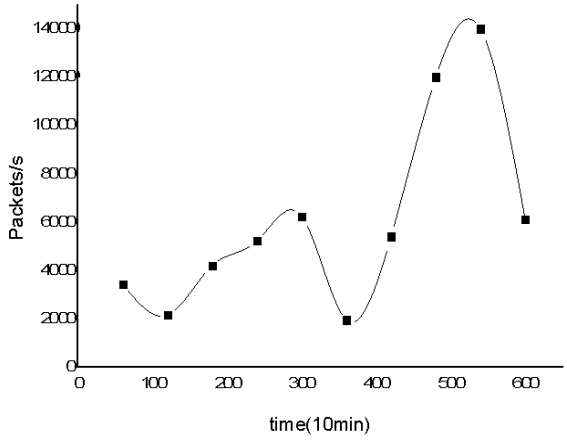


图 4　53413 端口数据

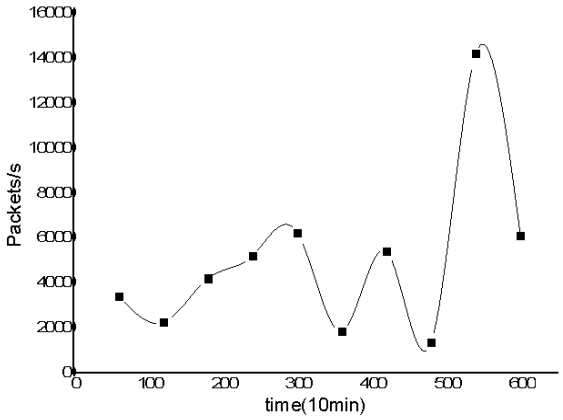


图 5 复杂异常网络流量对原始数据的检测结果

4.3 性能比较

算法的性能也可以用流量异常检测率[17-18] C_D

与 E_F 误报率来讨论。C_D 和 E_F 的值由下式计算：

$$异常检测率C_D=\frac{正确检测的异常攻击流量}{总流量} \quad (43)$$

$$误报率E_F=\frac{误检测出的异常攻击流量}{总流量} \quad (44)$$

我们取文献 8 及文献 10 的检测算法与本文进行比较，不同算法的检测结果如表 3 所示。

表 3 取不同 d 值的系统检测效率

检测方式	文献 8 检测	文献 10 检测	本文检测
已知的异常 DDOS 流量	15	15	15
正确匹配的异常 DDOS 流量	9	11	13
误检测的异常 DDOS 流量	3	5	0
异常检测率 C_D（%）	0.60	0.73	0.87
误报率 E_F（%）	0.36	0.21	0

图 6 为三种检测算法的概率与运行时间关系图，在相同运行时间里，根据不同的检测概率来验证三种算法的性能。从仿真的实验里，假设概率为 X，

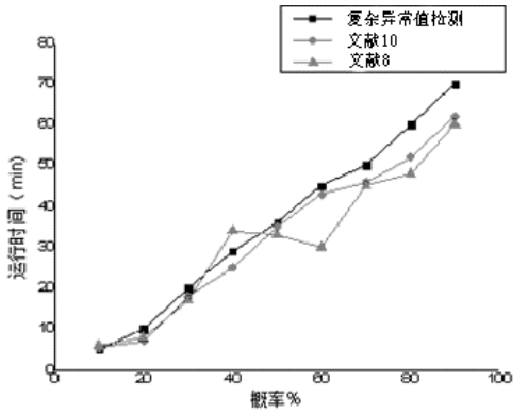


图 6 三种算法概率与运行时间的关系

我们可以看出，当概率 X 在运行时间为 30 分钟时，本文检测方法的概率强于其他两种的检测算法。

5 结论

本文通过基于复杂异常值的的 DDOS 异常网络流量检测在校园网上的应用，能够较快检测出网络中的 DDOS 异常流量。同时测试表明，复杂异常值与文献 8 和文献 10 检测算法的检测性能。对于复杂异常值算法，15 个已知异常点有 13 个被检出，检测率为 87%，误报为 0；文献 8 算法中 15 个已知异常点有 9 个被检出，检测率为 60%，误报率 36%；文献 10 检测算法中 15 个已知异常点有 11 个被检出，检测率为 73%，误报率 21%。由此看来，在测试过程中，复杂异常值检测算法的性能较优，可靠性较强。

但由于本文算法的检测效率并不是固定的，其与攻击流的特征有密切的关系：好的特征过滤效率高，差的特征过滤效率也就差，每一个攻击都有其不同的效率，对于某些特殊环境下的精心构建的攻击甚至失去流量特征，因此此算法并没有一个确定的效率理论值。但是对 前出现的常规异常流量攻击方法，此算法还算相当有效的，如何进一步挖掘拒绝服务攻击的有效特征，还待进一步解决。

参考文献：

[1] Rajeev Singh,SudeepTanwar,TeekParval Sharma. Utilization of blockchain for mitigating the distributed denial of service attacks[J]. Security and Privacy,2020,3(3).

[2] 薛田良,刘希懋,张赟宁,曾阳阳.拒绝服务攻击下的分布式弹性负荷频率控制[J].电测与仪表,2020,31（7）:233-2361-6

[3] Hassidim A, Raz D, Segalov M, et al. Network

utilization: the flow view[C]//Proceedings of the 2013 IEEE International Conference on Computer Communications (INFOCOM '13),Turin,Italy,2013.Piscataway,NJ,USA:IEEE,2013:1429−1437.

[4] Braga R, Mota E, Passito A. Lightweight DDoS flooding at−tack detection using NOX/OpenFlow[C]//Proceedings of the 2010 IEEE 35th Conference on Local Computer Net−works (LCN '10), Denver, USA, Oct 2010. Piscataway, NJ,USA: IEEE, 2010:233−236

[5] SareenaKarapoola,Prasanna Karthik Vairam,ShankarRaman,V. Kamakoti. Net−Police: A network patrolling service for effective mitigation of volumetric DDoS attacks[J]. Computer Communications,2020,150.

[6] Qazi Z A, Lee J, Jin Tao, et al. Application−awareness in SDN[C]//Proceedings of the 2013 ACM SIGCOMM Confer−ence on Data Communication (SIGCOMM '13), Hong Kong,China, 2013. New York, NY, USA:ACM, 2013:487−488.

[7] 薛少勃. 基于流量的网络异常行为检测方法研究[D].哈尔滨工程大学,2019.

[8] 刘纪伟, 李睿楠, 张玉等. 一种增量式 GHSOM 算法在 DDoS 攻击检测中的应用[J]. 南京邮电大学学报(自然科学版), 2020, (3):82−88.

[9] 高一为, 赖英旭, 吴欢等. 基于数据预处理的 DDOS 攻击检测方法研究[J]. 电子技术应用, 2013, (1):139−142.

[10]宋宇波,杨慧文,武威,胡爱群,高尚.软件定义网络 DDoS 联合检测系统[J].清华大学学报(自然科学版),2019,59(01):28−35.

[11] 王平辉,郑庆华,牛国林,管晓宏,蔡忠闽.基于流量统计特征的端口扫描检测算法[J].通信学报,2007,20(12):14−18.

[12] 顾晓清,王洪元,倪彤光,丁辉.基于时间序列分析的应用层 DDoS 攻击检测[J].计算机应用,2013,33(08):2228−2231.

[13] 刘仁山,孟祥宏.含自适应阈值的 ARMA 网络流量异常检测算法[J].信阳师范学院学报(自然科学版),2013,(2):296−300.

[14] T H Grubesic, et al. Comparative approaches for assessing network vulnerability [J]. International Regional Science Review, 2008, 31(1):88 —112.

[15] WU D, LIAN Y F, CHEN K, et al. A security threats identificationand analysis method based on attack graph [J]. Chinese Journal of Computers, 2012, 35(6):1938−1950.

[16] ALHAZMI O H, MALAIYA Y K, RAY I. Measuring, analyzing and predicting security vulnerabilities in software systems [J]. Computers & Security, 2007, 26(3):219−228.

[17] 余建,林志兴,谢彬.灰色关联模型的网络安全态势感识预测方法[J].实验室研究与探索,2019,38(02):31−35+70.

[18] 余建, 林志兴. 一种基于 SDN 中网络最大流的异常流量检测方法[J]. 三明学院学报,2018,35(4):47−54.

基于人工免疫系统的安全运营中台

林文伟

中电福富信息科技有限公司

摘　要：该文阐述了基于人工免疫系统的安全运营中台的基本概念，介绍了他的定义、背景、体系构建和达到的目的，对他的应用价值、关键技术、系统架构进行了简述，最后对比现状展望了该中台未来的研究建设方向。

关键词：安全分析，态势感知，动态防御，安全运营

1. 定义

人工免疫系统是各类信息处理技术等计算机科学利用生物免疫学原理或机制而衍生出来的智能系统的统称。人工免疫系统是人工智能研究领域的重要分支，它的研究发展目前涉及如网络安全、机器学习、模式识别及数据挖掘与分析等诸多领域。基于人工免疫系统的安全运营中台，就是借鉴了生物的免疫系统利用其独特的运行机制来抵御病原体入侵的原理，并以数据中台、技术中台、业务中台、算法中台构建安全运营中台体系。

2. 背景

随着《网络安全法》和《国家网络空间安全战略》的相继出台，我国的网络安全形势上升到了战略高度。面对来自国内外日益严峻的网络空间安全挑战，网络空间安全治理的地位不断上升，我国的网络安全运营体系的发展从萌芽到热潮再到低谷，网络空间安全的治理体系的发展曲折，面对高速发展且复杂多变的网络环境并且 5G 网络的快速普及，网络空间安全至关重要。在人工智能、大数据等技术的不断发展，中台概念在企业迅速铺开，基于这些技术、框架不断的被挖掘、开发、普及，也给网络安全体系带来了新生力量。基于人工免疫系统的安全运营中台便是继续这些高速发展的互联网技术和框架中衍生出来的安全运营体系，他的目的就是解决传统安全运营体系中的一些问题，如数据处理与分析能力低下、低质量的告警和情报、工具和流程碎片化、情报信息机制不畅、缺乏主动防御能力等问题。

3. 体系构建

建立基于人工免疫系统的安全运营中台，首先要明确我们防守的目标和防御的范围，第一步就是梳理盘点我们有多少资产，如主机、网络设备、安全设备、应用系统、存储设备等，第二步就要梳理我们资产间的网络拓扑关系，第三步就是盘点全网的数据资产，如结构化数据、非结构化数据，完成这些动作，就能明确我们的目标和范围，形成数据中台。

然后就是对数据源的收集，基于网络层面的有完全的数据包、会话数据、包字符串数据、网络入侵告警数据、防火墙日志、数据吞吐量统计等；基于主机层面的有系统事件日志数据、登陆登出信息、账号创建与修改、文件系统权限变更、软件安装、系统重启、病毒告警、基于主机的入侵告警、应用日志、主机安全日志等。通过对各种数据源的收集，建立数据中台，通过算法中台的各类算法模型进行初步对数据源进行分析进而缩小焦点。通过技术中台的入侵检测机制，基于受害信标与特征结合信誉度检测和 IDS 规则进行特征检测；基于统计数据异常如流量排名、服务发现并与其基线进行对比进行异常检测；通过蜜罐系统采集恶意程序和攻击样本，利用算法中台的自学能力，对攻击样本的特征进行学习，实现动态更新特征库，产出告警数据。

最后通过业务中台对各类告警进行溯源、取证、研判与决策，并且利用技术中台的编排技术进行安全编排，进行自动化处置、响应；基于人工免疫系统技术，利用算法中台对历史的安全事件和正在入侵的安全风险进行学习，使用技术平台对安全事件进行处置，实现收集、检测、监测、分析、处置的安全运营闭环，结合算法平台提供的人工免疫算法，形成人工免疫系统来对威胁、风险进行主动防御。

4. 达到目的

收集：数据的收集是检测和分析的基础，收敛组织需要于网络架构等一切可利用的资源

检测：对采集数据进行分析产生告警数据，对网络安全进行持续监控，快速发现各类网络威胁。

分析、响应：针对告警进行溯源、情报、取证分析，对威胁的影响范围、攻击路径、目的、手段进行快速研判，有效的支撑安全决策和响应。

预测、预防：建立威胁情报中心、漏洞中心以及蜜罐系统，利用相关预测算法对安全威胁进行预测，并提前对网络或主机进行加固预防。

防御：通过人工免疫系统，识别已知的安全威胁、风险进行主动防御。

5. 应用价值

快速识别威胁：“抗原识别”是基于人工免疫系统的安全运营中台重要的部门，是快速识别威胁的手段，建立对全网资产的安全保障。

高效分析研判：“抗体形成”利用人为的研判分析和自学习算法来抑制和促进抗体形成，并通过“亲和力计算”高效的分析研判，保障威胁正确响应处置、逐步完善免疫体系。

情报融合分析：利用模糊 AIS 算法结合威胁情报对全网网络行为进行仿真实验，对威胁进行快速挖掘。

实时安全监控：利用主机探针、流量探针对数据实时采集，通过算法中台和技术中台的检测分析，对全网资产进行有效的监控。

6. 关键技术

6.1 NSM 数据采集

会话数据：会话数据是文字记录和统计数据的集合，利用收集器从网络设备上或者服务器上甚至是网络线路上捕获收集 netflow、IPFIX 活其他流类型的数据。

全包捕获数据：全包捕获数据（FPC）是非常重要的取证材料，FPC 的高力度对网络威胁的上下文分析具有极高的价值，它最常见的形式就是 PACP 数据格式，它的完整性十分重要。

包字符串数据：包字符串数据是因为 FPC 回溯成本太高，而会话数据提供的信息有限，而包字符串数据，可以让安全分析进一步定位，在准实时和回顾性分析中有这极高的价值。

6.2 入侵检测机制

基于特征的检测机制：通过受害信标和特征如常见的主机信标，注册表键值、文件名等；或者如网络信标，IP 地址、X509 证书哈希等。信标根据不同性质还有其他分类，还有以静态信标、可变信标等，基于信标来做特征检测，需要长期对特征进行调优。

基于异常的检测机制：通过统计数据异常来检测是，基于异常的检测机制中一种重要的手段，如基于流量和服务的统计排名，来建立基线，通过统计结果，进行深度检测和回归计算，形成告警。

基于蜜罐的检测机制：蜜罐属于一种安全资源，它能捕获到哦攻击者的攻击行为和攻击路径，通过攻击者攻击时蜜罐掌握的攻击日志,通过算法因子进行调优,形成 IDS 规则提供给技术中台进行检测。

6.3 人工免疫算法

基本免疫算法：基本免疫算法是学习生物免疫系统的机制，利用体细胞理论与网络理论相结合，实现抗原识别、抗体产生、亲和度计算、记忆和自我调节、群体更新等构建基本的免疫模型。

否定选择算法：否定算法是借鉴了生物免疫系统的特异性,即胸腺 T 细胞生成时的否定选择过程。通过系统对异常网络行为的识别，区分自己和非己的信息，通过随机生成的候选检测器，通过亲和力计算，识别出非自体元素，从而进行告警。

克隆选择算法：克隆选择算法是一种基于自学习的进化算法，通过模拟克隆过程进行优化，对新

“抗体”的生成有关键作用，提高对网络威胁的识别和响应。

模糊 AIS：免疫系统的机制就是可以面对无穷多的抗原和细菌，模糊 AIS 利用抗原–抗体匹配、识别过程中的不确定性和模糊性，来面对网络中各种形形色色的攻击行为。

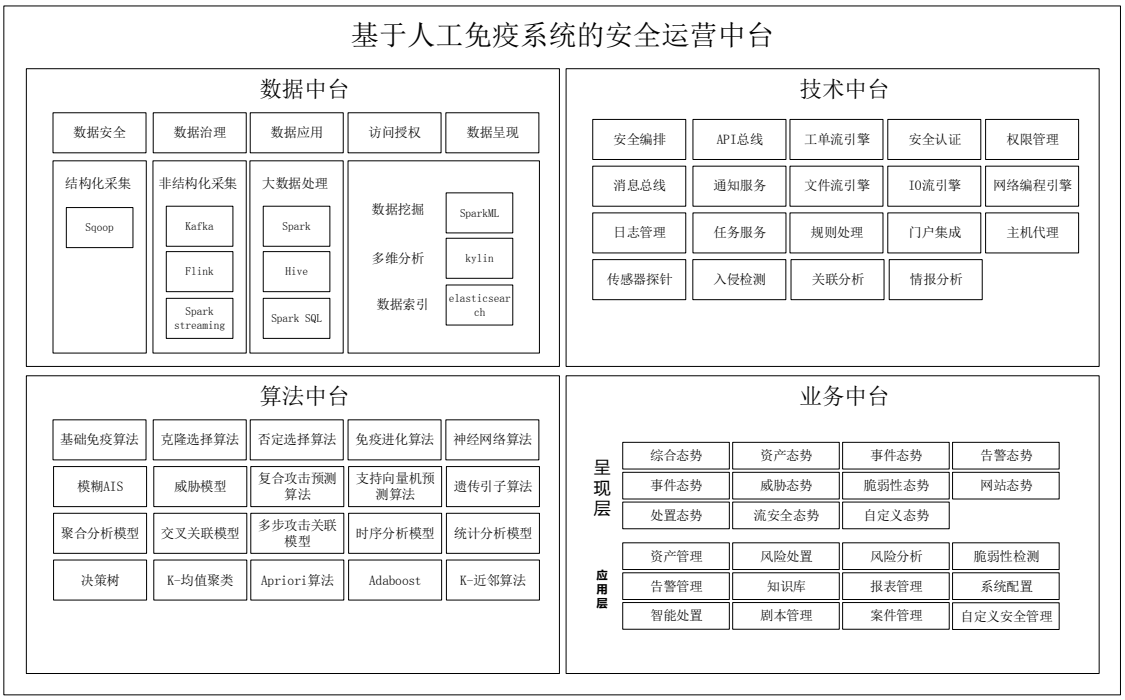
免疫进化算法：免疫进化算法基于免疫算法基础之上加入了遗传算子和记忆机制，提高了算法的群体多样性，具备较好的全局收敛，提高了对多变的网络威胁的准确度和敏感度。

6.4 安全编排

安全编排是将全网的安全系统或安全组件，通过 API 接口集成到技术中台上，实现全网安全能力的调度，并且可以按照一定的逻辑关系进行组合，对某种威胁进行安全操作的过程。通过工单流引擎将各类 API 接口进行自动化编排，实现安全威胁自动化处理或半自动化处理。

剧本的编排是为了让管理员聚焦安全操作的逻辑，而隐藏了具体安全 API 的操作和指令的编辑，让管理员从底层解放出来，真正投入到安全工作中去，而将指令编辑和 API 接口编程让开发者来完成。

7. 系统架构



系统架构图

数据中台：大数据时代的来临，一个数据汇聚中心的地位越来越重要,对数据的收集，分析计算，深度学习，已经变成了一个企业的核心竞争力，该体系建立了数据中台，以数据采集、数据仓储、数据治理、数据分析等大数据技术能力于一体的中台，对安全运营中台进行赋能。

技术中台：基础服务是一切平台的核心，面向技术将技术能力进行下沉，对其他中台进行能力开放，包括：安全认证，权限管理，工单流引擎，门户集成，消息总线，通知服务等等。这些底层技术通常与业务没什么关联性，但每个应用都可能会用到。

算法中台：将所有算法模型集成到算法中台，提供各类算法模型和高可用的计算能力进行赋能。

业务中台：将所有和安全业务强关联的功能进行提取，形成统一的业务模块，提供呈现层和应用层给用户使用。

8. 展望

目前大部分的安全管理平台都存在大量低质量的告警、数据量过大导致管理成本升高和分析能

力低下、工具碎片化、响应和处置时间过长等问题，并且长期困扰的被动防御问题，一直无法得到解决。在信息共享不断深入人心，人工智能和大数据技术快速发展，给安全管理平台带来了新的方向，变革是必然的。通过安全中台的框架，将各类安全能力下沉，业务需求提升，利用大数据技术建立的数据中台，有效的解决的种类繁多且数据量庞大的数据处理，利用人工免疫系统结合传统安全技术和威胁情报，提升检测、分析质量，并且结合安全编排和剧本管理，具备有效的响应处置手段，通过自学习和进化算法，来建立高效的主动防御体系。

基于网络流量解析的敏感信息发现

阮陈强

福建省海峡信息技术有限公司

摘　要：互联网的快速发展以及许多先进交互技术的出现，促使了移动终端的智能化以及普及化，移动终端成为了其使用者敏感信息的聚集地——姓名、帐号、密码、邮箱、地址等大量的信息被存储在移动终端中。然而在诸多的移动应用软件中，却存在着许多具有恶意行为的，可能对用户权益造成危害的应用软件，这些应用软件可能未经用户授权就将一些数据传输至网络上；企业开发人员有时不注意，导致一些敏感信息未经脱敏处理就在网络中传输。所以如何快速准确检测敏感信息在网络中传输，并对相关人员、企业进行告警，防止敏感数据泄露，具有重大意义。

关键字：敏感信息、数据泄露、流量监控

1. 引言

敏感信息（或敏感数据），是指不当使用或未经授权被人接触或修改后，会产生不利于国家和组织的负面影响和利益损失，或不利于个人依法享有的个人隐私的所有信息。

大数据时代，所有数据都具有了实际和潜在利用价值。企业在获得了大量的个人数据之后，他们会利用人工智能等技术来处理、分析数据，并且挖掘出有价值的信息，然后根据这些信息来促进业务的发展。价值的背后潜藏着巨大风险，大量敏感数据被贩卖、窃取和无授权滥用，这一问题已经严重危害到个人隐私、企业发展甚至国家安全。

敏感信息的泄露主要通过人为倒卖、手机泄露、电脑病毒感染和网站漏洞等途径实现。特别是现阶段在互联网应用普及和人们对互联网依赖背景之下，由于信息安全漏洞造成的个人敏感信息泄露事件频发。因此，为防范个人敏感信息泄露，保护个人隐私也越来越重要。

针对大型企业及政府机构来说，数据资源中往往包含大量的敏感和重要信息，敏感信息的防护极为重要，一旦数据遭到泄露或者遭到非法利用，将会给个人、企业甚至是国家带来无法弥补的损失。

这些与个人生活、工作密切相关的信息受到不同行业和政府数据隐私法规的管制。如果负责存储和发布这些信息的企业或政府无法保证数据隐私，他们就会面临严重的财务、法律或问责风险，同时在用户信任方面蒙受巨大损失。

2. 确定敏感信息

敏感信息包含了个人敏感信息和商业敏感信息。

（1）个人敏感信息是指与个人利益密切相关，一旦泄露、披露或滥用可能危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等的个人信息。

个人敏感信息包括以下几类：

①基本信息：如姓名、身份证号码、电话号码、及家庭住址等，有时甚至会包括信仰、职业、工作单位、收入、病历、生育等内容。

②设备信息：是指个人信息主体使用各种计算机终端设备（包括移动和固定终端）的基本信息，如 IP 地址、MAC 地址等。

③账户信息：主要包括银行帐号、第三方支付帐号，社交帐号和邮箱帐号等。

（2）商业敏感信息为不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利采取保密措施的技术信息和经营信息。

①技术信息主要是指权利人采取了保密措施保护不为公众所知晓（未取得工业产权保护）的，具有经济价值的技术知识，如：设计、程序、产品配方、制作工艺等。

②经营信息是指权利人采取了保密措施不为公众所知晓的具有经济价值的有关商业、管理等方面的方法、经验或其他信息，如：企业的战略规划、管理方法、商业模式等。

1. 网络流量发现敏感信息的一般流程

（1）流量捕获：捕获网络中的流量，一般都是 http 报文。

（2）格式解析：对捕获的 http 报文进行解析，确定数据格式，包括 html、xml、json、图片等格式。

（3）内容检测：通过内置规则或用户自定义规则，对数据进行整体扫描、分析，自动识别敏感信息。

（4）统计分析：将识别出的敏感信息进行分类、分级、告警并进行识别质量评估。

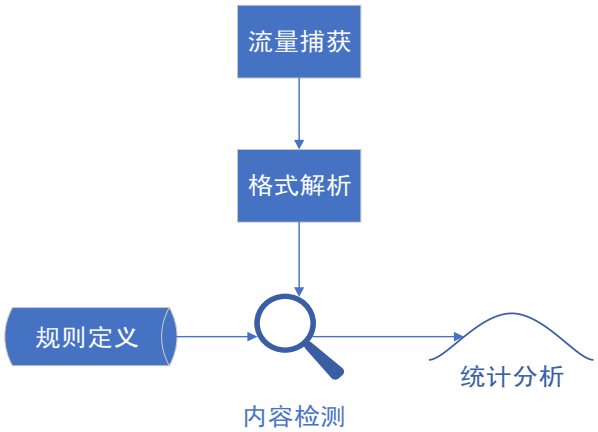


图 1 网络流量敏感信息发现的一般流程

3. 敏感信息的识别方法

3.1 关键字匹配

姓名、账号、密码等字段规则不明确，可能是任意字符串，可以通过配置关键字来进行匹配。

关键字匹配是一种比较常见的并且简单的识别方法，该方法的重点在于关键字的构建，关键字可以是单个、成对、组合的形式存在。进行复杂数据的匹配识别时，通常需要配合关键字权重、顺序、等多种其他参数使用。此方法的优势是关键字构建相对简单，对形式固定的数据识别效果不错，例如 json 格式的数据；缺点在于试用范围较窄，对于复杂数据格式的识别准确率比较低。关键字匹配法适用于特征较为明确、形态较为固定的数据格式识别。

关键字可以有两种方式进行配置，一种是内置关键字，内置的关键字有时候满足不了需求，所以另一种是用户自定义相关的关键字。

如何发现代表性关键字也是一个难点，有相关研究就是关于敏感词库的设计，一种常见的方法就是扫描数据库，识别敏感信息对应的关键字，由于

数据库比较庞大，扫描的代价较大，所以可以定期进行全库扫描。

具体的工程项目实现可以将敏感字段及其有代表性的关键字保存到数据库中，要识别敏感信息的时候，再读取出来进行匹配。

常见的敏感字段及其有代表性的关键字如下：

表 1 敏感字段及其关键字

敏感字段	关键字
账号	username、useralias、loginname
密码	pwd、passwd、password
电话	phone、telephone
邮箱	email、useraddr

假设有 http 报文经过格式解析后数据格式为 html，样例如下：

图 2 html 部分截图

图 2 所示的 html 片段含有账号和邮箱，像这种 html 文档一般都非常大，直接去遍历用正则表达式匹配非常耗时，所以可以用 html 解析器去解析这个文档，然后分析相关标签的属性，最后提取相应的值，识别结果如图 3 所示。

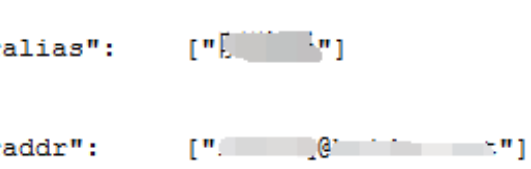


图 3 识别结果

3.2 正则表达式匹配

邮箱、银行卡号、身份证号、电话等字段有明确的规则，可以根据关键字匹配或者进行正则表达式匹配。

正则表达式通常被称为一个模式（pattern），用来描述或者匹配一系列符合某个句法规则的字符串[1]。正则表达式匹配是一种工程项目中比较常用的识别相关字符串的方法，通过对有明确规则的敏感数据进行特征提取和抽象，形成正则表达式，对数据内容进行正则匹配，通常为了保证识别准确率还需要与数据内容长度限制、过滤机制等参数配合使用。此方法的优势是对于简单数据的内容匹配比较准确，缺点是正则表达式的编写对专业性要求高，面向复杂数据和超长数据的识别比较乏力。正则匹配法适用于数据特征较为明确，数据结构相对简单的数据识别。

像身份证、银行卡这类信息，通过正则表达式匹配出来的值，可能格式是合法的，但实际是不存在的，所以还可以通过相关验证算法的过滤。

对于这种识别方法，具体工程项目实现时，要先去调研相关字段的数据特征，进行归纳总结，然后经过专业人士编写对应的正则表达式，最后对原始数据进行匹配识别。

3.3 机器学习

图片、音频、视频等，没有明确规则，可以通过深度学习、自然语言算法等其他开源算法库来识别。

机器学习法是当下比较热门的数据识别方法[3]，首先构造学习模型，然后通过对大量的数据样本进行学习，提取数据特征，最后基于词法分析、语义分析等技术手段对数据内容进行处理后，进行特征匹配。此方法对于技术要求比较高，同时需要提供大量的样本数据进行学习以保证最终的识别效果；

优势是充分学习后识别准确率高，且具备自学习能力，可适用的数据内容范围广。

4 结束语

本文分析了当前敏感信息泄露的问题，以及如何识别出敏感信息在网络中传输的方法，从而对相关人员、企业进行告警提醒，防止数据泄露。随着数据的价值和重要性在企业业务运行中的不断强化，数据识别和分类分级将逐步成为企业的常态化能力，为企业的数据价值挖掘和数据保护提供方向和指导。而当前主流的关键字匹配、正则表达式匹配等传统的数据识别方法，将逐渐无法应对越来越丰富和复杂多变的数据形态。未来，随着的人工智能技术的发展，其将有望成为复杂多变的数据形式下最有效的数据识别手段之一。

参考文献

[1]https://zh.wikipedia.org/zh-

[2]刘明辉，张尼，张云勇，胡坤，宫雪，曲大林. 云环境下的敏感数据保护技术研究. 2014.

[3]于海，郭燕慧. 利用卷积神经网络进行非结构化文本的敏感信息检测. 北京邮电大学网络空间安全学院. 2019.

[4]刘耕，方勇，刘嘉勇. 基于关联词和扩展规则的敏感词库设计. 四川大学信息安全研究所. 2010.

浅谈主机安全防护技术在金融机构网络空间安全的应用

兴业银行总行　郑鹏飞

摘　要：金融科技时代背景下，随着银行、证券、保险、基金等金融机构信息化水平的飞速发展，互联网应用受到的黑客攻击愈演愈烈，网络空间安全已成为金融行业重点关注问题。本文将以主机安全防护技术作为一个起点，浅谈该防护技术在金融行业中的应用趋势，以及如何通过该技术提升金融机构网络空间安全水平。

关键词：主机安全、金融、信息安全

自 2017 年我国《网络安全法》发布以来，网络空间安全已上升至国家层面，网络空间作为除“海陆空天”之外的第五空间，与物理空间不同，我们在现实生活中无法真切的感受到，但又与我们生活密切相关，2017 年的勒索病毒在我国企事业单位的爆发，令公众意识到网络空间对生活的影响。而 SWIFT 的转账交易系统遭黑客攻击，导致孟加拉国央行损失 8100 万美元的惊天大案更为各金融机构敲响警钟。在金融业网络空间安全治理上我们仍有很长一段路要走，针对网络空间中的威胁，我们应该针对性的对网络空间从外到内的每一个节点进行防护，而主机安全则是网络空间安全中的最后一道防线，意义重大，无论黑客的目的是进行系统破坏还是数据盗取，服务器主机都是他们最渴望的目标。

一、金融行业网络空间安全形势

关于金融行业的网络空间安全形势的相关研究，汪嵘明在其《大数据时代金融信息安全研究》

一文中认为，金融行业信息网络化、数据化属性进一步增强，必然会通过互联网、智能设备网络参与数据交换，原本封闭的环境呈现开放态势，会增加被攻击、被入侵的几率。[1]崔传桢、曾昭平、赵尚根据长期的研究认为，随着第三轮经济全球化以及数字经济时代发展，传统金融体系必须进行更新，金融行业尤其应该重视金融信息安全战略的新趋势。[2]多位学者研究都说明了随着金融科技带来的技术革新，金融行业信息安全变得更为脆弱，伴随着新技术而产生的新漏洞不断增加，攻击者手段更为多元化，如何应对挑战，完善信息安全战略，是金融机构应解决的重点问题。

二、主机安全防护技术的发展现状

随着金融行业系统开放，攻击者入侵和攻击的途径趋向多元化，但无论手法如何，攻击者最主要的目标仍是系统服务器主机，随着攻击手段的不断演进，主机安全防护技术也在不断更新、迭代。根据不同层次的攻击者，主机安全防护技术也可细分为三个级别。

（一）第一级：应对自动化攻击者

自动化攻击者一般是利用网络上已有的漏洞利用工具或者社会工程学数据，批量、自动化的对暴露在互联网上的资产进行无差别、大范围的攻击，目标是尽可能多的感染存在某漏洞的主机，攻击手法不包括 0 Day 攻击或手动攻击，例如 2017 年 Wannacry 勒索病毒爆发就是一类自动化攻击。

为应对自动化攻击者，主机防护技术重点为主机资产清点、配置基线、补丁管理。其中，资产清点确保清点组织内部所有服务器主机，根据重要性划分资产等级、明确资产责任人，还应包含主机上组件信息的清点，明确组件版本信息。配置基线针对主机的各类安全策略、服务及端口配置、日志审计配置等，根据网络空间安全动态制定各类配置的安全基础要求，并具备主机配置的检查手段。补丁管理针对的是网络上层出不穷的各类操作系统或组件漏洞，因为漏洞数量庞大并且持续增加，补丁管理应制定漏洞优先级，如对常见软件漏洞、高危漏洞进行优先修复。

（二）第二级：应对机会主义攻击者

机会主义攻击者指利用自动化工具作为攻击起点，随后，横向移动扩大攻击范围。这个级别的攻击者寻求简单、便捷的攻击路径，利用已知漏洞发起攻击，然后利用通用的商业软件进行继续渗透，例如 Slammer 蠕虫攻击。

为捕获机会主义攻击，主机防护应该从第一级的基础加固扩展到检测、响应、控制、隔离。其中，检测能力需要借助 HIDS 等技术工具，通过收集主机端信息并进行监控来发现潜在威胁。响应即为漏洞响应能力，包括对 Windows、Linux、应用组件等新爆发的漏洞进行检测及高效响应。控制包括对应用程序以及脚本的控制，例如控制应用程序权限，监控 PowerShell 使用。隔离主要是指对不同重要程度的主机进行网络隔离，利用隔离限制攻击者的横向移动。

（三）第三级：应对高级持续性攻击者

高级持续性攻击者通常有强烈的目标性，会利用各种方法进行攻击，在攻击成功后会自我潜伏，达到窃取重要信息等目的。高级持续性攻击通常会利用 0 day 漏洞等新的攻击方式，针对金融机构等关键信息基础设施的网络攻击已经开始出现这种高级攻击形式。

应对高级持续性攻击者，主机防护需要进一步深化、细化、常态化，包括持续测试、持续威胁捕获、供应链安全管理等。持续测试可通过红蓝对抗形式，一方面寻找组织内部存在的薄弱点，另一方面可以检验级别二中的检测、响应能力。持续威胁捕获可通过主机、应用程序的日志来深度分析可疑用户行为，可用欺骗防御技术为辅助，例如蜜罐、蜜网、沙箱等技术手段，可针对性检测活跃且目标明确的攻击者。供应链安全管理主要针对可访问企业系统和数据的外部合作伙伴或者供应商，攻击者可以利用这条路径潜入内部系统，对于目的明确的攻击者，供应链的风险发现及安全加固也是重要一环。

三、金融行业主机安全防护技术应用趋势

关于金融行业安全防护技术现状，孙枫认为，

由于我国金融行业信息系统外包的普遍性，导致系统无统一数据接口、运用多种开发技术等，导致安全防护变得十分困难。[3]目前金融行业主机安全普遍在二级左右的水平，针对高级别攻击的检测和响应能力建设还有很长一段路要走。金融机构从二级提升至三级防护水平的重点是如何强化针对高级别攻击的防护能力，主机安全防护技术在金融行业应用可参考 Gartner 针对高级别攻击曾提出一套自适应安全架构理论，该架构旨在将安全工作者从防御和应急响应的思路中解放出来，加强监测和响应能力以及持续的监控和分析能力，Gartner 提出的架构图如图 1 所示。

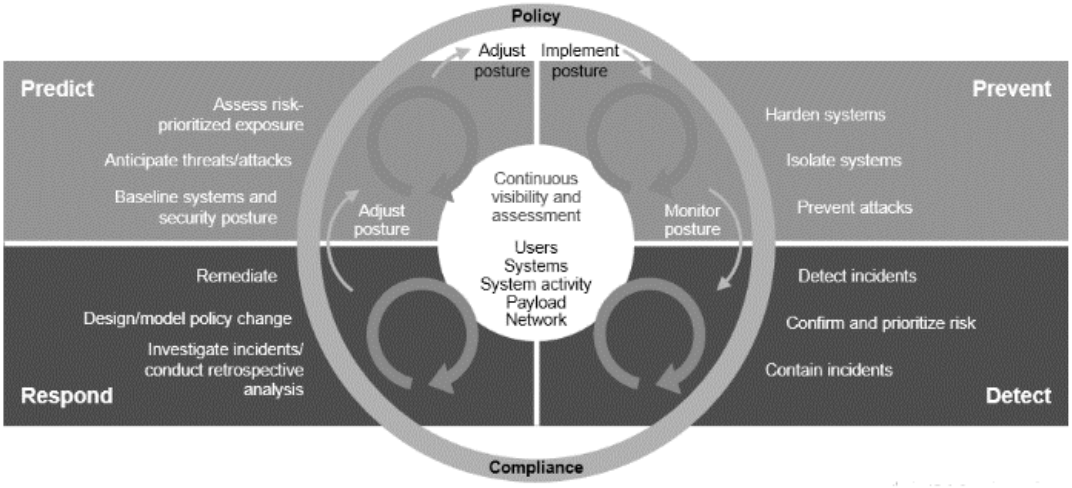


图 1 Gartner 针对高级别攻击的自适应安全架构 2.0

结合金融行业现阶段安全防护技术水平以及自适应安全架构提出的阻拦、检测、响应、预测四个象限循环，主机安全防护技术在金融行业的应用趋势如下。

（一）提升阻拦能力，改进主机安全测试方式

金融行业主机安全防护的安全阻拦能力想上一个台阶，需要进一步改良测试方式，通过测试验证、强化阻拦能力，如前文介绍的红蓝对抗形式，可以应用更为先进的框架，例如 ATT&CK 这个攻击框架，提升红蓝对抗水平，在真实的演练环境中扩展阻拦手段。

（二）加强检测及响应，常态化主机安全运营

为加强检测及响应能力，可考虑在主机安全运营过程中引入自动化编排及响应系统（SOAR），通过 SOAR 可显著提高平均检测时间 MTTD 和平均响应时间 MTTR，引入此类自动化运营系统，可减少安全运营人员压力。同时，可以通过 SOAR 进行报警的有效性验证，提高响应速度，进一步提高安全运营水平。

主机安全相关事件与安全运营中心（SOC）的联动也是加强检测及响应能力的有效手段，通过 SOC 进行统一管理，可通过多类别安全设备的关联分析，使检测手段具备新视角、新维度，有效提升应对高级别攻击的检测及响应能力。

除了技术手段，加强日常安全运营管理能力也是金融行业主机安全防护工作重点。例如日常的资产梳理、资产发生变化的更新流程、新发布的漏洞威胁预警、补丁修复和通知流程、弱密码的整改推动流程等等。这些都不单是技术手段可以解决的，需要管理手段同步跟上。

（三）建设安全预测能力，深度利用威胁情报

为达到更高级的防护水平，在前文主机安全防护前序能力建设完善的基础上，通过加强威胁狩猎（Threat Hunting）能力，具备一定的安全预测能力。金融机构通过深度利用威胁情报，可在发生安全事件后准确的追溯溯源并进行高效响应，同时，威胁

情报在一次次迭代与更新中会更加精准，可以通过这些情报及历史数据实现对攻击者后序行为的提前预测。

四、结束语

金融机构无疑是金融科技时代的主角，大数据、人工智能、物联网等新技术飞速发展的同时也带来了相应的安全风险，多样化的信息载体也提供了多样化的入侵路径，固步自封的传统安全防护已经无法确保核心资产的安全。主机防护技术作为核心资产的最后一道防线，具备风险发现全面、入侵检测准确等优点，在金融科技时代注定成为各大金融机构网络空间安全体系建设必不可少的一环。

参考文献：

[1]汪嵘明.大数据时代金融信息安全研究[J].中国集体经济,2019(32).

[2]崔传桢，曾昭平，赵尚.数字经济时代金融信息安全国家新战略[J].信息安全研究,2020,6(1).

[3]孙枫.知识图谱在金融机构网络安全中的应用[J].金融科技时代,2020(6).

泉州港口发展中心网络信息安全形式与对策研究

黄韵玲

福建省泉州港口发展中心

摘　要：目前信息化建设步伐的加快，网络和电子信息技术在泉州港口发展中心日常工作领域应用日益广泛和重要。网络和电子信息技术在给工作带来极大便利的同时，也面临着巨大的安全挑战。黑客攻击、网络诈骗、数据泄露等网络安全问题频发。如何在网络信息化条件下做好网络信息安全工作成为政府管理部门亟需解决的一个重要课题。

关键词：港口、信息化、保密

根据《中华人民共和国网络安全法》等相关法律法规及相关文件要求，围绕“坚决防止发生重大网络安全事件”的总体目标和网络安全的总体要求，按照“统一领导、集中指挥、分工负责、属地为主”的工作原则和“严之又严、细之又细、实之又实”的工作要求，充分发挥各方职能作用，坚决防止发生重大网络与信息安全事件，确保交通重要信息系统和门户网站的安全稳定运行。但由于种种原因，基层网络运行维护中仍存在着不少问题，严重影响着信息系统的安全和数据的质量，本文拟通过对网络安全管理中存在问题的分析，探寻加强基层网络安全管理的方法和途径。

一、我中心网络安全管理现状和基本情况

我中心自组建以来，通过积极实施“科技兴政”战略，信息化建设的显著成就，较好地促进了政务职能作用的发挥。实现了无纸化办公，网上公文起草、流转和查询。在网站建设上，实现了政务公开，公开的政务信息内容的丰富，为创新政务公开的形势和方法提供了有效的手段和宽广的舞台。同时，我中心建设有全港区视频监控系统、船舶政务管理系统、航道政务管理系统等，这些系统的建立形成了各机构协同管理体系，提高了整体工作效率，推

动了电子信息化政务工作的发展。

目前我中心网络包括电子政务内网（内网）和互联网（外网）两部分，所有硬件设备集中于中心机房各个独立区域，互相物理隔离。内网主要为中心内部办公使用，处理日常公文流转、人员管理等，安装有 360 天擎终端管理系统，配备防火墙实现内网中服务器及办公电脑与内网其他设备的逻辑隔离及安全区域间的访问控制。外网主要为中心提供互联网服务，安装有 360 网络版杀毒软件，配备防火墙实现外网中办公电脑与外网其他设备的逻辑隔离及安全区域间的访问控制。当前中心虽然配置了防火墙，但入侵防御、行为审计等设备缺失。同时，中心现有内外网是租用电信公司的线路，在发生网络故障判定问题在于线路时，由于没有相应的机制，对方常常不能在最短时间内解决故障。

二、我中心面临的网络安全问题

科技是一把双刃剑，其在加强政务工作的同时也会对其造成不利影响。如何让计算机网络系统得到有效保障，最大化地促进政务信息管理工作效率是每个部门最值得关注和解决的问题。我中心的网络与信息安全防护工作所面临的形势也十分严峻。

（一）安全防范意识淡薄，人员配备不足

不少干部认为，网络安全是信息管理部门的事情，在网络运行和维护管理中存在不设置口令或设置弱口令、随意设定共享目录、随意卸载防病毒软件等现象。此外，下属单位未配备专业技术人员，中心机关也仅有 2 名技术人员，技术力量不足，加之平时外出参加业务培训机会少，防范知识更新慢，网络安全管理知识不能有效地得到补充。

（二）面临的网络威胁增多，安全防范技术薄弱

近年来，针对应用软件程序和应用服务协议安全漏洞的攻击越来越多，病毒、蠕虫、木马、恶意代码等网络威胁呈日趋严重的态势。黑客攻击，修改政务公开网站的页面，发布反动口号，严重影响政府形象。我中心虽然配置了防火墙，但是缺乏入侵防御、行为审计、终端检测响应等设备，运维安全管理系统未部署，单位网络及信息系统仍存在着相当大的安全隐患。

三、网络安全管理方法和途径的小探究

网络的安全稳定和畅通是政务信息化工作的生命线，必须借助信息化手段，加强网络安全设备的作用，构建信息数据的安全，同时必须建立和完善各项管理机制。

（一）建立网络安全管理联动机制

采用专业的制度管理平台提供管理制度优化和调整，提供安全管理制度设计、安全运维流程执行、安全维护工作记录，在线进行组织、协调、授权、审核和记录，通过界面实时监督和控制数据中心的各项安全管理和安全运维工作所涉及的人员、对象和维护内容、时间计划等。管理制度优化服务覆盖以下方面：（1）建立信息安全责任制度。建立安全组织机构，落实安全责任单位、运营单位、安全服务提供商、系统集成商、软件开发商、网络/安全设备厂商责任。（2）梳理安全管理流程。梳理大型活动安全保障流程、事件响应流程、上线测试流程、安全检查流程、通报预警流程、漏洞管理流程等。（3）完善安全监管措施。梳理风险评估、安全加固、数据流控、事态预警、应急处置、漏洞跟踪等工作流程，完善日常运维工作流程及安全“事中事后”监管措施。（4）建立等级保护管理体系。构建总体方针、管理制度、管理规范、记录/证据四层结构体系，涉及安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面。

（二）建立网络安全应急处理预案机制

制定应急预案管理的责任部门，建立统一的应急预案框架，框架应包括事件分级方法、各级事件启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；在应急预案框架制定不同事件的应急预案，应急预案要指名适用的系统、设备等，要结合系统实际状况。比如针对门户网站的网页篡改、针对业务系统的入侵等。找第三方专业安全服务团队作为信息网络应急保障队伍，并定

期开展应急演练，做好应急演练相关文档记录。同时针对单位自身的网络实际情况，并结合网络安全应急处置相关的政策要求，设计出符合单位要求的网络安全应急预案，并组织技术力量协同单位共同完成网络安全应急演练。

（三）建立重要数据备份机制

建立完善有效的备份机制，做好关键政务信息的备份工作，是抵御灾害、突发事件破坏，确保信息安全的一项重要措施。结合工具和人工方式来备份相关数据库信息，通过定期检查和备份，来解决因为系统安全漏洞、安全配置不正确而产生的数据安全风险。同时建立数据灾备机房、双机热备和集群技术，根据业务特点的不同，通过主从、互备、并行等工作方式来进一步降低数据库系统本身的风险，加强数据库系统账号、密钥、权限、数据等带有安全风险的配置，从而从整体上提升数据库系统的安全性。

（四）建立网络安全培训机制

通过安全意识宣贯，降低内部员工疏忽或有意造成的数据泄露，减少因不规范操作所引起的系统故障。改变以往一对多枯燥的演讲培训，使用手机、电脑、电视、广告机、办公现场环境布置等承载方式，在日常潜移默化下增强员工安全意识，宣贯网络安全主旨及《中华人民共和国网络安全法》核心思想。安全意识宣传包括：防泄密、防止重要文件泄密、内外网上网安全、办公信息、业务信息、管理信息、个人信息等。

（五）建立网络安全评估机制

定期开展安全措施有效性验证工作，验证核心网络设备、安全设备的安全配置符合数据中心安全策略要求，验证安全设备的策略是否为最小权限、最小服务，设备的安全审计日志正常工作，能够正确记录安全事件的来源和事件。定期对政务信息系统中的服务器进行入侵清查，登录到服务器进行入侵痕迹检查、后门检查、Rootkit 检查。对网站源代码进行后门代码检查，发现源代码中的危险函数和 Webshell 脚本。

（六）建立漏洞扫描和修复机制

根据安全风险评估与安全巡检结果，针对高危漏洞给出相关漏洞修补计划和修补建议，明确安全整改责任人，督促安全整改工作，及时跟踪漏洞修补状况，促进风险的处置措施。同时需要采取“先于黑客”的安全理念，做到事前预防，事中监控，事后处置。在日常运维过程中要做好网络安全保障服务工作，针对重要系统重点做好安全修复服务工作。

（七）建立网络安全日常考核机制

加大对网络安全日常考核，对信息资产进行管理和考核。通过准确掌握自己所辖网络中资产、应用的基本情况和安全状态的功能目标。

（八）建立等级保护安全服务机制

为保障重要信息系统安全，安排对重要信息系统进行等级保护自查与整改、测评等工作，建立等级保护安全管理，对等级保护定级范围内的安全设备和核心资产进行等保安全合规状态管理。提供等级保护定级范围内安全资产（如安全设备等）的添加、维护、查看，对政务信息系统中所涉及的物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复等方面的安全指标和基线进行管理。并综合采用各种先进的安全技术和产品，加上制度和管理的保证，保证网络的安全稳定运行。对于大规模部署的系统，采用集中管理平台，对系统中的网络设备、安全产品、应用软件等进行集中的管理和部署。

（九）建立运维经费保障机制

保障必要的网络与信息安全专项经费，用于网络与信息安全技术防范设备的添置、升级、更新，以及外聘专业网络与信息安全服务团队、内部工作人员培训的费用。仅靠政府自身的力量维护信息安全，经常力有不逮，需要更多调动社会力量，发挥企业和市场的作用。同时为了要使得安全保障体系发挥最大的功效，除安全产品的部署外还应提供有效的安全服务，根据网络系统具体现状及承载的重要业务，全面而细致的安全服务会提升信息系统安

全保障能力。安全服务就需要把安全服务商的专业技术经验与行业经验相结合，结合实际量身定做才可以保障其信息系统安全稳定的运行。

四、结束语

综合来看，加大政府部门的网络信息化防护工作力度十分有必要。在进行防护的过程里，不仅要在技术层面上加大力度，还要通过相应信息安全管理制度进行防护。在对相关人员进行安全知识培训以后，提高其对网络信息化的认识，提高员工的安全意识。通过理念上的重视和技术水平的提高，使工作人员综合素质提高，应对风险的能力也进一步提高。对于管理者来说，要和具体状况相结合，实施严格的管理，贯彻落实相关制度，完善网络信息化防护体系，为网络信息化建设提供基础。

网络安全 AI 工具箱的探索及实践

俞捷

中国移动通信集团福建有限公司

摘　要：伴随着互联网的爆炸式发展，网络安全已上升到国家战略层面，新一代网络安全产品和解决方案已经普遍将机器学习当作必要功能来进行开发。中国移动福建公司安全专业人员需要打造一种工程能力，该能力能够让安全人员脱离单纯的点对点的竞争，有必要建设自己的人工智能安全专业工作站，构筑自己的人工智能网络安全专业工具箱。已在三方面取得突破（1）基于 Linux 系统调用日志（/usr/include/asm）进行漏洞检测，特征提取采用 N-Gram 和 TF-ID 模型，采用 Keras 模型作为深度学习工具特征提取采用，针对性强，准确度高，训练精度达到 94%，验证精度稳定在 91%；（2）根据网络流量数据包进行入侵检测，采用 k-近邻算法、决策树算法、朴素贝叶斯算法、逻辑回归算法，制定了不同机器学习算法对比分析优化的方法，优选 k-近邻算法、决策树算法，精度达到 99%和 100%；（3）基于 Url 的数据识别 XSS 攻击，采用隐式马尔可夫算法，有效从已观察序列推测隐藏序列，并通过合理地调节阀值，使精度达到 96%。这种工程能力和防御体系的结合，一方面可能让安全人员在面对某些未知威胁时，达到以不变应万变、获得天然免疫的理想状态；另一方面在安全专业系统建设、设备选型、合作开发等方面化被动为主动，以自身的工程能力优势，完善网络安全防御体系，支撑日益多元的中国移动网络及业务的大发展。

关键词：网络安全、工程能力、人工智能、专业工具箱、防御体系、漏洞检测、特征提取、对比分析

一、网络安全防御 AI 化的必要性

伴随着互联网的爆炸式发展，网络安全已上升到国家战略层面，新一代网络安全产品和解决方案已经普遍将机器学习当作必要功能来进行开发。面对威胁的同时，计算和存储资源已不再是安全团队的瓶颈，中国移动福建公司安全专业人员需要打造一种工程能力，该能力能够让安全人员脱离单纯的点对点的竞争，case by case 的对抗，转而从更高的维度上来审视业务，发现潜在的异常事件，而这些异常事件可能会成为安全人员主动深入防御的突破点。我司网络安全专业团队，有必要建设自己的人工智能安全专业工作站，构筑自己的人工智能网

络安全专业工具箱。这种工程能力和防御体系的结合，一方面可能让安全人员在面对某些未知威胁时，达到以不变应万变、获得天然免疫的理想状态；另一方面在安全专业系统建设、设备选型、合作开发等方面化被动为主动，以自身的工程能力优势，完善网络安全防御体系，支撑日益多元的中国移动网络及业务的大发展。

网络安全 AI 工具箱的发展其实刚刚起步，从现阶段的成果来看，还在不断地丰富完善中，每隔一段时间就会有新的工具能够添加进来。其实网络安全一直和 AI 相伴相生，从网络安全诞生的那一天起，人们就一直试图使用自动化的方式去解决安全问题。网络安全专家一直试图把自己对网络威胁的理解转换成机器可以理解的方式，比如黑白名单、正则表达式，然后利用机器强大的计算能力，夜以继日地从流量、日志、文件中寻找似曾相识的各类威胁。似乎这一切就是那么天经地义并无懈可击。但事情似乎又没有那么简单，机器其实并没有完全学到人的经验，网络安全专家一眼就可以识破的变形，对于机器却难以理解；更可怕的是，恶意程序数量呈指数级增长，各类新型攻击方式层出不穷，依靠极其有限的网络专家总结的经验和几个安全厂商所谓的样本交换，已难以以应付现在的网络安全威胁。如果安全专家一眼就可以识破的威胁，机器也能够自动化发现甚至做出相应的响应，这已经是很大的进步；如果让机器可以像阿尔法狗理解围棋一样理解网络威胁，那将是巨大进步。本工具箱的开发者，在网络的安全运维领域已经有 4 年多的搬砖经验，一方面苦于网络安全运维支撑手段难以赶上网络安全威胁的增长，另一方面也日益感觉到网络安全运维工作，受限于既有的安全工具，既有安全工具对安全团队都是黑箱，限制了安全团队的工程能力。

得益于这几年，特别是 2013 年以来，在世界范围内机器学习，特别是深度学习正以狂热的步伐前进。新技术的采用日新月异，激发了安全专业人员投入到网络安全 AI 工具箱的研究当中。当前网络安全 AI 工具箱，不是一个已经完成的事务，根本不是一个静止的存在。从规划开发网络安全 AI 工具箱的第一天起，就是将其作为一个不断丰富其内容工具的载体。工具箱中的各工具呈阶段性地产生，实际是网络安全 AI 研究的一个螺旋上升的一个过程，从最初的二分法，到多种算法并行比较，从监督学习到无监督学习（如隐式马尔可夫算法），是不断向前向上发展的。

二、几种主要安全威胁分析

网络安全 AI 工具箱，主要在于提高生产系统的安全性，因现阶段主要 3 个算法工具，也涉及到网络安全的三个方面，以下将逐一做出说明：

Linux 系统是一套免费使用和自由传播的类 Unix 操作系统　是一个基于 POSIX 和 Unix 的多用户、多任务、支持多线程和多 CPU 的操作系统它能运行主要的 Unix 工具软件、应用程序和网络协议 ,支持 32 位和 64 位硬件。发展至今已经可以安装在各种计算机硬件设备中，比如手机、平板电脑、路由器、视频游戏控制对、台式计算机、大型机和超级计算机。Linux 的流行让它成为众多黑客攻击的目标。

随着信息网的迅速发展和企业信息化程度的不断提高，如何保证信息网的网络可用性和关键业务的畅通运行对网络运维管理有着至关重要的作用。网络流量作为信息网网络的主要存在以下问题：网络流量无法实现实时监控，对流量异常的终端网络设备也无法排查，在一定程度上增加了终端网络安全的风险。 业务形式越来越丰富，网络流量占用率也急剧增长，当网络发生故障或者攻击时，由于整个网络庞大，整个故障排查过程耗时耗力，不能及时定位故障源、消除通信故障，给安全生产带来了一定的风险。

XSS(Cross Site Scripting，跨站脚本攻击)，是一种经常出现在 Web 应用中的计算机安全漏洞，它允许恶意 Web 用户将代码植入到提供给其他用户使

用的页面中。XSS 的危害包括:1、盗取各类用户账号，如机器登录账号、用户网银账号、各类管理员账号；2、控制企业数据，包括读取、笨改、添加、删除企业敏感数据的能力；3、盗窃企业重要的具有商业价值的资料；4、非法转账；5、强制发送电子邮件；6、网站挂马；7、控制受害者机器向其他网站发起攻击。在国内高居 Web 漏洞前三。

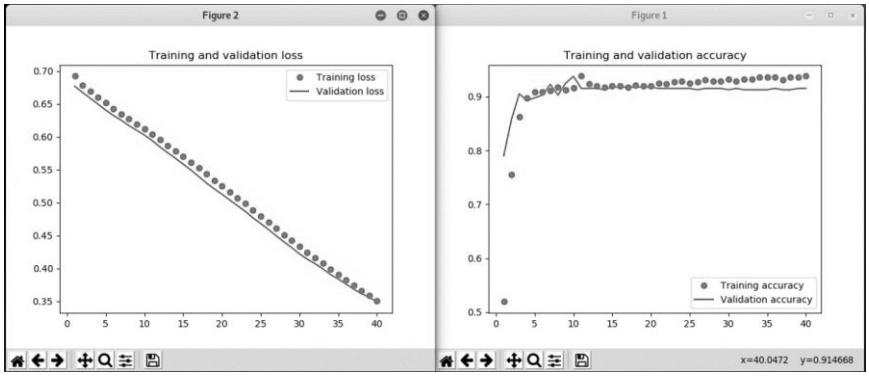
三、AI 化安全工具的探索

当前的网络安全 AI 工具箱从开始构建深度学习工作站到具备当前成果，前后大约 8 个月的时间（从 2019 年 11 月−2020 年 06 月）。第一阶段：构建深度学习工作站，从 2019 年 11 月到 12 月，在办公笔记本电脑上以虚拟机的方式构建 Liunx 工作站；第二阶段：完成 Linux 调用日志的漏洞检测算法工具，从 2020 年 01 月到 02 月，通过神经网络实现；第三阶段：完成网络数据包的入侵检测算法工具，从 2020 年 03 月到 04 月，通过朴素贝叶斯算法、决策树算法、k−近邻算法、逻辑回归算法，并采用了交叉验证的算法，选取出最优的算法是决策树算法；第四阶段：完成从 POST 和 GET 数据包中 URL 检测出 XSS 攻击载荷的算法工具，从 2020 年 05 月到 06 月，通过隐式马尔可夫算法，并通过优化阀值实现。

网络安全 AI 工具箱，完全自主开发，当前网络安全 AI 工具箱的算法，基本实现步骤大致如下：（1）定义问题，收集数据；（2）选择衡量成功的指标；（3）确定评估方法；（4）准备数据；（5）开发比基准更好的模型；（6）扩大模型规模：开发过拟合模型；（7）模型正则化与调接参数。采用的主要技术手段包括 Python 语言，Kares 深度学习框架，scikit−learn 的 StandarScaler 数据标准化库、TfidTransformer 实现 TF−IDF 处理，sklearn 的 naive_bayes 朴素贝叶斯算法、tree 决策树算法、KNeighborsClassifier k−近邻算法、LogisticRegression 逻辑回归算法、CountVectorizer 进行词袋 N−Gram 处理、cross_val_score 交叉验证库，hmmlearn 隐式马尔可夫算法模型，joblib 模型用于模型存储，三层神经网络进行深度学习。当前有 3 个主要算法工具，其实现方式将逐个做出说明:

(1)Linux 调用日志的漏洞检测算法工具，这是一种新颖的漏洞发现方式，选取 Linux 调用日志，从 Linux 操作系统的/usr/include/asm 目录下，找到 unist_32.h(32 位操作系统或 unist_64.h（64 位操作系统）中找到相关调用号，以这些整数的集合作为漏洞及攻击检测的对象。在本工具中将各个调用号仍然看作自然语言的单词，采用 N−Gram 处理（N−Gram 是基于一个假设，即第 n 个词出现与前 n−1 个词相关，而与其他任何词不相关）和 TF−IDF 处理（称为词频与逆向文件频率模型 Term Frequency−Inverse Document Frequency 词的重要性与它在文件中出现的次数成正比，但同时与它在语料库中出现的频率成反比。）的方式进行特征提取，采用三层神经网络进行学习，并采用训练损失和验证损失，训练精度和验证精度对比的方法，确定在不发生过拟合的情况下，验证精度能稳定在 91%。

```
#define __NR_swapon 167
#define __NR_swapoff 168
#define __NR_reboot 169
#define __NR_sethostname 170
#define __NR_setdomainname 171
#define __NR_iopl 172
#define __NR_ioperm 173
#define __NR_create_module 174
#define __NR_init_module 175
#define __NR_delete_module 176
#define __NR_get_kernel_syms 177
#define __NR_query_module 178
#define __NR_quotactl 179
#define __NR_nfsservctl 180
#define __NR_getpmsg 181
#define __NR_putpmsg 182
```

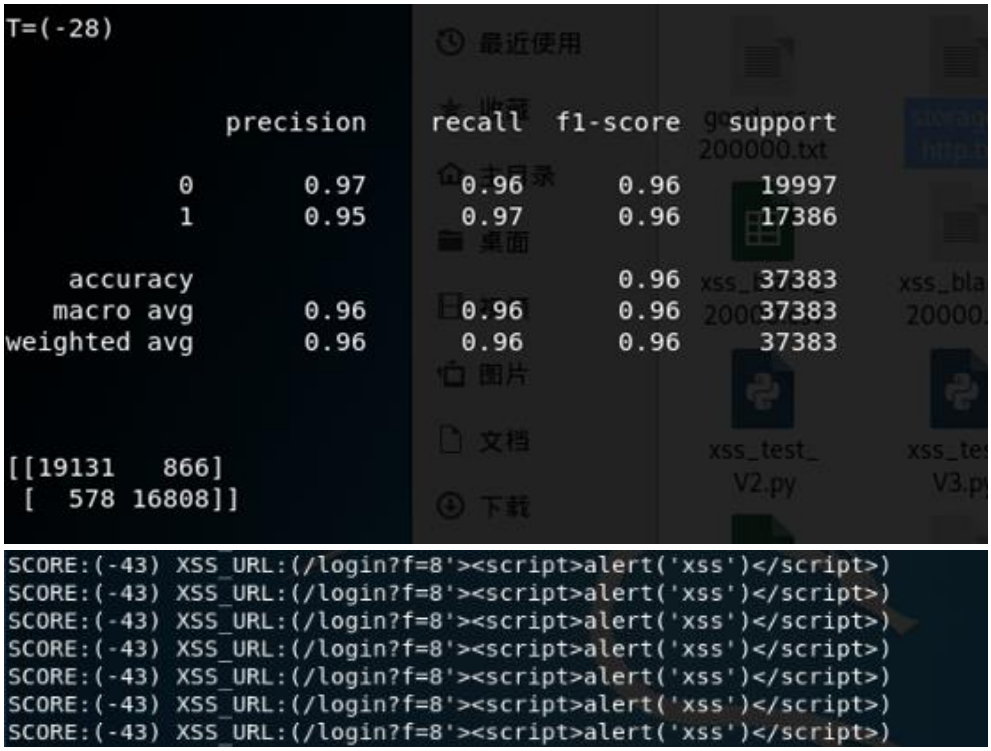


(2)网络流量数据存在定性数据和定量数据，特征标准化之前将定量数据分类出来，定量数据采用高斯分布（均值为 0，方差为 1）进行标准化，并将定性数据全部按照定类等级的方式进行编码，数据合并后采用朴素贝叶斯算法、决策树算法、k−近邻算法、逻辑回归算法分别计算，采用交叉验证的方式，选取最优算法。

```
X_test
       duration  src_bytes  dst_bytes  ...  protocol_type  service  flag
2900   -0.113551  -0.010093  -0.039310  ...              1       46     5
11640  -0.113551  -0.010081  -0.039310  ...              2       46     9
16662  -0.113551  -0.010089  -0.039310  ...              0       13     9
21545  -0.113551  -0.010093  -0.039310  ...              1       63     5
8384   -0.113551  -0.010011  -0.022840  ...              1       22     9
...          ...        ...        ...  ...            ...      ...   ...
19427   1.344107  -0.009893  -0.000685  ...              1       57     9
14558  -0.113551  -0.010000  -0.024979  ...              1       22     9
17698   4.368485  -0.009546   0.070576  ...              1        0     4
23808  -0.113551  -0.009964  -0.020982  ...              1       22     9
21860  -0.113551  -0.009999   0.006238  ...              1       22     9

[7558 rows x 40 columns]
```

```
=========Decision Tree Classifier Model Evaluation =========

Cross Validation Mean Score:
 0.9960869883971739

Model Accuracy:
 1.0

Confusion matrix:
 [[8245    0]
 [   0 9389]]

Classification report:
              precision    recall  f1-score   support

     anomaly       1.00      1.00      1.00      8245
      normal       1.00      1.00      1.00      9389

    accuracy                           1.00     17634
   macro avg       1.00      1.00      1.00     17634
weighted avg       1.00      1.00      1.00     17634
```

(3)从 URL 中检测出 XSS 攻击载荷，在数据处理中首先要将攻击载荷序列化，有针对性采用正则表达式进行切分，形成有针对性词袋，采用隐式马尔可夫算法形成并保存模型，采用循环语句不断调优阀值，现大补偿枚举，再小步长枚举，得到最佳阀值。在这过程中，着眼点在精确度 accuracy，从−100 开始缓慢上升，拐点在 T=−25，之后又缓慢下降，并且 T=−25 时精度已经到达 95%，且召回率（recall）和 f1 分数（f1−score）也非常令人满意，最终选取的 T 阀值为−28。



现阶段的突破点有 3 个：（1）基于 Linux 系统调用日志（/usr/include/asm）进行漏洞检测，特征提取采用 N−Gram 和 TF−ID 模型，采用 Keras 模型作为深度学习工具特征提取采用，针对性强，准确度高，训练精度达到 94%，验证精度稳定在 91%；（2）根据网络流量数据包进行入侵检测，采用 k−近邻算法、决策树算法、朴素贝叶斯算法、逻辑回归算法，制定了不同机器学习算法对比分析优化的方法，优选 k−近邻算法、决策树算法，精度达到 99%和 100%；（3）基于 Url 的数据识别 XSS 攻击，采用隐式马尔可夫算法，有效从已观察序列推测隐藏序列，并通过合理地调节阀值，使精度达到 96%。以上三种工具从操作系统、数据流量、URL 等三个维度，给网络安全支撑提供了有力的 AI 支撑手段。目前处在小范围试点应用阶段，在本单位的 26 台主机、内部网络和 Web 页面展开应用，取得了一定现网运营经验，因内网环境相对单纯，而模型算法来自于更丰富的样本，相关检测质量非常优异，达到 100%。

四、部署应用方式

当前的网络安全 AI 工具箱，适用于各维护单位的安全管理人员，对自身维护的主机、网络和 Web 网站进行安全评估，不与现网已经具备的系统漏洞扫描、Web 漏洞扫描、合规扫描系统相冲突，可以说是对现有网络安全工具的一种补充。涉及到三个应用场景：

（1）Liunx 的主机的漏洞发现：安全管理员可以从/usr/include/asm 目录下，找到 unist_32.h(32 位操作系统或 unist_64.h（64 位操作系统）中找到相关调用号，并整理为如下格式的 txt 文件（注意要保存为 utf-8 格式）：

```
175 174 174 174 57 175 54 175 6 3 6 174 174 174 174 174 174 174 174 174 174 174 174 174 174 174 174 174
174 174 11 45 33 192 33 5 197 192 6 33 5 3 197 192 192 6 33 5 3 197 192 192 192 6 33
5 3 197 192 192 192 6 33 5 3 197 192 192 6 33 5 3 197 192 192 192 6 33 5 3 197 192 192 6 192 192 243 125
125 125 125 125 125 125 125 125 91 258 311 240 240 174 174 175 191 122 268 45 45 5 197 192 3 3 6 91 5 54
54 220 4
```

加载已经完成学习的 h5(HDF5)文件，执行代码对系统漏洞进行判断。

（2）网络流量入侵检测：安全管理员可以从网络流量的日志文件中，整理成 vcs 文件，如下格式：

duratic	protocol_type	service	flag	src_byt	dst_byt	land	wrong_f	urgent
0	tcp	private	S0	0	0	0	0	0
0	tcp	private	REJ	0	0	0	0	0
0	tcp	private	S0	0	0	0	0	0
0	tcp	private	S0	0	0	0	0	0
0	tcp	remote_job	S0	0	0	0	0	0
0	tcp	private	S0	0	0	0	0	0
0	tcp	private	REJ	0	0	0	0	0
0	tcp	private	S0	0	0	0	0	0
0	tcp	ftp_data	SF	334	0	0	0	0
0	tcp	name	S0	0	0	0	0	0
0	tcp	netbios_ns	S0	0	0	0	0	0
0	icmp	eco_i	SF	18	0	0	0	0
0	tcp	mtp	S0	0	0	0	0	0

加载已经完成学习的 pkl(pickle)文件，执行代码对入侵检测进行判断。

（3）Web 网站 XSS 攻击检测：安全管理员可以通过抓包工具，抓取 GET 和 POST 包，并将其中的 url 取出来，单条或批量存到 txt 文件（注意要保存为 utf-8 格式）中：

```
/0_1/api.php?op=map&maptype=1&city=test%3Cscript%3Ealert%28/42873/%29%3C/script%3E
/0_1/api.php?op=map&maptype=1&defaultcity=%e5%22;alert%28/42873/%29;//
/0_1/api.php?op=map&maptype=1&defaultcity=%E5%8C%97%E4%BA%AC&api_key=%22%3E%3C/script%3E%3Cscript%3Ealert%28/42873/%29;%3C/script%3E
/0_1/api.php?op=map&maptype=1&defaultcity=%E5%8C%97%E4%BA%AC&field=%29%3C/script%3E%3Cscript%3Ealert%2842873%29%3C/script%3E//
/0_1/api.php?op=video_api&pc_hash=1&uid=1&snid=%3C/script%3E%3Cscript%3Ealert(/42873/)%3C/script%3E//&do_complete=1%20
/0_1/api.php?op=video_api&uid=1&snid=1&pc_hash=%3C/script%3E%3Cscript%3Ealert(/360/)%3C/script%3E//&do_complete=1
/0_1/?callback=%3Cscript%3Eprompt(42873)%3C/script%3E
```

加载已经完成学习的 pkl(pickle)文件，执行代码对系统漏洞进行判断。

目前处在小范围试点应用阶段，在本单位的 26 台主机、内部网络和 Web 页面展开应用。系统内其他单位引入，硬件上需要准备 1 台 Linux 主机或虚拟机，最低配置要求是 4G 内存，2 核 CPU 和 80G 的硬盘，软件上要求安装 Python3、TensorFlow、Keras、Pandas、scikit-learn、sklearn、joblib 等。涉及的优化参数按照全局变量设置并提供参考建议值以便根据实际情况做出调整。

五、总结及展望

研究 AI 工具箱最大体会是，只有适用的才是最好的。比如神经网络是一种深层次算法，但是我们也不能忽略浅层的算法。一部分原因在于，网络

安全领域的数据集，与神经网络不断探索的图像数据集、视频数据集、自然语言数据集有很大的不同，可能更浅层的机器学习算法能带给意想不到的结果；还有一部分原因是机器学习的基本算法是构建神经网络的基础和前身，如果不把机器学习算法掌握好，神经网络能否用好必然存在一个问号；而且简单就未必不好用，奥卡姆剃刀（Occam’s razor）原理的说法：“如果一件事情有两种解释，那么最可能正确的解释就是最简单的那个”，简单模型比复杂模型可能更好用。我还是相信，一般不存在最好的算法，对每种学习算法，都可以使用其他的机器学习技术来改进其性能，发现最好算法的关键是反复试错的迭代过程。

同时研究过程中也又意外的收获。关于 XSS 攻击载荷之所以采用隐式马尔可夫算法，就属于意外的收获，一开始研究全流量系统的采集日志并没有考虑到要引进一个之前完全没有接触过的算法。因为对全流量系统采集日志的分析中，意外发现了一种适用于对日志中的 XSS 攻击识别的算法。中间也有困惑的时候，就是现场采集的数据，根本不足以支撑一项机器学习工作的时候，一度觉得无从下手。得益于前期研究工作经验，不一定局限于手头的数据，现网数据只是问题的提出，我们要找问题解决的办法。问题的解决，是需要得到一个合适的工具，至于这个工具怎么来的，并不重要。跟前期的其他学习一样，从网络上找资源，找算法、找数据。可以说走上了一条产学研相结合的道路，生产、学习、研究在网络的运维部门，本来就是相辅相成的工作，运维部门的定位是生产，学习、研究是辅助手段。生产是学习、研究要解决的问题，学习、研究不应该脱离生产实际。可以给学习、研究提供一些助力，但现网毕竟有其局限性，我们应当因地制宜，充分发挥主观能动性，化被动为主动。不能等、靠、要，主动创造条件，寻求适合自己当前目标的方法、手段、资源。现在 AI 项目组的研究工作，已经往运维方向走出了第一步，以后将有更广阔的前景。

在实际运维工作中如何达到高效地运用，还有一段路要走。现有的网络数据，需要经过整理、规范化、标准化后，才能进行分析，达不到实时分析。达到实时分析，前面还要解决一个实时采集的问题，实时采集可能以两种方式：一种是依托现有的系统和工具；一种是在采集方面开发新的手段。现有的系统和手段，来源于不同网络安全厂家提供的一些产品，有软件，也有硬件，无论困难如何，网络安全 AI 工具箱将继续丰富完善，将日臻强大，日臻实用。给网络安全运维提供更加可靠的支撑。

参考文献

[1]（美）彼得.哈林顿（Peter Harrington）著，李锐、李鹏、曲亚东、王斌译《机器学习实战》，人民邮电出版社，2013 年 6 月。

[2]（美）克里斯.阿尔本（Chris Albon）著，韩慧昌、林然、徐江译《Python 机器学习手册：从数据预处理到深度学习》，电子工业出版社，2019 年 7 月。

[3]（土）锡南.厄兹代米尔（Sinan Ozdemir）、迪夫亚。苏萨拉（DivyaSusarla）著，庄嘉盛译，《特征工程入门与实践》，人民邮电出版社，2019 年 6 月。

[4]（美）弗朗索瓦.肖来（Francois Chollet）著，张亮译《Python 深度学习》，人民邮电出版社，2018 年 8 月。

[5]刘焱编著，《Web 安全深度学习实战》，机械工业出版社，2018 年 9 月。

新一代“智慧海洋”建设的网络安全架构

林竹明　张彦

（福建省海洋预报台　福建省　福州市　邮编 350003）

摘　要：我国 “智慧海洋”建设已经进入到战略加速时期，随着新兴技术的发展，传统的边界防护，已无法满足“智慧”时代的网络安全需求。面对形形色色的网络安全威胁，“智慧海洋”应该从网络安全建设、云平台安全建设、数据安全建设、安全管理体系等方面进行安全规划，并且与“零信任”体系共同形成安全、可信、合规的海洋大数据体系，从而确保业务的可持续发展及数据的全程可知、可管、可控、可查。

关键词：智慧海洋、网络安全、“零信任”体系

1. 引言

党的十八大首次提出了“海洋强国”战略，党的十九大报告再次指出，坚持陆海统筹，加快建设海洋强国。福建紧随党的政策，“数字海洋”与海洋信息化项目按照集约建设、联通内外的原则，搭建起全省“数字海洋”业务体系，构建了行业应用平台,业务涉及政务信息服务、行政业务管理、海洋防灾减灾、渔业安全管理等。而随着“智慧海洋”建设进入到战略加速时期，平台体积之庞大、数据范围之广泛、通信要求之复杂，传统的安全设备已不足以为其全面护航。如何通过整体统筹构建地角度安全保障“智慧海洋”的业务与相关数据，本文通过从网络、云平台、数据、管理体系等方面进行安全规划，并与“零信任”体系形成行业大数据的纵深防御体系，从而确保“智慧海洋”业务可持续发展以及数据的全程可知、可管、可控、可查。

2. 现状及问题

随着海洋信息化的逐步开展，福建通过“数字海洋”项目建设了政务服务、行政审批、海洋立体实时观测网、海洋防灾减灾预警报制作、海洋灾害应急信息发布服务、渔业安全应急指挥、视频监控与应急会商、水产品质量安全追溯、海洋与渔业基础信息等各类业务应用系统，基本上涵盖了海洋与渔业的主要政务业务领域。数据方面也积累了大量海洋观测数据、海域使用基础数据、渔业船舶数据等广泛涉海数据资料。“智慧海洋”的各类信息系统建设降低了办公成本、提高了政务服务的质量，为“数据应用，综合治理”提供了有效的技术支撑。而随着信息化建设日益提升，海洋数据将更加趋于集中，平台价值不可估量。由此，平台的安全性也将面临以下风险：

2.1“智慧海洋”数据安全

“智慧海洋”数据与业务涉及到自然资源、生态环境、农业、海上交通、能源等各部门，涉及的用户有沿海居民、港口商户、渔船、商船、旅游人群、海洋工程等，且数据量还会随着业务的规模、服务的扩张而不断增加。为提升海洋政务服务和防灾减灾需要，系统内部的数据也将从封闭可控走向愈加开放和共享的状态，这使得传统的边界防护设备难以界定访问机制并发挥作用。而汇聚了大量涉海数据中心的核心数据库与服务平台还面临恶意篡改、数据泄露、数据污染等风险。

2.2 终端采集设备安全

随着北斗卫星、AIS、宽带卫星、5G、移动信息技术、视频识别技术、边缘计算技术等新兴技术的广泛应用，“智慧海洋”的终端设备和通讯协议将日益复杂化，安全保障仍依赖于各个实体执行环境的信任度[1]，这样平台将难以判断如此复杂的设

备是否安全和可靠性，“脆弱”的终端也将面临更大安全风险，此类终端一旦接入网络，将使安全风险快速扩散，为黑客打开大门，进而导致整个“智慧海洋”的网络“失控”。

2.3 云环境下的主机安全

现今“智慧海洋”平台是部署在省统一的政务云平台上，云环境为主机安全带来了新的威胁与挑战：

（1）主机安全边界越来越模糊，安全威胁情报无法与主机终端及时联动。

（2）公有云、私有云和混合云环境中遇到的安全及管理问题。

（3）(云)等保 2.0 对于(云)主机安全带来的新的合规性问题。

面对上述问题，传统安全设备不能适应“智慧海洋”场景下的新威胁，主要由于防火墙、杀毒软件、入侵检测、桌面管理系统等技术手段均属于传统的边缘层防护措施，技术的局限性使得传统安全防护手段受制于病毒库、特征库、木马库滞更新后的问题，造成信息安全“头痛医头、脚痛医脚”的现象无法改变。

3. 新一代“智慧海洋”的网络安全架构

针对习近平总书记强调的：“没有网络安全就没有国家安全”[2]。新一代“智慧海洋”的网络安全架构在建设之初就考虑到 IT 基础设施在行业变革中所面临的冲击，规避了传统安全设备的问题，避免了系统被破坏、数据失窃的风险。整个架构是“零信任”体系与网络、云平台、数据等安全建设一体规划，规划形成了纵深式防御体系，保障了“智慧海洋”的系统安全，实现数据的可知、可管、可查、可控，保障各项业务的持续稳定发展。

3.1 网络安全架构

基于“零信任”体系的网络安全架构，将默认“智慧海洋”主体（用户、设备、应用）不可信、环境不安全、操作不合规，通过多维身份认证、环境风险评估、动态功能访问控制、精细化标记数据等级，以及分级、分类、精确授权以强化审批动态审计等手段，对主体、客体、行为及主体相关环境要素开展动态安全防护、动态信任管理、动态审批监管。实现了对“智慧海洋”体系内的复杂数据环境、复杂终端设备的风险评估，通过主动预警响应、主动协同管理，确保数据全程可知、可管、可控、可查，形成了安全、可信、合规的大数据全生命周期纵深防御体系，总体架构如图 3.1“零信任”体系架构所示。

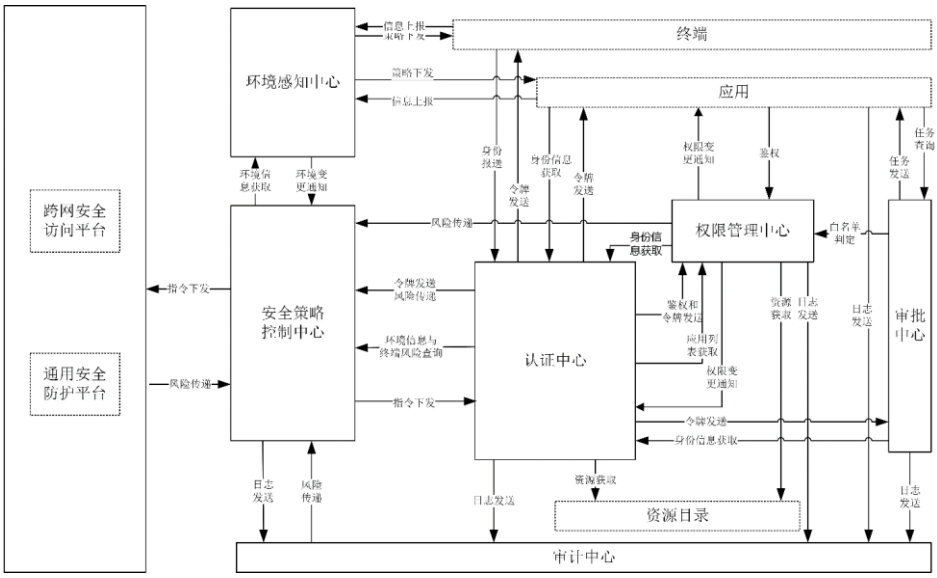


图 3.1“零信任”体系架构

1)认证中心负责统一的身份管理和身份认证服务，囊括“智慧海洋”所连通的各部门、用户。

2)环境感知中心负责终端设备（海洋视频采集、浮标信息、物联网设备、移动终端设备等）采集和分析，并向安全策略控制中心通报风险。

3)安全策略控制中心负责风险收集、风险综合分析判定和控制指令传递下发。风险来源包括环境感知中心、权限管理中心、审计中心和认证中心等，控制指令接收方包括认证中心，安全防护平台和跨网安全访问平台。

4)权限管理中心负责对权限进行维护，并对访问资源的请求进行鉴权，同时权限管理中心按照数据安全分级分类的有关要求，对接入“智慧海洋”平台的政府机构、科研部门、涉海企业等第三方用户提供精细化的业务应用权限管理。

5)审批中心负责审批工作的信息化、流程化和规范化，实现任务的上传下达、工作督办监督体系、规范数据查询和侦控手段。

6)审计中心负责接收认证中心、权限管理中心、审批中心、环境感知中心和应用系统的业务日志；对用户访问敏感数据、执行关键操作行为等各类业务日志进行真实、全面的记录；对各类业务行为进行审计，并提供异常行为分析、发现、告警和处置的能力。

3.2 网络安全建设

在总体架构下，“智慧海洋”网络安全建设针对参与其中的自然资源、生态环境、农业、海上交通、能源部门、涉海企业等机构的业务类型与数据特点归集形成了不同安全域的不同管控，并在政务云平台中共享相同的安全策略。通过安全域的划分把一个大规模复杂的安全问题，化解为更小区域的安全保护问题，是实现“智慧海洋”大规模复杂信息系统安全的有效方法。安全域划分是以保障业务安全为出发点和立足点，把网络系统划分为不同安全区域，以“零信任”思想为指导对各区域进行纵深式防护。由于每个区域的安全功能设计是根据每个区域的系统特点进行定制的，因此可以独立部署而不影响其他区域，适用于分阶段部署的模式[3]。具体可分为：

1)网络管理区：部署网络运营管理、网络资源管控等相关服务器和设备；

2)业务管理区：部署业务运营管理、业务服务质量监测等相关的服务器和设备；

3)安全管理区：部署安全运营管理相关的安全大数据、安全应用和运行管理等平台；部署安全基础设施的管理组件；

4)云平台管理区：部署云计算管理平台；

5)大数据管理区：部署大数据运维管理平台；

6)公共服务区：部署针对政府机构、科研部门、涉海企业等形成不同的服务组件；

7)运维访问控制区：部署可信运维代理、可信代理控制、身份管理、身份认证、权限管理等运维访问控制安全服务。

3.3 数据安全

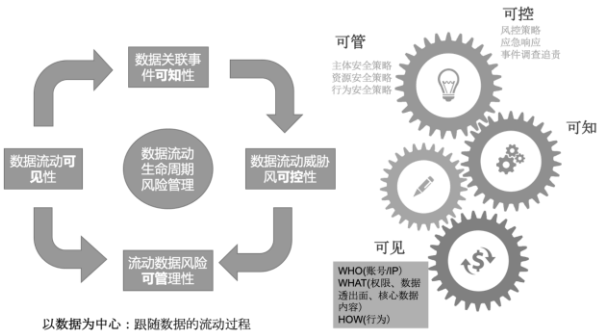


图 3.2 数据安全建设思路

如图 3.2 数据安全建设思路所示数据安全以“零信任”体系为理念，以数据安全为核心，结合“智慧海洋”业务服务流程，在传统的物理安全、设备安全、网络安全、数据库安全、系统安全等信息化安全保障措施之上，围绕着“数据应用、综合治理”的思想，设计涵盖了“ 数据治理、数据共享、大数据存储与分析”各阶段的数据安全总体框架和数据流程，满足了涉海数据全生命周期的安全保障需求，同时针对数据资产中涉及的隐私敏感信息、区域敏感数据等进行区别性防护，重点关注敏感数据在业务体系内的供应链，打破数据流动“黑盒”。

3.4 云主机防护

基于“智慧海洋”政务云平台的云主云机安全：采用先进的自适应安全架构及端点检测及响应（EDR）解决方案，提供云+端的云安全管理平台。为“智慧海洋”用户解决云环境中可能遇到的安全及管理问题；提供了包含安全体检、资产管理、漏洞风险管理、入侵威胁管理、安全监控、安全防护、合规基线、安全报表、安全告警等功能，如图 3.3 云主机安全防护框架所示。

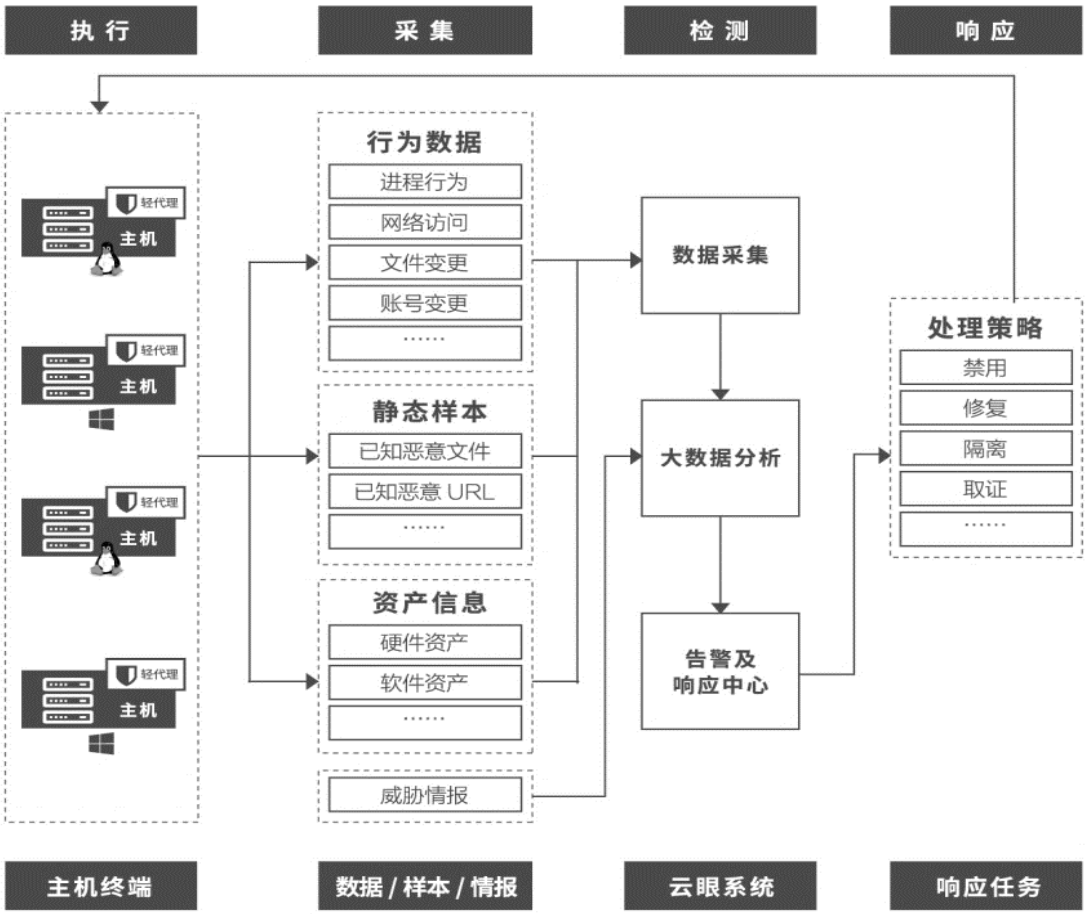


图 3.3 云主机安全防护框架所示

整体架构包含两个主要模块：

➢云：基于“零信任”构建的安全大数据平台，能够根据轻代理收集到的安全日志进行快速分析及挖掘，准确定位各种漏洞风险及入侵威胁，并第一时间进行预警。

➢端：轻代理部署在服务器上（支持物理服务器、虚拟化服务器），提供多个层面的安全监控和安全保护，可快速识别及阻断黑客攻击；同时轻代理会将相应的攻击数据和日志跟云端进行联动，利用云端的大数据分析能力进一步确定是否被黑客攻击及入侵。

3.5 网络安全管理体系

基于“零信任”的理念下，针对“智慧海洋”网络安全管理体系集成了认证、授权、动态重构、业务访问控制的功能，同时还以保护数据、功能资产为核心，以防高级持续性威胁为目标，通过立体防护，风险主动感知，动态威胁检测，实时响应处置的闭环保护实现对恶意攻击行为的事前主动预

防、事中积极对抗，事后及时响应的一体化安全保卫体系。

4. 结束语

针对我国“智慧海洋”发展的总体思想与架构，在新的数据场景下就应有新的安全管控思路。“零信任”体系与网络安全建设、云平台主机安全建设、数据安全建设、安全管理体系等方面进行全面规划是下一代网络安全的方向，这也将解决“智慧海洋”在实现共享、开放、创新的基础上具备足够的防御能力抵御新的威胁，这也将使安全防护跟随平台的发展升级同步改进更新，实现安全高效的更新迭代和可持续发展。

参考文献

[1].陈宇翔，张兆雷，卓见，等. 基于区块链的身份管理研究 [J]. 信息技术与网络安全，2018，37（7）：22-26.

[2].引领网信事业发展的思想指南——习近平总书记关于网络安全和信息化工作重要论述 [J].保密工作，2018（12）：4-5.

[3].李军 , 王翔 . 云数据中心网络安全的新挑战 [J]. 保密科学技术 ,2013(08):6-11.

云存储环境下基于矢量量化的图像伪装加密方法

柳晓龙　郑思飞　纪祥敏　陈日清

福建农林大学计算机与信息学院

摘要：为提高云环境下图像存储的安全性，本文提出了一种新型的图像伪装加密方法。该方法以矢量量化与离散小波转换为基础，采用“明文—明文”的伪装加密方式，不仅可以如传统加密方法一样保护云端图像，更提供了额外的视觉伪装功能。实验结果表明，该方法不仅能够有效提高云端图像的存储效率，还具有更好的视觉效果与伪装特性。

关键词：伪装加密，矢量量化，图像加密，云存储安全

1 引言

在信息技术日益发展的当今时代，云存储将数据存储服务带入了一个新时代，为大众提供了便捷的网络访问和数据共享方式。近年来，随着云存储技术的飞速发展，存储在第三方数据库上的云端图像文件与日俱增，然而随之而来的是日益增多的泄密事件[1]。在此背景下，用户对将含有个人隐私或敏感数据的内容直接暴露在开放的信道或不可靠的数据库中颇 具顾虑。因此，基于保证隐私性等目的，图像所有者有必要在图像传输至云端服务器之前先进行加密，避免未经授权的访问。

目前，学者们已经提出了许多基于频域或空间域的图像加密算法以保护云端图像[2-4]。频域图像加密算法[5]通常被设计为在频域中使用安全密钥系数更改图像数据或更改变换函数，例如离散分数阶傅里叶变换、量子傅里叶变换和倒数正交参数变换等，以达到图像加密的目的。空间域图像加密算法[6]基于著名的替代置换网络（SPN），利用替换过程更改图像像素值，并利用置换过程更改图像像素位置。这些置换和替换过程是空间域图像加密算法的核心，包括 P-Fibonacci 变换、随机网格、和混沌系统等技术。空间域和频域图像加密算法都能够以高

度的安全性保护图像，然而，它们输出的加密图像在视觉上都类似纹理或噪声。从安全的角度来看，这种类似纹理或噪声的特征是明显的视觉信号，表明存在可能包含重要信息的加密图像。因此，这些图像无疑会引起攻击者的关注，从而导致大量不同类型的密码分析、非法编辑、甚至删除图像内容等恶意攻击与分析[7]。

针对上述问题， Lee 等人[8]曾试图利用色彩转换技术将原始图像转换成一幅同样大小的可见秘密碎片马赛克图像，以达到图像伪装的目的。然而这种方法在解密时会造成图像失真，并不能完整地还原出原始图像。Bao 和 Zheng 等人[9, 10]分别提出了基于离散小波转换与最低有效位修改的图像伪装加密算法，虽然能够完整地还原原始图像，但是伪装加密后的图像大小将急剧扩张，严重影响存储效率。为使伪装图像与原始图像的大小保持一致，学者们相续提出了基于图像块分类的伪装加密算法[11-13]，其基本思想是根据图像块的标准差分别对原始图像和目标图像进行固定分位数分类，进而实现不同图像的自适应分类与块之间的匹配。然而以上基于块分类的转换方式没有考虑子块间的边缘失真问题，伪装加密后的图像有较大失真，视觉质量与安全性有待提高。

因此，为进一步提高云端图像存储效率与伪装图像的视觉质量，本文提出了一种新型的基于矢量量化(VQ)的图像伪装加密机制。在对原始图像进行伪装加密之前，通过矢量量化将原始图像转化为 VQ 索引表。接着利用离散小波转换（DWT），以“明文—明文”的伪装加密方式掩盖原始图像内容的同时隐蔽加密行为本身。本方法不仅可以像传统加密方法一样以正常方式保护图像，而且还提供了额外的视觉伪装保护。实验结果表明，本方法伪装加密后的图像具有良好的视觉效果与伪装性能。

2 伪装加密算法

2.1 图像伪装加密阶段

图像伪装加密阶段提供一种“明文–明文”的新型图像加密方式，可以从根本上掩盖秘密图像信息与加密行为本身。此阶段拟引入一张与原始图像完全不同的参照图像，通过对图像载体先后执行矢量量化、预加密与伪装转换完成“原始图像–参照图像”的转换。图像伪装加密基本流程如图 1 所示。

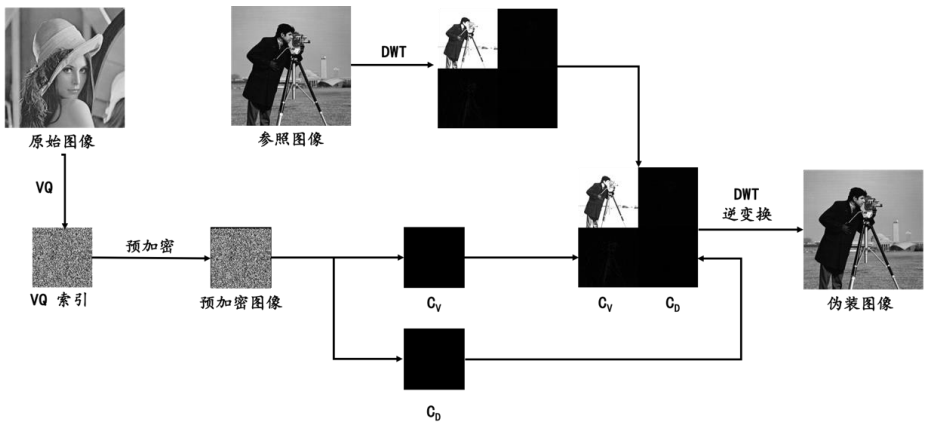


图 1 图像伪装加密流程图

1. 矢量量化

矢量量化（VQ）[14]是一种广泛使用的图像编码技术，具有简单框架和高效解码过程的特性，广泛应用于图像处理的各个领域。在矢量量化过程中，首先将原始图像分割为多个块，每个块由 4※4 个像素组成。假设原始图像大小为 4m※4n，则将该图像分割为 m※n 个 4※4 大小的像素块。量化过程中所使用的码书是通过大量训练生成的数据集，包含许多称为代码字(cw)的代表性图像块。通常码书的行数为 256，列数为 16，如图 2 所示。矢量量化过程中，取出分割出的原始图像块中的一个，将其对应的 16 个像素值与码书中每一行的 16 个值计算欧几

里得距离。计算结果中欧几里得距离最小代表的是这个块与码书中对应的行最为接近，可以用当前行的值代替原始图像中的像素值，并将该行对应的行号存入 VQ 索引表中。对原始图像中的每一个块进行上述相同的操作，将所有块对应的值存入 VQ 索引表中，即得到 VQ 索引表，具体实例如图 2 所示。

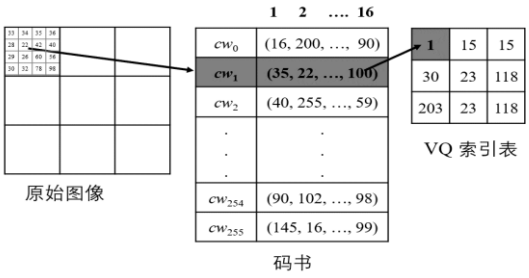


图 2 矢量量化实例

2. 伪装加密

经过矢量量化后的 VQ 索引表将作为伪装加密过程的输入图像，其大小为 m※n。为了进一步保护原始图像的内容以提升安全性，在将 VQ 索引表进行伪装加密之前需要将其进行预加密处理。预加密通过排列和替换来改变 VQ 索引表中像素的位置和值的大小，其公式定义如下:

$$P = T(O, K), \qquad (1)$$

其中 P 是经过预加密处理之后得到预加密图像，O 代表 VQ 索引表，K 是进行预加密处理里时所需要的密钥，T 是预加密处理的变换函数。预加密处理所使用的预加密算法可以使用传统加密算法进行加密。

在预加密过程之后，对预加密图像进行伪装变换（F）来将其转换为伪装图像。具体处理公式如下

$$E= F(P，R), \qquad (2)$$

其中 E 表示最终的伪装图像，P 代表经过预加密处理的预加密图像，R 代表参考图像。在伪装转换过程中，首先将参考图像 R 进行离散小波变换 (DWT)，得到 CA、CH、CV、CD 子带。随后将预加密图像经过二进制转换后嵌入到经过变换的参考图像的 CV、CD 子带中去。最后将该经过变换的参考图像进行 DWT 逆变换，得到最终的伪装图像。伪装变换过程以图 3 为例，假设参考图像的大小为 8※8，经过矢量量化与预加密后的预加密图像大小为 2※2，图中的每一个数字代表当前像素点的像素值。首先将参考图像进行 DWT 变换得到四个子带，由 DWT 的特性可知，分解得到的 CA、CH 分量包含了原始图像的主要能量，而其他两个中频分量 CV 与 CD 表达的是图像的细节部分，代表的图像信息相对较少。因此将预加密图像 P 转换为二进制数值并嵌入 CV、CD 子带中将并不影响伪装图像的视觉效果。以第一个像素 59 为例，其二进制数为 00111011，将其直接替换 CV 子带的相应位置即可完成嵌入操作。对图像 P 中的所有像素值执行完相同操作后，再将该经过处理的参考图像进行 DWT 逆变换，即可得到最终的伪装图像。

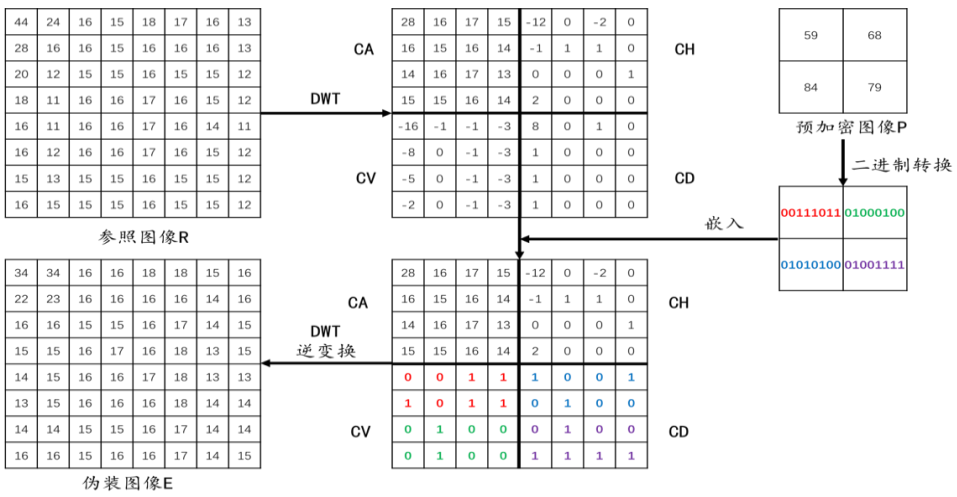


图 3 伪装变换实例

从上面的例子中可以看出，由于参考图像经过 DWT 变化后的 CV、CD 中的像素值普遍较小，故将其用数字 0 或 1 代替后对整体图像的改变较小。因此，最终得到的伪装图像像素值与参考图像差异不大，且一定程度上保留了像素之间的相关性，保证了最终伪装图像的视觉效果。将这样一张具有视觉意义的伪装图像放置到具有大量图像的云环境中很难将其与普通图像区分开来，从而躲避被攻击的风险，提升云环境下图像存储的安全性。

2.2 图像还原阶段

具有解密密钥的授权用户能够从云环境中将伪装图像下载下来，并将其恢复出原始图像。具体流程图如图 4 所示。

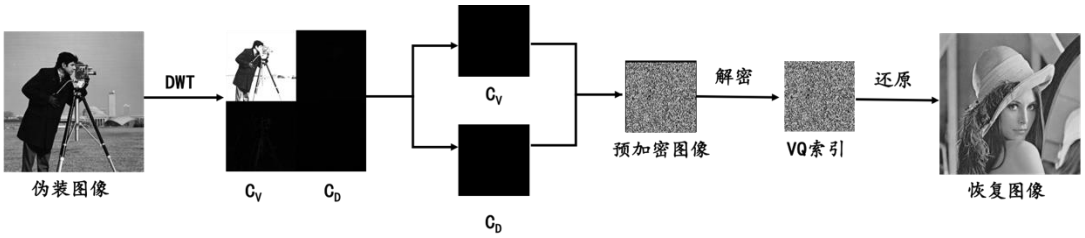


图 4 图像还原阶段流程图

图像还原阶段是伪装加密阶段的逆过程。首先将伪装图像进行 DWT 变换，得到 CA、CH、CV、CD 子带。随后提取出 CV、CD 子带中的像素值，按照嵌入阶段相反的过程进行重组即可得到预加密图像，如图 5 所示。从提取结果可知，伪装转换没有在转换过程中损失预加密图像的任何信息，在保证安全性的基础上也保证了信息的完整性。最后使用与预加密算法对应的解密算法并使用解密密钥 K 进行解密，即可得到经过矢量量化的 VQ 索引表。

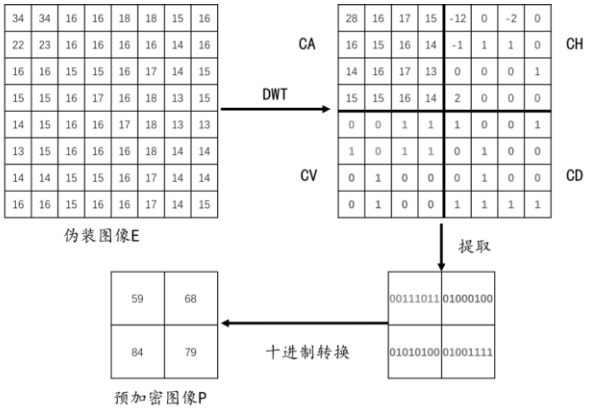


图 5 预加密图像提取实例

对于 VQ 索引表中的每一个值，找到码书中该码字编号(cw)所对应的 16 个像素值，即可将其恢复为原始图像中所对应的块，如图 6 所示。完成 VQ 索引表的所有块恢复之后即可得到最终的恢复图像。

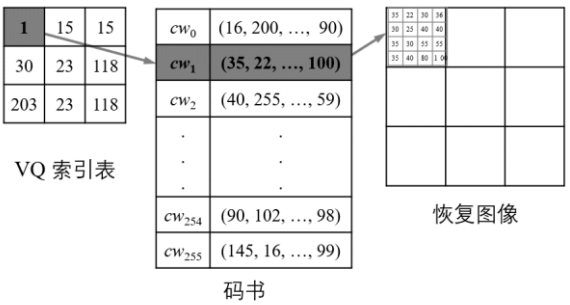


图 6 图像恢复实例

3 实验结果与分析

本实验测试图像采用 8 张来自 USC-SIPI 的代表性灰度图像，大小为 512*512，如图 7 所示，其中 A～D 为原始图像，E～H 为参考图像。实验结果首先将直观地通过视觉进行评估图像的视觉质量。除此之外，为了进一步准确地评估图像的视觉性能，通过对图像峰值信噪比(PSNR)的计算来准确评估图像的视觉质量，越高的 PSNR 值代表着越佳的视觉质量。PSNR 的计算公式如下:

$$PSNR = 10 \times log_{10} \frac{(255)^2}{\frac{1}{(512\times512)}\sum_{i=1}^{512}\sum_{j=1}^{512}\left(x(i,j)-x'(i,j)\right)^2}\ dB, \quad (3)$$

其中 x(i,j)与 x^' (i,j)分别表示两张图像在位置(x，y ）上的像素值。值得注意的是，30dB 为一张好的重构图像的阈值，当大于这个阈值时，两张图像之间的差异性很难被人眼所识别。

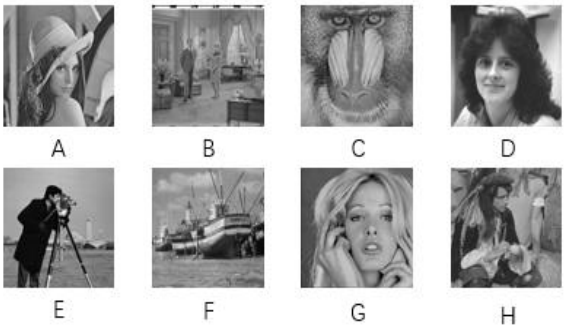


图 7 测试图像

使用不同的原始图像与不同的参考图像得到的 PSNR 值如表 1 所示。可以看出，PSNR 值主要受到参考图像的影响，不同的参考图像对 PSNR 的影响较大，而不同的原始图像对 PSNR 值影响较小，几乎可以忽略不计。此外，实验中所有 PSNR 值均大于 30dB，所以从视觉上很难将参考图像与伪装图像区别开来。

表 1 本方法伪装加密后 PSNR 值统计表

参照图像 / 原始图像	E	F	G	H
A	35.8182	31.0006	31.6277	33.0745
B	35.8137	31.0024	31.6253	33.077
C	35.8136	30.9995	31.6226	33.0711
D	35.814	31.0007	31.6245	33.0732

为了更好的展示出本方案所具有的伪装性能，我们将本方法与 Bao 等人的方法[9]进行对比。由于本方法使用的原始图像与参考图像均为 512*512 大小，而 Bao 等人的方法只能实现将具有参考图像四分之一大小的原始图像嵌入到参考图像中，即只可将 256*256 大小的原始图像伪装成 512*512 的参考图像。因此，Bao 等人的方法在伪装加密后的图像大小将急剧扩张，严重影响云端图像的存储效率。

从伪装后的图像视觉效果的角度出发，以原始图像 A 嵌入到参考图像 F 为例，图 8 显示了本方法与 Bao 等人方法在伪装加密后视觉效果的对比结果。可以看出，本方法的伪装加密图像跟普通图像并无太大差异。而 Bao 等人方法的伪装加密图像虽然在外观上与参考图像之间具有一定的相似度，但其图像上显现的条状曲线颇为明显，容易使人将其与普通图像区分开来。因此，相比于 Bao 等人的方法，本方法伪装加密后的图像视觉效果更优，具有更高的伪装性。

图 8 伪装加密图像视觉效果对比

为进一步对比两个方法在伪装加密后的图像视觉效果，表 2 展示了本方法与 Bao 等人方法的 PSNR 值对比结果。从表中可以看出，在相同的原始图像与参考图像的条件下，本方法的 PSNR 值均高于 Bao 等人方法的 PSNR 值。两种方法在面对较为简单的参考图像时的 PSNR 值都比较高，都表现出较为良好的特性。因此，总体来看，提出的方案在各种条件下都表现出更好的性能，能够为图像伪装加密后提供更高的安全保障。

表 2 伪装加密后 PSNR 值对比结果

原始图像	参考图像	本方法	Bao 等人方法
A	E	35.8182	30.5985
A	F	31.0006	28.6626
A	G	31.6277	29.0846
A	H	33.0745	29.7341
B	E	35.8137	30.3392
C	E	35.8136	30.5973
D	E	35.8140	31.6504

4 结论

本文提出了一种新型的图像伪装加密方法，本方法利用矢量量化与离散小波转换的特性，以“明文—明文”的伪装加密方式从根本上掩盖了原始图像在云存储环境下的内容与加密行为。本方法不仅可以像传统加密方法一样以正常方式保护图像，而且还提供了额外的视觉伪装保护。实验结果表明，本方法在伪装加密过程中可以很好地保留原始图像的图像信息。此外，最终产生的伪装图像在视觉与 PSNR 值上都表现出了良好的性能。与相关研究相比，本方法不仅能够有效提高云端图像的存储效率，还具有更好的视觉效果与伪装性，能够为图像伪装加密后提供更高的安全保障，在提升新时代云环境下图像存储安全性的同时，具有广泛的应用前景。

参考文献

[1].陈永府，宋鹏，王启富,等. 云环境下的数据防泄密存储技术[J]. 计算机应用与软件，2016, 33(10):288−293.

[2].芮坤坤. 基于离散傅里叶变换融合双混沌映射的图像加密算法研究[J]. 计算机应用与软件, 2014(10):327−330+334.

[3].张晓强，王蒙蒙，朱贵良. 图像加密算法研究新进展[J]. 计算机工程与科学, 2012(5):1−6.

[4].李昌刚，韩正之，张浩然. 一种基于随机密钥及"类标准映射"的图像加密算法[J].计算机学报.2003，26(4),465−470.

[5].梁晏慧，李国东，& 王爱银.基于分数阶 chen 超混沌的频域自适应图像加密算法[J]. 计算机科学.2019(S2):488−492

[6].朱淑芹，王文宏，&孙忠贵.对一种混沌图像加密算法的安全分析和改进[J]. 计算机工程与应用，2019, 055(001), 115−122.

[7].陈少鹏. 高级加密标准攻击方法的性能分析[D]. 2014.

[8].Y. Lee and W. Tsai, A new secure image transmission technique via secret−fragment−visible mosaic images by nearly reversible color transformation[J], IEEE Transactions on Circuits & Systems for Video Technology, 2014, 224: 695−703.

[9].L. Bao and Y. Zhou, Image encryption: Generating visually meaningful encrypted images[J], Information Sciences, 2015, 324: 197−207.

[10].S. zheng，X Liu，R. Chen，and S. Yuan，LSB−based visual image encryption scheme in cloud environment[C], 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, 2019:891−896.

[11].D. Hou, W. Zhang, and N. Yu, Image camouflage by reversible image transformation[J], Journal of Visual Communication & Image Representation, 2016, 40:225−236.

[12].刘小凯，姚恒，秦川. 基于图像块分类阈值优化的改进可逆图像伪装[J]. 应用科学学报，2018, 36(2):237−246.

[13].H. Yao, X. Liu, Z. Tang, Y. Hu and C. Qin, An Improved Image Camouflage Technique Using Color Difference Channel Transformation and Optimal Prediction−Error Expansion[J], in IEEE Access, 2018, 6:40569−40584.

[14].郑勇，周正华，朱维乐. 二维网格编码矢量量化及其在静止图像量化中的应用[J]. 电子与信息学报, 2002, 24(012):1906−1911.

优秀解决方案

5G 时代数据安全保护的属地化推进

龚晓波

中国移动通信集团福建有限公司莆田分公司

摘　要：数据安全日趋受到重视的今天，因 5G 的应用逐步推进，数据安全的严峻性随着数据量的暴增而暴增，我司各类现有的数据安全保护体系的属地化推进成为数据安全的重中之重。本文根据我司的属地化工作实际情况提出构建从反向主动控制、人员管理、4A 系统管理、权限管理、数据操作审批、数据提取控制、文档管控、操作行为审计等方面来加强数据安全控制，并以此为亮点提升本地竞争力。

关键词：数据安全，反向主动控制，意识管理，安全审计

1 数据安全保护在 5G 时代的思考

随着5G时代的到来，5G网络高速率、低时延的特性，必然导致边缘计算、云技术、大数据等应用的爆发，万户互联产生的海量数据将在终端和边缘端、边缘端和云端、云端内部来回穿梭，导致数据安全的边界越来越模糊、触点越来越多、风险越来越大。

另一方面，近年来，随着防范打击通讯信息诈骗的专项行动推进，诈骗案件多发，从中暗藏的数据安全泄露问题日愈凸显，数据安全保护日趋受到重视，万物互联中产生的数据，所有权归客户所有，作为网络的运营商，移动公司（以下简称我司）必须承担保护职责，对于出售或非法提供的行为将受到刑法处罚。

我司业务支撑系统（BOSS）、经营分析系统、CRM、网管系统、客服系统等均积累和掌握了大量的客户数据信息。

根据我司规定，客户数据信息包括客户基本资料、身份鉴权信息、通信信息、通信内容等 4 大类。进入 5G 时代后，客户数据信息的范围将持续扩展，将包括但不限于设备信息、计算数据等，本文主要探讨 5G 时代数据安全保护属地化推进过程中客户

数据信息的保护以及经验的业务层面价值。

我们认为，万变不离其宗，进入 5G 时代，数据安全仍然应该回归本源，紧抓安全管理“三分技术七分管理”的核心原则不变，在各个地市 5G 时代“边缘”位置着手，做好属地化的推进。

2 数据安全保护 5G 时代属地化推进目标

根据我司《数据安全保护管理实施细则》和《数据安全控制矩阵》及上级领导机关的相关管理办法的要求，我司数据安全保护属地化推进的目标如下：

（1）依托信息化的数据安全保护体系系统和审计体系，对数据安全相关的数据泄露、数据篡改开展包括但不限于事前预防、事中控制、事后审计等相关工作。

（2）通过数据安全管理体系、流程的细化与强化，落实日常管理与审核，做到数据安全泄露事件的及时发现、及时处理、及时惩罚。

（3）通过逐级管控，加强对一线员工的数据安全管理，补齐短板，防止非预期泄露。

（4）通过推广行之有效的数据安全保护体系，体现数据安全保护业务层面价值。

3 数据安全保护属地化推进要求

数据安全保护属地化推进的总体要求如下：

（1）落实《数据安全保护管理实施细则》与《数据安全控制矩阵》的要求。

（2）通过强化管理体系与流程，实现业务、系统层面的数据安全漏洞的及时发现、及时处置、及时弥补。

（3）依托信息化的数据安全保护体系体系加强数据安全管控，降低数据泄露、篡改风险。

（4）对违反数据安全保护的行为坚决落实问责。

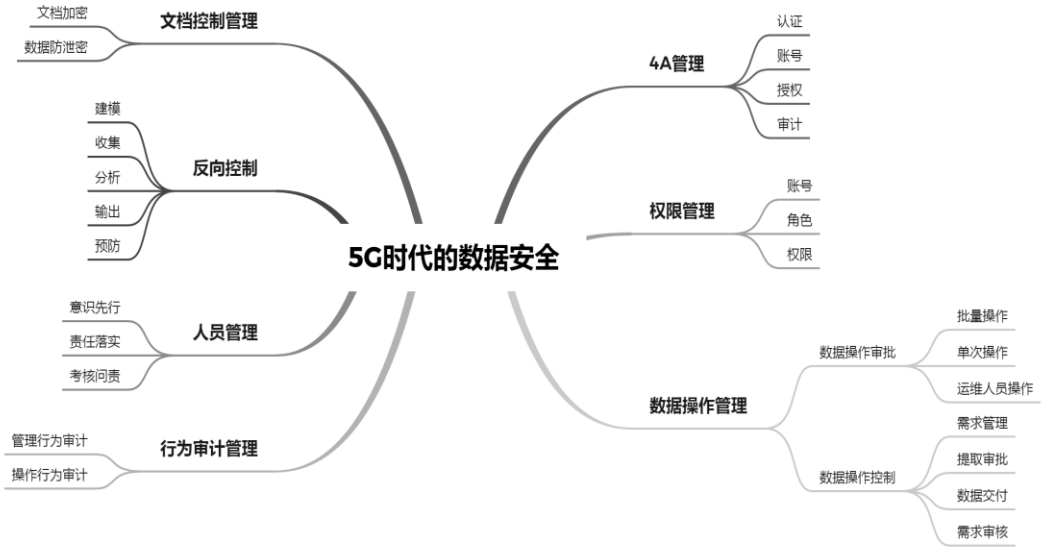


图 1 数据安全保护属地化管理结构图

4 数据安全保护反向主动控制

为精准控制客户数据信息的操作行为，对客户数据信息的操作行为进行管控，从风险管理的角度及时发现操作风险行为并发出预警，得到输出结果后由信息安全管理人员主动发起操作行为控制，做到数据安全风险“抓早抓小”，提前预防。

整体流程如下图所示，针对客户数据信息操作行为，分为建模、数据收集、数据分析、结果输出、

反向控制预防五个部分，形成一个闭环的反向主动控制管理流程。

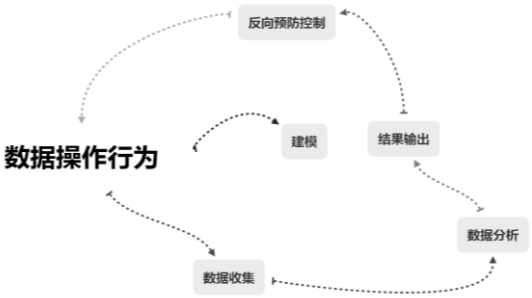


图 2 数据安全保护反向主动控制示意图

4.1 建模

根据《数据安全保护管理实施细则》与《数据安全控制矩阵》的要求，对所有客户数据信息操作行为进行数字建模，为后续数据收集、数据分析、结果输出提供数字模型。

①识别

建立识别客户数据信息操作行为的数字模型，便于数据收集环节对操作行为数据进行收集

②分析

建立分析客户数据信息操作行为的数字模型，便于数据分析环节利用大数据数据挖掘各类方法对数据进行分析

③风险预警

依据 SCL 法，建立各类操作的风险发生可能性与危害性等级数字模型，便于结果输出环节对数据分析结果进行风险定级，预警高风险行为。

风险R=事故发生可能性L×事故后果严重性S

图 3 风险预警建模 SCL 法公式

4.2 数据收集

将所有客户数据信息操作行为数据（只记录行为数据，不记录操作结果，以避免二次风险）进行全量收集。

（1）客户数据信息数据集群化管理

将客户数据信息集群化管理，避免分散的客户数据信息导致管理面过大，便于集中管理、集中调度、集中维护。

（2）客户数据信息操作行为数据模型化

根据建模阶段建立的数据识别数字模型，将操作行为数据模型化。

（3）操作行为数据收集

数据采集设备将操作行为模型化数据进行收集整理，存储至专用数据库。

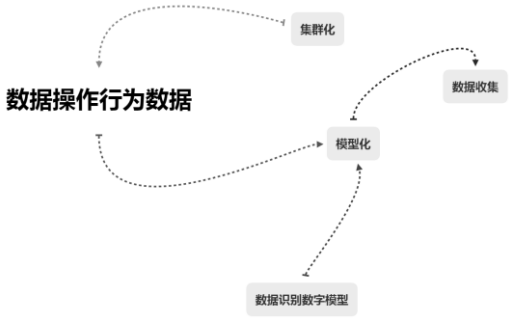


图 4 数据操作行为数据收集示意图

4.3 数据分析

采用爬虫、探针等数据挖掘、清晰技术，对对操作数据收集后形成的大数据，根据前期建立的数据分析模型，对数据进行清洗、核对、整合，主动分析操作行为。

（1）数据模型化

根据建模阶段建立的数据分析数字模型，进行数字模型化处理后投入数据挖掘分析处理。

（2）数据核对

对数据模型化结果进行核对，避免模型化过程对数据完整性、准确性造成影响。

（3）数据整合

将操作行为收集数据进行最终整合，形成最终待分析数据

（4）数据分析

采用分类、估计、预测、相关性分组、聚类等多种方法主动挖掘分析操作行为数据。

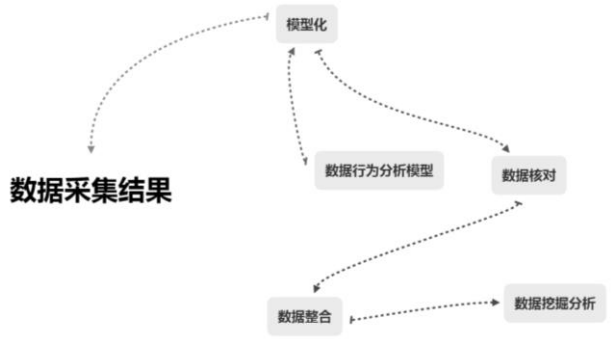


图 5 数据操作行为数据分析示意图

4.4 结果输出

根据操作行为分析的结果，依据风险预警数字模型进行结果模型化，给出风险等级指标，对风险行为发出预警。

（1）数据分析结果风险模型化

根据建模阶段建立的数据分析数字模型，进行数字模型化处理。

（2）风险行为标记

根据模型化结果，计算得出风险等级。

（3）风险行为预警

根据风险等级触发相应等级预警，提醒信息安全管理员采取相应操作。

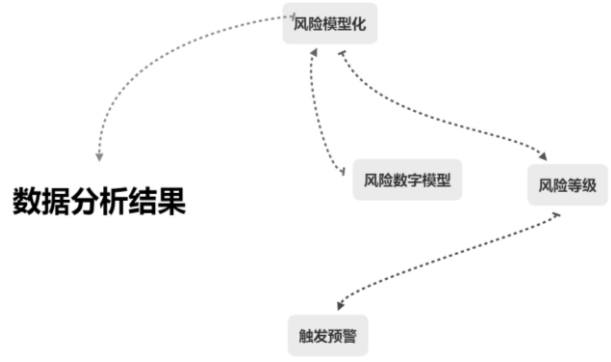


图 6 客户数据信息操作行为风险输出结果示意图

4.5 操作行为反向控制预防

信息安全管理人员根据客户数据信息操作行为风险输出结果，反向对操作人员的行为进行主动控制预防。主要针对超范围访问、超频次访问、数据操作失当等三个方面进行反向控制预防。

（1）超范围访问

回溯权限分配行为，对审批不到位的部分进行纠正、问责，及时调整角色权限，确保操作人员权责匹配。同时对超范围访问过程中是否涉及客户数据信息泄露，落实相应审计并问责。

（2）超频次访问

对超频次行为进行审核确认，明确是否岗位必要，非必要情况的超频次行为采取提醒、警示、关闭权限等操作，必要情况落实问责。

（3）数据操作失当

对于客户数据信息操作人员的操作失当行为，如资源占用过大、数据误操作等，根据数据操作规范及时纠正操作人员行为，确保客户数据信息数据集群数据安全。

5 数据安全保护属地化人员管理

5.1 数据安全责任意识先行

在属地化推进过程中，我司借鉴安全生产教育的“三级安全教育”体系，构建的“三级数据安全教育+案例警示教育” 信息安全责任意识教育体系，实现数据安全保护意识先行，形成全员主动性。

（1）入司数据安全培训

在所有新员工入司都必须经过入司培训中，增加数据安全培训环节，采取独立课程、保证学时、紧抓要点的方式，使所有新员工具备基础的数据安全保护意识，守住红线，自觉地在生产经营实际中落实数据安全保护的相关工作要求。

（2）岗位数据安全培训

针对具体涉及客户数据信息收集、调阅、提取、操作等方面工作的人员，根据具体工作内容，有针对性的开展岗位数据安全培训， 做到全覆盖、重专业、好执行，确保所有具体专业人员熟知本岗位数据安全工作细节，使数据安全管理要求落实到工作实处。

（3）公司数据安全培训

定期以宣传短信、微信公众号、网上学习、视讯会议、应知应会考试等多种形式开展全公司范围

的数据安全培训，不断强化信息安全保护意识。

（4）数据安全警示案例

结合各类渠道收集的数据安全保护相关案例，定期开展警示教育，让员工知道违反数据安全管理规定的严重性，轻则内部问责，重则追究刑责，防微杜渐。

5.2 数据安全责任层层落实

通过制定责任矩阵在前、落实责任矩阵在后、书面承诺为辅的方式层层落实数据安全责任。

（1）明确数据安全责任矩阵

信息安全管理部门牵头组织各专业、各单位建立或完善更新各专业线条直至全公司的数据安全责任矩阵，明确数据安全敏感信息操作各环节的操作人员、内容与责任，为全公司落实责任提供整体框架。

（2）落实责任矩阵

以建立好的责任矩阵为准绳，规范各专业的数据安全保护管理工作，做到有章可循、有理有据、违规必究。

（3）书面承诺层层签署

要求涉及敏感信息系统维护和使用的各专业线条部门领导、相关科室经理、员工全面落实签署《数据安全责任承诺书》，实现书面承诺全覆盖。

5.3 数据安全保护考核与问责

在属地化推进过程中，通过制定《员工问责实施细则》、《管理人员问责实施细则》、《信息安全考核管理办法》、《数据安全管理实施细则》、《防范打击通讯信息诈骗问责实施细则》等各种管理办法，对内部员工发生的数据安全泄密事件，根据造成的影响及相关责任主体的态度，作出如批评教育、书面检查、通报批评、绩效处分、政处分、法律责任等处分，而且处分不仅可以单独适用，也可以同时适用。对合作单位、数据安全相关单位的类似行为，根据所造成的的影响进行相应的考核、处罚、停止合作、法律追责等处理。

6 数据安全保护管理推进

结合数据安全保护属地化推进要求。主要从 4A 系统管理、权限管理、数据操作审批、数据提取控制、文档管控、操作行为审计、人员管理、反向主动控制等方面加强数据安全管理推进，提高数据安全保障能力。

6.1 4A 系统管理

认证、授权、账号、审计构成的 4A 管理平台采用堡垒主机的技术，由省级统一建设，实现对数据安全相关数据资产的集中化授权与访问控制。

属地化推进过程中，重点加强用户权限控制、金库模式应用管理、工号管理员操作控制、敏感数据操作控制等，实现 4A 系统管理的灵活应用，确保全线条数据安全管理。

6.2 权限管理

数据安全保护属地化推进过程中，帐号的权限分配遵循“十二字”准则，即“权限明确、职责分离、最小权限的原则”。

在属地化推进过程中，由各级工号管理员建立“角色”视角，对使用涉及数据安全相关数据资产的各类业务系统、平台的全量岗位进行“角色”梳理、匹配、合并、规范，形成标准化的“角色”。

建立角色体系后，根据岗位特征与数据需求对相关人员进行角色级授权，不同的岗位角色拥有不同的权限。

各岗位角色权限的分配，通过三种方式授权：省级统一角色、市级统一角色、单菜单权限。

6.3 数据操作审批

在数据安全的属地推进过程中，数据安全相关数据资产的操作人员主体为业务人员、运维支撑人员、开发人员等，在遵循“事前审批授权”的前提下，操作人员经过相关审批、审核后可以获取此类数据资产。

根据本地实际，本地建立电子审批系统与本地个性化应用导航系统。

本地电子审批系统实现账号管理（包括账号新增、修改、删除）、账号权限管理（包括权限新增、

权限调整与删除）、金库模式应用审批流程、前台客户数据信息需求管理等。

本地个性化应用导航实现本地个性化需求管理，所有个性化需求必须经过管理系统审批，由需求人——需求人主管领导审批——需求可行性确认——支撑主管领导审批——信息安全管理人员确认——支撑实施人——信息安全管理人员实施后确认——主管领导审批——需求人，实现信息安全管理闭环，信息安全管理人员对所有需求有一票否决权，由信息安全管理人员对个性化需求中数据安全进行管控，并由主管领导对信息安全管理人员实行主管监督。

① 涉及客户数据信息的批量操作

数据安全相关数据资产的批量操作包括但不限于批量查询、批量导入导出、批量为客户开通、取消或变更业务等，必须遵循如下要求：

a. 针对客户数据信息的批量查询、批量导入、导出必须经过主管领导审批后，由信息安全管理员依据数据安全管理要求分析确认后，方可进行相应操作。

b. 批量为客户开通、取消或变更业务

对于通过业务人员(客户经理、现场促销人员)驻点收集办理的业务，业务人员需制作批量业务申请单，用户、业务人员签字确认后进行批量操作。

对于通过外呼确认或短信确认办理的业务，业务人员提交批量业务受理需求单，由部门领导（三级经理以上）审批，同意开通的号码需留有外呼记录及短信确认记录才能进行批量处理。

② 涉及客户数据信息的单次操作

数据安全相关数据资产的单次操作主要是因业务受理、投诉处理等情况下的单次特殊查询，此类操作应遵循如下要求：

a. 数据安全相关数据资产中用户资料信息类的查询，须获得客户的同意，方可按照正常的鉴权流程后才能查询并保留鉴权、业务受理凭据。鉴权包括但不限于有效证件、业务密码。

b. 数据安全相关数据资产中详单级别的查询，服务营销人员原则上应引导客户通过电子渠道查询通话详单，再根据通话详单作好答疑、解释工作。

遇到特殊情况（如资费投诉、自助话单打印设备故障等），服务营销人员必须通过电子工作流并结合本地工单系统，由专业投诉处理人员提取客户通话详单并回复客户。

c. 数据安全相关数据资产中因维系服务、营销等需查询相关集团客户详细资料，未在响应客户请求时，应经审批后方可查询所辖集团客户详细资料。

d. 针对数据安全相关数据资产中因投诉处理、营销策划、经营分析等工作需要查询和提取客户数据信息的，由业务人员提交查询需求，经业务管理部门领导审批通过后方可查询，并定期由专人进行严密的事后审核。

③ 运维支撑人员对客户数据信息操作

运维支撑人员对客户数据信息的操作应遵循如下要求：

a. 运维支撑人员未经授权、未收到需求严禁私自对客户数据信息进行操作，这是基本原则。

b. 针对数据安全相关数据资产全生命周期的各类业务系统、平台，应由对应运维支撑部门按照账号权限角色化管理流程建立对应的角色权限矩阵，明确数据安全访问权限与对应的黑白名单管理机制。

c. 运维支撑人员对业务系统的应用层的访问权限必须经过该系统的业务主管部门管理员审批，对系统层访问权限必须经过本部门领导（三级经理以上）审批。

d. 数据安全相关数据资产中因因业务投诉、统计取数等进行的客户数据信息查询原则上需要有业务主管部门的相关公文或工单，如遇业务支撑部门自发的运营监控分析、数据分析等情况可免除业务主管部门的公文或工单，客户基本资料查询必须经过上级主管审批，客户通话详单查询必须经过部门领导（三级经理以上）审批；因批量业务操作、

批量数据修复等进行的客户数据信息变更，原则上需要经业务主管部门的审批或需求，包括但不限于相关公文或工单，如遇业务支撑部门自发的运营监控分析、数据分析等情况可免除业务管理部门的公文或工单，必须经过部门领导（三级经理以上）审批。

e. 数据安全相关数据资产中因业务投诉、统计取数、批量业务操作、批量数据修复等进行的数据查询、变更不得扩大操作范围，必须在申请操作工单中保留操作原因、来源的工单（公文）编号和具体使用的数据源表，并由专人负责审核，审核人员应记录审核结果，并进行每月汇总分析，总结存在的问题并逐级上报。

f. 数据安全相关数据资产中因应用优化、业务验证测试需要而产生的数据查询、修改，原则上只能利用测试号码进行各项测试，不得使用真实客户号码，如遇到测试号码无法进行的特殊情况，必须提交操作申请，客户基本资料查询操作必须经过上级主管审批，客户通话详单查询、批量数据修改必须经过部门领导（三级经理以上）审批。

g. 数据安全相关数据资产中因系统维护而进行的数据迁移（数据导入、导出、备份）必须填写操作申请，并经过部门领导（三级经理以上）审批。

h. 严禁运维支撑人员导出客户数据信息到开发测试环境，对需导出的信息必须经过部门领导（三级经理以上）审批并进行模糊化处理。

④ 数据提取控制

基于生产运营相关的生产分析、市场策划、审计检查等需求需要，我司在生产经营过程中必然存在批量取数需求。此类操作根据数据安全存在较大的安全隐患，各需求部门应加强对需求部门的需求审批管理。

a. 在属地化推进过程中，各单位数据需求部门指定数据分析员专人专职负责本部门的数据提取需求，运维支撑部门只接受需求部门数据分析员的数据提取需求；由该部门或上级业务主管部门负责需求的审核；运维支撑部门指定数据管理员专人专职负责数据提取需求的提取及复核，数据提取和数据复核人员原则上要为不同的人员；如发生人员变动，应由相应部门在 1 个工作日内及时通知对口部门。

b. 为确保数据安全，数据需求结果不得交付给非需求人员，数据安全相关数据资产全生命周期均需在经审批确认的人员中流转。

c. 数据需求涉及的数据安全相关数据资产应由需求部门数据分析员进行审核并作详细描述，支撑部门的数据管理员有责任按“最小够用”原则提供数据，原则上只接受统计、分析类取数需求，如遇到特殊情况（如客户关怀、二次营销等情况）需批量提取数据信息的，需要有业务主管部门的相关公文或工单，如遇业务支撑部门自发的运营监控分析、数据分析等情况可免除业务主管部门的公文或工单，客户基本资料批量提取必须经过上级主管审批，客户通话详单批量提取必须经过业务支撑部门领导（三级经理以上）审批。

d. 数据需求的提取必须由专人负责“事后审核”，分为按次、按周、按月对数据需求的提取情况进行审核，审核内容包括但不限于：数据需求的分析规范性、操作执行规范性、复核稽核过程规范性、资料文档规范性。审核人员应充分利用信息化手段规范记录结果，并按月进行汇总分析与相关存在的问题的逐级上报。

⑤ 文档管控

运维支撑部门通过加强管控及审计，防止客户数据信息泄密事件发生

a. 数据安全相关数据资产的数据需求过程，必须遵循“受控可控”原则，严禁明文传输数据资产，数据的提取结果必须为受控文档。受控文档是指脱离公司内部办公环境后无法打开的采用包括但不限于加密、授权、数字水印、数字签名等技术手段的受安全保护的文档进行安全保护后的文档章。

b. 因业务需要，第三方人员若需要使用涉及客

户高价值信息的，数据安全相关数据资产中高价值客户数据业务主管部门不得直接提供给第三方需求人员，必须在指定平台上遵循“受控可控”原则进行编辑和处理，不得存放在指定平台外的任何主机上。

⑥ 操作行为审计

数据安全保护的属地化推进过程中，我司将操作行为审计重点放在工号管理行为的审计与数据安全操作日志审核上。

① 工号管理行为审计

为实现数据安全保护过程中对管理行为的管理，必须严格落实工号管理行为的审计。

a. 账号管理行为审计

针对工号管理人员对账号的新增、删除、调整行为进行审计，对未经审批的账号管理行为进行追究问责。

b. 权限管理行为审计

针对权限的新增、删除、调整行为进行审计，确保严格遵循“权限明确、职责分离、最小特权”的原则。

② 信息安全操作日志审核

信息安全操作日志审核即对数据安全相关数据资产的操作日志进行审核，具体操作为将日志与工单等原始凭证进行比对，分析查找违规行为。

基本要求如下：

a. 业务部门和运维支撑部门根据“谁主管谁负责、谁使用谁负责”的原则，对各部门所使用的涉及客户信系统的操作进行定期信息安全审核；

b. 数据安全相关数据资产的管理应根据“职责不相容”原则设置安全员，业务部门和运维支撑部门应确保安全员与系统管理员、业务操作人员分开，根据属地化推进经验，安全审计不能局限于审计员，必须由安全审计员指导督促归属部门安全员定期开展安全审核；

c. 属地化推进过程中，数据安全相关数据资产的各系统应完整、准确记录各类关联到具体责任人的行为数据，包括但不限于帐号与授权管理、系统访问、业务操作、客户数据信息操作等行为；

d. 属地化推进过程中，数据安全相关数据资产管理中用于安全审核的原始日志应完整、准确包含可定位到具体责任人、明确具体操作行为与审核痕迹的日志类数据信息，基于安全原则严禁审核原始日志包含明文的具体数据资产内容；

e. 根据《网络安全法》等相关法律法规要求，数据安全相关数据资产相关系统的日志记录范围、留存日期、灾备必须符合要求，在线至少保留 3 个月，离线至少保留 1 年，除日志日常维护涉及数据迁移外，任何人不得对日志信息进行更改、删除；

f. 属地化推进过程中，数据安全相关数据资产的安全审核相关原始日志、审核结果须单独保存并做好相关灾备；

g. 属地化推进过程中，数据安全相关数据资产的各类操作依据、凭证、凭据至少保留 1 年。

7 数据安全保护的长远意义

数据安全保护的属地化推进是以强化数据安全管理，实现信息安全为最终目的。通过对系统权限、操作日志、访问控制等安全措施，满足我司在数据安全保护方面的需求，提升抗数据安全风险能力，由此助力业务发展，提升客户感知，保持公司可持续性健康发展势头，具有长远的意义。

（1）提升客户感知

数据安全保护的不断加强将遏制电信诈骗势头，客户在信息安全方面的感知必将得到提升，产生更强的专业信任感，梳理更好的品牌形象。

（2）形成行业标准

结合 YD/T 2670−2013《基础电信运营企业移动网络数据安全管理框架》和 YD/T 2671−2013《分权模式（金库模式）数据安全保护技术要求》两个行业标准，形成数据安全管理工作统一标准。

（3）保持公司可持续性健康发展

数据安全作为我司业务形象的生命线，抓好数据安全保护工作，将持续维护我司业务形象，保持

我司可持续性健康发展。

同时可以实现将我司一整套成熟的数据安全保护体系作为我司的实力产品，向需要做好数据安全保护的行业如电力、银行、保险、教育等领域推广，为社会整体公民个人信息安全事业做出贡献的同时也为公司政企业务发展新增发展点。

8 结束语

本文在分析了我司数据安全保护属地化推进过程的目标、要求及举措办法上对数据安全保护的具体实施进行了研究与探讨。在实际应用中需要紧密联系生产经营实际，发现数据安全保护的薄弱点，实现对架构、方法的更新，持续加强数据安全保护工作。

参考文献

[1] 客户信息安全保护的标准化进展及解决方案. 刘佳，杜雪涛，冀文，张琳. 北京：中京邮电通信设计院，2015

[2] 中国移动业务支撑网客户信息安全保护.徐党生. 北京：中京邮电通信设计院，2014

[3] 5G 时代的信息安全及相关对策研究.蒲东. 无线互联科技.2019

风电场网络信息安全风险辨识探讨

林晋洪

（福建省三川海上风电有限公司　福建莆田　351100）

摘　要：网络信息安全是影响电网能否正常稳定运行的重要因素，风电场因其数量多，分布范围广，其网络信息安全与否是影响电网安全运行的关键。本文从风电场的网络结构特点出发，探讨风电场网络信息安全风险辨识及风险分级方法与管控建议，促进风电场网络信息安全风险分级管控和隐患排查治理双重预防体系的构建，保障安全生产。

关键词：风电场、网络信息安全、风险辨识、分级管控

引言

2020 年 3 月份某风电场 220kV 送出线路出现线路双套保护快速通信通道同时中断故障，导致线路紧急停运，严重威胁电网安全。网络通信是电网的重要组成部分，风力发电作为新能源开发利用的一种主要方式，正快速发展中，风电场的网络信息安全与否对电网的安全稳定运行影响日趋严重，其网络信息安全的风险辨识及防控更是电网安全运行的薄弱环节。当前，构建安全风险分级管控和隐患排查治理双重预防体系是党中央国务院加强新时期安全生产工作的重要部署，是电网安全稳定运行的重要保障体系。本文从风电场网络特点及存在问题出发对其网络信息安全风险辨识进行分析探讨。

1 风电场网络结构特点及存在问题

1.1 风电场网络结构及特点

风电场不同于变电站和传统发电厂，其所含的主要设备为分布范围广、设备安全防护有限的风力发电机组，另外包括升压站、集电线路、送出线路等。风电场电力监控网络包含生产大区和信息大区两部分，其中生产大区分为控制区（Ⅰ区）和非控

制区（Ⅱ区），涵盖调度数据网、远动主机、测控装置、五防系统、保护装置、故障录波系统、PMU 装置、风机监控系统、风功率预测系统、AGC/AVC 系统、电能量采集系统等；信息大区包含综合数据网、调度 OMS、气象服务器、视频监控系统等[1]。

风电场电力网络安全总体策略遵循电网“安全分区、网络专用、横向隔离、纵向认证”的原则。一般生产大区和信息大区之间通过部署防火墙进行逻辑隔离，强度近似物理隔离，子站间的出入口部署纵向加密装置进行加密传输，生产大区与广域网的纵向连接采用纵向加密装置进行隔离，采用认证、加密及访问控制等措施实现数据安全传输及边界安全防护。

风机是风电场的主要设备组成部分，风机监控系统通过网络采集每台风机状态信息，其底层结构基于光纤环网，通过光纤环网交换机与控制室核心交换机连接的服务器进行实时通信[2]。风机网络结构具有分布范围广，线路走向复杂，现场环境不稳定等特点。

风电场升压站安防设施较为完善，网络物理安全较为可靠，但是风机部分因分布在各种区域环境中，无法做到有效监控，主要依靠视频监控及运维人员的定期巡视，其网络安全防控是整个风电场的薄弱环节。

1.2 风电场网络信息安全存在问题

风电场网络信息安全在设备设施方面存在问题主要有：①风机分布范围广，现场无法有效管控，安全防护不到位等易遭人为破坏导致网络受攻击；②风机监控系统、风功率预测系统和风机基础监测系统等因业务需要横跨安全Ⅰ区、安全Ⅱ区以及外部网络，在边界防护上横向隔离装置、防火墙缺失；③风机通常采用光纤集线方式组网，当集线线路中间节点断开导致整串风机通讯中断，网络可靠性低；④因网络设备配置原因部分风电场实时通道和非实时通道对安全Ⅰ区和Ⅱ区数据接入未进行区分，出现通道混用现象。

风电场网络信息安全在运行管理方面存在的主要问题有：①风机依靠远程监控或定期巡查无法第一时间发现现场存在的安全隐患，进而导致网络信息安全事故发生；②网络通信设备设施定期检查及隐患排查治理不到位，导致网络通道受到破坏；③风电场运行检修人员技术水平有限，对风电场网络结构及配置掌握不足，需要借助外部力量解决问题；④运行检修人员网络安全保护意识不强，内网外网移动存储介质混用，计算机账户密码未统一管理保存及定期修改，浏览不安全网站等。

2 风电场网络信息安全风险辨识

2.1 危险点确定

危险点可分为静态危险点和动态危险点，风电场网络安全防护静态危险点主要包含所有网络设备设施，如交换机、路由器、纵向加密装置、监控主机、工作站、各类监测系统、服务器等。动态危险点为环境因素和人为因素导致的危险，如出现恶劣天气、地质灾害，风电场人员日常生产活动伴随的风险等。

2.2 危险源辨识

通过上述确定的危险点可以判断其可能带来的危险源，对于静态危险点可以建立设备设施危险源辨识清单，对于动态危险点可以建立生产活动危险源辨识清单。设备设施危险源辨识清单可参照风电场网络安全分区将对应设备进行重要程度划分，根据设备故障可能导致的网络安全威胁进行危险辨识。生产活动危险源辨识清单根据动态危险点所包含的环境因素和人为因素分别罗列，如设备运行环境异常、恶劣气候、地质灾害等引起网络设备故障导致的事故，运维人员日常检查维护不全面、网络设备设施恶意破坏或使用不当以及外界非法手段攻击等因素引起的事故。

2.3 风险评价

风险评价是通过对上述辨识的危险源所伴随的风险进行定性和定量地分析预判，在评定风险大小后确定风险等级和管控层级[3]。风险评价通常采用 LEC 评价法，其中 L 是事故发生可能性，E 是暴露于危险点中的频繁程度，C 是发生事故可能造成

的后果程度，D 为三者乘积，即 D=LEC，为风险危险程度判定值。LEC 风险评价法分数值及危险程度判定具体如表 1 所示。

表 1 LEC 评价法分数值表

发生的可能性（L）	分数值	暴露于危险点中的频繁程度（E）	分数值
完全可以预料	10	连续暴露	10
相当可能	6	每天工作时间暴露	6
可能，但不经常	3	每周一次，或偶然暴露	3
可能性小，完全是意外	1	每月一次暴露	2
很不可能，可以设想	0.5	每年仅几次暴露	1
极不可能	0.2	非常罕见的暴露	0.5
实际不可能	0.1	/	/
发生事故可能造成的后果程度（C）	**分数值**	**危险程度（D=LEC）**	**分数值**
大灾难，10 人以上死亡，或造成重大财产损失	100	极其危险，不能继续作业	＞320
灾难，3-9 人死亡，或造成很大财产损失	40	高度危险，要立即整改	160~320
非常严重，1-2 人死亡，或造成一定的财产损失	15	显著危险，需要整改	70~160
严重，重伤，或较小的财产损失	7	一般危险，需要注意	20~70
重大，致残，或很小的财产损失	3	稍有危险，可以接受	＜20
引人注意，不利于基本的安全要求	1	/	/

举例如有危险点风电场风机维护后忘记锁门，危险源辨识为可能引起外部人员进入风机，人为破坏导致风机停机或入侵风机监控系统攻击网络等。风险等级评价具体为：L 取 1，E 取 10，C 取 15，可得 D=150，为显著危险级别，需要及时整改。根据风险危险程度可以制定具体的预防措施和隐患发现后相应的管控级别、责任部门及责任人等。

3 风电场网络信息安全风险管控建议

针对上述网络信息安全风险辨识情况建议采用风险分级管控措施，首先根据风险导致事故的影响程度制定相应的管控资源和措施，再根据风险等级确定管控方式及责任归属。网络信息安全风险管控具体措施可以从物理安全和运行管理两方面考虑。

物理安全方面：①虽然大部分风机目前配有人员入侵告警功能，但对偏远机位不能及时有效地阻止人为破坏，建议增设光、电告警装置；②风机监控等系统涉及跨区的业务通过串口通讯方式实现物理隔离，无法实现的需配置必要的防火墙及加密装置等；③对移动存储介质如 U 盘、纸质档案和电子档案分类标识，建立专门介质库统一管理。

运行管理方面：①主机口令定期更换，建立登录失败处理策略；②定期对网络系统和操作系统进行漏洞扫描，对发现的网络系统及操作系统安全漏洞进行及时的修补，关闭不必要的服务、组件、端口及应用程序等；③安装入侵检测/入侵防御系统及包含入侵防范模块的多功能安全网关等；④加强运维人员网络信息安全保护意识，提高运维人员相

关业务技能水平以及聘请网络安全专家作为常年顾问等。

4 结束语

风电场网络信息安全是影响电网安全稳定运行的重要因素，通过网络信息安全风险辨识能够有效构建风电场网络信息安全风险分级管控和隐患排查治理双重预防体系，达到将网络信息安全隐患关口前移，构筑预防为主的网络安全目标，保障电网安全稳定运行。

参考文献

[1]仝新强,刘晓波.浅谈新能源发电场站电力二次系统安全防护[J].电力科技,2019(10):191.

[2]陈育聪.基于风电场远程运维网络安全的现状研究及分析[J].科学与信息化,2018(11):38-41.

[3]张子英.安全风险分级管控与隐患排查治理双重预防体系的建立与推广应用[J].中小企业管理与科技,2019(29);114-115.

福建移动互联网电视平台安全防护整体解决方案

上官涛　吴篁　林伟　董健业

中国移动通信集团福建有限公司

摘要：互联网电视是运营商最复杂的一项业务，不仅要对接牌照播控平台，还要对接能力平台、CDN平台、BOSS 系统、终端厂家等。移动集团要求按照“零重大网络故障、零重大安全事件、零重要客户投诉”目标提供业务保障。为此我司建立了端到端的安全防护体系，在内容源、EPG、平台、CDN、网络、终端等各个环节，全面提升安全防护能力。

关键词：互联网电视、安全防护体系、防篡改、流量清洗

1 引言

互联网电视系统面向公众提供服务，来自公网的攻击类型多、行为频密。互联网电视是党和国家重要的思想文化宣传阵地，内容如果被恶意篡改，不仅用户会对运营商造成信任危机，同时也会对社会带来严重的政治影响。为了确保互联网电视业务内容安全、传输安全、播出安全，需要建立端到端的安全防护体系，使业务和安全，从简单相“加”，迈向深度相“融”，促电视业务有序发展。

2 安全体系

从内容源、EPG、平台、CDN、网络、终端、监测、管理等各个环节进行全方位安全管控，建立端到端的安全防护体系。终端侧，部署异常进程监测、卸载防护能力，实现一键清理；网络侧，对接态势感知能力平台，实现一键关断；平台和 CDN 侧，建立基于协议监测的白名单式防护体系，实现 7 大场景一键关停，推动电视安全从“外生安全”向“内生安全”的转变。

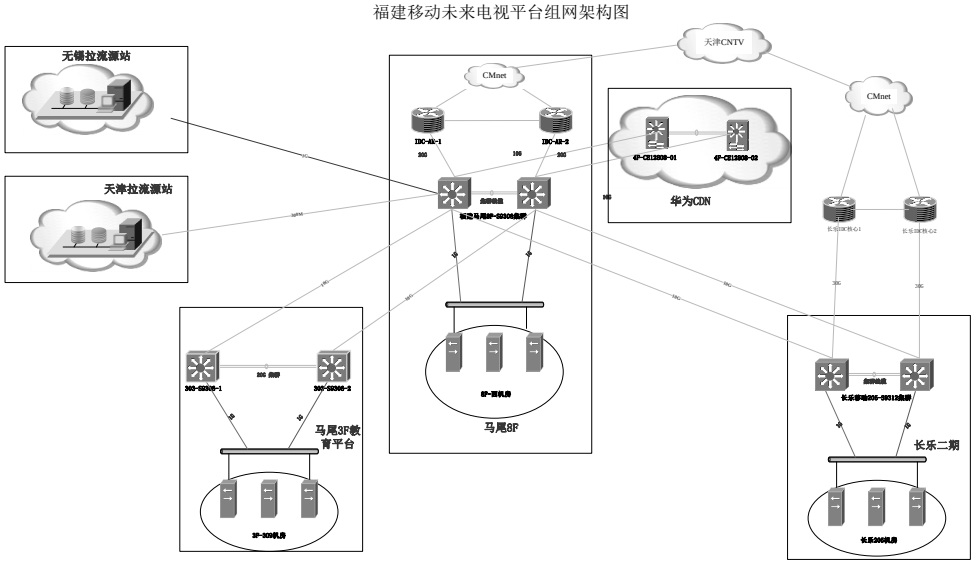
2.1 内容源安全

牌照提供的内容源是互联网电视平台中传输内容的源头，内容源安全是整个平台安全的根本。内容源分为直播和点播。

2.1.1 直播内容源安全

直播业务对传输的及时性要求很高，同时为防止传输期间被篡改，直播信号全部采用专线传输。为了防止单点故障，特意在无锡和天津建立异地容灾源站；而且分别建设了“从无锡到福州”和“从天津到福州”的传输专线。

福建移动未来电视平台组网架构图



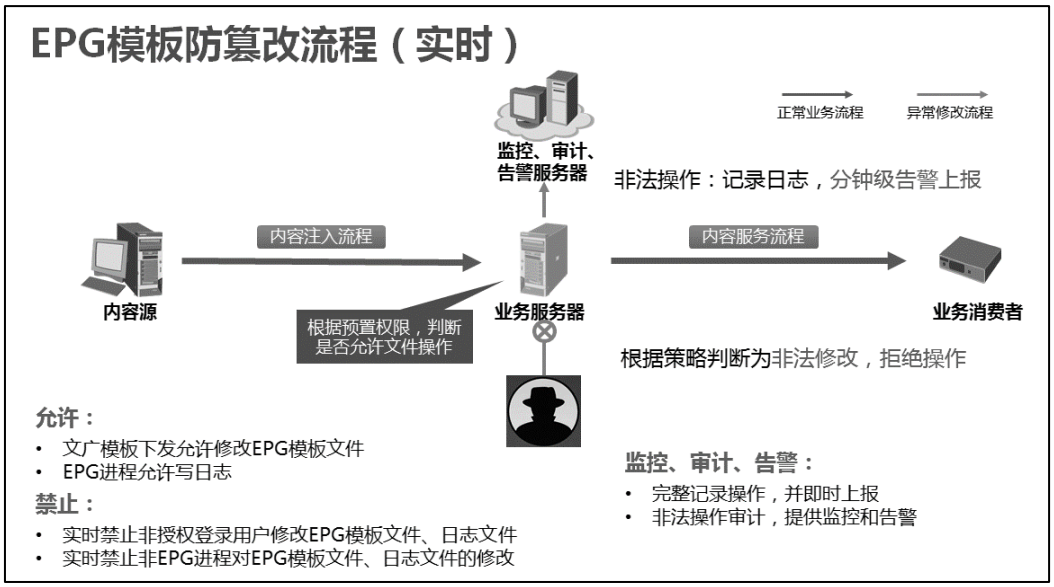
2.1.2 点播内容源安全

随着高清和 4K 内容的兴起，点播内容的 TS 文件越来越大，一般都采用公网传输。为了防止传输期间被篡改，在央视 C2 规范的基础上扩展了 MD5 的字段。CDN 平台到牌照 FTP 服务器下载完 TS 文件后，如果 MD5 值校验错误，将把节目丢弃，并触发告警。

				议为 CP 平台方内容主键值(最长 32 位)
以下为 Property 所需字段				
4	FileURL	String	是	内容分发时拉流文件地址（分发前的地址，如需要分发，该地址必须填）
5	PlayURL	String	是	播放地址（分发后的地址）
6	Definition	String	是	清晰度（1:高清 HD、2:流畅 LD、3:标清 SD、4：XD，默认 SD）
7	CdnPlatform	String	是	媒体需分发（或已分发，无需内容注入平台分发的媒体）的平台号，多一个以英文逗号“,”隔开。注：该值请联系项目的对接人提供
9	BitRateId	String	否	比特率
10	Dispatch	String	是	是否需通过内容注入平台进行媒体分发;1-分发，0-不分发;不填则默认进行分发，到 IPTV 平台的注入不能填 0
11	Md5	String	否	需要分发的话，此值必填，媒体分发时的拉流源文件 MD5 值，格式为小写，供 cdn 平台校验使用，如无需通过内容注入平台进行分发，此项可不填
12	IsTranscode	String	否	媒体分发时是否需要进行转码处理：1-转码，0-不转码；不填则默认不转码

2.2 EPG 安全

平台 EPG 防篡改监测，实时禁止非授权用户修改 EPG 模板文件，实时禁止非 EPG 进程对 EPG 模板进行修改。防篡改监控流程如下图所示。



如果篡改发生，可以通过各级业务监测、比对，还可实现一键 EPG 调度、直播切换、单频道关停、点播下线、节目单下线等保障安全。

为了防止网页在网络传输期间被劫持、篡改，特意对 HTTP 页面做了 HTTPS 改造，通过数字证书、加密算法、非对称密钥等技术完成互联网数据传输加密，实现互联网传输安全保护。

2.3 一键 EPG 调度

EPG 管理系统中有用户组和 EPG 分组的对应关系，修改对应关系后，机顶盒重启后则会下发新模板。

2.3.1 一键直播流切换

如果直播流被篡改了，可以紧急切换到备流为用户提供服务。

2.3.2 一键频道关停

如果频道的主备信号都被篡改，可以通过一键关停频道来规避风险。

2.3.3 一键点播内容下线

如果点播内容被非法篡改，可以通过删除点播内容来规避风险。

2.3.4 一键节目单下线

如果频道的回看内容非法，可以通过删除节目单来规避风险。

2.3.5HTTPS 改造防路由器篡改

用户自行安装的路由器越来越智能，部分路由器会不定时给盒子推送小广告，导致盒子显示游戏、红包等弹窗。这不仅影响用户体验，而且存在重大的政治风险。

为了解决这个问题，特意对互联网电视业务中的 WEB 页面做了 HTTPS 改造。

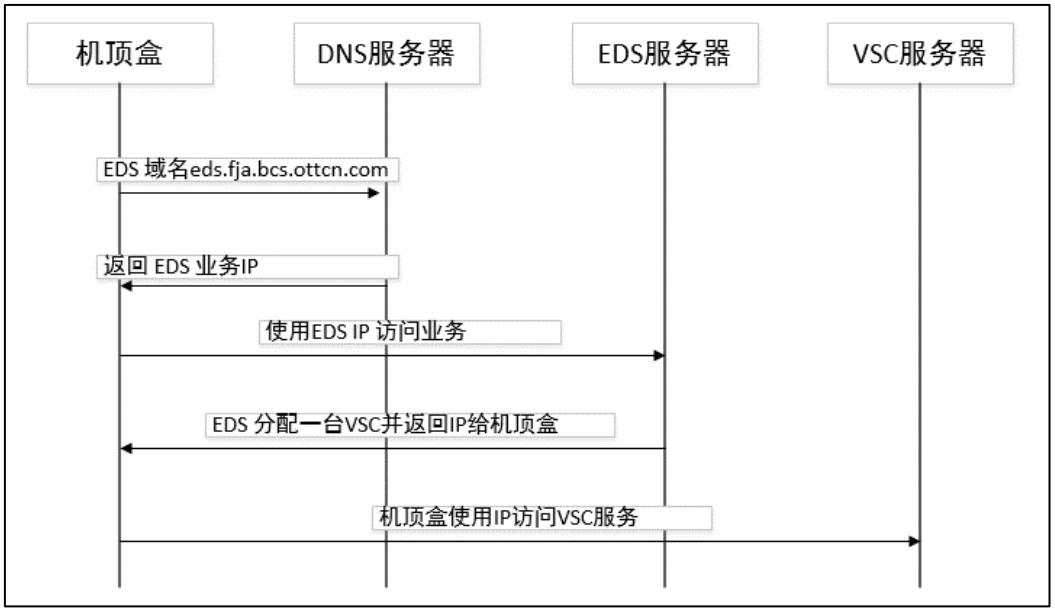
2.4 平台安全

互联网电视管理平台作为业务的核心，承载了

包括内容管理、终端认证、业务播放等重要能力。管理平台的安全是业务正常体验的基础，为保证平台安全，从业务接入、部件集群、部件容灾等方面保障安全能力。

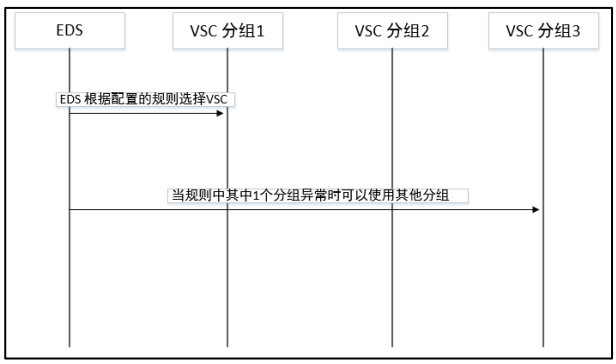
2.4.1 业务域名接入

互联网电视使用域名进行业务访问，当主平台异常时可以通过修改 DNS 解析切换到备平台，保证业务安全可靠。下面以 EDS 访问为例：

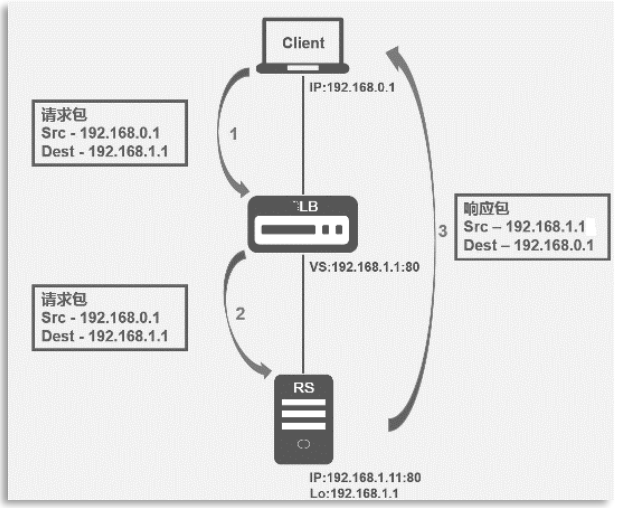


2.4.2 分组与集群

VSC 是平台的鉴权部件。平台建立了不同的 VSC 分组，不同分组对应不同的 redis 数据库。当配置规则中的 1 个分组异常时，可以选择其他分组的 VSC 服务器，从而保证鉴权认证业务的安全可靠。

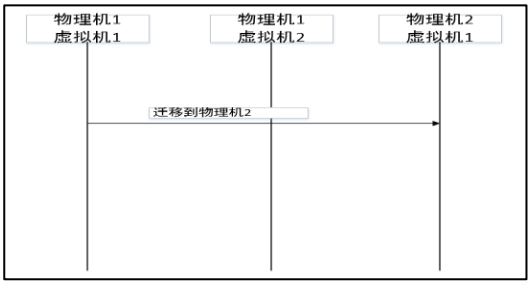


分组内使用弹性负载均衡的方式对集群里的设备进行访问。弹性负载均衡（Elastic Load Balancing）通过将访问流量自动分发到多台弹性云主机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能，保证部件的安全性。资源访问过程如下图所示：



2.4.3 虚拟化部署

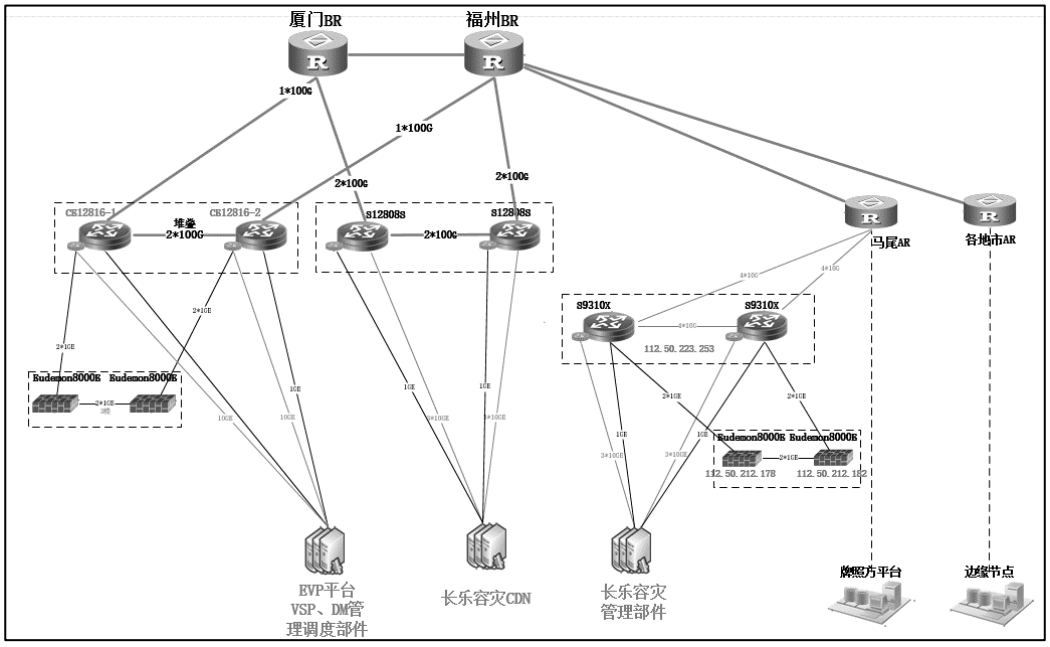
VSC、CMI、MM 等业务部件使用虚拟化部署。当物理宿主机出现故障时，虚拟机自动迁移到其他宿主机，保证了业务安全可靠性。如下图所示：



2.4.4 部件容灾

互联网电视平台针对重要部件实现了异地容灾，包括 MRF、EDS、VSC、LTC、RRS。当主平台的某个部件故障时，异地容灾部件将自动接管业务，保证业务可用性。

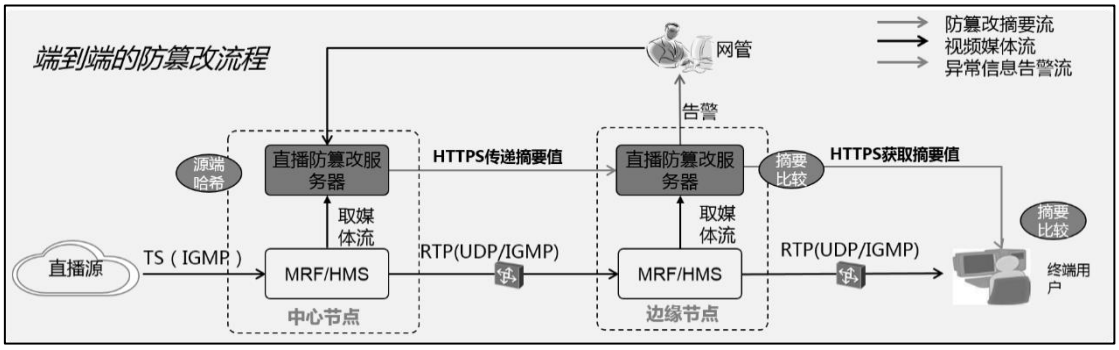
整体容灾架构如下图所示。



2.5CDN 安全

2.5.1 防篡改

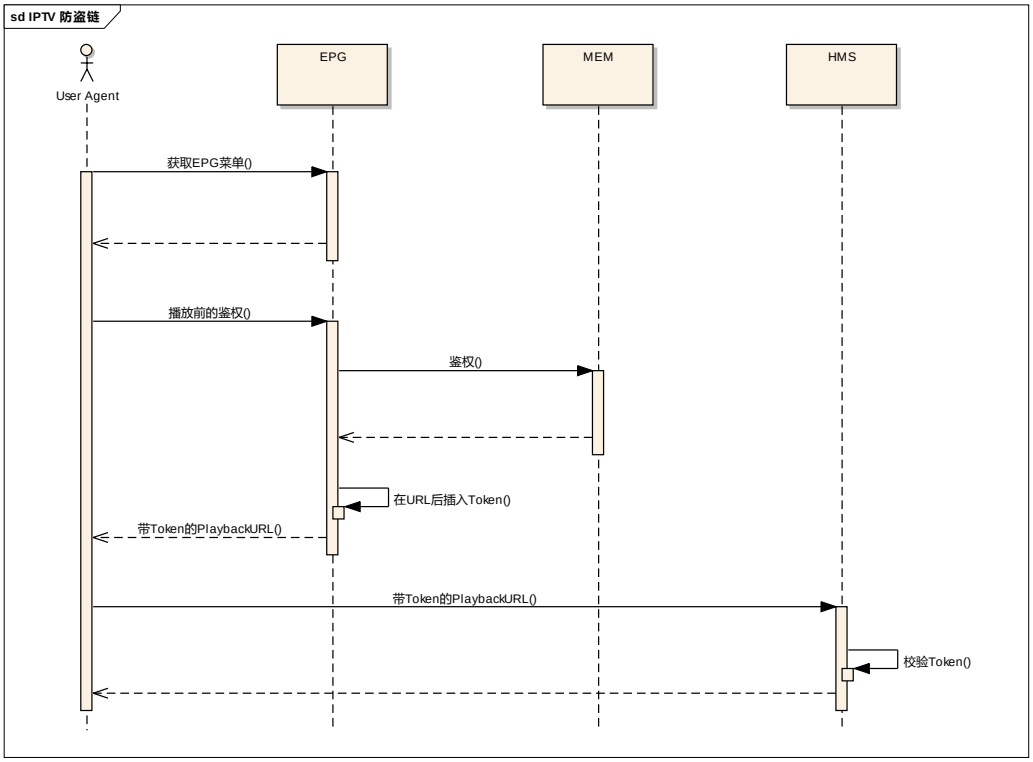
直播和点播信号从中心节点到边缘节点，途经大量网络设备。为了防止攻击者通过网络劫持对内容进行篡改，首先，对服务器业务相关路径进行特定用户绑定处理，仅白名单用户可对其中文件进行修改，实现 CDN 点播防篡改。另外，部署直播防篡改服务器，在源端服务器计算媒体流的哈希值，哈希摘要通过 HTTPS 传输至下端服务器和终端设备，下端服务器和终端设备通过相同的哈希算法计算摘要进行比较，一旦检测直播流被修改则停止该频道直播业务并触发告警，实现 CDN 直播防篡改。



2.5.2 防盗链

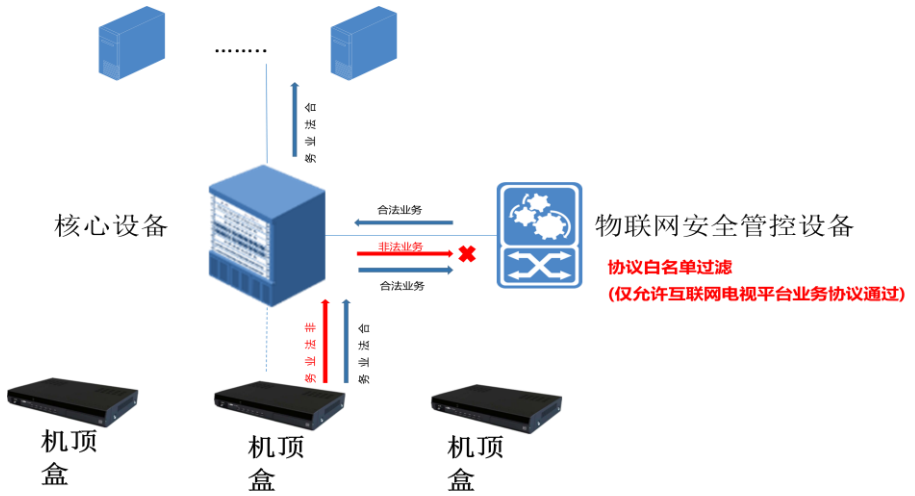
在源站和 CDN 侧分别预制共享密钥，源站和 CDN 分别采用相同的算法对防盗链信息进行加解密，加密的防盗链信息中含有时间戳等关键信息，

CDN 通过 AES 解密校验防盗链的 key 加密的有效　　性。



2.5.3 协议级安全防护

终端与平台和 CDN 之间路由可达，平台和 CDN 又与其它系统想通，非法攻击者就会利用这条通路，进行探测、渗透、并利用漏洞进行入侵。因此，在平台和 CDN 侧建设物联网安全管控设备，对出入的数据进行实时分析，实现了基于协议的安全防护。依托互联网电视业务特征相对固定的特点，适配业务协议、报文长度、报文结构、内容特征、关键字段等手段，建立业务白名单模型，实现 cdn 和平台侧的协议防护体系。



2.5.4 部署杀毒软件

在 CDN 服务器上部署杀毒软件，及时更新病毒库，定期进行病毒扫描，预防潜在安全风险。

2.6 网络安全

互联网电视业务穿透公共互联网，应用协议复杂，且无法“一刀切”进行简单粗暴的屏蔽、关闭。

针对这种情况，考虑对接省内态势感知平台，提升 IPS、WAF 传统安全防护设备的响应效率，并联动网络设备，实现网络端口一键关断。

2.6.1 网络基础安全

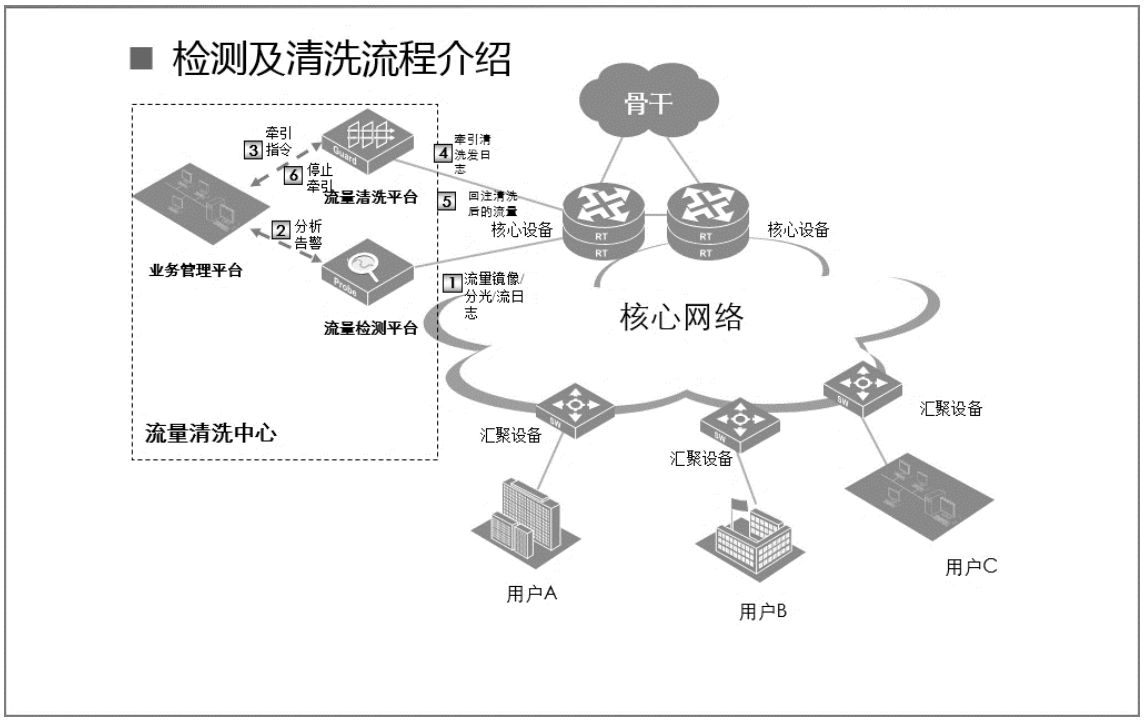
采用双节点、双路由器保障网络安全；

终端侧采用完全隔离的互联网，通过独立 VLAN 接入网络，并采用 IPOE 认证。

在网络边界部署抗 DDOS、IPS、WAF、防火墙等安全防护系统防止攻击，对接省内态势感知平台，提升 IDS、IPS、WAF 传统安全防护设备的响应效率。并联动网络设备，实现网络端口一键关断。

2.6.2 抗 DDOS 流量清洗系统

为保障网络安全，实现网间实时异常流量清洗，CMNET 省网部署了抗 DDOS 流量清洗系统。 流量清洗原理图：



省级抗 DDOS 系统总共分为检测、牵引、清洗、回注四个步骤，以下为这四个步骤详解：流量检测：通过检测策略判断流量是否为攻击流量，并将攻击事件上报给业务管理平台。

流量牵引：业务管理平台给防护设备下发防护策略，将需要保护的 VIP 用户流量牵引到防护设备上进行防护。

流量清洗：流量清洗设备收到牵引过来的流量后进行攻击识别，对识别出来的攻击报文进行清洗。

流量回注：防护设备将清洗后的用户合法流量回注到核心网，同时上报清洗日志到业务管理平台生成报表。

2.7 终端安全

针对现网终端型号多、厂家多、版本多的实际情况，且底层系统安全性不高，部署在用户侧存在高破解风险。通过建立智能机顶盒系统软件安全链，保证终端软件系统的安全性。

2.7.1 限制第三方应用

终端安全风险主要来自于非安全软件应用入侵终端系统。为此所有发布的安装包必须经过安全加固检测，限制第三方应用的安装，禁止用户安装非官方应用。

2.7.2 目录权限控制

互联网电视采用了系统目录权限控制，控制应用的目录访问权限，非授权不可访问，同时隔离各个应用的相互访问权限。系统管理打开权限控制，需要向厂家发送动态二维码，取得动态秘钥解锁。当设备重启后自动关闭系统控制权限，需重新获取权限，保证终端系统的安全管控。

2.7.3 部署软探针进行实时监测

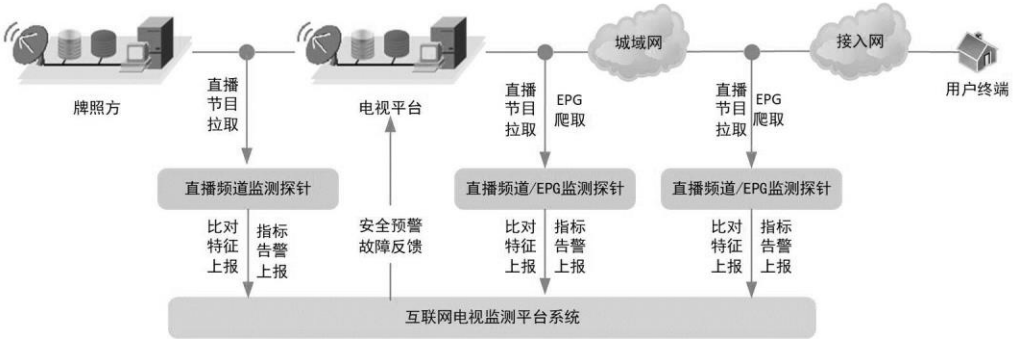
部署终端监测软探针，从开机自启实时监测终端应用、服务进程、资源及网络活动，将实时告警对接终端网管平台。监控设备应用安装行为，非官方应用阻止安装，并上报后台。监控进程活动，针对非白名单进程，强制退出，并生成告警上报后台。监控系统资源和网络活动，针对资源使用异常和网络使用异常，生成告警上报后台。

2.7.4 部署终端网管平台

终端网管平台可根据软探针监测到的告警信息，对单一异常终端进行一键清理异常进程，卸载异常应用，清理可疑文件等操作。

2.8 业务监测

通过在牌照方输入、电视平台输出、地市 CR、BRAS 之后部署监测节点，实现大范围的直播频道、EPG 内容的监测覆盖，从而实现互联网电视故障主动监测、实时报警、快速故障定位等功能，同时和电视平台充分联动起来，将报警详情、故障定位准确信息实时上报，协助平台在故障情况下及时的处置，保证提升用户收视感受的同时，最大程度的保证了服务内容的安全。



2.8.1 直播安全监测

（1）直播节目传输安全监测

在传输端(AR 侧、BRAS 侧）各监测点部署直播频道监测探针，对每个监测点的直播频道进行实时监测，采集关键数据并上报，实现对省中心总前端、地市节点的组播频道质量的监测。

（2）直播节目内容安全监测

在不同节点对 UDP、RTSP、HLS 等不同的流媒体直播节目的视音频指纹特征进行采集，经加密后回传到安全播出监控平台，再由平台将不同节点回传的特征进行一致性分析，进而判断各监测点的直播是否发生了被篡改等安全事件。

2.8.2EPG 内容安全监测

通过自动拨测和特征值采集，监测平台能及时发现 EPG 异常内容，实现 EPG 业务的安全传输。EPG 内容获取主要依赖爬虫技术，部署在云资源池上的 EPG 安全监测子系统通过合法的用户名及密码，在鉴权认证之后访问目标 EPG 服务器的各个模板、栏目及具体的页面，再对参考点和监测点两个资源的指纹进行比对，确定内容是否一致。

2.9 安全管理

2.9.1 制定管理制度

安全传输是互联网电视业务的生命线，为确保安全播出工作顺利开展，强化网络安全管理与防范措施，制定管理制度，明确职能管理部门，落实管理责任。按照“谁主管谁负责、谁接入谁负责、谁运营谁负责”的原则，确立各环节的安全责任部门和安全责任人，建立责任追究机制，执行重大信息上报制度。

制定日常运维管理机制，以每日播出日报、每周例会、季度巡检的形式形成量化监测检查报表，对网络的安全、事故、故障实行全面的监控管理。

2.9.2 建立资产安全管理平台

全部节点设备，均要纳入安全管控，通过安全验收。网元要接入 4A 系统进行集中维护，严禁未纳入 4A 管控的数据系统设备入网，严控绕行 4A 直接登录网元的行为，严控多人共用4A账号的行为。

严格落实“同步规划、同步建设、同步使用”三同步管理要求，包括安全规划、设备入网安全、风险评估、防护加固、审计检查等关键环节。数据系统负责人定期对系统设备进行核查盘点。

3 实践

3.1 日常安全扫描与加固

在日常定期进行漏洞扫描、高危端口扫描、弱口令扫描、合规扫描；网元在版本升级后再次进行安全扫描；对发现的问题及时进行安全加固，提升整个平台的健壮性。

3.2 重大保障

对重要节日、重大活动、重点时段，包括对金砖会议、70 周年国庆、春节、两会、疫情等进行安播保障。事前全面排查风险，制定应急预案，进行故障演练。活动期间，协同所有相关单位做好现场集中保障。

4 结束语

通过建立端到端的安全防护体系，福建移动互联网电视业务一直平稳运行，实现了“零重大网络故障、零重大安全事件、零重要客户投诉”的目标，为用户提供了优质的业务体验，促进了互联网电视业务的良性发展。

互联网医院网络安全风险闭环管理体系

林 锴　赵 贤

福建中信网安信息科技有限公司

摘　要：互联网+医院网络安全闭环管理是构建安全基因，并进行相对应安全防护，再对现有资源进行实时状态监控及时做好闭环运维，基于大数据和人工智能技术，从海量的运维数据中学习和总结规律进行智能分析和决策。主动监测，主动预警，能第一时间启动处理预案，及时有效处理，深度安全防护，保障医院业务系统的稳定运行。

关键字：智能运维管理、风险闭环管理、持续安全防护

随着国务院制定“互联网+”行动计划，推动移动互联网、云计算、大数据、物联网等与现代产业结合，移动互联网已在多个方面融入医院业务。互联网+医疗成为新的行业热点，各互联网巨头包括百度、阿里巴巴、腾讯均投入重金开发医疗领域市场。

互联网医院系统的建设，包括医院微信公众号、支付宝服务窗和手机 APP 等系统，功能覆盖了网上预约、网上复诊、报告查询、就诊管理、智能分诊、健康管理、在线支付等。病人可直接通过手机自助完成上述就诊流程，大大提升了病人的就诊体验，但是在方便了病人的同时，医院网络开放性也大大增加，新的安全风险被带入医院。

重点在于关键信息系统的稳定性和未知的新型网络攻击监测对互联网+医院正常业务开展的支撑程度越来越紧密，一旦关键信息系统运行出现故障，对医院业务正常经营造成重大影响。在互联网+医院业务系统上线后，网络设备、服务器、数据库、中间件等 IT 资源大量增加。现使用人工巡检已无法及时管控关键信息系统的异常和严重威胁信息，更难有效保障关键信息系统正常、稳定运行，因此需要基于各类网络安全智能运维管理平台对

医院关键信息系统全面监控并实现网络安全风险闭环管理。

一、互联网+医院面临的挑战：

互联网+医院系统等关键应用一旦投入运行，要求每天 24 小时不间断运行，其安全问题就成为系统能否持续正常运行的关键。一旦爆发系统瘫痪、信息泄露等安全事件，造成的后果和危害远超出医院信息系统本身的范畴。互联网+医院主要存在以下挑战：

1.医院新技术应用，使网络边界模糊，增加安全风险攻击面

1)互联网+医疗应用：微信挂号、移动 0A 等，缺乏有效边界隔离;

2)为优化医院工作流程，提升病人满意度，医院内外网无线 WIFE 逐步覆盖，网络边界被扩展;

3)业务升级，医院逐步向云迁移，虚拟化流量不可视、虚拟化安全不可控。

2.传统安全设备堆叠，难以应对新威胁，增加发现和防御的的难度

1)医院历经多次安全加固，FW、IPS、WAF 串接堆叠，防御割裂;

2)内网络端众多，HIS、LIS 等系统复杂，0Day 漏洞、社工、APT 等新型威胁易潜伏，静态的安全策略难适用。

3.安全可视能力不足，全网安全风险不可视

1)医院现有安全设备重防御，缺乏检测与可视能力，风险难看懂、难分析;

2)人员复杂，系统众多，看不清医院业务访问关系，看不清威胁，安全运维难管理。

4.信息化技术人员缺乏，缺乏全生命周期的安全运维，网络安全运维压力大

1)大多数医院的信息化部门编制仅 3 人左右，信息化人员匮乏，安全运维能力不足;

2)“报告式”安全服务，有安全问题但无解决办法，事件不能快速响应。无法体系化、持续性的对网络安全风险进行闭环管理。

二、互联网+医院安全闭环管理

（一）构建安全基因

网络安全域的划分决定了医院信息系统是否具有有效的安全防护基因。根据互联网医院需向互联网用户开放的业务需求出发，由内至外建立医院核心数据区、医院外部数据交换区（专网/互联网）、医院外部应用区（专网/互联网）的架构。

医院核心数据区、医院外部应用区、医院外部数据交换区的三层结构，各区域属性和数据流设计如下：

互联网应用区，部署互联网系统应用服务器（网站、掌上医院等，多数为 WEB 类应用），可被互联网直接访问；

内外网数据交换区，部署互联网系统的数据库服务器（如数据库可从内网业务系统中剥离）和前置机（如数据库系统因数据量等原因无法从内网业务系统中剥离），具有访问医院业务网区的权限和被互联网应用区访问的权限；

业务网区，医院内网，部署医院核心业务系统，可被内外网数据交换区访问，不可被互联网应用区访问；

（二）软件定义安全，建立纵深防御体系

基于 SDN 技术，为医院实现动态的安全边界及安全策略配置，及时防护和处置风险。

SDN 服务链技术可实现软件定义网络结构与流量，在旁路部署的物理防火墙基础上通过软件配置生成虚拟防火墙进行逻辑串联部署，实现各区域的边界防护。

管理员只需定义一个安全业务组合，形成一条服务链。然后定义用户组，将用户组访问某些资源的流量与服务链建立关联。服务链可以重复应用于多种用户组的访问路径上。 形成一条有状态防火墙，它与网络设备配置的安全策略、即无状态防火墙结合起来实现防护园区网络的各个方向的流量，并将这两种防护做到统一界面配置和呈现，简化用户配置。通过服务链方案可以将边界安全资源池化，并将资源池虚拟化，可以将服务资源按需引流，较多节省业务资源。当服务节点能力无法满足业务需求时，可以增加新的防火墙扩容边界安全资源池。并将新的资源引入服务链，即可实现业务的扩容，

做到服务节点的增删自如，不影响网络流量。

与传统的安全服务串接网络相比，一旦服务链的服务节点发生故障，可以将服务节点直接 Bypass 掉，可以做到不影响网络流量。

基于 SDN 技术和各类边界安全措施，形成下列数据流向控制与安全边界纵深防护能力。在数据中心区核心交换机旁挂安全设备形成安全资源池，结合 SDN 的服务链技术实现数据中心区核心服务器区、非核心服务器区、业务交互区等服务器区域间的安全隔离与防护。包括：

抗 DDoS 攻击：清洗互联网来源的 DDoS 攻击流量，避免互联网医院系统资源被非法流量耗尽；

WEB 应用安全防护：互联网医院系统等多为 Web Service 类应用，采用 WEB 应用安全网关提供针对 Web 类系统的抗攻击能力；

网页防篡改系统：恢复非法网络篡改，提供对互联网网站、APP 主页等的防篡改保护；

入侵防御系统：根据攻击代码特征，对网络入侵攻击进行检测，发现时及时阻断，过滤有害数据流；

流量控制系统：对各系统各类型流量进行管控，优先保障重点系统带宽，对网络行为进行审计记录；

安全隔离网闸：对接医院业务网区，网闸特有的区别于常规 TCP 连接的私有传输机制，通过数据同步功能将 HIS 数据库中必要的数据摆渡至内外网数据交换区，实现内外网的安全数据交换；

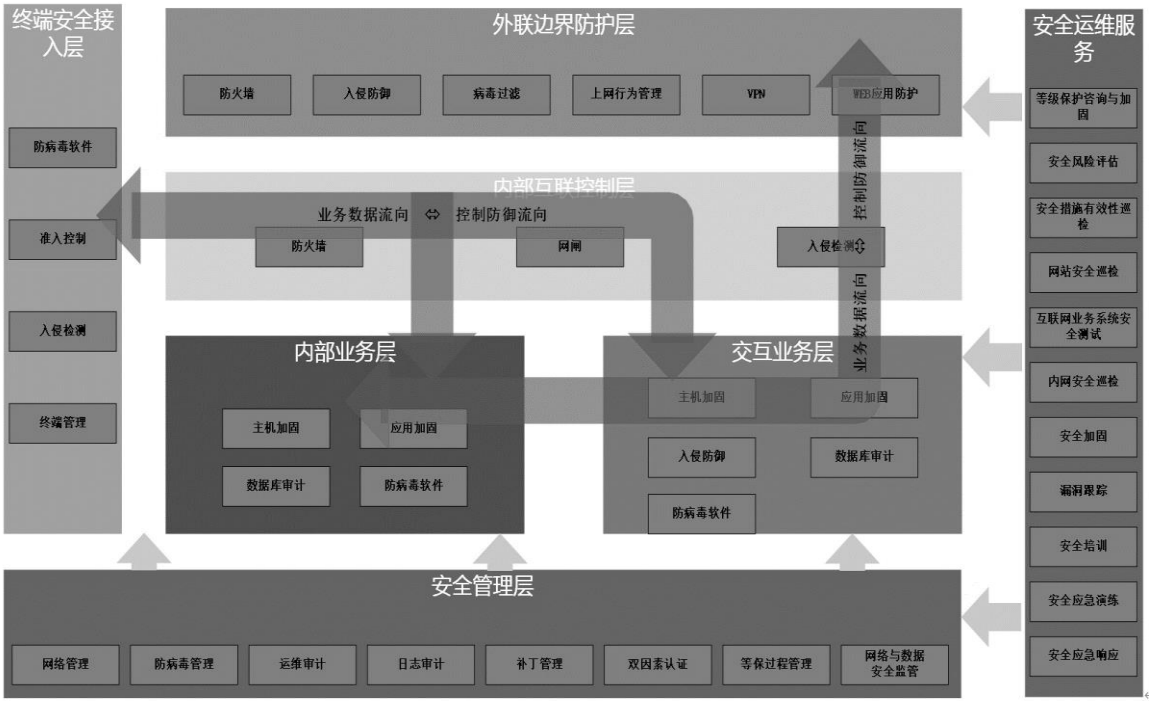


图 1　医院业务数据流向与控制防御流向示意

（三）构建云网联动的智能运维平台，实现安全风险闭环管理

构建基于本地及云端安全大数据+威胁情报的智能运维平台，实现统一运维服务平台，以安全事件为主线的风险闭环管理，对网络与数据安全态势进行实时监控，集成威胁检测探针支持大数据及沙盒技术集成，对勒索病毒和 APT 类似的未知新型网络攻击进行监测和分析，迅速定位恶意代码及勒索病毒源头，并自动生成风险处置与跟踪工作需求，联动安全设备及安全运维人员处置风险，形成安全运维的闭环。

安全运维管理服务是整体防护系统中极为重要的一环。基于安全运维服务建立起一线处置人员、二线分析人员、三线安全专家的风险管理团队，结合现场安全设备、安全管理中心、安全云平台提供的智能分析、威胁情报能力，形成针对安全风险的

多层逐级升级的安全风险发现、分析、处置、跟踪　　体系。

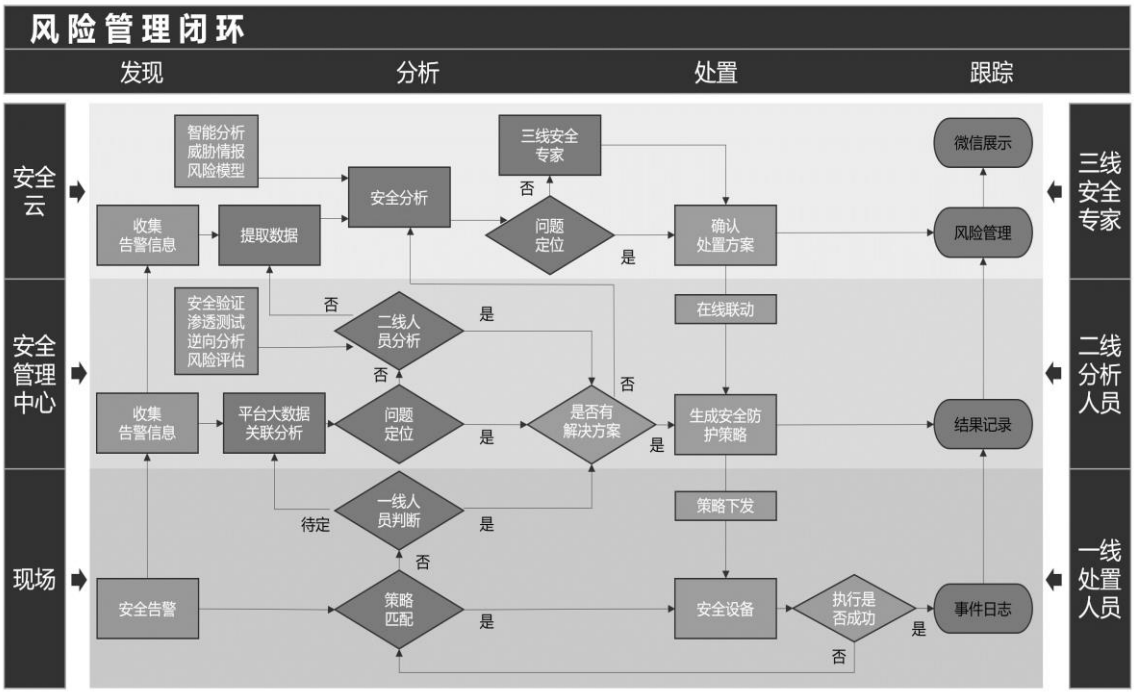


图 2　网络安全风险管理闭环示意

风险管理系统系统建立之后，不管是对安全检测系统发现的问题，还是用户发现的可疑文件，都能进行快速的分析和方案提供。针对问题出现—>产生需求—>问题分析—>提出解决方案—>风险处置—>风险跟踪—>在线展示，这样一套覆盖风险管理闭环的安全运维机制，既满足医院的整体安全服务要求，也是满足等保合规。

三、思考与总结

关于业务发展与安全保障的关系，习近平总书记说：“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业”。互联网+医疗模式下，医院业务形态发生巨大变化，信息安全是随之而来压在信息部门的一座大山。在便民、利民、惠民的基础上，如何保障网络安全，一直在我们思考问题。因此，我们应该深刻分析互联网应用系统所面临的安全风险，对医院互联网区进行完整安全规划，依据互联网医院业务属性进行网络架构设计，建立多层次的纵深安全防御体系，构建基于本地及云端安全大数据+威胁情报的智能运维平台，进行以安全事件为主线的风险闭环管理，最终实现主动防御。

基于智慧中台打造新入网用户一站式风险防控运营体系

崔文迪

中国移动通信集团福建有限公司厦门分公司

摘　要：为全面提升运营商对于诈骗违法犯罪行为的高压态势和防控成效，福建移动通过创新探索新型技术手段和管理模式，通过技术与管理双驱动的创新模式搭建“一个团队+一套流程+一套标准+一个平台”四位一体的新入网用户风险防控运营体系，并通过体系引领，依托企业级智能中台核心能力自主规划建设新入网风险防控平台，实现事前预判关停、事中全景跟踪、事后智能迭代的一站式智慧运营能力。

关键词：防范打击通信诈骗，智慧中台，新入网风险防控

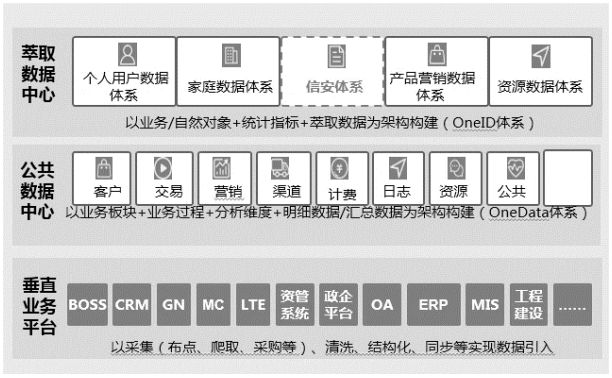
一、项目建设背景和意义

近年来，以电信网络诈骗为代表的新型犯罪持续高发，已成为上升最快、群众反映最强烈的犯罪。当前，电信网络诈骗犯罪发案总量不断上升；今年上半年，全国共破获电信网络诈骗案件 10.1 万起，抓获犯罪嫌疑人 9.2 万名，同比分别上升 73.7%、78.4%。福建公司防范打击通信诈骗治理工作相当严峻，黑灰产犯罪问题突出，整体面临诈骗团伙专业化、诈骗手段日趋隐蔽、人员防范意识薄弱、技术手段单一、反诈管理流程空缺等问题，现有传统救火式的单一防控模式已无法满足新形势下的反诈防控要求。当前中国移动启动智慧中台战略规划，福建公司作为首批试点省份也在积极思考与探索基于智慧中台技术革新和组织流程重构的信息安全一站式运营创新之路，以全面提升福建移动对于诈骗违法犯罪行为的高压态势和防控成效。2019 年下半年福建移动成立由集团级安全领域专家和架构规划领域专家为技术核心的课题项目组，通过创新探索运营商如何构建新入网用户的一站式风险防控运营体系以及运营商如何基于智慧中台的战略转型打造核心能力和优势。通过技术与管理双驱动的创新模式搭建“一个团队+一套流程+一套标准+一个平台”四位一体的新入网用户险防控运营体系，并通过体系引领，依托企业级智能中台核心能力自主规划建设新入网风险防控平台，实现事前预判关停、事中全景跟踪、事后智能迭代的一站式智慧运营能力。也是福建公司基于中国移动智慧中台战略转型阶段在信息安全领域的创新试点与探索。

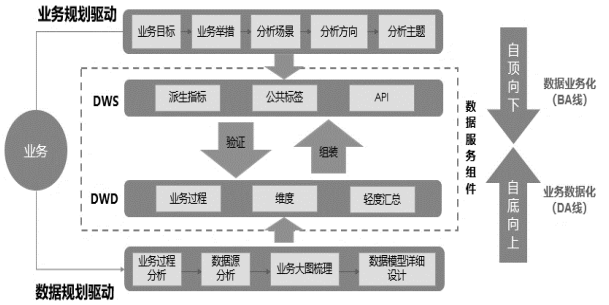
二、智慧中台介绍

福建公司作为中国移动智慧中台首批试点省份，在智慧中台建设过程中引入阿里成熟的数据中台 DATAPHIN 平台，集成 ONE DATA 数据服务设计的方法论及规则，实现大数据和 AI 的设计、开发、运营、运维全过程线上一体信息化，为运营 DT 能力提供平台条件。并根据“业务数据化，数据业务化”原则，自有人员负责全域统一的数据服务规划、服务组件设计；通过融智业务场景或应用驱动数据服务化开发，形成自主掌控的积木化、可复用、云化数据服务能力资产。

福建移动数据中台是“数据+技术+产品+组织”的组合体，是大数据平台的发展延伸，是新时期（移动互联网时代，以用户为中心，数据为王）从技术回归业务，企业开展新型运营的一个中枢系统。数



据中台着重打造标准数据服务、AI 服务，形成数据能力、数据产品，形成数据融通。实现数据与业务的无缝衔接，为业务运营提供多样化的能力输出，赋能 C、H、B、N 各领域，驱动业务运营和业务智能化。福建移动在数据中台建设过程中充分借鉴了阿里巴巴的 OneData 方法论体系，并与福建移动实际情况相结合，落地为本地化、可执行、可复制的方法论。该套方法论除了能够指导福建移动数据中台建设外，也可以复制和应用到集团、各省公司的数据中台建设中。



基于 OneData 方法论，以业务出发，分别从业务规划驱动和数据规划驱动双线建设数据中台的数据模型。

（1）回归业务：一切从业务出发，回归业务本身，与业务部门探讨并识别公司重点业务，建立业务的分层和分类体系。

（2）自底向上的数据规划驱动：基于维度建模思想，识别企业核心价值链，对核心业务的做业务过程分析，数据域分析，再做业务大图以收敛业务过程和维度，并最终设计和建设可供上层调用的数据模型组件（DWD 层）。

（3）自顶向下的业务规划驱动：从业务目标出发，识别业务举措、分析场景、分析方向和分析主题，把业务分析共性的业务要素识别出来，解耦并沉淀形成可复用的派生指标和公共标签（DWS 层），未雨绸缪，业务复用，实现从“表级复用”到“指标级复用”的跃变。

三、新入网用户风险防控运用体系

（一）运用体系

福建公司作为中国移动智慧中台首批试点省份率先在全网通过技术与管理双驱动的创新模式搭建 “一个团队+一套流程+一套标准+一个平台”四位一体的新入网用户风险防控运营体系。

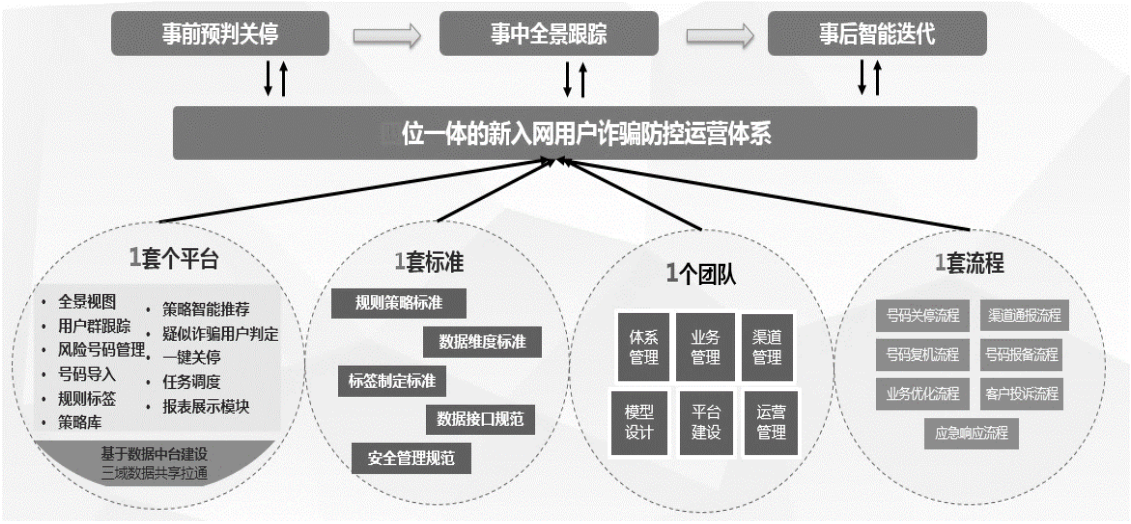
一是组建一支专业团队。网络安全领导小组和小组办公室明确了各协同部门在反诈防诈及新入网防诈骗风险防控体系搭建工作中的角色和职责，组建一支以模型设计人员、平台搭建人员、平台管理人员为开发模块主力，体系管理人员、业务管理人员、渠道管理人员为运营模块主力的双驱动专业队伍，同步强化跨部门联动和横向压力传递考核通报，增强团队合力和能力。

二是梳理一套完备流程。由专业团队负责梳理体系运营中涉及到的号码关停流程、号码复机流程、异常号码报备流程、渠道通报流程、客户投诉流程、业务优化流程、诈骗号码应急响应流程、黑名单管理流程等，并宣贯至各通路，确保平台体系搭建完成后，各项工作按时有序开展。

三是明确一组可行标准。明确规则策略标准、数据维度标准、标签策略标准、数据接口规范和安全管理规范，创新搭建多领域、多视角、可扩展的新入网用户属性标签、规则标签、策略库模型，为智能决策分析提供全面实时的基础能力。

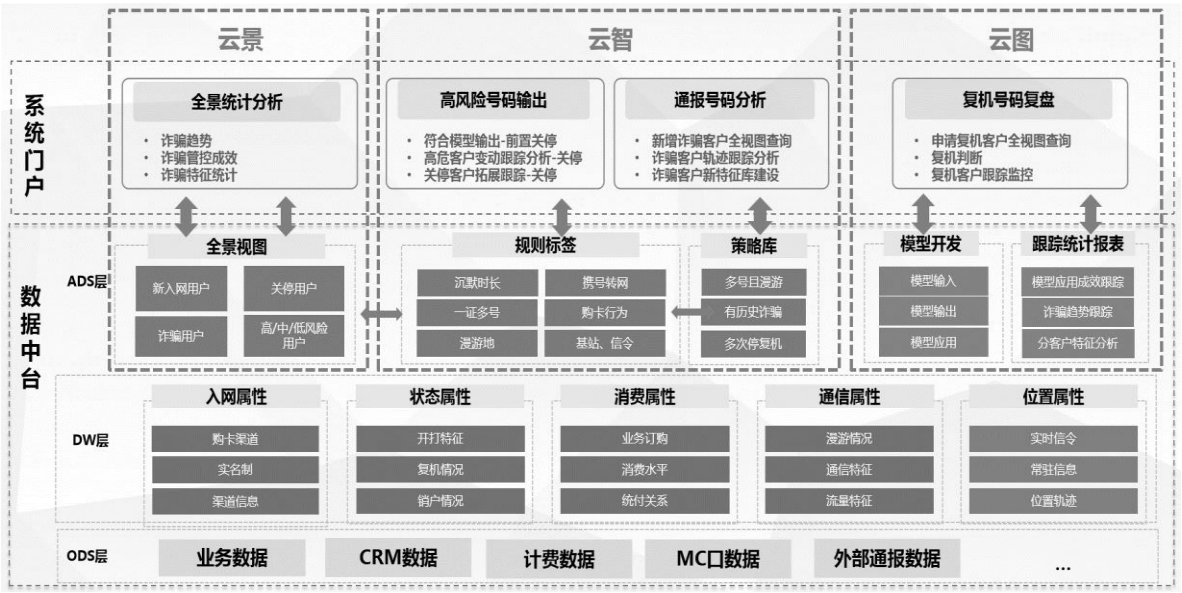
四是搭建一个智能平台。团队、流程、标准到位后，福建移动基于智慧中台沉淀的跨域多维度的数据资产及服务能力，打造大中台、小前台的运营模式和技术框架。重点实现用户全景视图展示、属性标签分类、数据模型智能分析、任务自动化调度、预警策略迭代等功能。通过针对新入网用户特征进行分析，通过策略库识别出诈骗风险用户进行关停，新入网用户行为进行跟踪，模型针对后续发生诈骗和关停复机用户进行自学习继续优化策略库，新入

网风险防控体系通过平台形成闭环。



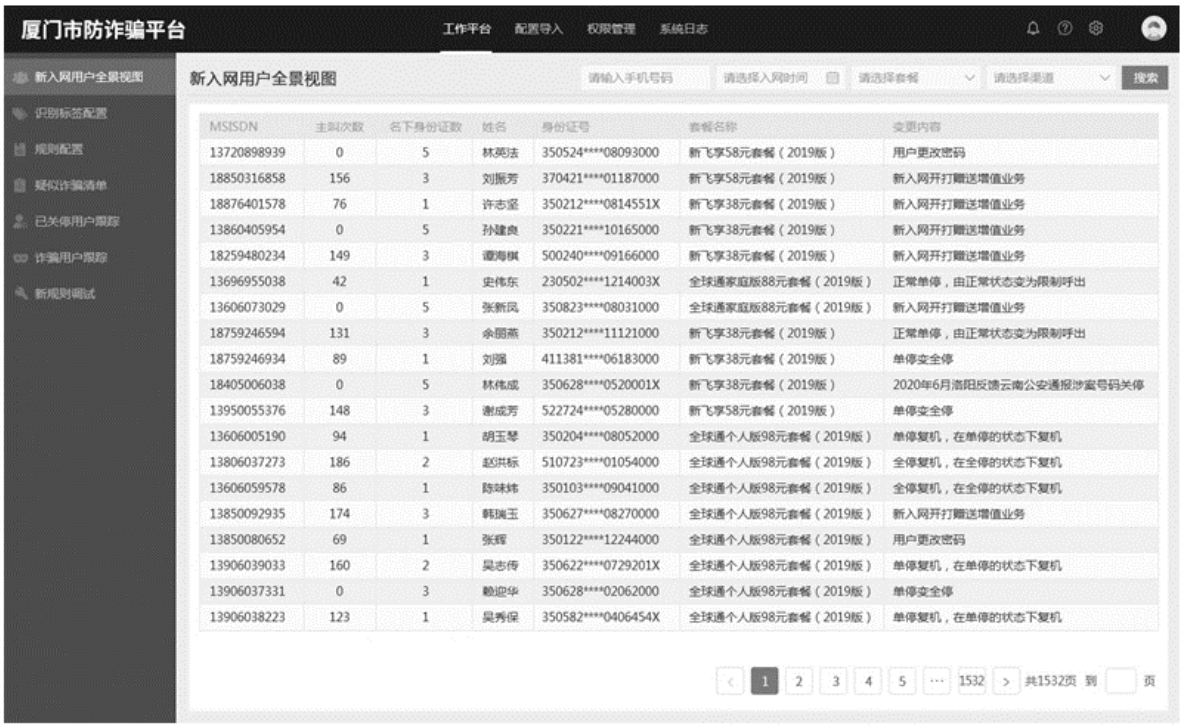
（二）系统构架

系统基于福建移动数据中台建设，采集 B 域和 O 域数据，系统分成云景（新入网用户全景视图）、云智（规则标签、自学习策略库）、云图（风险用户识别和风险用户群跟踪）。

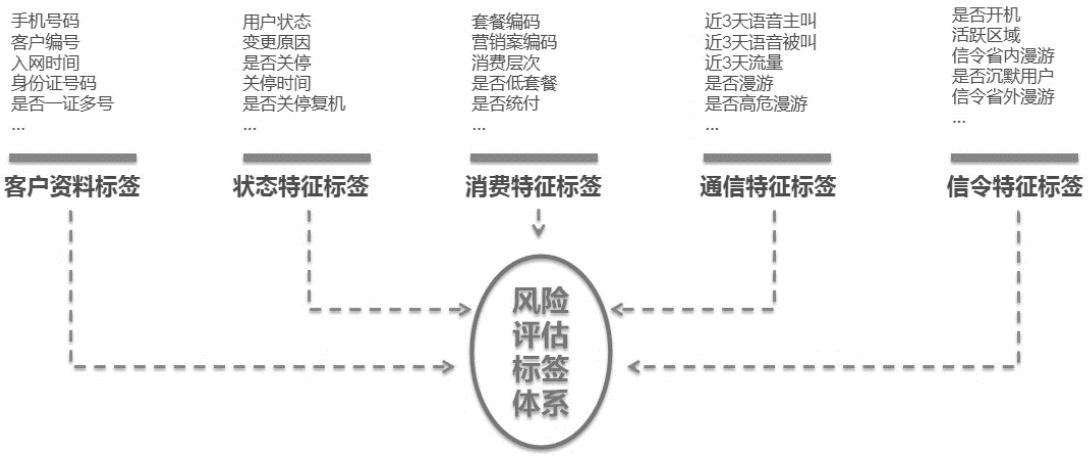


1. 云景：新入网用户全景视图与风险评估标签体系

新入网用户使用一个视图的方式展现新入网用户的入网签约属性、身份属性、业务属性、语音入网属性、高危诈骗渠道属性、位置行为属性等数据，通过全景可以快速查阅客户特征为关停或复机用户提供数据依据。



建设风险评估标签体系，对新入网用户群从客户资料标签、状态特征标签、消费特征标签、通信特征标签和信令特征标签等五个方面对新入网用户进行风险评估和等级划分。



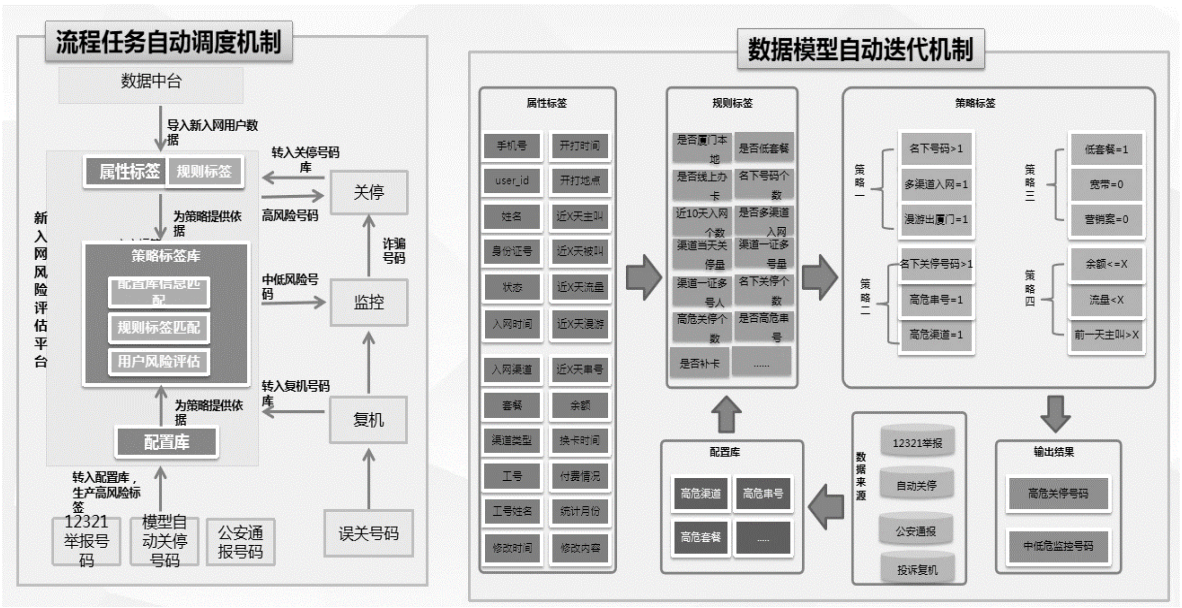
2 云智慧：风险评估策略库自学习

福建移动结合反诈部门和本公公司具有多年反诈工作专家，成立专家团队，采用专家评分法建立十数的专家经验建设新入网用户风险评估策略库，通过策略库识别风险用户，模型识别的查全率达到 73%，准确率达到 90%以上。专家风险评估策略库有效扼制了电信诈骗和骚扰等行为的发生，但是随着与犯罪分子犯罪手法的升级，与犯罪分子的斗争需要长期斗智斗勇。因此系统提供了风险评估策略库自学习功能，为专家和犯罪分子斗争提供有力工具。

依托数据中台科学算法平台，平台实现风险评估策略库自学习能力。针对未成功提前识别的风险客户群，平台需要自学习新的识别策略。在案发之后往平台导入风险用户群，平台自动随机抽取输入正负样本；通过关联风险评估标签体系，对标签进行归一化处理形成矩阵化；通过调用科学算法平台决策树算子算法，调整和输出新的可能适配的匹配

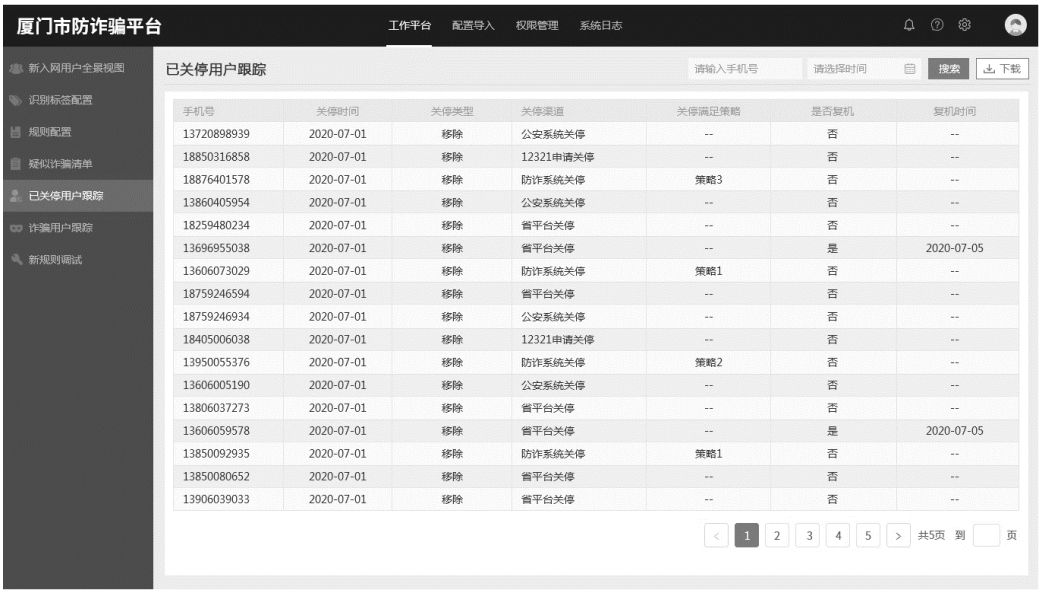
规则；使用历史标签验证新规则的查全率和准确率后，经由反诈专家确认后丰富优化风险识别策略库。

该平台创新实现流程任务的自动调度机制和数据模型的自动迭代机制，通过任务引擎，实现了原始数据采集、全景数据更新、策略规则匹配、目标清单输出、关停号码审核、涉案号码导入分析等核心主流程的自动化运营能力。提高新入网用户风险防控的及时性。该平台还实现了数据模型的自动迭代优化机制，通过建立新入网用户与规则标签相对应的参数矩阵，并引入人工智能和专家经验的规则策略运营和闭环评估机制，动态实现属性标签、规则标签和策略库的优化更新，动态调整各规则标签对应的影响参数，形成可自动迭代优化的数据模型。



3. 云图：风险用户群跟踪

平台还对已经关停用户和中低风险用户进行跟踪。跟踪关停用户是否复机，以及复机后的情况是否正常使用，针对复机后出现电信诈骗或骚扰的用户，追究申请复机人的违规申请行为；跟踪中低风险用户是否转为高危或者恢复成正常用户，针对中低风险用户发起二次认证审核；使新入网用户管控体系形成一个闭环。



四、项目创新点

（一）一套防范打击通信诈骗“智慧运营”顶层体系

基于“以人民为中心”的防范打击通信诈骗的政治任务，依托企业级智能中台作为能力基座，通过创新探索新型技术手段和管理模式，搭建 “一个团队+一套流程+一套标准+一个平台” 四位一体的新入网用户诈骗防控运营体系，通过体系引领，将信息安全防控体系融入业务生产运营流程中，依托数据中台，整体搭建新入网风险防控能力 。

（二）一个基于新入网用户为视觉的基于企业级中台模式的风险防控

全网首个以企业级智能中台设计模式，分层分域、自主规划支持多场景的新入网用户风险防控平台，融合传统 BSS 核心系统能力，形成可复用、可快速迭代的中台体系能力，探索构建全网领先的一站式新入网用户诈骗风险防控平台。

基于用户入网行为进行分析，通过用户属性和渠道属性全方位的监测新入网用户，从用户买卡到第一次拨打诈骗电话前的一系列行为进行跟踪，结合之前新入网风险客户的特征维度综合分析，识别出入网高风险客户，在号码卡寄送到作案地前及时关停，具有一定的前瞻性和预见性。

（三）通过机器学习方法闭环断完善标签和策略规则，提升识别精确度

基于科学算法平台：在用户风险评估完成后，通过机器学习方法，建设新入网用户规则标签以及对应的参数矩阵，动态调整各规则标签对应的影响参数，形成一个可自学习的风险评估模型，将模型结果输出到策略库。

形成诈骗号码闭环管理： 从对新入网号码事前监控，事中跟踪，事后复盘三方面出发，不断优化模型策略，对新增的涉案号码做到及时研判及时发现潜在风险号码，形成闭环管理。

五、项目成效

（一）运行情况

该项目在 2020 年初上线,在厦门公司试运行，通过半年的运行，厦门公司防范打击通信诈骗治理能力有明显的提升

1）厦门公司被公安部、工信部通报的号码由 2019 年月均 78 例，下降至 2020 年月均 21 例，有效打击了诈骗分子的诈骗行为。

2）项目上线后，每月关停疑似诈骗号码近 1000 个,投诉复机率不到 10%,模型准确度达到 90%;

3）通过涉案号码分析，自动优化策略 10 例，及时修补业务漏洞 5 个，模型准确度进一步提升

4）制定关停、复机、报备等反诈管理流程 8 个，一线人员及时报送异常入网号码 231 个，研判关停号码 122 个，限制异常复机号码 428 个，有效的阻止了诈骗号码的二次漫延。

（二）项目已产生的效益

1）项目上线后涉案通报号码较 2019 年明显下降，按照平均一个受害人被骗 10 万元计算，该项目每月为人民群众挽回近 500 万元的损失。

2）显著提升了疑似诈骗号码的识别效率，结合数据中台高效的数据运维能力和调度能力，疑似号码发现由原有的 4 个小时缩短至 30 分钟，减少 4 人/月的反诈运营人员投入。

3）通过梳理反诈工作的各类流程，实现体系高效运转，将原有疑似诈骗号码关停时限由 4 小时/天降低至 30 分钟每天，复机时限由 2-3 个工作日降低至 1 个工作日内，人员由原有 3 人/月下降至 1 人/月。

基于智能协同的主动防御体系模型研究与实践

赖建华　唐敏

福建省海峡信息技术有限公司

摘　要：为应对政企数字化转型以及大智物移云等新技术应用场景下传统安全防御体系面临的安全问题与挑战，本文提出基于智能协同的主动安全防御体系模型，从情报驱动、智能分析、软件定义、协同运营等四维度，建设主动安全防御体系。模型围绕威胁情报共享为核心，基于大数据和人工智能技术构建智慧大脑，通过安全编排自动化与响应进行秒级处置与响应，达到精准防护、主动防御的运营效果。同时，基于模型构建了主动防御体系的安全运营平台，并在实践中获得了预期效果。

关键词：主动防御；智能协同；威胁情报；安全运营

1 引言

自从疫情爆发以来，以在线办公、远程医疗、远程教育为代表的数字生活成为刚需，政府企事业单位加大力度实施数字化转型，国家部署新基建战略，网络安全的重要性越发显现。特别是，网络安全法施行以来，各级行业监管部门对于安全持续重视，政府企事业单位的关键业务系统必须按照网络安全等级保护制度的要求进行合规建设。同时，勒索、挖矿、蠕虫木马等自动化恶意代码攻击事件持续增加，严重影响着业务系统的安全。企事业单位安全管理者需要能够快速进行安全风险的监测和响应处置，开展协同联动与预警，全面遏制安全威胁的发生。

2 当前安全防御体系面临的问题

传统的安全防御体系受制于技术的发展，采用的是被动防御方式。随着大智物移云等新技术深化应用，企业在提升信息化建设水平的同时，也面临着不断增长的安全威胁，安全风险处置工作面临严峻的挑战。

首先，企事业单位部署的大部分安全产品是单点防御，缺乏联动机制，因而产品的安全效果完全局限于自身的能力。一旦单点产品的安全防御能力失效，就无法抵御攻击。特别是在高级威胁攻击场景下，只有各个安全组件联动一体，才能有效防范

攻击威胁。

其次，安全风险监控能力不足。企业自身的安全产品的能力不足以应对日益增强的攻击，也缺少统一的安全运营平台将单点安全产品能力整合成有机协同的整体；同时，由于网络安全形势瞬息万变，新型安全威胁从产生到大规模爆发的时间窗很短，企事业单位由于缺少安全情报而导致预警和安全处置的动作严重滞后。

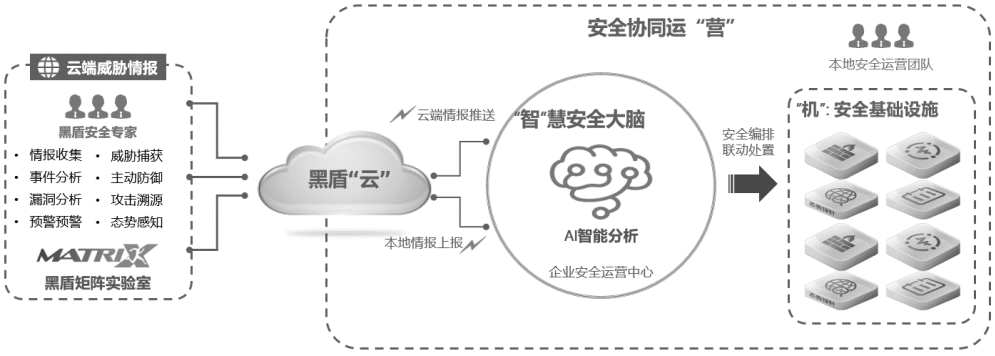
最后，安全专业人员短缺。企事业单位的安全专业人员配置少，对安全事件的分析和处置经验缺乏。在紧急安全事件发生时，往往不能快速排查、溯源定位以及紧急处置，以致安全事件悬而未决，应急处置机制如同虚设。

3 基于智能协同的主动防御体系模型

为了应对传统安全防御体系在单点防御、风险监控能力以及对专业人员的要求等方面的问题，提出了基于智能协同的主动安全防御体系模型，从情报驱动、智能分析、软件定义、协同运营等四个维度打造主动安全防御体系。

基于智能协同的主动安全防御体系的核心思想主要包括四个方面:(1)情报驱动。通过云端威胁情共享机制，将威胁情报应用到企业客户部署的各类安全产品组件中，增强单点产品的安全威胁发现速度和准确性。(2)智能分析。主动防御体系需要基于大数据安全分析引擎，对各安全产品产生的日志、告警、资产、脆弱性，进行多维度关联分析，包括用户行为分析、统计分析、异常流量分析，通过机器学习、深度学习技术提升安全风险发现的深度与广度，打造智能安全大脑，实现从被动防御到主动防御的转变;(3)软件定义。基于软件定义安全的理念，通过智能编排将不同的系统或者组件的安全能力通过可编程接口进行逻辑组合，完成特定安全操作，并支持用户自定义设备接口及联动响应操作。编排与联动响应基于工作流引擎的剧本编排、可视化剧本编辑器，并以可视化方式自定义剧本、应用和动作。在网络安全攻防对抗日益激烈的实战形势下，智能安全编排与响应可提升安全响应的速度和效率。(4)协同运营。通过安全运营平台构建安全运营闭环，能够根据网络环境，进行威胁感知、分析、预判，调用安全能力，主动进行威胁防御，协同运作，构建快速响应、高效处置的一体化运营体系。

基于上述核心理念，我们设计了基于智能协同的主动防御体系模型，模型由四大部分组成：“云”、“机”、“智”、“营”，如下图所示：



● “云”：指云端威胁情报共享。通过整合开源的恶意 IP 库、恶意域名库等安全威胁情报，以及各种安全资源能力，共享协同安全威胁情报，向“机”、“智”、“营”提供实时有效的安全情报、知识库以及安全能力服务。

● “机”：安全基础设施组件，部署在用户网络的各安全域，既可以是黑盾品牌产品，也可以是友商的安全组件产品；安全组件包括：主机安全防护组件、边界安全防护组件、安全审计组件、数据安全组件、应用安全组件等。安全基础设施组件产生的数据为企业安全运营提供支撑。

● “智”：指安全运营中心，作为主动防御体系模型的智慧大脑。通过安全运营中心的大数据采集、实时关联分析、用户行为分析、异常流量分析、

人工智能建模分析、多维态势安全视图、安全联动闭环，打通各环节的安全组件，协同内外部安全能力，将不同安全解决方案有机组合，实现各类安全风险的监控与处置。

●“营”：指安全协同运营。通过与企事业单位客户合作组建的安全运营团队黑盾矩阵实验室安全专家输出安全数据分析、事件溯源、情报分析等专业化服务，实现安全工具无法实现的安全需求，并通过驻场运营团队完成对云、机、智的协同补充。

4 关键技术研究

基于智能协同的主动防御体系模型围绕威胁情报共享为核心，基于大数据安全分析技术构建主动防御的智慧大脑，并通过安全编排自动化与响应，进行实时处置与响应，从而达到精准防护、主动防御的实际运营效果。

4.1 基于 AHP 分层分析法的共享威胁情报评价

主动防御体系的核心是高质量的威胁情报共享。从探针、开源情报、外部专项情报等数据源采集的威胁情报质量不一、分析价值各异、有效性不同，因而需要建立一套威胁情报评价体系，对威胁情报的质量进行评估分析。模型引入 AHP 层次分析方法,将威胁情报的评价分解为不同的组成因素，按照因素之间的相互影响，不同层次的聚集组合，形成一个多层次的分析结构模型，构建了威胁情报的定量评估分析方法,实现对威胁情报的质量评估。

基于 AHP 的威胁情报评价方法的预设特征包括：威胁情报的来源比例信息、命中比例信息、及时性信息、丰富性信息、差异性信息。其中：

●来源比例信息

该指标评估情报源推送威胁情报占全部威胁情报的比例，用于衡量情报源的情报交付数量和占比。统计方法是对一段时间内，各个威胁情报源的情报交付数累加并计算与情报总数的占比，占比越高情报质量越好。

●命中比例信息

该指标评估各情报源在情报查询中的命中比例，用于衡量情报源的命中质量。统计方法是对一段时间内，一条威胁情报被情报查询命中的次数在总的威胁情报查询次数的占比情况。情报的命中比例越高越好。

●及时性信息

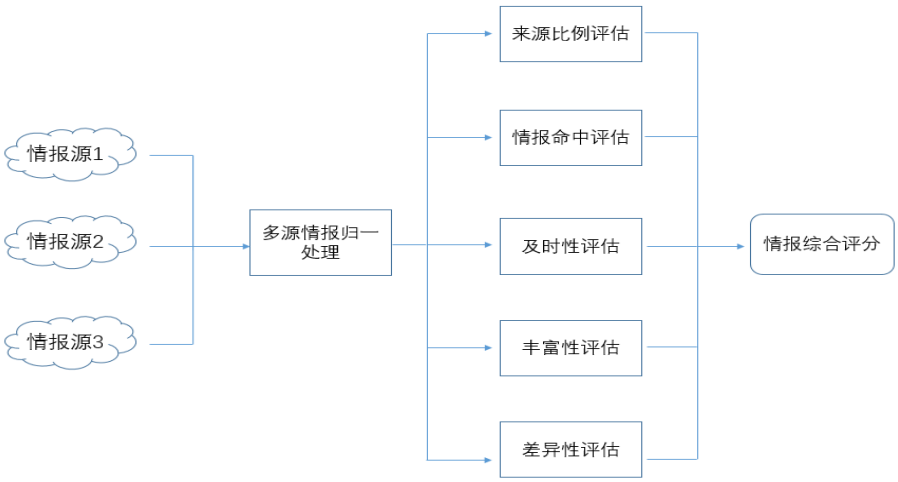
该指标评估情报源的情报活跃度，用于衡量情报源的交付情报及时性。统计方法是一段时间内，威胁情报首次收录的数量占该来源威胁情报总数的比例。如果同样的威胁情报由多个情报源上报，则以提交时间最早的情报源为准。

●丰富性信息

该指标评估情报源的内容质量，用于衡量威胁情报辅助信息的丰富度。具体辅助信息包括：域名 WHOIS 信息、恶意样本信息、RDNS、端口、服务、域名、应用组件版本、开发框架、数字证书、签名摘要等信息，作为后续溯源、复盘、研判跟踪的重要依据。如果一条威胁情报被 N 个源提交，则该情报源的丰富性指标加 N；如果同时有历史威胁信息，以及当前有效的威胁标签，则按照历史威胁信息和威胁标签的数量累加。统计方法是对一段时间内，情报源的每条情报的丰富度评估取值，加权平均后得出情报源的丰富度。

●差异性信息

该指标用于评估情报源的情报差异性，用于衡量情报源独立产出情报的能力。统计方法是对一段时间内，情报源的独家情报数量（单一情报源，未被多个情报源提交录入）占情报源提交情报总数的占比。差异性指标越高越好，有利于不同情报源信息的互补。



如图所示，系统对情报源推送的情报信息进行统一格式规范化，并按照上述的五个维度的评估指标进行模型计算，得出情报源的综合质量评估值。系统在提供情报共享的同时也提供情报源质量评分，供情报消费者选取合适的威胁情报，进行情报关联分析。

4.2 基于大数据安全分析的主动防御大脑

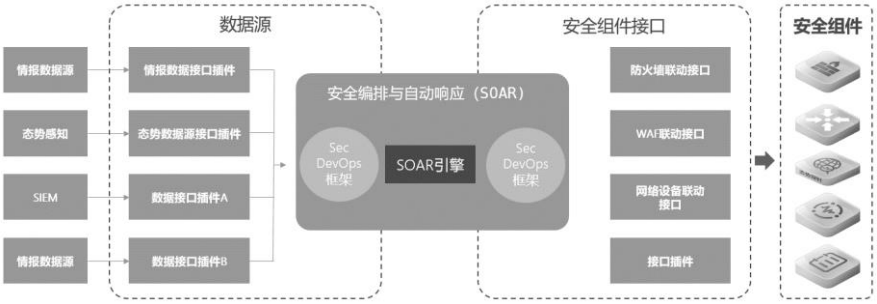
大数据安全分析是主动防御体系的智慧大脑，从告警日志、网络流量、配置信息、恶意样本等多维异构数据入手，采集企业网络关键节点的安全数据，基于大数据分析基础框架，结合安全场景，检测分析原始数据中潜藏的异常行为，进行异常流量分析、用户异常行为分析、安全风险分析、事件关联分析、聚类分析等多层次安全分析检测。

主动防御大脑的大数据采集支持全面的数据源，并将异构数据源产生的安全数据进行统一格式化处理，提炼出清晰有价值的字段信息，同时由于海量原始数据中存在着大量的不完整、不一致的异常数据，严重影响到后续大数据分析的效率和准确度，系统需要对数据进行清洗、集成、规约、转换等一系列操作，也就是数据预处理。通过数据预处理后输出的信息面向数据分析，同时按照不同的安全主题进行了归类，如日志库、流量库、漏洞库、资产指纹库等。

主动防御大脑的大数据安全分析以场景为导向，以大数据分析基础框架为支撑，将资产信息、威胁情报、攻击行为、异常流量以及脆弱性进行综合分析、汇总。大数据分析处理包含 CEP 复杂事件处理分析、图分析、大数据挖掘分析等大数据分析技术，对重点事件、异常流行为、嫌疑对象、跳板主机、攻击溯源等提供数据分析和挖掘处理。应用实时算法、离线算法、基于行为分析算法等，对数据和风险建立风险模型、威胁分析模型、行为轮廓模型等安全模型进行分析预测。通过综合关联分析预测事件发生的可能性，将大数据分析的结果进行告警输出。

主动防御大脑的目标是对企业网络的安全信息进行汇聚融合，形成安全事件的时间、地点、人物、关系的攻击链。从“时间” 的角度评估安全事件的时间跨度、历史发生情况等；从“地点” 的

角度评估安全事件的活动路径和轨迹；从“人物”的角度评估攻击者的身份、团伙关系以及动机意图等；从“关系” 的角度评估采用的工具手段、网络条件以及攻击对象等。



4.3 基于安全编排的自动联动响应

为了能够对网络中发生的安全事件进行快速、持续的响应，需要通过自动化方式执行安全处置任务。以勒索病毒为例，为了控制其在网络中横向渗透的威胁，系统需要在检测到威胁发生的同时阻断攻击的路径，防止纵向和横向的攻击蔓延。系统基于安全编排自动化技术实现对安全事件的编排策略和联动响应。

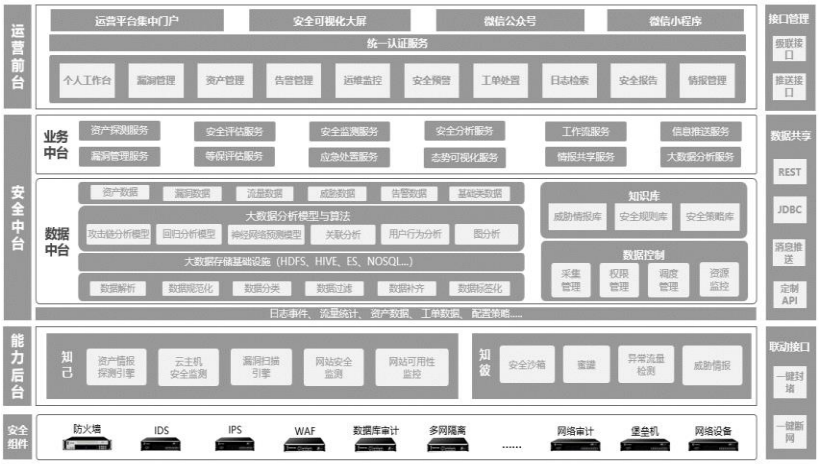
安全编排自动化与响应分为安全编排、自动化、以及响应这三环节。在安全编排环节，是指将网络中部署的安全产品组件的安全能力通过 API 接口进行封装，包括：下一代防火墙、Web 应用防火墙、路由交换设备等。将安全组件的访问控制能力按照场景化的逻辑关系组合，完成对攻击源、攻击目标的封堵、解封、断网、解除等安全操作过程。

自动化环节是指对编排过程的自动化处理。系统调用各产品组件的接口，通过脚本的方式自动化执行编排过程。自动化的过程基于安全组件的 API 接口 ，并采用了平台联动策略引擎，基于对安全事件的关联分析规则条件，触发相应的自动化接口，针对性的对攻击源、攻击目标进行处置，同时对联动策略模型快速验证测试，形成案例经验库。

响应环节是指对安全事件处置的全生命周期过程，包括：告警的生成、通知响应、工单流转、处置报告等。平台与工作流引擎对接，通过流程化处置告警与响应，实现安全事件处置过程的可记录、可度量、可追溯。同时，积累事件处置经验案例，持续化地对安全事件进行追踪。

5 基于主动防御体系的安全运营平台

基于主动防御体系模型思想，我们构建了安全运营平台。该平台集安全监测、采集、分析、预警、响应处置等功能于一身， 分为三层：能力后台、安全中台与运营前台。



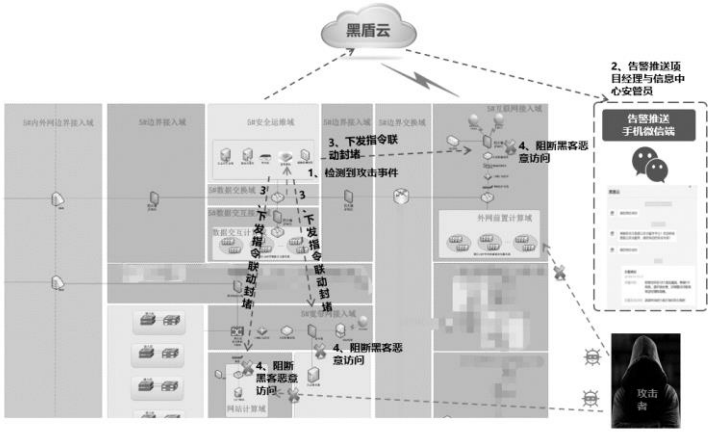
●运营前台。提供安全运营的门户，包括：用户门户、可视化大屏、以及微信公众号客户端等。同时运营平台中提供了安全运营的业务功能模块，包括：个人工作台、漏洞管理、资产管理、告警管理、运维监控、安全预警、工单处置、安全通报、情报管理等。

●安全中台。是安全运营平台的核心，细分为业务中台和数据中台两部分。业务中台对上提供业务服务封装；数据中台提供安全大数据分析能力，对上提供数据服务。同时包括了知识库以及数据控制。

●能力后台是安全运营平台的能力引擎，包括资产探测引擎、云主机安全监测、系统扫描引擎、网站安全监测、可用性监测等知己的能力；也包括：沙箱、蜜罐、异常流量监测分析、威胁情报等知彼的能力。

6 主动防御体系应用实践

以某三甲医院用户最常见的主机感染挖矿木马/勒索病毒的场景为例，当医院终端区一台电脑中了挖矿木马，不断发起访问矿池服务器。同时通过跳板攻击的手段，尝试向网站计算域的网站服务器发起攻击；部署在宽带网接入域的安全探针接收到矿池服务器域名访问行为；同时，对网站服务器的 Web 攻击也被探针监测到，告警日志发送到安全运营平台；安全运营平台接收到告警日志，结合情报云的恶意域名库，触发失陷主机告警事件。告警事件通过微信推送到安全管理员手机。同时，安全运营平台启动联动封堵策略，对互联网接入域的防火墙、宽带接入域防火墙、以及网站计算域的防火墙下发封堵指令，阻断失陷主机的互联网访问通道，以及对网站服务器的攻击通道。安全运营平台启动终端准入系统联动封堵策略，通过准入系统来隔离失陷主机，进行处置。封堵成功的消息通过微信推送给安全管理员。至此，失陷主机安全事件已经自动处置完毕。整个处置过程在秒级完成，极大提升了客户对安全事件处置效率，提升主动防护水平。



基于智能协同的主动防御体系依托情报云、医院安全运营平台及安全产品，获取安全态势信息，通过大数据安全分析、以及威胁情报，有效监控医院网络内外部安全威胁；基于智能协同的主动防御体系思路，与安全基础设施组件联动一体，自动化执行安全策略，从而实现动态、自适应、智能化的安全运营效果。

7 结束语

基于智能协同的主动防御体系模型以威胁情报为驱动，围绕安全运营平台维中心，对威胁、风险、行为和合规等态势进行多维感知，实现全网的安全风险态势感知、事件响应处置及协同联动，达到“情报驱动、智能分析、软件定义、协同运营”的主动安全防御能力。该体系模型已经应用在政府、医疗、教育等行业客户，并在安全攻防实战演习，以及常态化安全威胁发现与处置中发挥出很好的效果，提升了企事业单位的主动安全防御水平。未来，我们将从情报聚合、智能分析以及可视化编排等方向不断深化演进主动防御体系模型，服务于更多的政企行业客户。

使用深度学习对网络攻击行为识别的研究

郑 炎

中电福富信息科技有限公司

摘　要：本文给出了一种使用深度学习技术进行网络入侵攻击行为的识别方法。可以在不需要强依赖专家经验的情况下，通过模型的自我学习达到自动的特征提取以及结果预测。实验数据表明，该方法对于应用在实际的网络入侵攻击行为识别的生产环境下有很好的鲁棒性，对比起传统的规则匹配法和统计机器学习法准确性以及模型的泛化能力有很大的提升。

关键词：网络入侵、网络攻击、深度学习、卷积神经网络、机器学习

背景

随着互联网时代互联网用户的日益增长，如今全世界的网络信息安全面临前所未有的挑战。据不完全统计，2019 年一年中有 19.8%的用户计算机遭受了至少一次恶意软件 Web 攻击。全球共发现 975491360 次攻击，其中 Web 防病毒组件将 273782113 个唯一 URL 识别为恶意 URL，卡巴斯基检测到 24610126 个独立恶意对象，755485 名用户计算机受到加密攻击。2259038 用户计算机受到挖矿攻击。

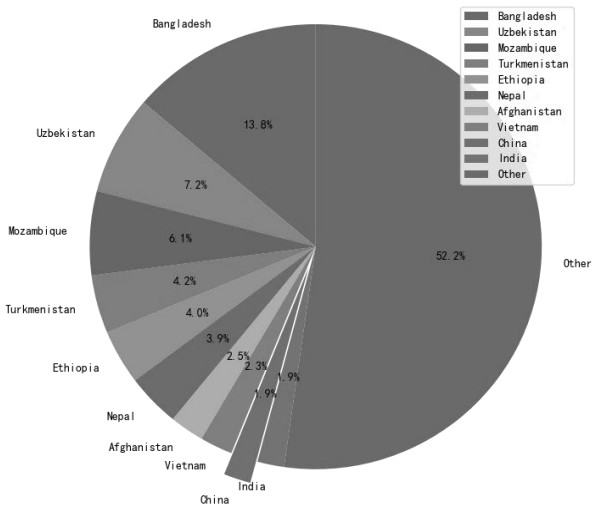


图 1 主要被攻击的国家和地区的占比

从图 1 可以看到我们中国也是受到攻击的次数非常高的国家，排在了第 9 位。然而这里面的还只是整个网络信息安全威胁的冰山一角。

从以往的历史上看，光是 2017 年上半年，勒索病毒 WannaCry 在全球范围内肆虐，通过网络造成一场严重的灾难，至少感染了 150 个国家的 30 万台电脑，波及了众多行业，包括金融、能源、医疗等，造成经济损失约达 80 亿美元，成为这几年以来影响力最大的病毒之一。

挑战

不断爆发的大规模网络攻击一方面证明了传统安全防护技术的缺陷和不足，另一方面则急迫需要新的网络安全技术的出现，来更加智能和高效的检测识别出网络入侵行为，网络异常流量检测和基于载荷的 Web 攻击。

最早在上个世纪 80 年代提出了入侵检测技术，之后网络安全领域也一直在这个方向进行着不懈努力的研究。传统入侵检测采用的方式是特征工程加规则匹配或者机器学习模型的方式进行分析。具体说来，特征工程就是指先从网络日志中过滤掉噪音信息，提取出具有分析价值的多维特征信息。然后交给规则匹配程序进行规则匹配，这部分也叫特征分析。而所谓的规则是指一些恶意的程序标识或一些恶意的行为描述，规则匹配就是对这些信息按照人工定义的方式，编写规则匹配的程序代码进行匹配分析。一般来说只要能够与规则相匹配到的程

序代码或者网络行为，就会被认定为是攻击行为。但是实际上，这种方式只能应对那些已知的攻击，对于那些新型未知的攻击只能束手无策。所以，对于后期的网络安全研究方向也开始慢慢转向机器学习的方式来进行分析。这种分析方式主要是通过收集正常的程序数据和网络行为数据，通过特征工程提取多维度的特征，在此基础上通过训练分类机器学习模型（通常有朴素贝叶斯，决策树，SVN 和随机森林等）。在检测阶段，与正常值在特征空间中的中心的欧氏距离超过了容限的程序代码或者网络行为会被认为是恶意代码或者网络攻击行为。与基于规则的方式相比，基于机器学习的方式在对那些新型的未知攻击进行检测的时候会有比较好的检测效果。实践表明机器学习模型极度依赖与特征工程，特征工程的优劣直接决定了机器学习模型的识别准确率。而作为特征提取工作的特征工程主要是由领域专家人工完成，使得该工作严重依赖于专家经验，所以人工成本以及行业门槛较高，而且无法自适应于不同的应用场景。

方案

随着 2012 年采用深度学习方式的 AlexNet 在 ImageNet 的图像分类比赛中碾压第二名的 SVM 的分类算法，深度学习开始在人工智能领域大放异彩。伴随着互联网的高速发展，全球的数据以每秒 PB 级的量级增长，从而为需要大量数据的深度学习提供了绝佳的环境。

深度学习的优势主要体现在以下 4 方面：

●能够通过海量数据自动学习特征提取能力。

●网络层数高，理论上可以拟合任意函数。

●比起传统的机器学习有更强大的泛化能力。

●数据量越大模型拟合效果越好，上限高。

而这些优点正是传统机器学习方式所需要解决的。也正是因为这样，我所在的团队正在尝试将深度学习技术应用在网络入侵行为检测的研究上。

与机器学习的方式类似，深度学习进行分析的过程也需要进行以下 6 个步骤：

1)获取并分析源数据

2)数据预处理

3)多维度特征提取

4)构建模型结构

5)将训练数据输入模型进行训练

6)将模型用于分类预测并输出结果

如下图 2 所示：

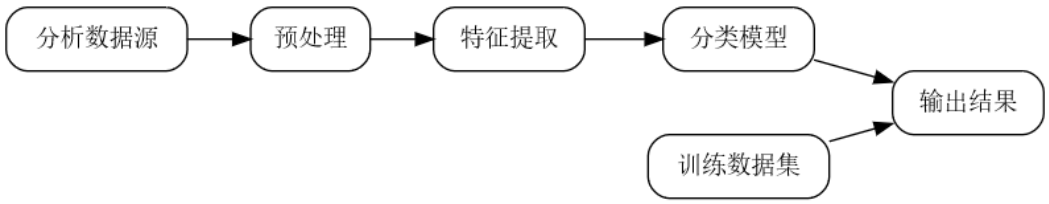


图 2 网络入侵攻击行为检测总体流程

但是比起机器学习来说除了样本数据的收集和标注外，深度神经网络可以自我学习并自动完成。接下来我简要介绍下研究工作及思路。

● 人工进行样本数据收集与标注

入侵行为分析一般由一些网关的网络采集日志或者 SOC 平台（网络安全管理平台）在网络中采集全网安全事件信息作为分析的数据源。如果有条件的团队可以通过获取过去历史发现的入侵行为的日志信息进行样本收集，一般的团队可以模拟各类入侵攻击方式进行样本采集。然后根据入侵行为对样本进行分类标注，作为训练使用的数据集。

● 多维度特征提取

这部分收集到的信息内容一般包括了像网络数据包这样的非结构化数据和像通过程序解析出的安全事件信息这样的结构化数据。传统的方式是通过编写规则模板和匹配代码，对这些内容进行规则匹配，得到特征信息。但是正如前面所说，这种方式人工成本太高，而且太过于依赖专家经验。但

是我们可以利用深度学习来进行特征提取能力的自我学习，这里我采用了三组卷积层来进行特征提取。利用卷积层的范围特征提取能力，再配合神经网络的反向传播来进行权值更新，从而使模型具备了自我学习的能力。整个模型的模型结构如下图 3 所示：

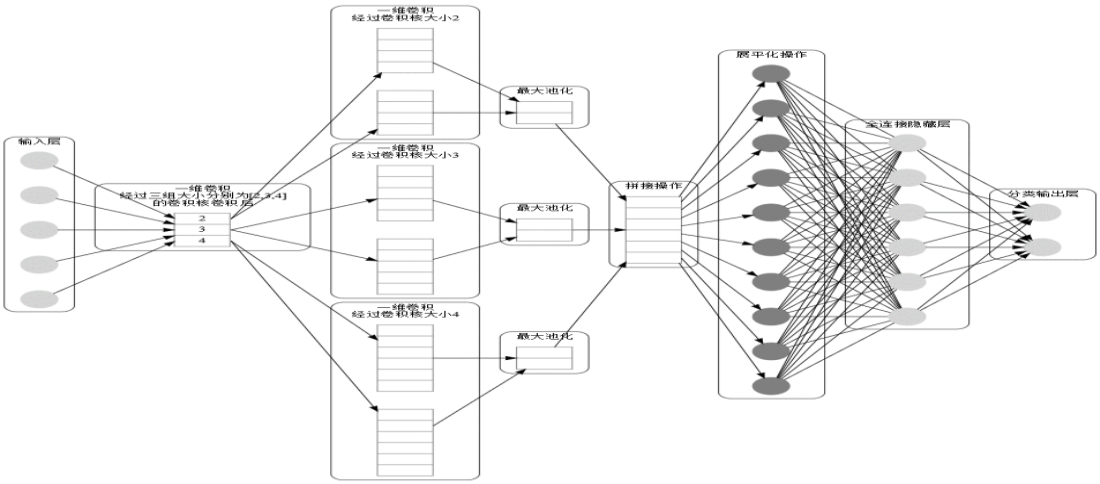


图 3 模型结构（该图只是用来理解模型的结构，不代表真实的维度信息，具体的维度信息需要根据业务场景进行设计）

特征提取层的原理是通过将预处理后的数据传入三组分别大小为（2，3，4）的一维卷积核，每个卷积核的通道数为 2。使用卷积操作的是因为卷积比起多层感知机来说可以使用更少的权重参数，同时又兼顾有很好的特征提取能力。采用 1 维卷积的原因是我们传入的数据不是 2 维的图像数据，而是 1 维的字符编码数据。这里使用三组不同大小的卷积核是参考了 TextCNN 模型的结构，利用三组卷积分别将注意力集中不同的感受野，能够更好地挖掘特征数据。三组卷积后的特征先分别经过 ReLU 激活函数后再进行最大池化操作，也就是进一步的强化特征，并降低维度。

这部分用数学公式表示：

$$\begin{aligned} for \quad & (i = 1\ to\ 3): \\ & Z^{[i]} = Conv_{1D}(X, W^{[i]}) \\ & A^{[i]} = ReLU(Z^{[i]}) \\ & P^{[i]} = MaxPool(Z^{[i]}) \end{aligned}$$

这里说明下 Relu 函数的定义：

$$ReLU(z) = max(0, z) = \begin{cases} z, if\ z \geq 0 \\ 0, if\ z < 0 \end{cases}$$

采用 Relu 函数作为激活函数的原因是考虑到 Relu 会降低梯度消失的可能性，如果实际情况还有梯度消失的问题的话，可以考虑改用 Leaky Relu：

$$LeakyRelu(z) = max(\lambda z, z) = \begin{cases} z, & if\ z \geq 0 \\ \lambda z, & if\ z < 0 \end{cases}$$

● 分类预测

接下去再将分别三条线路的输出结果在第一维度上进行拼接（这里的第一维度是指暂时不考虑数据批量化的维度）：

$$M = Concat(P^{[1]}, P^{[2]}, P^{3})$$

由于后面要进行全连接，所以要将拼接后的结果进行展平成向量：

$$F = Flatten(M)$$

展平后接下来就是常见的两层全连接层，第一层还是采用 Relu 激活函数，最后的输出层由于是分类问题，我们采用 Softmax 作为激活函数（为了可以扩展为多分类我们采用 Softmax 而不用二分类的 Sigmoid 函数）：

$$\begin{aligned} Z^{[4]} &= (W^{[4]})^T * F + b^{[4]} \\ A^{[4]} &= Relu(Z^{[4]}) \\ Z^{[5]} &= (W^{[5]})^T * A^{[4]} + b^{[5]} \\ \hat{Y} &= Softmax(Z^{[5]}) \end{aligned}$$

这里说明一下 Softmax 函数的定义，Softmax 函数是用来对传入的向量参数的每一维的值都分别

求做 e 的指数，然后再分别除以所有值 e 的指数的和：

$$Softmax(V) = \frac{e^{V_i}}{\sum_j e^{V_j}}$$

● 训练过程

前向传播后，通过反向传播然后用梯度下降法来训练模型的权重。首先我们可以拿预测值与真实值去做比较，采用交叉熵作为损失函数：

$$\xi(\hat{Y}, Y) = -\sum_{j=1}^{n} Y_j \, log\hat{Y}_j$$

n的值等于输出分类的个数，$\hat{Y}$是预测值Y是真实值。

如果是批量训练数据的话还需要对批量数据集计算平均损失函数，那么损失函数的表示形式就变成下面这样：

$$J(\hat{Y}, Y) = \frac{1}{m} * \sum_{i=1}^{m} \xi(\hat{y}^{(i)}, y^{(i)}) = \frac{1}{m} * \sum_{i=1}^{m} (-\sum_{j=1}^{n} y_j^{(i)} log\hat{y}_j^{(i)})$$

上面的Y代表这一批的真实值，$\hat{Y}$代表这一批的预测值，y和$\hat{y}$分别代表这一批里的单条数据。

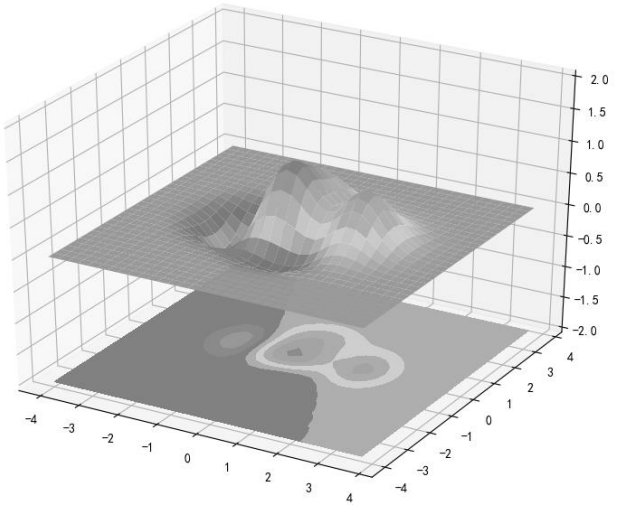


图 4 损失函数 3 维可视化示意图

再接下去我们可以采用梯度下降法来更新权重。如图 4 所示的损失函数的 3 维示意图，梯度下降法就是通过计算当前点在损失函数的梯度，然后将权值参数按照梯度方向的反方向进行更新，从而找到全局的最小值，也就是图上的深蓝色区域。梯度的计算方式可以按照分别求损失函数在各个权值参数方向上的的偏导数，然后分别更新权值参数的值。

权值偏导的计算方式：

$$J(\hat{Y}, Y) = J(A^{[l]}, Y) = \frac{1}{m} * \sum_{i=1}^{m} \xi(\hat{y}^{(i)}, y^{(i)})$$

$$dA^{[l]} = \frac{\partial J(A^{[l]}, Y)}{\partial A^{[l]}} = \frac{\partial J}{\partial A^{[l]}} = J'(A^{[l]}, Y)$$

$$dZ^{[l]} = \frac{\partial J}{\partial Z^{[l]}} = dA^{[l]} * g^{[l]\prime}(Z^{[l]}) = \frac{\partial J(A^{[l]}, Y)}{\partial A^{[l]}} * g^{[l]\prime}(Z^{[l]})$$

$$dW^{[l]} = \frac{\partial J}{\partial W^{[l]}} = dZ^{[l]} * A^{[l-1]}$$

$$db^{[l]} = \frac{\partial J}{\partial b^{[l]}} = dZ^{[l]}$$

$$dA^{[l-1]} = \frac{\partial J}{\partial A^{[l-1]}} = dW^{[l]} * dZ^{[l]}$$

$$dZ^{[l-1]} = \frac{\partial J}{\partial Z^{[l-1]}} = dA^{[l-1]} * g^{[l-1]\prime}(Z^{[l-1]})$$

$$dW^{[l-1]} = \frac{\partial J}{\partial W^{[l-1]}} = dZ^{[l-1]} * A^{[l-2]}$$

$$db^{[l-1]} = \frac{\partial J}{\partial b^{[l-1]}} = dZ^{[l-1]}$$

...

$$dA^{[1]} = \frac{\partial J}{\partial A^{[1]}} = dW^{[2]} * dZ^{[2]}$$

$$dZ^{[1]} = \frac{\partial J}{\partial Z^{[1]}} = dA^{[1]} * g^{[1]\prime}(Z^{[1]})$$

$$dW^{[1]} = \frac{\partial J}{\partial W^{[1]}} = dZ^{[1]} * X$$

$$db^{[1]} = \frac{\partial J}{\partial b^{[1]}} = dZ^{[1]}$$

其中J代表当前批次的平均损失，l代表神经网络的层数，m代表当前批次的样本数量，A代表前向传播各层经过激活函数后的输出值，g代表各层的激活函数，Z代表各层经过激活函数前的输出，W代表各层的权值，b代表各层的偏置值。

各层的权值更新,α代表学习率：

$$for \quad (i = l \; to \; 1):$$
$$W^{[i]} := W^{[i]} - \alpha * dW^{[i]}$$
$$b^{[i]} := b^{[i]} - \alpha * db^{[i]}$$

对于梯度下降的优化算法，我感觉使用 Adam 的效果会比较好。

通过不断迭代前面的过程就可以完成对模型的训练。

● **结果输出**

通过 Softmax 输出的结果为结果的概率分布，即如果定义的分类类型为 5 类，那么输出的结果就为一个 5 维的向量，向量的五个维度的值的和为 1。值最大的那个维度对应的分类就是模型预测出的分类结果。

总结

通过深度学习这种端到端的训练模式，模型可以自动学习到特征的提取能力，从而大大减少人工提取特征的工作量，减少耗费在特征工程上的时间。也由于深度学习可以通过增加隐藏层的数量来增加拟合能力，对于检测的错误率是可以逼近至贝叶斯最优错误率，也就是理论上的最好检测效果。而这个是规则匹配方式和传统机器学习所不能比拟的，这也是目前行业内的共识。为了验证行业内的这种观点，我做针对这三种方式用了 7 组不同数据量的训练样本进行验证，分别是 2000，5000，10000，15000，20000，35000 和 50000，机器学习采用的是规则特征提取加 SVM 支持向量机进行分类。由于规则的方式依赖于专家经验，为了避免由于人为的因素造成的偏差，这部分网络攻击行为的规则我和我从事网络安全方面的朋友做了大量的规则分析工作。

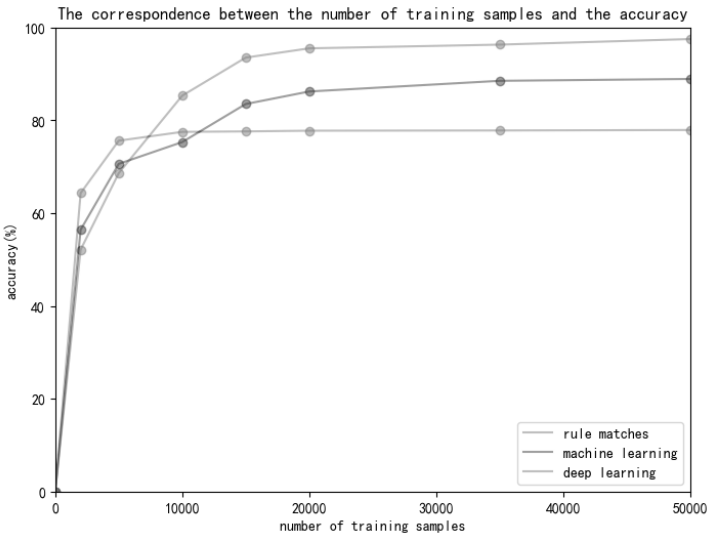


图 5　三种检测方式的样本数量与预测准确率的对应关系

经过 7 组不同样本数量采取深度学习方式与传统机器学习和规则匹配法进行对照实验，结果如图 5 所示。可以看到在样本数量只有 5000 以下的时候，规则匹配的效果应该是最好的，但是随着样本数量的增加，规则匹配由于受限于人工的领域知识范围，所以很难有更大的提升空间。而机器学习的方式虽然准确率的上限较规则匹配的方式来说有较大提升，但是缺点也很明显，同样依赖专家经验，而且由于机器学习本身的拟合能力有限，当样本的分布偏差较大的时候，传统的机器学习也很难在准确率上有较大的突破。深度学习模型由于权重参数较多，在样本较少的时候，卷积层由于没有足够多的样本来学习出好的特征提取的能力，所以在对于样本数量较少的时候优势并不明显，但是随着样本数量的增加，深度学习模型的准确率明显超过另外两种方式，而且由于省去了大量的规则分析，只需要进行样本标注分类，所以相较而言大大节省了人工成本。目前全世界互联网每秒产生的数据都在 PB 级以上，如此大的数据量为深度学习奠定了数据基础。加之纵观深度学习，不管在特征提取上的模型自我学习

还是在准确率的上限上，深度学习都必然是未来信息安全行业的趋势。

参考文献：

[1] Kim Y. Convolutional neural networks for sentence classification[J]. arXiv preprint arXiv:1408.5882, 2014.

[2] D. E. Rumelhart, G. E. Hinton, and R. J. Williams. Learning representations by back-propagating errors[J]. Nature, vol. 323, no. 6088, pp. 533－536, 1986.

[3] 周志华 机器学习[M] 清华大学出版社 2016

[4] 李航 统计学习方法[M] 清华大学出版社. 2012

未来网络安全流量分析解决方案

邹芳

中国移动通信集团福建有限公司

摘　要：关于未来网络安全分析体系建设，网络流量分析是网络安全领域重要的研究方向，利用多种引擎交叉检测、智能检测、情报关联、行为分析、隐蔽信道检测等关键技术对网络流量进行全面检测分析，及时发现隐蔽攻击、远程控制、高级威胁、暗网流量、失陷主机等各类网络攻击和安全风险，深入分析攻击者的攻击途径、关联关系等，为攻击溯源和处置等提供有效帮助，充分说明了网络流量分析技术在应对安全威胁方面的重要性。

关键词：元数据、关联分析、机器学习、0DAY

1 背景概述

随着互联网技术飞速发展，人工智能、云计算、大数据、物联网和 5G 等新技术的出现和应用，新技术带给人们更好的服务，同时也带来了很多新的安全挑战，网络空间对抗日趋激烈，目前网络攻击倾向于更复杂、更隐蔽和更高的危险性，比如“火焰”病毒、超级工厂病毒攻击和 Nitro 攻击等 APT 攻击活动，能够逃避检测，隐蔽窃取信息和情报收集，造成严重危害和影响。

传统功能的安全设备堆叠方式，是一种基于已知威胁的被动防护方式，不仅对环境空间、投资成本和运维管理都带来不便，而且传统检测方式无法发现 0day 和 APT 等未知高级威胁，脆弱的感知能力是网络安全监测的最大问题，同时，安全事件发生后，无法进行追溯取证，缺乏有效的复盘数据，无法定位问题所在，也就无法进行改进提升。

未来网络安全防护体系会更加侧重于网络攻击威胁的快速监测发现和应急处置能力，能够利用多引擎交叉检测、智能检测、情报关联、隐蔽信道检测等关键技术对网络流量进行全面检测分析，及时发现隐蔽攻击、远程控制、高级威胁、暗网流量、失陷主机等各类网络攻击风险，深入分析攻击者的

攻击途径、关联关系等，为攻击溯源和处置等提供有效帮助，大幅提升应对未知、隐蔽和新型的安全威胁能力。

2 需求分析

2.1 传统安全问题

1. 传统的安全设备基于特征匹配和黑名单的检测方法，是针对已知威胁，缺少对未知威胁的感知能力，基本无数据存储功能，只能产生安全告警和阻断，对于 0day 漏洞或者隐蔽性强的高级威胁，无法进行检测分析发现。

2. 传统的网络安全监测缺乏追踪取证能力，黑客攻击手段愈发的隐蔽狡猾，知道如何绕过大多数的安全监测工具，重点在于试图或者已经绕过安全系统造成严重危害前发现并处置；无法还原事件发生的经过，只有了解整个攻击过程，才能知道影响程度和范围，同时做出响应和防御措施。

3. 传统安全设备的堆叠和单一检测机制的问题，导致产生大量的无效安全告警，误报率高，需要关注的重要告警，有价值的告警被埋没，在日常安全监测防护工作中，缺乏告警分析研判的可执行性，容易遗漏重要网络安全事件告警产生严重后果。

4. 传统的安全产品缺乏全面的综合监测能力，主要是静态的被动防护，主动发现网络威胁的能力较差，缺乏威胁情报等关联分析，无法及时有效发现存在安全风险隐患的设备资产。

2.2 需求分析

1. 能够综合利用多种技术（网络异常检测、沙箱行为检测、多种引擎交叉检测、敏感信息和窃取行为检测、威胁情报检测、人工智能检测等）对各区域流量进行全面检测，检测网络全流量以及从流量中还原出的文件，准确发现高级威胁、暗网流量、隐蔽攻击，识别和定位被植入恶意威胁的失陷主机。

2.从网络流量中提取元数据，数据关联存储，基于时间线分析还原攻击过程，实现网络安全攻击的追溯、取证功能，具有各种安全场景的分析能力，不仅可以对安全事件进行追溯，还可以查询常见协议的会话过程，如 web 协议相关协议、文件相关协议和 mail 相关协议等，支持对 0dayNday 漏洞利用和恶意代码攻击行为检测。

3. 能够自动化、智能化和可视化帮助运维人员发现网络安全薄弱点和安全风险隐患，检查安全运维的有效性，快速发现非法外联等可疑线索，评估安全事件的影响范围和处置建议；当出现热点漏洞的时候，能够发现网络中的漏洞利用情况，在漏洞爆发前及时进行预警通知，对信息系统提供重要预防手段。

3 网络安全流量分析系统设计

3.1 整体架构

网络安全流量分析解决方案整体架构分为数据源、数据中心、数据分析和呈现。最底层的是各类需要分析的网络信息系统数据源，主要包括实时的网络流量数据、威胁情报中心提供的威胁情报数据和资产信息数据等；数据中心层主要作用是对采集的网络原始流量等数据源进行进行深度解析后，自定义策略进行筛选，再从流量中提取元数据和文件进行归一化处理并检测，同时分类存储原始流量和解析后的协议日志；数据分析层不仅包含了规则检测引擎、异常行为检测引擎、威胁情报监测引擎、文件检测引擎、Yara/SSL 检测引擎等专项检测引擎，还有关联引擎和机器学习引擎。通过这些引擎综合分析原始流量中的安全威胁，并利用关联引擎进行更深入的关联分析，实现对已知和未知威胁发现和全方位分析；最上层将分析后的各类威胁事件、失陷资产与风险情报信息进行可视化呈现，通过感知威胁态势，掌握全局安全风险，主要包括威胁监控、资产监控、场景监控、情报分析和溯源取证等功能。

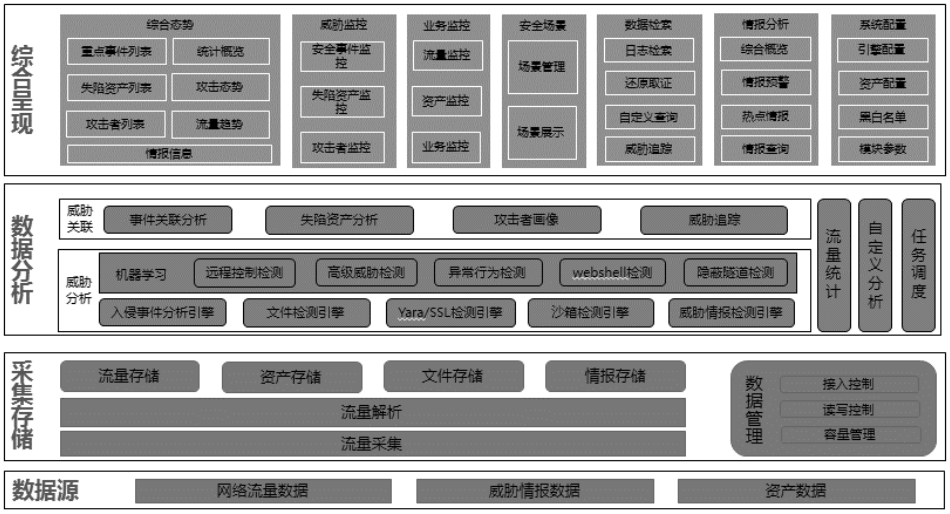


图 流量安全分析架构图

3.2 技术功能模块

网络安全流量分析解决方案主要分为三个部分，分别为流量采集提取模块、数据分析系统、和威胁情报中心，最后进行可视化综合呈现。

流量采集提取模块主要对全流量数据的采集、进行进行深度解析后，自定义策略进行筛选，再从全流量中提取元数据和文件数据，同时分类存储原始流量和解析后的协议日志，把解析后的元数据信息送至分析系统进行进一步检测和关联分析。

数据分析系统对采集的流量元数据深度解析，利用规则检测引擎、行为检测引擎和 Yara/SSL 检测引擎等专项检测引擎，还有基于机器学习和综合关联分析。实现对 Web 攻击、漏洞木马攻击、恶意代码攻击等网络攻击行为的检测、识别发现敏感信息泄露和窃取行为已经存在威胁的失陷主机，基于时间规则还原追溯整个攻击过程，实现快速监测和响应能力。

威胁情报中心分析存储 IP 情报、域名情报、URL 情报以及文件情报，支持从工信部网络安全威胁信息共享平台等公共漏洞发布平台获取情报，通过威胁情报，可及时获得全球网络安全热点信息和漏洞信息，及时进行自动化关联排查安全隐患。

综合呈现系统将分析结果进行可视化，为维护人员提供交互式可视化界面，包含综合态势、攻击态势、资产态势和流量态势等信息，安全场景定义呈现，提供各种条件的筛选，威胁情报的关联查询和预警通知，支持安全事件自定义条件搜索，支持源 IP、目的 IP、攻击类型、攻击时间等条件搜索和溯源取证查询。

3.1.1 流量采集提取

流量采集提取模块主要对全流量数据的采集、进行进行深度解析后，自定义策略进行筛选，再从流量中提取元数据和文件进行归一化处理并检测，同时分类存储原始流量和解析后的协议日志，把解析后的元数据信息送至分析系统进行进一步检测和关联分析。

流量元数据是后续多引擎检测和关联分析的主要来源数据，以 HTTP 访问为例，流量元数据主要记录会话中的时间戳、五元组、HTTP 头部等关键字段。

3.1.2 数据分析系统

数据分析系统对采集的流量元数据进行加工整理，包含了规则检测引擎、行为检测引擎、威胁情报监测引擎、文件检测引擎、Yara/SSL 检测引擎

等专项检测引擎，还有关联引擎和机器学习引擎等多种检测引擎。实现对 Web 攻击检测、漏洞扫描和利用检测、捆绑流行恶意代码的已知或未知文件检测、识别发现恶意威胁的失陷主机、隐蔽信道检测、敏感信息泄露和窃取行为检测等，并利用大数据关联引擎进行威胁情报交互查询、网络会话分析、网络协议分析、回溯分析和资产信息等关联分析，多维度多角度进行长时间跨度综合分析原始流量中的安全威胁，实现包括利用 0DAY 漏洞的 APT 网络安全攻击在内的快速监测和响应能力，提供对安全事件进行还原追溯取证，准确把握事件发生的过程及影响。具备特定安全场景分析能力，实现自定义安全场景并进行场景分析。

3.1.3 威胁情报中心

威胁情报中心建立威胁情报的全生命周期管理，为数据分析提供威胁情报信息支持，内容包含恶意 IP、恶意域名/URL、C&C 节点、僵尸网络、钓鱼网址、Tor 节点、DGA 域名、恶意文件、安全漏洞、IP 地理信息、安全事件（如 APT 攻击、数据泄露、病毒木马、Webshell）、安全资讯等，支持从公共漏洞发布平台（如工信部网络安全威胁信息共享平台等）获取漏洞信息，也支持自定义的情报信息的导入，支持威胁情报的归并整合等，以提高分析的准确性，支持情报共享（可选择）；支持自动/人工方式同步威胁源 IP、、恶意文件、漏洞等威胁信息，能够自动关联匹配威胁情报进行威胁检测。

4 方案创新能力

4.1 全面的威胁检测能力

该方案采用了多种检测引擎技术检测流量数据，更加综合全面的检测网络安全威胁，不仅可检测常见的安全威胁，也可以检测高级可持续性威胁（APT），内置的多种检测技术可进行交叉检测和交叉验证，提升检测的准确性。

除了具备常规的威胁检测功能外，它还能对从网络流量中还原出的文件（HTTP、SMTP、POP3、IMAP、FTP、SMB 等协议）进行病毒检测、基因检测与沙箱检测；通过提取的网络流量元数据，进行异常检测、木马病毒检测、隐蔽隧道检测、情报检测和行为检测等；然后将所有安全威胁进行关联分析，输出检测结果。

4.2 机器/深度学习能力

流量分析系统采用了机器学习/深度学习技术；通过大数据分析技术，对大量安全数据进行学习，使得系统具备检测未知威胁的能力，大大提升威胁分析工作效率。

（1）通过结合机器学习/深度学习、图像分析技术，将恶意代码映射为灰度图像，通过恶意代码家族灰度图像深度学习模型，建立检测模型，对恶意代码及其变种进行检测。可以有效的避免反逆向逻辑、反追踪和混淆代码，也能效地检测使用加壳的恶意代码。

（2）恶意代码（包含：Windows 环境、Linux 环境和 Mac 环境下的恶意文件）所产生的流量数据可以映射为流量基因图谱，因为同家族的变种恶意代码通信模式往往保持不变，流量基因图谱也具有相似性。可通过流量基因识别恶意代码，配合沙箱有效地检测出恶意代码。

（3）利用关联算法通过与加密会话关联的 DNS 协议、HTTPS 协议和 HTTP 协议，提取恶意加密流量与合法加密流量 HTTP 元数据等多种特征，构造恶意加密流量指纹，采用分类算法构建加密流量检测模型，检测恶意加密流量。

（4）对僵尸网络用于 C&C 通信的 DGA 域名进行编码，再利用不同的深度学习模型对 DGA 域名进行学习，交叉验证后进行分析判定。对于僵尸网络 C&C 通信的 DGA 域名具有优异的检测能力，系统资源消耗低、速度快、准确率高，同时也能够检测僵尸网络控制服务器和僵尸网络分类。

（5）由于不同应用程序功能、加密算法、通

信模式的不同，指定时间窗口内其数据包传输模式差异比较明显。利用这些差异进行特征提取，构造应用程序的步态指纹，再通过深度学习算法训练分类器区分威胁流量和合法流量，可实现暗网流量的检测。

4.3 高效的网络异常检测能力

该方案的威胁检测系统能够识别丰富的网络协议，通过对协议分析和网络异常行为模式匹配等检测技术能够快速鉴别出 C&C 通讯、SQL 注入、DGA 恶意域名、DNS/ARP 污染、DDoS 攻击、SSH/FTP 暴力破解、漏洞扫描和漏洞攻击等网络恶意行为，及时发现网络异常情况。

4.4 便捷的回溯取证能力

使用传统方案，在检测规则出来之前，很有可能出现攻击漏检的问题，或者攻击者切断样本通信，使得事件影响无法深入调查。

该方案基于全流量数据存储，可解析 HTTP、FTP、SMTP 等几十种协议，并对协议元数据进行存储，具有完整的追溯取证能力。通过可视化分析，能够快速定位攻击者，识别出攻击者的 IP、攻击方式、攻击协议和攻击目标等详细信息，可以很好的解决传统方案的局限性。

4.5 威胁情报关联分析能力

威胁情报中心的安全经验和情报数据汇总积累，及时提供包含恶意域名、安全漏洞和安全事件等威胁情报信息，流量数据结合威胁情报的关联分析，可有效帮助维护人员分析研判威胁风险，明确信息系统资产和安全状况，根据自身资产的重要程度和影响面，进行相关的漏洞修补和风险管理，可以了解最新的安全动态、威胁环境和攻击者使用的战术技术等，比如 APT、勒索病毒等，并及时采取威胁防御和处置措施，通过威胁情报的管理和关联，更加准确的进行威胁追踪和攻击溯源。

5 方案价值

未来网络安全流量分析解决方案通过实时采集网络原始流量，对网络流量信息进行存储、深度分析和关联，提取元数据和文件，建立多种网络安全威胁检测机制，大数据智慧安全分析，可视化呈现，在日常安全保障中，能够及时发现已知、未知、新型、高级和隐藏的网络安全威胁风险以及失陷主机情况，弥补传统方式的不足，确保信息系统的网络安全。

福建省 2020 年国家网络安全宣传周网络空间安全治理优秀论文及解决方案　鼓励奖名单

（排名不分先后）

类别	论文题目	公司	作者
论文	ARP 协议泛洪攻击及防范	福建三明机场有限公司	陈张鑫
论文	超融合技术在安全领域应用实践	福建信息职业技术学院	詹可强
论文	对运用大数据技术防范治理电信网络诈骗工作的探索	福建省通信管理局	崔艺竞
论文	关于美国 5G 策略的研究	福建省通信管理局	陈煜航
论文	关于省级工业互联网安全技术保障平台的应用探讨	福建省通信管理局	潘伟锦
论文	关于网络空间安全面临的威胁及保障	福建三明机场有限公司	潘江龙
论文	国产密码在医疗卫生领域的应用与实践	福建中信网安信息科技有限公司	王美桑
论文	UEBA 在网络空间安全威胁感知中的应用	北京福富软件技术股份有限公司	何秋芸
论文	基于福建省网络安全复杂新形势下监管工作开展的思考	福建省通信管理局	戴德春
论文	基于零信任的企业安全架构的探索	中电福富信息科技有限公司	舒玉凤
论文	基于内生式安全的智慧调度能力中心探索与实践	中电福富信息科技有限公司	杨　莉
论文	基于区块链的信息可信存储系统设计	中电福富信息科技有限公司	陈仙住
论文	政务数据安全风险的法律防范	福建省委党校	陈晓勤
论文	基于医疗保障应用框架的安全体系建设	福建省医疗保障基金中心	杨勇鹏、康建设、陈正勤
论文	建设良好生态网络 牢牢掌握舆论话语权	福建社会科学院华侨所	邓达宏
论文	论个人信息保护在网络安全防范中的重要性	福建省通信管理局	林俊杰
论文	敏感数据全生命周期安全防护方案探讨	中国移动通信集团福建有限公司	谢锋林
论文	浅谈水电厂电力监控系统网络安全防护	福建棉花滩水电开发有限公司	钟富明
论文	浅谈网络空间安全治理	福建三明机场有限公司	李　建
论文	浅谈委内瑞拉大面积停电事件的原因及启示	国网长乐区供电公司	石丹东
论文	全面分层化管理 提升网络治理成效	福建省通信管理局	谢茹绿
论文	人工智能在网络安全领域的应用	福建省通信管理局	邓杰藐
论文	网络安全与防范	福建三明机场有限公司	刘泽文
论文	网络空间中人脸识别技术的法律规制研究	福建农林大学 公共管理学院	余　磊
论文	危机情境下的网络谣言与公众信任的心理学解读	福州大学人文社会科学学院	白丽英、张艺瑶

类别	论文题目	公司	作者
论文	物联网时代下信息安全面临的挑战	中电福富信息科技有限公司	吴宝花
论文	探究移动 APP 的个人信息收集使用问题与对策	福建省通信管理局	黄晨晖
论文	疫情对金融网络安全的影响及思考——风险分析和应对措施	中国人民银行三明市中心支行、福州中心支行	郑力天、苏有宝、徐　挺
论文	因势而谋、应势而动、顺势而为，构建高校网络意识形态领域风险防范化解机制	闽南师范大学	朱艳丽
论文	中华优秀传统文化视域下习近平新时代网络安全思想的构建	福建社会科学院	郭　莉
解决方案	5G 边缘计算安全威胁分析与应对措施	中国移动通信集团福建有限公司	林　秀
解决方案	打造云清洗公共服务平台	中国移动通信集团福建有限公司	廖　伟 、谢锋林
解决方案	构建安全合规的数据库运维管控体系	福建中信网安信息科技有限公司	吴慧明
解决方案	基于 Fuzzing 技术的 Web 渗透和漏洞挖掘的研究与应用	中国移动通信集团福建有限公司三明分公司	廖尚斌
解决方案	基于大数据的安全威胁情报分析平台的研究与应用	中国移动通信集团福建有限公司三明分公司 、中国移动通信集团福建有限公司	廖尚斌、谢锋林、林慧博
解决方案	基于大数据的骚扰诈骗号码标记识别模型的研究与应用	中国移动通信集团福建有限公司三明分公司	廖尚斌
解决方案	基于等级保护综合管理系统支撑平台的等级保护建设解决方案	福建师范大学数学与信息学院	周赵斌
解决方案	基于多源数据及机器学习的威胁监测系统架构和功能设计	中电福富信息科技有限公司	任竹艳
解决方案	基于关联分析的自动封堵解决方案	中电福富信息科技有限公司	黄小峰
解决方案	基于机器学习的 SQL 注入和 XSS 攻击检测技术研究	福州大学数学与计算机科学学院	林荣胜
解决方案	基于诈骗多情景的风险预防解决方案	中国联合网络通信有限公司、亚信科技有限公司	范　京、周立萍 、郑　明、张　燕
解决方案	金融业安全研发服务平台	兴业数字金融服务股份有限公司	曹　杰、张金龙、向海钰
解决方案	威胁情报监测与处置	中国移动通信集团福建有限公司	邹　芳、邱琰琛
解决方案	政务数据汇聚共享数据监管解决方案	福建中信网安信息科技有限公司	陈梦辉
解决方案	基于透明加解密的敏感数据外发管控系统	福州市“智慧福州”管理服务中心	张　君
解决方案	广电媒体行业数据安全解决方案	莆田市广播电视中心	郭灶华
解决方案	基于自适应安全的电网行业安全建设实践	国网福建省电力有限公司	罗富财、纪　文、粟仁杰、张和琳、傅　杰
解决方案	基于安全编排自动化与响应在安全攻防实战演习中的研究与应用	福建省水利信息中心	赖桂春、许建航 、林中人

中信网安
ZHONG XIN NETWORK SECURITY

数据安全守护者
Data Security Guardian

关于我们 | ABOUT OUR COMPANY

福建中信网安信息科技有限公司（简称“中信网安”）致力于下一代互联网信息安全和业务核心数据资产安全领域，是一家集研发、生产、销售和服务于一体的高新技术软件企业。

中信网安云集了各行业资深安全专家，提出多维度涵盖“云、网、端、数”的动态安全监管技术体系，构建了“华安星”系列数据安全监管系统、等级保护综合管理系统、云安全风险管控平台、网络安全防护平台等全线安全产品和解决方案。

全面的数据安全产品研发及技术创新能力，荣获福建省级新型研发机构、福建省“专精特新”中小企业、福建省科技小巨人领军企业、福州市网络与信息安全行业技术创新中心、福州市企业技术中心等荣誉，并入选2020年度福建省数字经济领域瞪羚企业以及2020年度福建省重点上市后备企业名单。

我们产品 | OUR PRODUCTS

华安星数据安全监管系统 CSS-DAS	华安星等级保护综合管理系统 CSS-ISP	华安星安全一体化系统 CSS-SIS	华安星运维安全管理系统 CSS-OMA	华安星网络安全审计系统 CSS-NAC
华安星安全威胁检测与防御系统 CSS-TDP	华安星防火墙系统 CSS-FW	华安星安全隔离与信息交换系统 CSS-GAP	华安星WEB应用防护系统 CSS-WAF	华安星密钥管理系统 CSS-KMS

解决方案 | SOLUTION

中信网安智慧城市安全保障方案，以安全管理保障、安全技术保障、安全运营保障3维视角，整合基础安全防护措施、结合安全技术专家团队、利用安全大数据等技术提升智慧城市安全运营能力，提供覆盖政务云、数据、网络、终端的多维安全保障，为智慧城市保驾护航。

中信网安智慧医院安全解决方案，配合医院互联网+、区域医疗、智慧医疗的业务发展需求，结合等级保护2.0等网络安全标准。为医院梳理网络安全架构、构筑多重安全边界防护、设计医疗数据安全开放流转与开发应用机制、建立安全管理与运维保障中心，实现医院从被动防御到主动防御的转变。

通过各校端部署华安星网络安全审计系统，为学校提供完善的网络带宽管理、用户实名认证、网络行为审计与网络安全监测。并通过集中管控平台实现城域网安全数据的汇聚与分析，为教育局实现覆盖完整教育城域网的网络安全风险态势与网络行为监管，给教育城域网安全管控提供有力抓手。

福建中信网安信息科技有限公司
Fujian Ctrust Information Security Technology Co.Ltd
Add：福建省福州市晋安区横屿路东二环泰禾城市广场5号楼903
Net：http://www.cicisp.com
Tel：0591-87895020 0591-87301318

扫一扫关注

网络安全为人民
网络安全靠人民