计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(7):102−109 [doi: 10.15888/j.cnki.csa.007983]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

智能防御的私有云打印系统①

林　潇, 吴　怡

(福建师范大学 光电与信息工程学院, 福州 350007)
通讯作者: 吴　怡, E-mail: wuyi@fjnu.edu.cn

摘　要: 针对打印服务中普遍存在的易受攻击、数据泄密等安全风险以及它的安全等级完全依赖外部环境的信息安全建设的特点, 提出一种基于智能防御的私有云的安全打印架构. 该架构以私有云技术为基础采用虚拟打印技术为打印服务提供统一的透明的访问接口, 并结合身份验证和打印安全策略对打印业务流进行监控管理, 同时应用一种端末的网络访问控制策略实现打印输出端在网内的安全隔离, 以达到按需访问和智能防御的目的. Jmeter 进行系统压测和 hping3 进行安全性测试的结果表明, 在没有遭受攻击时, 提交作业和作业输出这 2 个业务流分别在 400 并发用户连续发起 100 次的请求下, 系统执行无误的响应时间仍在 2 s 以内; 在遭受 5000 SYN 包/s 攻击时, 系统在上述请求下执行作业输出的异常率也只有 3.62%. 在防范打印风险的同时, 仍具有良好的用户体验和健壮性.

关键词: 私有云; 虚拟打印; 打印安全管理; 智能防御

引用格式: 林潇,吴怡.智能防御的私有云打印系统.计算机系统应用,2021,30(7):102–109. http://www.c-s-a.org.cn/1003-3254/7983.html

Private Cloud Printing System Based on Intelligent Defense Mechanism

LIN Xiao, WU Yi

(College of Photonic and Electronic Engineering, Fujian Normal University, Fuzhou 350007, China)

Abstract: The current print service is faced with many security challenges, such as network attack and data leakage, and its security level completely depends on the information security of the external environment. As such, a secure printing architecture based on private cloud and intelligent defense is introduced in this paper. The architecture with private cloud as the core provides a unified and transparent access interface for print service by virtual printing. It monitors and manages the printing business flow on the basis of authentication and printing security policies. Meanwhile, it securely isolates the printing output device from the client network and the data center network with an access control mechanism for the end point, realizing the on-demand access to print service and intelligent defense against network exceptions. The Jmeter-based stress testing and the hping3-based security testing demonstrate that the system with this architecture has good user experience and strong robustness. To be specific, it spends less than 2 s successfully handling 100 consecutive requests from 400 concurrent clients respectively for submitting and outputting print jobs when it is not attacked, and the exception rate of outputting print jobs for the same requests is only 3.62% when the system is attacked by 5000 SYN packets/s.

Key words: private cloud; virtual printing; management of printing security; intelligent defense

① 基金项目: 福建省高校产学合作项目 (2018H6007); 福建省中青年教师教育科研项目 (JAT170126); 福建省海洋经济发展补助资金 (ZHHY-2020-3)
Foundation item: Industry-University Cooperation Project of Higher Education of Fujian Province (2018H6007); Mid-aged and Young Talent S&T Program of Education Bureau, Fujian Province (JAT170126); Special Fund for Marine Economic Development of Fujian Province (ZHHY-2020-3)
收稿时间: 2020-11-02; 修改时间: 2020-12-02; 采用时间: 2020-12-09; csa 在线出版时间: 2021-06-30

在信息化时代, 打印设备的使用在信息技术中发挥着不可或缺的作用, 涉及到政府军队, 企事业等重要部门, 以及与国计民生相关的金融、电信、能源、教育和电力等各行各业. 随着云计算、嵌入式技术的发展, 打印技术也逐渐进入了云打印模式. 2010 年 4 月, 谷歌提出云打印概念: 以互联网为基础, 整合打印设备资源, 构建漫游共享打印平台, 向全社会提供随时随地的质量标准化的打印服务, 通过其 Chrome 操作系统的 API 来实现云打印功能. 同年 11 月, 惠普也发布云打印技术 (HP ePrint), 通过向云打印机唯一的 E-mail 地址发送邮件的方式, 来实现云打印功能[1].

云打印模式的引入, 也发展了打印管理与审计、打印数据的加密传输等不同的安全打印技术[2,3], 但在实际应用中仍存在以下主要问题:

(1) 仅依靠基础设施安全, 各打印安全功能孤立化, 缺少多种不同技术方案的融合. 文献 [4] 和文献 [5] 中实现的安全打印主要采用数据加密技术来保证打印作业到云打印机的可靠交付, 但在打印管理和审计方面没有涉及. 特别是文献 [4] 应用的谷歌云打印系统需要将打印文档先通过 Internet 上传到国外的云服务器上, 除了使用公有云的开放架构易受攻击之外, 还存在很大的隐私问题. 文献 [6] 的安全打印主要通过安全管理模块维护用户与授权打印机的对应关系, 通过日志系统追朔打印作业的执行过程, 但在打印数据的非授权访问方面没有涉及.

(2) 用户桌面与打印机驱动高度耦合的技术模式易产生应用风险. 文献 [7] 虽然通过服务器实现打印监控与审计, 但是用户桌面与打印机驱动高度耦合, 当桌面维护人员的介入后, 容易接触到用户的桌面或待打印的文档信息, 从而引起数据泄密的信息安全事故.

(3) 忽视打印输出端上的系统加固与主动智能防御. 为了避免打印桌面的暴露, 打印输出端一般会设计为 3 种应用模式: 1) 像谷歌或惠普的云打印方案中的那种面向特定协议的专用打印机, 但这意味着扩展性不足, 不适合普通的打印机接入云打印系统; 2) 采用无用户交互界面的基于 PC 的代理网关系统对不同类型的网络打印机进行统一的协议控制与访问[8]; 3) 设计嵌入式控制器驱动打印机[9]. 但是无论采用哪种模式, 均没有在打印输出端上进行安全加固, 这会使打印输出设备成为潜在的被攻击的对象, 存在病毒传播及数据泄密的风险.

因此, 针对上述问题, 本文以技术融合为出发点, 创新地提出了一种智能防御的私有云打印系统的安全云打印架构. 采用私有云的网络架构限制云打印系统的访问范围, 采用虚拟打印技术屏蔽打印的细节为用户提供统一的访问接口, 采用面向过程的安全管理技术对整个打印业务流进行监控、审计与授权访问, 采用智能防御技术对打印输出端进行安全加固. 整个系统主要由云打印客户端、云打印服务器和池打印控制器构成. 云打印客户端是面向用户的接口, 用户通过其登录云打印系统, 把待打印的数据形成打印作业后提交至云打印服务器. 云打印服务器采用 Web 架构, 它首先对用户进行身份鉴别, 然后对其提交的打印作业进行过程控制, 包括审核、审计和作业数据的存储, 一旦打印作业审核成功, 后续在需要时将被送往该作业准入的池打印控制器. 池打印控制器采用 Windows Embedded 系统, 它通过读卡器来实现当前打印作业用户的鉴别, 只有在鉴别到作业用户后才下载打印作业并通过 USB 接口驱动打印机实现收到作业的打印输出, 以防止作业数据的丢失. 系统的应用架构如图 1 所示.

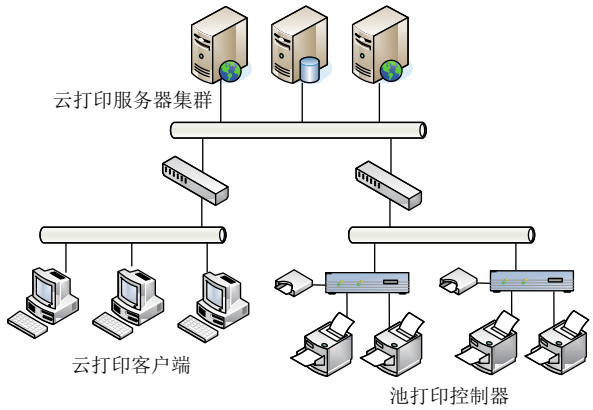

图 1 系统的应用架构图

1 私有云安全打印技术

私有云安全打印技术是系统工作的基础, 它通过虚拟通道打印、文档格式转化机制把用户提交的本地打印作业中的打印数据转为一个加密型的 PDF 中间件格式, 传输到云打印服务器. 当用户就近访问系统中的打印机, 并在打印输出端上完成身份认证后, 云打印服务器才把之前用户提交的打印作业下发给打印输出端进行打印输出, 其功能架构如图 2 所示. 该技术主要体现在云打印客户端和私有云安全打印通信协议的设计中.

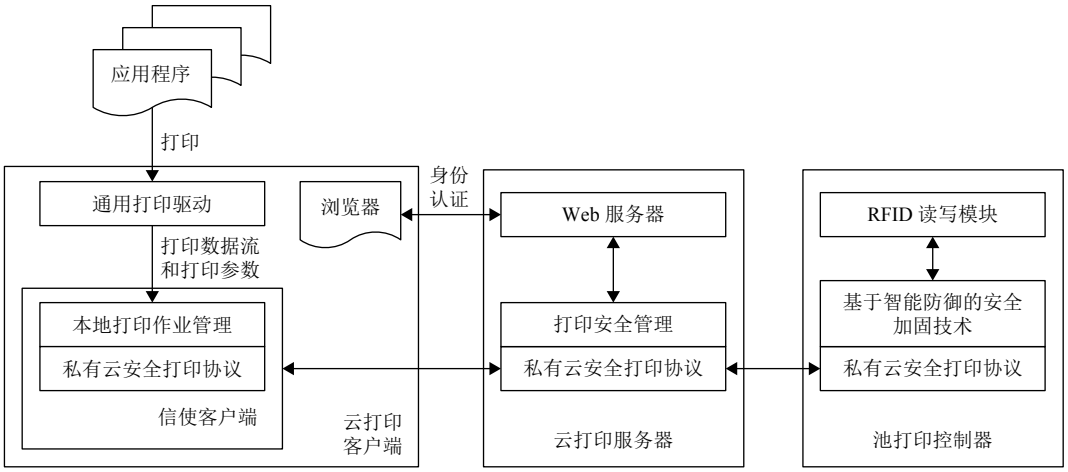

图 2 私有云安全打印技术的功能架构图

1.1 云打印客户端

云打印客户端主要由浏览器、通用打印驱动和信使客户端构成, 是系统提供给用户的打印输入接口. 它主要实现了用户的身份验证、虚拟打印、本地打印作业的管理、与系统进行协议交互的功能.

(1) 用户的身份验证: 用户通过浏览器访问云打印服务器完成身份验证. 用户一旦登录成功则上报登陆主机的身份信息 (IP 地址和 MAC 地址等), 用于后续交互的用户数据的标识.

(2) 虚拟打印: 它是由通过定制基于 Microsoft PostScript (PS) 的打印机驱动插件实现的通用打印驱动来完成的. Microsoft PostScript 打印驱动由一系列的动态库 (pscript5.dll、ps5ui.dll 等)、文本文件 (PPD 文件) 和二进制数据文件组成. pscript5.dll 用于处理文本输出和呈现图像, 然后将文本和图像数据发送到打印后台处理程序; ps5ui.dll 用来提供打印界面; PPD 文件是打印机的数据文件, 为打印机属性提供可选配置, 例如打印纸张大小、颜色模式等, 可以通过修改 PPD 文件来修改打印参数.

通用打印驱动采用 COM 技术, 主要实现以下功能: 它使用 Winspool 中的 AddPrinter 函数完成虚拟打印机的安装及打印机名称的自定义设置, 用户通过该虚拟打印机名称实现对系统中所有在线打印机的统一访问; 它通过定制 PS 驱动中的界面自定义用户插件和修改 PPD 文件实现打印参数的配置; 它实现了 PS 驱动中的 IPrintOemPS2::WritePrinter 方法来获取通过虚拟打印机提交的打印数据, 原始的打印数据为 PS 数据流; 它对打印流程的控制则通过实现 PS 驱动中的 IPrintOemPS2::EnableDriver 方法中定制的打印机挂钩函数来完成, 挂钩函数包含 INDEX_DrvStartDoc、INDEX_DrvEndDoc、INDEX_DrvStartPage, 这些函数主要处理文档开始打印、打印结束、打印某页的逻辑.

(3) 本地打印作业的管理: 主要包括本地打印作业的提交和取消, 以及打印结果反馈. 应用程序通过虚拟打印机执行打印操作时, 通用打印驱动会将收到的 PS 打印数据流和打印参数通过管道发送给信使客户端. 为了保证打印数据的安全性以及可扩展性, 信使客户端通过第三方的 ghostscript 库将 PS 数据流转成 PDF 文件, 经加密后连同打印参数一起上传至云打印服务器完成打印作业的提交. 而云打印服务器则根据打印安全策略对用户提交的打印作业进行审核, 并把审核结果反馈至信使客户端进行显示. 在此过程中, 通用打印驱动还可通过 Winspool 中的 AbortPrinter 函数对提交的打印作业进行取消, 并通告信使客户端以完成取消打印消息到云打印服务器的进一步提交.

(4) 与系统进行协议交互: 云打印客户端与云打印服务器的数据交互主要通过信使客户端进行, 采用的是自定义的私有云安全打印通信协议.

1.2 私有云安全打印通信协议

私有云安全打印通信协议是系统各部件进行数据交互的基础, 通过其实现了私有云的独立架构, 即系统的数据只能在单一网络内流动, 对其他网络而言都是无效的. 它以 WebSocket 协议为基础, 扩展实现了打印

机注册管理、打印作业管理控制、输出端智能防御控制等功能, 其协议流如图 3 所示.

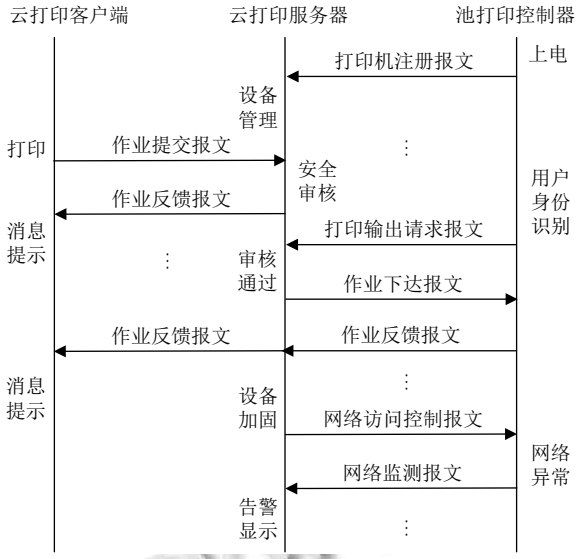

图 3 私有云安全打印通信协议的协议流图

(1) 打印机注册管理

池打印控制器每次上电接入网络时, 都会通过打印机注册报文向云打印机服务器进行注册, 通告自己的设备 ID 及连接的打印机状态, 只有注册成功的池打印控制器才能下载打印作业进行输出.

(2) 打印作业管理控制

云打印客户端通过作业提交报文向云打印服务器提交作业打印请求, 服务器则通过作业反馈报文通告审核结果. 一旦审核通过, 后续服务器将通过作业下达报文向池打印控制器发送作业输出指令.

由于在作业提交流程中, 作业文档的上传将耗费较多的带宽, 为了提高系统的响应速度, 作业提交报文被设计为请求文档、上传文档、提交完成这 3 个子类型. 完整的打印作业提交流程如图 4 所示, 云打印客户端首先通过请求文档报文在服务器中查找是否已存在待打印文档, 若存在则通过请求文档报文返回待打印文档存放在数据库中的唯一的文档 ID; 若不存在, 则通过上传文档报文向服务器上传待打印文档, 服务器在存储文档后同样通过请求文档报文返回文档 ID; 最后再通过提交完成报文向服务器提交待打印文档的 ID 和打印参数完成作业的提交. 在系统中采用 MD5 校验码和 CRC16 校验码组合的方式进行相同文档的匹配, 在请求文档报文中就包含有待打印文档的 MD5 校验码和 CRC16 校验码, 采用双类型码校验检索可以极大地降低误匹配率.

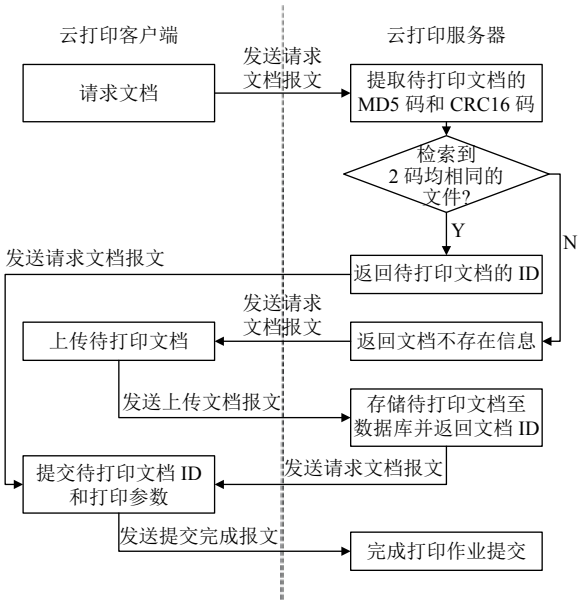

图 4 打印作业提交流程图

(3) 输出端智能防御控制

池打印控制器通过打印输出请求报文向云打印服务器发出打印机使用的请求, 一旦审核通过, 服务器就会通过作业下达报文向该池打印控制器下载请求用户的作业进行输出. 同时, 为了对输出端进行加固, 云打印服务器还会向池打印控制器下发网络访问控制报文进行智能防御, 而池打印控制器则会通过网络监测报文向服务器进行网络异常状态的通告.

为了保证私有云架构的安全性及可控性, 私有云之间通过私有云 ID 相互区分, 且通过加密算法及校验策略保证交互数据的完整性及可靠性.

2 面向过程的打印安全管理技术

面向过程的打印安全管理技术是云打印服务器功能的核心, 它以面向用户的打印安全策略为基础, 对整个打印过程进行监控, 包括打印作业的审核、审批和追溯, 以及打印机的监控与管理. 其中, 面向用户的打印安全策略由用户注册时的角色类型以及后续管理员的设定来决定, 它主要分为打印策略和文档访问安全策略这两个部分. 打印策略主要是对用户提交的打印参数进行限制, 包括: 允许打印、彩打/黑白、单面等. 文档访问安全策略主要是对用户打印的资源进行访问

控制, 包括: 文档密级、需要人工审批、信息追踪等. 其中, 文档密级用于限制用户能够打印的文档, 超过密级以上的文档用户将无法打印. 服务器会对用户提交的打印作业中的文档进行密级鉴定, 采用的是文档匹配、敏感词句匹配、人工审核相结合的方式. 即, 先根据作业中的文档 ID 提取待打印文档, 若该文档是历史上传文档, 其密级就是作业文档的密级; 若该文档是新上传文档则不存在文档密级, 此时进行敏感词句的匹配, 并把匹配到的敏感词句的密级作为该文档的密级; 若所有的敏感词句都匹配不到, 则提交管理员审核, 由管理员设定文档密级. 作业文档的密级一旦设定, 则打印流程继续, 文档密级的鉴定流程如图 5 所示. 而信息追踪, 则是对提交打印的文档加入基于用户名、提交打印主机 MAC 地址、打印时间戳的暗水印以实现打印泄密的源追溯.

面向过程的打印安全管理技术的工作流程如图 6 所示. 当用户提交打印作业时, 首先基于用户的打印策略对打印参数进行审核, 接着鉴定作业文档的密级, 并根据用户的文档访问安全策略进行审核. 所有审核通过后, 打印作业被存储在服务器中, 再根据后续的打印输出请求下发到池打印控制器进行按需打印输出. 除此之外, 服务器还会向池打印控制器下发网络访问控制策略, 并根据池打印控制器反馈的网络异常状态进行系统通告及阻断打印过程, 以实现打印机的监控与管理.

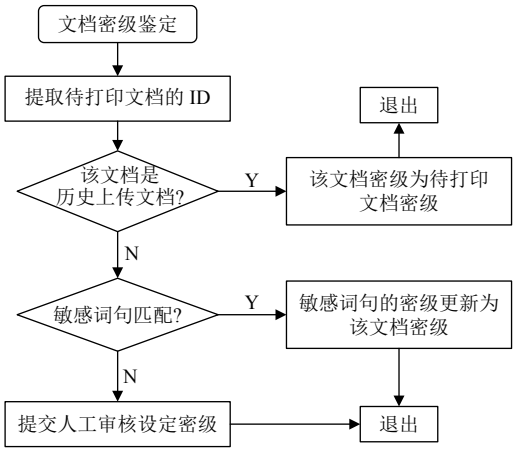

图 5 文档密级的鉴定流程图

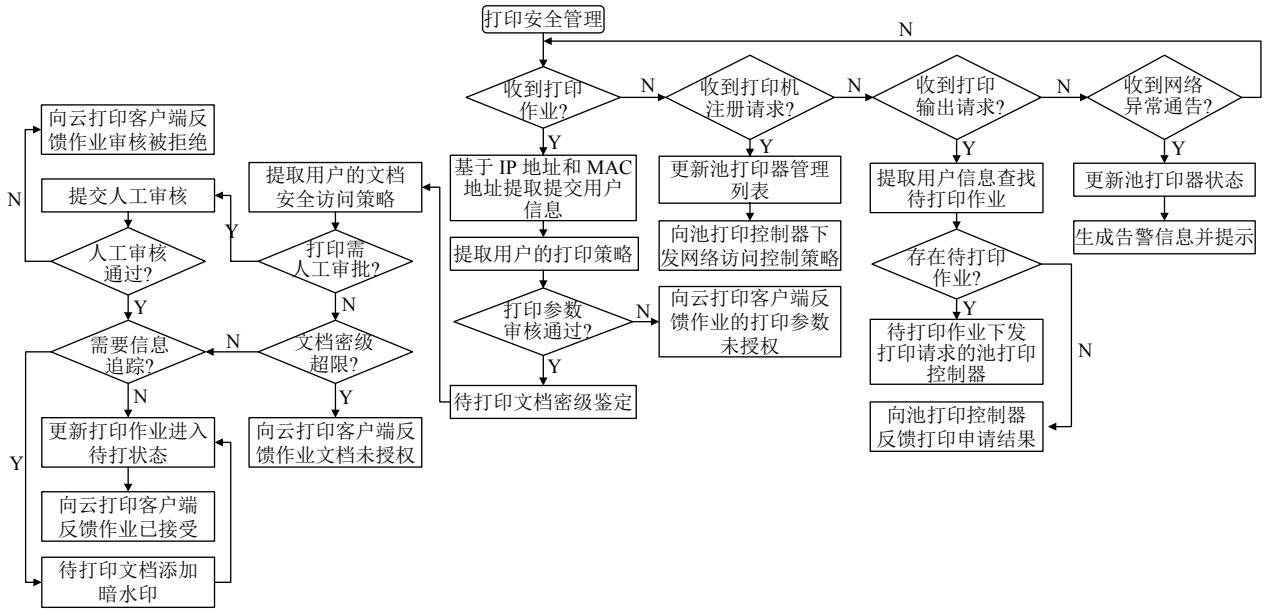

图 6 打印安全管理技术的工作流程图

3 打印输出端的智能防御技术

为了避免池打印控制器成为系统网络安全的短板——成为被攻击的对象或者攻击的发起者, 在设计中, 云打印服务器和池打印控制器之间进行了网络隔离. 传统的网络隔离技术, 一般通过配置交换机与防火墙实现, 对硬件要求较高, 兼容性较差, 在用户访问权限需要动态变化的情况下, 还需要频繁地对交换机进行设置, 使用繁琐. 因此, 系统在网络隔离方面提出了一种端末的网络访问控制策略, 即使用智能防御技术对打印输出端 (池打印控制器) 进行安全加固.

端末的网络访问控制策略的核心就是在池打印控制器的网卡驱动中添加过滤模块, 该过滤模块会加载从服务器下发的网络访问控制报文中解析到的网络访问控制列表, 并据其对网卡流入和流出的网络数据帧进行过滤, 拦截网络访问控制列表中禁止的网络行为, 以限制池打印控制器的能够访问的网络范围, 达到网络隔离的目的. 同时, 池打印控制器还会根据过滤模块统计的网络异常访问信息, 触发设备关闭或重启的操作, 利用 Windows Embedded 系统具有重启还原的特点, 让池打印控制器始终在可靠的状态下工作. 策略的工作流程如图 7 所示.

过滤模块所加载的访问控制列表包含基础流量信息 (IP 地址范围、本地端口范围、远程端口范围、Internet 使用的协议类型、网络数据帧的流量方向以及访问权限等) 和特征流量信息 (受限流量和非受限流量的端口速率、重复率、碎片率、误码率等).

4 系统测试

系统的应用效果如图 8、图 9 和图 10 所示. 其中, 图 8 为云打印服务器的 Web 管理界面, 图 9 为池打印控制器控制 2 台打印机的场景图. 当打印用户通过浏览器登陆云打印系统成功之后, 在本地的信使客户端中即可查询到当前用户能够访问的系统中已上线的云打印机信息、用户历史的打印作业信息, 以及对其正在提交的打印作业进行打印管理, 应用效果如图 10 所示.

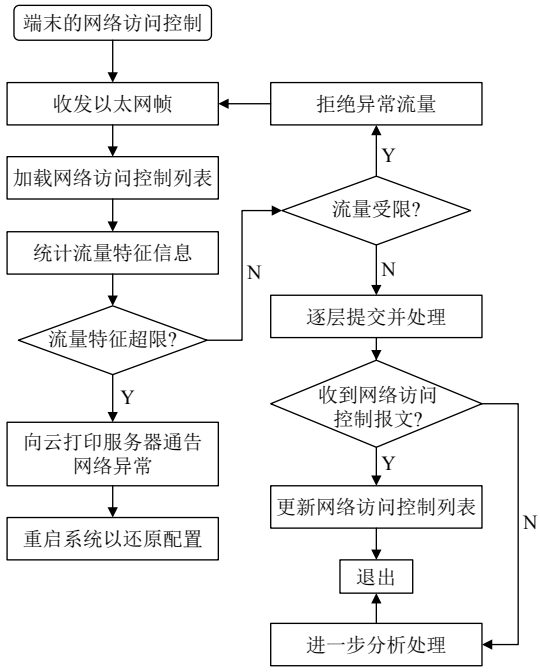

图 7 端末的网络访问控制策略的工作流程图

图 8 云打印服务器的 Web 管理界面

为了测试在保障良好的响应时间内系统能够承受的最大吞吐量, 即每秒同时提供的不同业务接口的最大值, 本文采用了 apache-jmeter-5.1.1 测试工具对系统进行了性能压测, 主要测试了安全路径下的提交作业

和作业输出这 2 个业务流. 同时还测试了池打印控制器在受到 DOS 攻击时, 系统执行作业输出流的平均响应时间和异常率. 系统的测试环境如表 1 所示, 其中, 云打印服务器采用群集的方式部署为 2 个基于 Web 的打印管理服务器和 2 个数据库服务器.

图 9 池打印控制器控制 2 台打印机的场景图

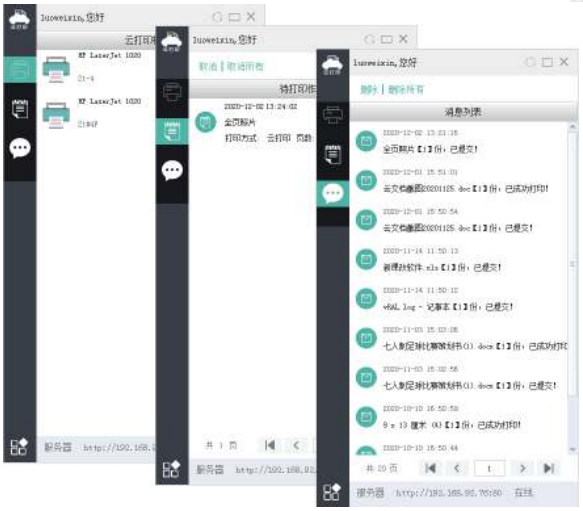

图 10 云打印客户端中的信使客户端运行界面

表 1 系统的测试环境表

设备描述	工作参数
打印管理服务器dev-front0	2 CPU, 4 GB内存
打印管理服务器dev-front1	2 CPU, 4 GB内存
数据库服务器dev-data0	4 CPU, 4 GB内存
数据库服务器dev-data1	4 CPU, 4 GB内存
压测客户机dev-test	win7 64位, 6 GB内存, 4 core, jdk1.8.0_201
安测客户机dev-dos	Ubuntu 18.10, 8 GB内存, 4 core

在测试环境中, 本文针对提交作业流程 (含请求文档 U1、上传文件 U2、提交作业 U3 这 3 个阶段), 模拟 400 并发用户连续发起 100 次请求进行测试, 测试数据如表 2 所示. 其中, 系统对提交作业流程各阶段的平均响应时间为 0.15 s, 最长响应时间为 1.995 s, 错误率是 0 (100% 执行成功), 吞吐量 (即每秒完成的请求数) 约为 2358.352.

表 2 提交作业测试数据表

标签	平均值	中位数	最大值	异常	吞吐量
U1	108	82	1259	0	786.4263
U2	222	178	1995	0	786.4881
U3	120	90	1269	0	786.7821
Tot	150	120	1995	0	2358.352

而针对作业输出流程 (含获取作业详情 D1、下载作业文件 D2、上报作业状态 D3 这 3 个阶段), 模拟 400 并发用户连续发起 100 次请求进行测试, 测试数据如表 3 所示. 其中, 系统对作业输出流程各阶段的平均响应时间为 0.448 s, 最长响应时间为 1.329 s, 错误率是 0 (100% 执行成功), 吞吐量 (即每秒完成的请求数) 约为 860.931.

表 3 作业输出测试数据表

标签	平均值	中位数	最大值	异常	吞吐量
D1	195	177	555	0.00	287.0408
D2	882	893	1329	0.00	287.0326
D3	266	261	1247	0.00	287.115
Tot	448	325	1329	0.00	860.931

根据表 2 和表 3 的测试数据分析可得, 一个完整的提交作业流程 (含 3 个阶段) 的平均响应时间为 0.45 s, 而一个完整的作业输出流程 (含 3 个阶段) 的平均响应时间为 1.343 s, 均小于 2 s, 根据 2/5/10 s 原则[10], 系统可以被用户认为是“非常有吸引力”的用户体验.

而对池打印控制器的安全性测试, 则在表 3 的模拟条件下附加 hping3 工具对其发起 TCP SYN Flood 攻击进行. 由于池打印控制器应用了智能防御技术, 过滤了非授权流量, 无法通过漏洞扫描探测其开放端口, 因此, 在测试中, hping3 攻击的池打印器端口显示给出. 测试数据如表 4 所示, 根据其分析可得, 在 S1 (1000 SYN 包/s) 攻击条件下, 系统能够正常及时地执行作业输出流; 在 S2 (5000 SYN 包/s) 攻击条件下, 系统能够较好地执行作业输出流, 但响应时间增加; 在特定攻击条件 S3 (伪造打印管理服务器 IP, 5000 SYN 包/s) 下, 作业输出流执行质量有一定的下降. 在 S2 和 S3 条件下, 随着攻击时间的持续, 池打印控制器均发生重启, 且打印管理服务器收到网络异常信息. 可见, 本文所设计的安全架构能够较好地保障系统功能的安全执行.

5 结语

为了解决打印服务存在的易受攻击、数据泄密等安全问题以及充分利用云计算集中式管理的便捷性与

高效性, 本文提出了一种融合私有云技术、打印过程监控及管理与智能防御技术的安全打印架构. 该架构以私有云为基础屏蔽了外部网络的非授权访问, 通过对打印过程的审计与管理实现打印数据的授权访问以及追溯控制, 最后还通过端末的访问控制策略实现打印输出设备的主动智能防御, 以避免末端成为系统网络安全的短板. 以该架构实现的系统经过压力测试和安全性测试后, 仍具有良好的用户体验和健壮性, 目前已部署于银行、保险等单位, 以待实践的进一步检验.

表 4 池打印控制器被攻击时, 作业输出测试数据表

标签	平均值	异常(%)	备注
S1	1976	0	—
S2	4238	3.62	—
S3	8756	27.83	池打印控制器重启

参考文献

1 Yun W. Research of cloud print key technology based on identity card. Proceedings of the 3rd World Congress on Software Engineering. Washington, DC, USA. 2012. 176–178.

2 蔡莉莉, 钱海忠, 王进华. 云打印系统关键技术研究. 金陵科技学院学报, 2015, 31(3): 26–31. [doi: 10.3969/j.issn.1672-755X.2015.03.006]

3 鲍豹. 云桌面打印映射关键技术. 计算机系统应用, 2016, 25(8): 227–232. [doi: 10.15888/j.cnki.csa.005279]

4 居特尼克 Y, 卢卡斯 K. 基于云的打印系统中的安全打印: 中国, 104428788A. (2015-03-18).

5 谭伟浩. 基于混合加密算法的云打印平台研究与应用 [硕士学位论文]. 西安: 西安理工大学, 2018.

6 武志学, 赵阳, 赵启卫, 等. 基于云计算技术的智能终端打印系统: 中国, 103412730A. (2013-11-27).

7 冯元丽, 张海梅, 乔建丽, 等. 一种 USB 打印机安全打印监控及审计系统: 中国, 103279720A. (2013-09-04).

8 方杰. 云端通信协议与控制协议融合技术 [硕士学位论文]. 武汉: 华中科技大学, 2017.

9 Huang MG, Zhao N. Cloud-based portable IoT inkjet printer. Proceedings of the 4th International Conference on Communication and Information Systems (ICCIS). Wuhan, China. 2019. 70–74.

10 陈能技. 软件测试技术大全: 测试基础 流行工具 项目实战. 2 版. 北京: 人民邮电出版社, 2011.