基于云计算业务的安全设备自动化运维

沈佳怡，顾思宇
（中国电信股份有限公司上海分公司，上海 200120）

摘　要：随着信息技术的迅猛发展，云计算在众多领域实现了广泛应用，为人们的生活和工作带来了极大便利。但与此同时，云计算环境下的运维问题也需要加以考虑。深入探讨了基于云计算业务的安全设备自动化运维的重要性。引入自动化运维技术，能大幅提高安全设备的管理效率，降低运维成本，能更有力地增强云计算环境的安全性。此外，自动备份等功能也为安全提供了多一层保障。Python脚本等技术在其中发挥着关键作用，为实现高效、稳定的安全设备自动化运维提供了有力支持。

关键词：云计算；安全设备；自动化运维；自动备份；Python
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000-0801.2025072

0　引言

云计算作为一种新型的计算模式，为企业和个人提供了便捷、高效的计算资源和服务。然而，云计算的开放性和复杂性带来了一系列的安全风险。安全设备作为保障云计算环境安全的重要载体，其运维管理面临着巨大的挑战。传统的人工运维方式已经无法满足在云计算环境下对安全设备的管理需求，因此，引入自动化运维技术成为必然选择。

1　现状分析

1.1　云计算环境下安全设备自动化运维的重要性

（1）提高管理效率

自动化运维可以实现安全设备的自动配置、监控和故障处理，大大减少了人工干预的时间和工作量，提高了管理效率。

（2）降低运维成本

自动化运维可以减少人力成本和时间成本，同时降低因人为错误导致的故障风险，从而降低运维成本。

（3）增强安全性

自动化运维可以实时监控安全设备的运行状态，及时发现和处理安全事件，提高云计算环境的安全性。

1.2　云计算环境下安全设备自动化运维面临的挑战

（1）设备多样性与管理复杂性

云计算环境下安全设备种类繁多，如WAF、IPS、网闸等。不同设备管理方式和接口各异，这增加了自动化运维的难度。同时，人工运维面临安全设备种类过多的问题，运维人员需要熟悉多种设备的操作和管理，耗费大量时间和精力。

（2）动态环境与配置调整难题

云计算环境动态变化，安全设备的配置和策

收稿日期：2024-11-20；修回日期：2025-03-06

略须随之调整。实现自动化的配置更新和策略调整颇具挑战。而在人工运维中，单种类设备因业务量大、台数过多，难以快速响应环境变化进行手动配置调整，容易导致安全漏洞。

（3）安全与效率困境

自动化运维涉及对安全设备的远程管理和控制，保证通信安全性和操作合法性至关重要。人工运维则存在重复输入账号密码浪费时间和人力资源的问题，且设备缺少自动备份或外发文件功能，需要手动操作下载所需文件，效率低下且增加了操作失误的风险。

1.3 云计算环境下安全设备自动化运维的解决方案

（1）统一管理平台

构建统一的自动化运维管理平台，实现对不同种类安全设备的全面覆盖，其建设架构如图1所示。

- 数据获取：运用API、SNMP、syslog等方式，高效传输巡检指标项的具体数据以及日志模块的详细分析数据。
- 状态实时监控：持续采集设备运行数据，包括CPU使用率、内存占用、磁盘容量等，在平台界面实时呈现设备状态，便于及时察觉异常情况。
- 拓扑自动生成或导入：平台能够自动生成或导入网络拓扑，清晰展现整个流量路径，为故障定位奠定坚实基础，当检测到设备故障时，平台自动启动预设的故障判断流程，如进行点对点的ping测，以最快速度判断问题节点，助力运维人员迅速定位、深入分析研判。
- 巡检：平台可制定自动化巡检计划，定期对安全设备的配置进行检查，确保其准确性与合规性，各安全设备参数及阈值表见表1。

（2）自动化配置管理

引入自动化配置管理工具，切实保障安全设备配置的高效性与准确性。同时，在系统中集成自动化备份功能，定期对安全设备的配置和数据进行自动备份，以便在设备故障或数据丢失时能够迅速恢复。

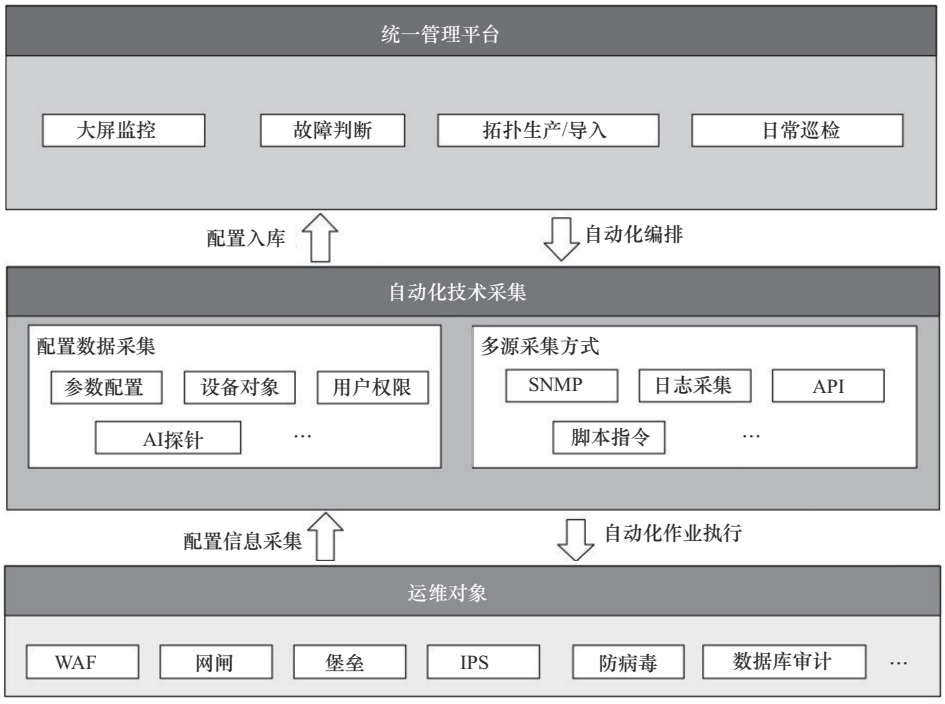

图1 统一管理平台建设架构

表1　各安全设备参数及阈值表

设备类别	巡检监控参数（自动化运维）	橙色阈值	红色阈值	获取数据方式
4A	CPU 使用率	80%	90%	云平台对接
	内存使用率	80%	90%	云平台对接
	根目录空间占用率	80%	90%	登录设备查看
	文件目录 drbd 空间占用率	80%	90%	登录设备查看
堡垒机	CPU 使用率	60%	80%	snmp
	内存使用率	60%	80%	snmp
	存储占用率	60%	80%	snmp
WAF	CPU 使用率	80%	90%	snmp
	内存使用率	80%	90%	snmp
	存储空间使用率	80%	90%	snmp
	设备告警	与阈值无关（关键字：重）	与阈值无关（关键字：重）	通过日志审计平台接收日志
	根目录空间占用率	80%	90%	脚本
	授权时间与维保时间监控	快到期 2 个月	快到期 1 个月	脚本
	admin 访问次数超过 10 次 1 分钟	1 分钟访问 10 次	1 分钟访问 15 次	通过日志审计平台接收日志
网闸	内端 CPU 使用率	80%	90%	snmp
	内端 内存使用率	80%	90%	snmp
	内端存储空间使用率	80%	90%	snmp
	内端连接数	12 000	18 000	snmp
	外端 CPU 使用率	80%	90%	snmp
	外端内存使用率	80%	90%	snmp
	外端存储空间使用率	80%	90%	snmp
	外端连接数	12 000	18 000	snmp
	HA 主备信息	/	/	snmp
	HA 健康状态	/	/	snmp
	日志告警	/	/	syslog（已对接日志审计平台）
IPS	CPU 使用率	70%	90%	snmp
	内存使用率	70%	90%	snmp
	存储使用率	70%	90%	snmp
	新建会话数	56 万/s	72 万/s	snmp
	并发连接数	1 400 万	1 800 万	snmp
防火墙	CPU 使用率	60%	80%	snmp
	内存使用率	70%	90%	snmp
	存储使用率	80%	97%	snmp
	在线并发	6 000 000	8 000 000	snmp
	新建连接数	25 万/s	32 万/s	snmp
网页防篡改	CPU 使用率	80%	90%	云平台对接
	内存使用率	80%	90%	云平台对接
	存储空间使用率	80%	90%	云平台对接
数据库审计	CPU 使用率	80%	90%	snmp
	内存使用率	80%	90%	snmp
	根目录空间占用率	80%	90%	登录设备查看
	数据分区空间占用率	80%	90%	登录设备查看
VPN	CPU 使用率	70%	90%	snmp
	内存使用率	70%	90%	snmp
	会话新建数	35 万/s	45 万/s	snmp
	SDcard 使用率	70%	90%	snmp
	并发连接数	1 120 万	1 440 万	snmp

（3）智能监控与分析

借助智能监控技术[1]，有效提升安全设备的运维水平。

- 实时监测：利用大屏监控，实时掌握安全设备的运行状态和安全事件。
- 巡检短消息通知：当智能监控发现问题或巡检结果异常时，自动发送短消息通知运维人员，确保及时进行处理。
- 故障发现：通过实时监测、数据分析、设备日志分析等多种手段，及时发现安全设备的故障，并启动相应的处理流程。

2 安全设备层面运维分析

2.1 自动化备份需求分析

（1）账号密码自动输入

自动备份板块实现了前端页面自动输入账号密码的功能。

在实际的信息管理过程中，人工输入账号密码不仅耗时，而且在面对多个账号时效率低下。而此板块的自动输入账号密码功能则克服了这一问题，它能够快速且准确地完成账号密码的填充，大大提高了备份的启动效率。

（2）精准模拟人工操作步骤

自动备份板块的另一大优势在于能够按照人工操作的步骤，精准地定位到界面上的每个按钮。

这一功能的实现使自动备份过程能够高度复刻人工操作的流程。在复杂多样的软件界面环境中，不同的按钮布局和操作逻辑对自动化流程提出了挑战。而本板块通过精准定位按钮，能够在各种环境下稳定运行，确保备份操作的准确性。无论是在具有复杂层级菜单的系统中，还是在界面设计频繁更新的软件中，它都能像经验丰富的操作员一样，准确找到所需按钮，保证备份操作按预定流程执行。

（3）下载至指定路径

自动备份板块还具备将备份文件下载至对应路径的功能。

在数据管理中，合理的文件存储路径至关重要。此功能确保了备份文件能够被有序地存储在预定的位置，方便进行后续的数据管理、查询和恢复操作。它避免了因文件存储混乱而导致的管理成本增加，提高了数据的可管理性。例如，在企业级数据备份中，不同部门的数据可以按照预先设定的路径进行存储，从而提高整体的数据管理效率。

2.2 利用Playwright框架原理介绍

Playwright是开源的自动化测试框架[2]，开发者能借此在多种浏览器与操作系统上进行端到端测试。它依靠Node.js的Puppeteer控制浏览器达成自动化操作，Puppeteer和Browser之间通过CDP（基于WebSocket协议的Chrome DevTools Protocol）通信，该协议可检测、调试Chromium、Chrome等基于Blink的浏览器，从而让Playwright与浏览器深度交互，像页面导航、元素选择、输入模拟等操作都得以实现。Playwright架构如图2所示。

在Playwright里，Browser代表浏览器实例，可包含多个Browser Context（浏览器上下文）。Puppeteer API分层且反映浏览器结构，通过Puppeteer控制浏览器实现自动化时，Browser实例中的Browser Context类似打开Chrome后再开隐身模式Chrome的情况，它有独立的Session、Cookie和Cache，相互不共享。

Browser Context能包含多个Page（即tab页面），可通过browserContext.newPage()实例化创建，browser.newPage()创建页面时使用默认Browser Context。Page可包含多个Frame（框架），每个Page至少有一个主框架main frame，可能还有由iframe标签产生的子框架。Frame至少有一个ExecutionContext（执行上下文），这是

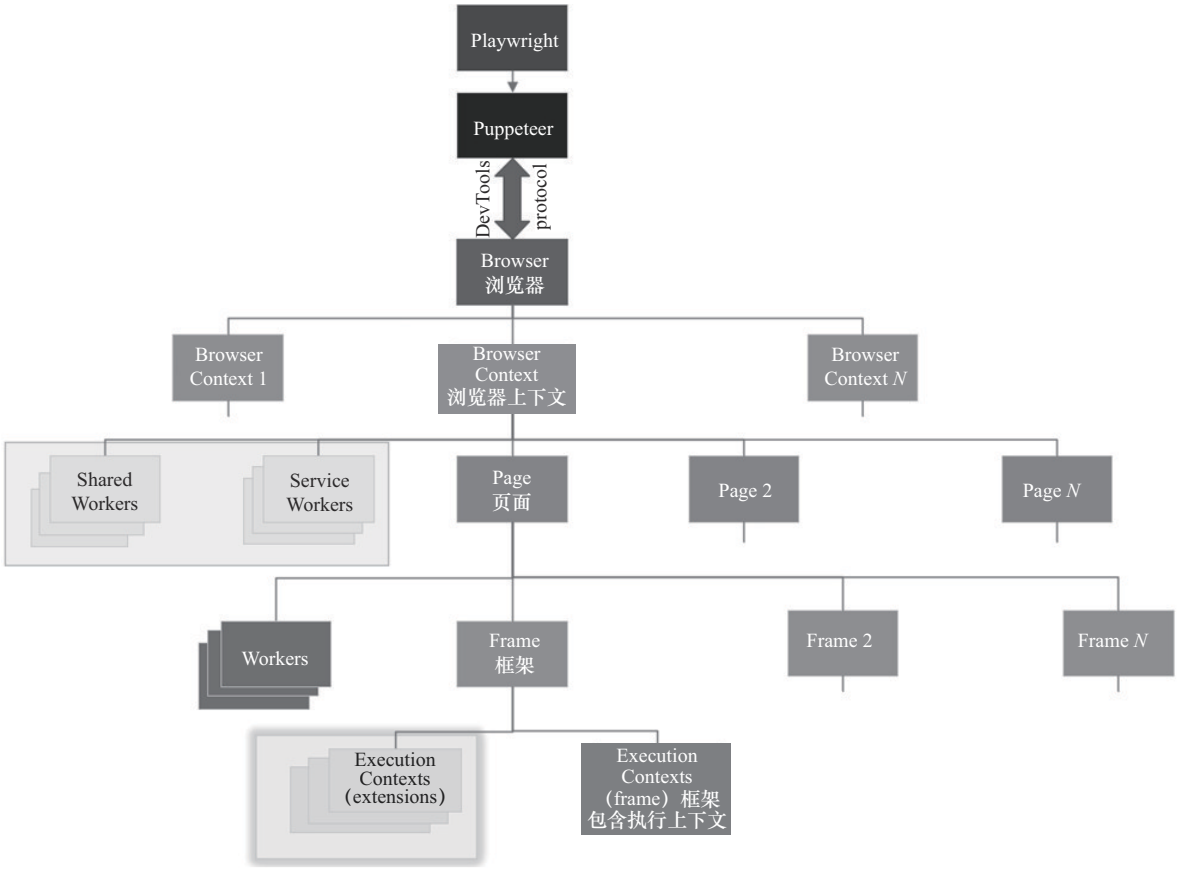

图2　Playwright架构

JavaScript执行环境，每个Frame都有默认的执行环境。Worker有单一执行环境，便于与Web-Workers交互。

此外，Playwright的server由nodejs构建，负责与client和不同Web浏览器引擎通信。通信协议上，client与Playwright server通过WebSocket协议通信，Playwright与Chromium用Chrome DevTools协议通信，对于Firefox和WebKit，Playwright实现了类似CDP的协议。这些技术与协议的融合，使Playwright成为功能强大且灵活的自动化测试工具。

2.3　自动化备份脚本具体执行

Python备份脚本在日常运维工作中发挥着至关重要的作用，它能够自动、高效地对重要数据和文件进行备份，为运维人员节省了大量的时间和精力[3]。无论是数据库备份、文件系统备份还是配置文件备份，Python备份脚本都能提供便利和可靠的保障。

本部分使用Python代码的Playwright框架编写自动化备份脚本。Playwright是一个强大的自动化测试工具，它可以模拟用户在浏览器中的操作，实现自动化任务。以下是具体的代码实现，如图3所示。

这段代码主要实现了对某云安全设备的备份和管理功能。代码利用了Playwright框架进行浏览器自动化操作，同时还进行API调用以与该安全设备进行交互。

首先，通过run函数使用Playwright框架启动Chrome浏览器，模拟人为登录设备管理界面操作，输入账号和密码后获取登录后的session、cookies信息，具体是提取出csrftoken和sessionid并格式化为特定字符串。

```
[redacted].py > ...
def run(playwright: Playwright) -> str:
    browser = playwright.chromium.launch(headless=False)
    context = browser.new_context(ignore_https_errors=True)

    page = context.new_page()
    page.goto("[redacted]")
    page.get_by_placeholder("请输入账号…").click()
    page.get_by_placeholder("请输入账号…").fill("[redacted]")
    page.get_by_role("textbox", name="请输入密码…").click()
    page.get_by_role("textbox", name="请输入密码…").fill("[redacted]")
    page.get_by_role("button", name="登 录").click()
    time.sleep(3)
    page.reload()
    cookies = (page.context.cookies())
    csrf_token = None
    session_id = None
    for cookie in cookies:
        if cookie['name'] == 'csrftoken':
            csrf_token = cookie['value']
        elif cookie['name'] =='sessionid':
            session_id = cookie['value']
    formatted_tokens = f'csrftoken={csrf_token};sessionid={session_id}'
    return formatted_tokens
```

```
问题  输出  调试控制台  终端  端口

份\WAF备份\1[redacted]
successd to download C:\备份\WAF备份\[redacted]管理项目_2024-10-02_22_24_27.zip
6 [redacted]信息系统(运维)
switch to [redacted]信息系统(运维)
successd to set up backfile[redacted]息系统(运维)_2024-10-02_22:24:37
C:\备份\WAF备份\1[redacted]信息系统(运维)_2024-10-02_22_24_37.zip
'mv' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
successd to mv C:\备份\WAF备份\1[redacted]信息系统(运维)_2024-10-02_22_24_37.zip C:\备份\WAF备份\[redacted]
successd to download C:\备份\WAF备份\[redacted]息系统(运维)_2024-10-02_22_24_37.zip
8 [redacted]（运维）
switch to [redacted]（运维）
```

图3 自动化备份脚本代码实现

接着，对该设备的API进行调用，可以发送GET、POST或DELETE请求，通过构建请求对象并设置合适的请求头信息，处理SSL验证问题后返回API的响应内容。通过调用该设备的API获取用户组列表，提取每个用户组的id和name并返回。代码设置备份任务，通过调用该设备的备份API并传递备份的注释、创建时间、选项等信息来发起备份请求。下载备份文件，先调用查询备份API获取备份列表，找到最新备份文件的id和注释信息后，调用下载API获取备份文件内容并保存为指定文件名，同时可以根据目标文件路径将文件移动到指定位置。

最后，foreach函数先获取所有用户组信息，然后遍历每个用户组，切换到该用户组后设置备份任务并等待一段时间让备份文件生成，接着下载备份文件并根据目标文件路径进行文件移动。

在主程序部分，使用Playwright框架的同步方式执行获取cookies，设置该设备的URL、cookies、备份文件生成等待时间和目标文件路径等参数后，调用函数执行整个备份流程。

3 业务层面运维分析

3.1 自动化巡检板块的关键功能

统一的自动化运维管理平台可按照固定需求，定时定点进行安全设备巡检，自动化巡检板块模式如图4所示。

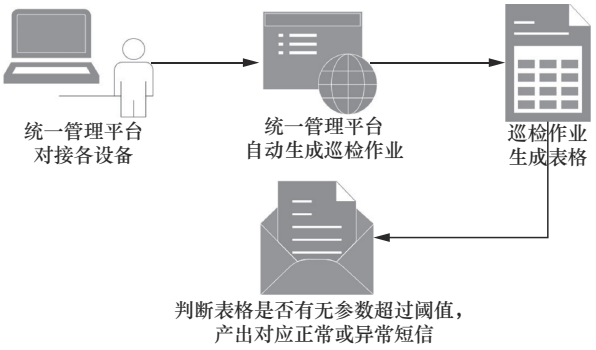

图4　自动化巡检板块模式

巡检数据统计完成后，可根据配置执行短消息发送操作。巡检短消息按照正常和异常进行区分，若配置为仅异常提醒，则正常巡检仅向24小时值班人员发出提醒，用于通知固定业务用户；若出现异常巡检情况，则可将提醒通知到安全运维人员，无须安全运维人员手动登录设备进行查看，大幅度地增加了工作效率。

3.2　故障排查板块的关键功能

故障排查板块在自动化运维故障处理方面，除了定时定点对CPU、内存、磁盘等基础参数进行自动巡检，还能够点到点地进行路由故障判断。

当导入统一管理平台拓扑，便开启了高效管理的新路径，云平台流量简洁流程如图5所示。此时，可以清晰地看到整个系统的拓扑结构以及流量的走向路径。凭借这一优势，能够精准地选定某一特定节点，对其进行全面且深入的路由测试。通过这样的方式，可以更好地了解该节点在整个网络中的性能表现和连接状况，为进一步优化网络、提升管理效率提供有力的依据，确保整个系统稳定、高效地运行，满足不断变化的业务需求。

图5中，用户通过个人终端登录用户站点，流量经过云WAF时会监控并过滤所有进出Web应用的流量。当用户站点故障时，难以判断是云WAF本身的问题，还是流量路径上的其他节点设备或配置发生故障。在统一管理平台上导入WAF站点清单后，能够借助故障排查板块便捷地进行一系列操作。首先，可以通过搜索功能确定某一特定源站所在的WAF主机位置，WAF主机自身状态在统一管理平台上也会显示。接着，利用外网探针针对清单中的站点进行流量测试，以此来模拟从用户终端出发的站点流量是否异常。这一系列操作有助于更高效地管理和维护网络系统，及时发现并解决可能出现的问题，确保网络能稳定运行和具有良好性能。

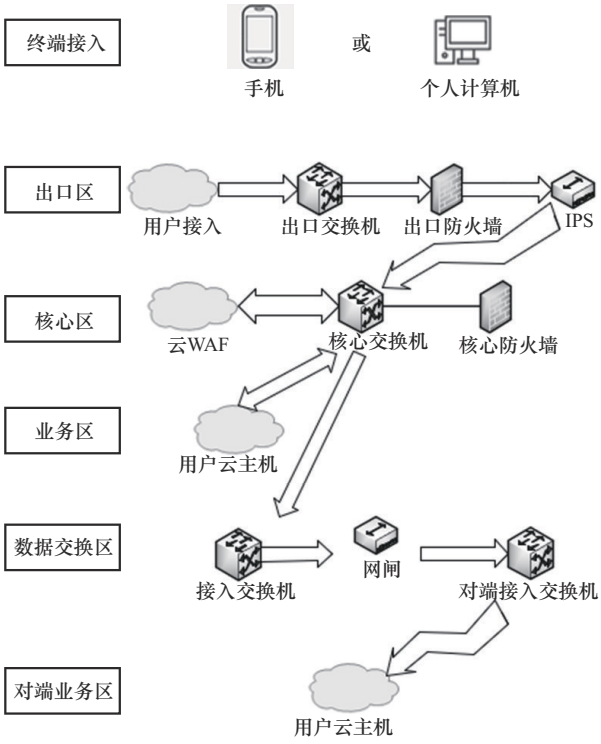

图5　云平台流量简洁流程

4　结束语

云计算环境下的安全设备自动化运维是保障云计算安全的重要手段。通过引入自动化运维技术，可以提高安全设备的管理效率、降低运维成本，并增强云计算环境的安全性。然而，自动化运维也面临着复杂性、动态性和安全性等挑战，需要采取相应的解决方案。在安全设备层面，利用Playwright框架实现自动化备份，提高数据管

理效率。在业务层面，自动化巡检和故障排查板块提升了工作效率和网络稳定性。未来，随着云计算技术的不断发展和安全需求的不断提高，安全设备自动化运维将不断完善和发展，为云计算环境的安全稳定运行提供更加有力的保障。

参考文献：

[1] 陈宝光. 政务云运维提升解决方法[J]. 中小企业管理与科技, 2018(25): 132-133.

[2] 徐基法, 刘超, 张悦, 等. 一种 Web 自动化测试方法及系统: CN114281680A[P]. 2022.

[3] 王金金. 浅谈自动化运维[J]. 广播电视网络, 2022, 29(5): 98-100.

[作者简介]

沈佳怡（2000– ），女，现就职于中国股份有限公司上海分公司，主要研究方向为网络与信息安全、云运维等。

顾思宇（1995– ），男，现就职于中国股份有限公司上海分公司，主要研究方向为网络与信息安全、云计算、人工智能等。