基于大数据分析的信息技术服务自动化通知平台设计与实现

文 / 罗霖 罗金平 陈俊宏

随着信息技术的快速发展，信息技术服务帮助台在事件通知、工单管理等方面依靠人工处理的工作模式已不能满足形势所需。为了提升信息技术服务响应速度和智能化水平，本文提出了一种基于大数据分析的信息技术服务自动化通知平台的设计和实现方案，在网络安全和信息技术服务等方面具有实践意义。

一、绪论

（一）研究背景和意义

随着互联网的发展，信息技术服务在学校和企业等各个领域扮演着越来越重要的角色。信息技术服务帮助台是其中的重要组成部分，其主要为用户提供信息技术服务支持。然而，在事件通知、工单管理等方面，信息技术服务帮助台主要依靠人工查询和手动操作等方式进行，存在重复劳动、费时费力、通知延迟等问题，严重影响了服务的工作效率和用户体验。

因此，研究和设计基于大数据分析的信息技术服务自动化通知平台就被提上日程，它能够智能化地执行信息技术服务事件的批量通知，将信息技术支持人员从重复性的劳动中解放出来。

（二）研究目的和内容

本文旨在设计一种信息技术服务自动化通知平台，实现网络安全事件通知自动化。通过此平台，各个领域能够批量导入数据，自动查询用户相关信息，自动生成事件工单，定制通知模板，自动发送消息通知，实时查询进度状态，可以智能化地完成相关基础工作。

二、大数据分析技术应用

信息技术服务自动化通知平台应用大数据分析技术批量处理和分析数据，能够实现事件通知的自动化处理和预测。

在数据采集方面，信息技术服务自动化通知平台能自动识别

源 IP 地址的业务类型，调用各类功能 API 接口，获取数据并将其导入平台中。大数据分析技术能够帮助技术人员更好地采集和识别这些数据，从而减少人为错误，提高数据的准确性和可靠性。

在数据存储方面，技术人员可利用大数据分析技术对采集到的大量数据进行统一存储，从而更好地管理和维护这些数据，以最大限度地发挥数据功能，保证数据的安全性和完整性。

在数据处理方面，技术人员可利用大数据分析技术将海量数据进行汇集和处理，打通各业务数据的壁垒，完成信息技术服务自动化平台的数据统计、归纳、分类，让数据更有价值。

在数据挖掘方面，信息技术服务自动化平台应用大数据分析技术帮助对 IP 地址及分布区域等数据信息、两种或多种数据之间存在的关系、数据量的增减变化等进行关联分析和挖掘，实现网络安全事件的发现和预测。

在数据展示方面，技术人员可以利用大数据分析技术更好地实现数据的可视化，从而更直观地了解数据整体情况和数据分析结果，为管理层和决策层提供依据。

例如，在自动化处理网络安全事件中，当信息技术服务自动化平台用户系统存在弱口令问题整改通知时，技术人员可以及时发现存在系统问题的 IP 地址，自动查询和定位这些 IP 地址的使用者信息，并实现自动批量发送通知，要求其限期整改。在这个过程中，技术人员可以借助大数据分析技术来处理和分析数据。信息技术服务自动化平台能够对相关 IP 地址进行智能分析，自动识别使用者身份信息、联系方式、具体地址以及出现网络安全事件的次数等数据，并发现数据背后的关联情况和规律，进行自动化处理和预测。

信息技术服务自动化平台还可以图表的形式呈现每日或每周自动化通知的处理数量、处理时间、区域位置等信息，从而方便技术人员更直观地了解网络安全事件的发展趋势，为制定和执行网络安全策略提供决策依据。

三、平台功能模块设计——以学校为例

(一) IP 地址源数据获取模块

(1) 信息技术服务自动化平台从网络安全态势感知平台、智能数据安全检测系统、WAF 应用防火墙等安全设备定时获取异常行为的 IP 地址信息。首先，信息技术服务自动化平台通过校园网 IP 地址库对接查询 IP 地址的业务类型，属于有线网络业务的，调用 ITSBM 校园网用户管理系统的 API 获取 IP 地址归属等相关信息；属于无线网络业务的，则调用 SAM+ 无线认证系统的 API 获取 IP 地址归属等相关信息。其次，信息技术服务自动化平台将获取到的数据信息自动导入系统中。

(2) IP 地址源数据获取模块适合批量数据导入，提高数据获取效率，并且支持单一 IP 地址的手工输入方式。

(二) 资源信息模块

资源信息模块主要管理和维护已导入的 IP 地址所归属的校区 / 校园、网络类型、具体地址、有效日期、IP 状态、封禁时间、解封时间等信息，对自动识别的用户信息、加入时间、操作者等数据进行管理和维护，将通知方式（邮件、企业微信）、通知联系阶段、事件工单等信息同步到信息技术服务自动化平台中。

(三) 监测资源更新模块

(1) 监测资源更新模块可以定时（例如每 10 分钟）巡查安全设备的最新 IP 地址，并通过 API 自动获取新增 IP 地址等相关信息，以确保系统中的数据能够得到及时更新。

(2) 监测资源更新模块可以监测工单信息及跟进信息的更新变化，以及处置时间超时、某校园或者 IP 出现次数较多等情况，并提醒该校园的信息技术支持人员及时留意和跟进处置。

(四) 工单信息通知模块

(1) 工单信息通知模块可以选择预设的通知模板，自动将通知信息发送至用户邮件或企业微信。

(2) 工单信息通知模块可以将通知发出后的信息同步至信息

技术服务工单系统中，并自动创建工单，以确保相关人员能够及时跟进工单处理流程。

（五）平台用户管理模块

平台用户管理模块用于管理和维护平台用户账号，为信息技术支持、网络安全管理相关工作人员配置用户账号和赋予相应权限。

（六）汇总展示

（1）信息技术服务自动化平台以图表的形式展示多种统计信息，以便技术人员快速了解和查询相关信息。

（2）信息技术服务自动化平台可以对各校园、时间等多维度的信息进行统计和显示，并展示处理数量和趋势信息等汇总情况。

四、平台技术实现

（一）平台实现

信息技术服务自动化平台采用前后端分离架构设计，由多语言编程实现。前端页面使用 React 框架开发功能模块以及 Axios 与后端进行数据交互，通过编写 JSX 代码来构建 Web 页面的结构和内容。在页面设计中，设计人员可使用 Chakra UI 框架实现页面的响应式布局。

后端应用接口的搭建和逻辑编写则采用 PHP 和 Python 语言来实现。平台使用 Flask 框架构建 Web 应用程序，编写 Python 代码实现各个模块之间的交互和数据传输。另外，MySQL 数据库用于存储 IP 地址等相关信息，通过 PHP 调用数据库 API 实现数据的增删改查等操作。在后端接口安全上，信息技术服务自动化平台可使用 JSON Web Token 对接口进行鉴权保护，避免数据信息泄露。

在数据处理和分析方面，信息技术服务自动化平台采用 Python 语言来实现。信息技术服务自动化平台使用 Pandas、Numpy 等 Python 库实现数据的处理和分析，通过对 IP 地址等信息的监测和分析，对网络安全事件进行自动化处理和预测；在前端使用 ECharts 展示分析结果，方便管理人员整体了解网络安全的状况。

（二）平台应用

信息技术服务自动化平台可广泛应用于各个领域的信息技术服务中，特别适用于网络安全事件的快速响应和处置。例如，在虚拟货币“挖矿”整治活动中，信息技术服务自动化平台可自动化推送通知信息至相关人员：当监测到网络中有设备出现虚拟货币“挖矿”行为时，平台将自动获取 IP 地址等相关信息，并根据拟定的通知模板，自动向相关人员发送通知信息，以便快速响应和处置网络安全事件。

在网络安全事件中，信息技术服务自动化平台可自动化监测和处理事件工单。通过对 IP 地址等信息的监测和分析，平台能够自动创建事件工单，并将工单信息自动推送至相关人员，提高事件处置效率。

除此之外，信息技术服务自动化平台还适用于系统弱口令问题整改通知、VPN 双因子认证通知、用户服务批量通知、网费到期通知等各种通知需求。

五、结语

信息技术服务自动化平台充分发挥了各种编程语言的优势，实现了网络安全事件高效、快速、准确的自动化处理和预测。在数据采集、存储、处理、挖掘和展示等方面，信息技术服务自动化平台可以更好地处理和分析数据，实现数据的自动化处理及快速响应。总之，信息技术服务自动化平台具有广阔的应用前景，在网络安全和信息技术服务等领域具有重要的意义和价值。

参考文献：

[1] 孙培岩 .Python 技术下的网络自动化运维 [J]. 电子世界 ,2021(23):182-183.

[2] 锁泉凝 . 基于 Python 的园区网络自动化运维 [J]. 长江信息通信 ,2021,34(6): 74-75, 78.

[3] 李济伟 , 董耀众 , 王怀宇 , 等 . 基于大数据平台的自动化运维及监控技术研究 [J]. 科技创新与应用 ,2021(11): 152-154.

[4] 宋跃明 , 谢科军 . 基于大数据平台的自动化运维及监控技术研究 [J]. 数字技术与应用 ,2017(6): 102-103.

（本文作者罗霖、罗金平，就职于中山大学网络与信息中心；陈俊宏，就读于中山大学）