交通大数据平台中安全系统建设

张 震[1],李庆杰[2],肖瑞洁[2]
(1.郑州大学 电气工程学院,河南 郑州 450001;
2.郑州大学 信息工程学院,河南 郑州 450001)

摘 要:经过多年来的信息化建设和积累,交通信息资源总量呈指数级增长,大数据带来的安全问题也日益突显。随着智慧交通系统的出现和快速发展,交通大数据已经成为基础性资源,涵盖了大量的敏感信息,此类信息一旦泄露被非法使用,将给用户的安全带来巨大威胁。交通大数据平台用于采集、管理交通大数据,获得了大量交通信息数据,因此存在信息丢失与泄露、被不法分子非法访问、恶意攻击等风险。文章分析了交通大数据平台中存在的安全隐患,对交通大数据平台中的安全系统建设进行了深入探究,基于纵深防御体系原理,提出了包括物理安全、网络安全、数据安全、管理安全等方面的安全系统建设,发现并阻断来自互联网的恶意网络扫描和攻击行为,规避了一系列信息安全风险,保障了交通大数据平台上各业务的安全运行。

关键词:大数据;智慧交通;安全系统;大数据平台;管理安全
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2021)10-0093-05
doi:10.3969/j.issn.1673-629X.2021.10.016

Safety System Construction in Traffic Big Data Platform

ZHANG Zhen[1],LI Qing-jie[2],XIAO Rui-jie[2]
(1.School of Electrical Engineering,Zhengzhou University,Zhengzhou 450001,China;
2.School of Information Engineering,Zhengzhou University,Zhengzhou 450001,China)

Abstract:After years of information construction and accumulation,the total amount of traffic information resources has grown exponentially,and the security problems brought about by big data have become increasingly prominent. With the emergence and rapid development of smart transportation systems,transportation big data has become a basic resource,covering a large amount of sensitive information. Once such information is leaked and used illegally,it will pose a huge threat to the safety of users. The traffic big data platform is used to collect and manage traffic big data and obtain a large amount of traffic information data. Therefore,there are risks of information loss and leakage,illegal access by criminals and malicious attacks. We analyze the hidden dangers in the traffic big data platform,and conduct an in-depth exploration of the security system construction in the provincial traffic big data platform. Based on the principle of the defense-in-depth system,the security system construction,including physical security,network security,data security,management security,is proposed to detect and block malicious network scanning and attack behavior from the Internet,avoiding a series of information security risks,and ensuring the safe operation of all services on the traffic big data platform.

Key words:big data;intelligent transportation;security system;big data platform;management safety

0 引 言

自智慧交通提出以来,经过多年来的信息化建设和积累,交通运输行业积累了大量的数据资源,交通信息资源总量呈指数级增长,现代信息技术的发展为处理交通产生的数据提供了契机。在大数据技术的支持下能够为各类交通安全问题的分析和解决提供重要的数据参考支持,从而提升智慧交通发展的有序性和协调性。但是从当前发展实际情况来看,智慧交通中大数据的应用在数据信息收集、数据信息存储、数据信息应用等方面仍然存在一些安全等方面的问题[1]。

在国外,智慧交通的概念提出较早,欧美等国的城市交通基础设施建设在当地被高度看重,并已经基本完备,在此基础上,发达国家开展了一系列的智能交通信息系统搭建,用以实现交通数据的采信、整理、共享、

收稿日期:2020-10-20 **修回日期**:2021-02-25
基金项目:河南省中长期和"十四五"科技规划重大战略研究专题(202400410017);2019年河南交通运输厅科技计划项目(20190335A)
作者简介:张 震(1966-),男,教授,博士,研究方向为多媒体信息安全、信息与通信工程;李庆杰(1996-),女,硕士,研究方向为计算机应用、网络空间安全。

应用,以推动交通有序运营,促进社会民生的全面发展[2]。然而,在大量的交通数据应用中,往往容易忽视对数据的预处理研究[3],导致数据冗杂,因此,大数据带来的安全问题也层数不穷,但是国内外对安全系统的建设还不够完备,需要专门建设面向交通大数据的安全系统。

文中对交通大数据平台中的安全系统建设进行了深入探究,综合交通服务大数据平台部署于政务专有云平台,物理层、网络层、主机层复用云平台提供的安全防护策略即可。安全系统主要从应用和数据方面加强安全防护,为部署于综合交通服务大数据平台(政务专有云机房、通信中心机房)各类业务应用提供基础的安全运行保障环境。交通通信中心是全交通运输行业交通专网汇聚节点,其网络安全对政务专有云平台至关重要,遵循国家等级保护相关政策、标准,文中对通信中心网络汇聚节点环境参照三级等保相关要求进行建设,构建从网络边界到内部网络分区的纵深防御体系。

1 安全隐患及设计目标

1.1 安全隐患

交通大数据平台在进行网络接入时存在遭受 DDoS 攻击的风险,无法控制试图非法登录访问数据的用户;移动网络忙接入过程中,大数据平台的数据可能遭到非法登录用户的访问,目前手持、移动设备需要接入较多,试图非法登录访问数据的用户无法控制。另外,虚拟化技术的应用使传统物理安全边界缺失。

交通大数据涵盖了大量的信息,其中不乏一些敏感信息,这些信息在集中存储的过程中容易出现泄露问题,泄露的数据信息一旦被非法使用则会对用户的信息安全带来威胁。另外,在庞大的数据量影响下,对敏感数据信息的界定也没有统一的标准,信息安全性得不到保障[4]。

各专业系统(如车辆、信号、通信、线路、BAS 等)均通过自身的管理软件进行业务监控。并未形成多专业联动监控。而且目前的信息技术及平台只能通过定时抽取、推送等方式实现信息贯通,造成业务信息滞后,风险监控不及时,引发业务安全风险和监管隐患[5]。大数据技术可以对内容进行翔实的分析,从而可以判断内容的真实性。但需要注意的是,城市交通信息涉及多个层面的隐私,具有保密性强的特点。居民个人、企业数据的安全和隐私存在泄漏的风险[6]。

1.2 设计目标

贯彻落实《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》(国发〔2012〕23 号),建立和完善交通运输行业网络与信息安全信息管理机制,保障行业网络和信息系统安全运行及业务正常开展。大数据平台应满足如下要求:

(1)贯彻落实国家有关部门信息安全等级保护工作要求,全面完善交通运输行业信息安全防护体系,确保等级保护顺利实施。

(2)根据部署于大数据平台的各业务系统各层面的共性和个性化安全保障需求,大数据平台安全体系参照国家安全等保三级建设共性需求。

(3)基于“策略、防御、检测、响应”(P2DR)的闭环控制动态网络安全模型,构建从边界到内部的纵深防御体系(IATF)。

(4)自云计算被提出以来,云计算技术带来诸多数据安全风险,考虑到可能出现的信息丢失与泄露、共享技术漏洞、不安全的应用程序接口等问题,设计相应的安全保护措施,明确相应信息安全责任。

(5)数据库作为数据存储的关键技术,对于数据库中的重要数据要做加密处理,用户密码等关键信息要加密存储。

2 安全系统总体架构

2.1 安全运行环境

(1)政务专有云平台通过安全域的划分和云盾技术的安全能力,实现防护来自互联网的 DDoS 攻击,发现并阻断来自互联网的恶意网络扫描和攻击行为;当云服务器向互联网发送恶意流量,对外发起 DDoS 攻击时,网络入侵防护系统有效识别云服务器的上述异常行为,开启自我防护功能;提供包括密码暴力破解、网站后门检测和处理、异地登录提醒等反入侵服务;提供 Web 漏洞检测、网页木马检测等服务,有效保障云平台的数据安全。

(2)通信中心配置 2 台下一代防火墙(核心)、2 台下一代防火墙(汇聚)、6 台千兆防火墙、1 套数据库审计系统、1 套终端安全管理系统(许可数量为 500 个终端)、1 套运维审计系统(堡垒机)、1 套安全隔离与信息交换系统。

综合交通服务大数据平台安全系统逻辑示意图如图 1 所示。

2.2 管理体系

“三分技术,七分管理”,从技术角度出发的安全方案必须有与之相适应的管理制度同步制定,系统方案的可操作性要从管理等多方面的角度去评估。

管理体系包括 1 项安全现状调研与风险评估、1 项等级保护管理体系建设、1 项等级保护体系宣贯,部署了云安全管理、云资源管理系统等的管理服务器,以实现对网络、安全、主机存储、数据等状态监控和管理,确保系统安全性。

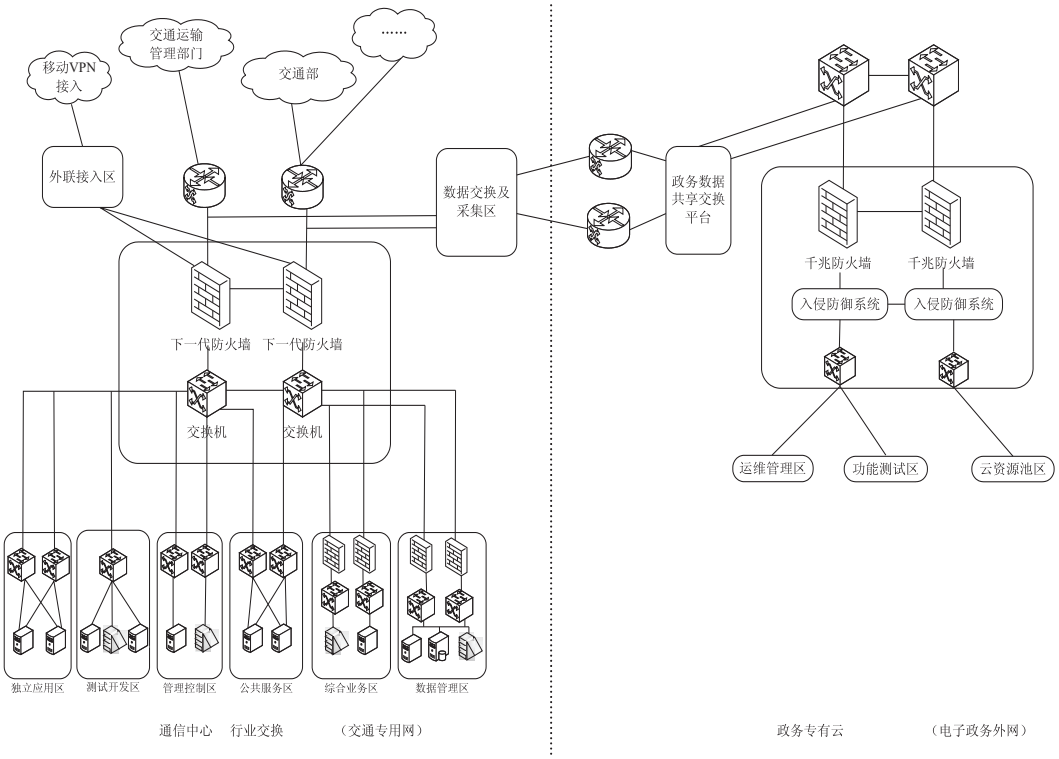

图 1　综合交通服务大数据平台安全逻辑框架示意图

3　技术体系

网络与信息安全是一项复杂的工程,从结构上来说涉及到物理、网络、主机、应用、数据等多个层面,采用“综合防范”的措施,通过多种手段或技术来综合实现安全防范。基于以上纵深防御体系原理,大数据平台安全防御体系依据由互联网进入内部数据处理流程,按照“控制、检测、防御、管理、审计”等思路,网络从边界到内部部署防火墙、IPS、防病毒系统、漏洞扫描系统、安全审计等技术手段,来实现在网络、主机、应用等层面建立起安全防御体系。

3.1　政务云平台

政务专有云平台安全系统采用信息安全等级保护三级建设,主要安全方案包括访问控制、接入控制、安全组防火墙和 VPC 隔离。

通过安全域的划分和云盾技术的安全能力,实现防护来自互联网的 DDoS 攻击,发现并阻断来自互联网的恶意网络扫描和攻击行为;当云服务器向互联网发送恶意流量,对外发起 DDoS 攻击时,网络入侵防护系统有效识别云服务器的上述异常行为,自动进行防护[7-8];有效保障云平台的数据安全。具体安全系统如表 1 所示。

表 1　云平台安全系统

序号	总体要求	安全需求	安全措施
1	云防护	防 DDoS 攻击	云盾防 DDoS 模块
2		安全隔离及访问控制	边界防火墙
3		恶意代码防护	云盾安骑士+防毒系统
4		远程接入安全	堡垒机+SSL VPN
5		网页防篡改	网页防篡改系统
6	云检测	入侵检测	云盾管控+入侵防御系统
7		漏洞扫描	漏洞扫描软件
8	云审计	启用安全审计功能	云盾云组件
9		集中管控和运维审计	堡垒机
10		集中分析	云盾管控平台
11	云恢复	本地和异地数据备份恢复	云平台本地备份+异地
12		关键组件冗余	云平台组件
13		剩余信息保护	云平台组件

3.2 物理安全

按照《信息系统安全等级保护基本要求》,物理安全方面涉及物理位置的选择、温湿度控制、防盗和防破坏、物理访问控制等,属于信息系统运行所需公共基础条件,因此,本着就高原则,物理安全方面满足《信息系统安全等级保护基本要求》中三级要求。

现阶段物理安防技术很多种类都已应用到计算机中,它在计算机中所起到的作用是维护网络链路的安全,这样自然因素或是人为因素对计算机所造成的破坏程度就会相应降低[9]。物理安全防护技术应用在交通大数据平台安全系统上,对用户身份以及进入权限进行严格的验证,用户信息在最大程度上得到了保障。

3.3 网络安全

按照《信息系统安全等级保护基本要求》网络安全方面涉及结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等。根据大数据平台安全域划分,结合各分区系统定级,本次工程按照信息系统安全等级保护三级要求进行网络安全防护。

综合分析信息系统安全等级保护三级对于网络安全的防护要求,文中分别从边界访问控制、网络入侵防护、安全审计、日志审计、恶意代码防范、边界完整性保护、协议过滤管理、网络设备安全配置等方面进行防护。

运用自主访问控制的方式,依据安全策略,严格控制主体对客体的访问。自主访问控制的覆盖范围包括与信息安全直接相关的主体、客体以及它们之间的操作;其粒度达到主体为用户级,客体为文件、数据库表级。在该方式下,由授权主体设置对客体访问和操作的权限,严格限制默认用户的访问权限。通过计算信任度,确认用户的信任安全问题,以防不法分子对网络的恶意攻击。

安全审计针对来自内部的网络安全威胁,覆盖到服务器上的每个操作系统用户和数据库用户,记录系统内安全的重要相关事件,包括网络数据采集、协议解析、日志分析等内容。网络数据采集系统采用分布式结构,将多个采集设备分配到一个中间汇聚服务器上,形成一个小的局域网,设置一个总的中央管理服务器对多个中间汇聚服务器进行汇总分析;日志分析采用基于数据挖掘的分析方法,将聚类分析和关联规则挖掘应用在日志分析中,从大量日志文件中提取重要信息,以实现对网络内容的深度解析。通过安全审计,网络数据采集的内容可以长期保存,有利于对过往的攻击事件进行追溯、分析以及反向追踪,为恶意行为的追查和追踪提供依据。

将入侵检测技术应用于系统,检测是否存在非法入侵和滥用网络等行为。其中,入侵检测主要运用了签名分析法检测计算机网络系统运行薄弱区域的攻击行为,从而防止不法分子的网络攻击。

恶意代码防范包括检测、识别和清除三个步骤。恶意代码攻击系统或数据时,启用数字免疫系统,及时发现并定位恶意代码,识别出代码的具体类型,进行屏蔽和清除。

网络与信息安全是一项复杂的工程,从结构上来说涉及到物理、网络、主机、应用、数据等多个层面,采用“综合防范”的措施,通过多种手段或技术来综合实现安全防范。在已有的安全技术的基础上,制定系统安全策略、设立安全机制、建立完善的防御体系,以抵御来自各方的网络攻击,达到维护网络安全的目标。

3.4 数据安全

实现数据安全性,要保障数据保密性、可用性和完整性[10]。

通过生产中心磁盘阵列[11-12],来构建“同城两中心”的备份架构,满足安全等保三级数据备份与恢复的要求。大数据平台建设考虑内、外网均部署有较多的业务系统,同时内外网之间有较频繁的、实时性强的数据的交互,采用高性能防火墙代替网闸,即采用逻辑隔离方式实现通信中心与政务专有云平台之间的隔离。

大数据平台安全防御体系依据由互联网进入内部数据处理流程,按照“控制、检测、防御、管理、审计”等思路,网络从边界到内部部署防火墙、IPS、防病毒系统、漏洞扫描系统、安全审计等技术手段,来实现在网络、主机、应用等层面建立起安全防御体系。

通过过滤 IP 和 MAC 地址机制,防止非法认证;对于交通大数据平台中敏感的系统管理数据和敏感的用户数据采用加密措施实现存储保密性,AES 密钥加密技术,采取定期更新密钥机制,为整个数据安全系统提供更加强大的安全防护。

针对大数据平台收集到的数据,个人要认识到数据安全的重要性,形成正确的信息安全防护意识,提高自我防护能力,从而提升数据保密性能。工作人员要认识到人员操作的重要性,通过约束、规范用户的操作,提升计算机信息系统的安全防护水平[13]。建立数据甄别、筛选机制,严格保护好隐私信息。交通大数据涉及大量信息,通过设置数据访问权限,防止信息泄露,严格建立数据安全机制[14]。

3.5 安全管理中心

按照《信息系统安全等级保护基本要求》及交通运输部下发的安全事件上报要求,交通专网复用通信中心现有安全管理平台(SOC),由其作为综合安全防护系统,需要对出现的事件进行综合分析,并把紧急修

订的措施及时下发执行,对不同的安全设备进行安全管理,与日志收集系统有效结合,实现对系统风险、系统脆弱性和系统安全事件的收集分析,集中化的监控、审计、预警、响应、报告。安全管理中心的架构如图 2 所示。

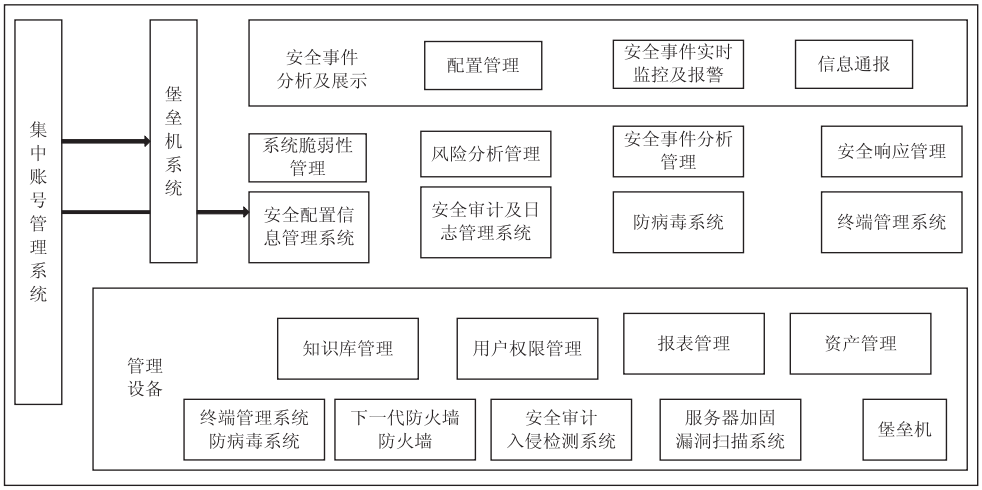

图 2　综合交通服务大数据平台安全管理中心

安全管理平台包括:集中账号管理系统、系统脆弱性管理系统、风险分析管理、内控堡垒主机系统、防病毒及终端管理系统、安全配置信息管理系统、安全事件管理、安全响应管理等功能。

安全管理体系依托大数据平台构建的安全管理中心,建立基础信息库,实现统一的安全集中管理功能与机制,通过安全管理中心定期生成综合性报表或报告,为总体安全管理决策和安全制度的完善提供科学依据,从而形成安全联动机制以及动态的综合安全效能,使得大数据平台的安保体系的各部分有机联系在一起,实现安全管理的规范化、流程化、体系化。

安全管理体系同时需要相关的机构、制度、流程等做基础,因此需要构建交通运输厅信息安全管理机构、信息安全管理人员、信息安全管理制度、业务系统安全管理、系统运维管理等来保障对业务系统的安全技术手段的实现。

4　结束语

在智慧交通快速发展的背景下,为避免来自互联网的恶意网络扫描和攻击行为,保障交通大数据平台上各业务的安全运行,最终建成了健壮、自主可控的交通大数据平台中的安全系统。安全系统通过构建从网络边界到内部网络分区的纵深防御体系,为交通大数据平台提供了全面的安全服务,对保证交通数据安全具有重要意义。

参考文献:

[1] 倪志云. 智慧交通大数据应用及相关问题研究[J]. 中国新通信,2019,21(19):101-102.

[2] 邵志骅,崔林山,卢梦奇. 基于 Hadoop 集群的公安交通信息云共享技术应用研究[J]. 中国公共安全:学术版,2016(1):65-69.

[3] 彭　晨. 物联网技术在城市交通网络中的应用分析[J]. 河南科技,2020,39(32):29-31.

[4] 林　珠,吴佩珊. 面向交通大数据的智能处理平台建设研究[J]. 计算技术与自动化,2017,36(3):114-117.

[5] 姜子旺. 大数据技术在城市轨道交通运营管理中的应用[J]. 科技创新与应用,2020(5):174-175.

[6] 曾联进. 基于大数据的城市智能交通系统设计研究[J]. 智库时代,2019(35):281-282.

[7] SINGH K J,HAOKIP J,CHANU U S. A novel approach to develop and deploy preventive measures for different types of DDoS attacks[J]. International Journal of Information Security and Privacy,2020,14(2):1-19.

[8] FUJINOKI H. Layered migrating overlay for effectively sieving internal DoS/DDoS attackers-its designs and effectiveness[J]. Journal of Network and Information Security,2018,1(6):1-11.

[9] 闫　雪. 计算机信息安全技术及防护研究[J]. 科学技术创新,2019(32):73-74.

[10] 史　歌,刘婷婷,高　琳,等. 大数据平台下城市轨道交通信息系统建设[J]. 微型电脑应用,2020,36(2):35-38.

[11] LE Q,AMER A,HOLLIDAY J. RAID 4SMR:RAID array with shingled magnetic recording disk for mass storage systems[J]. Journal of Computer Science and Technology,2019,34(4):854-868.

[12] BARZEGAR-PARIZI S. Graphene-based tunable dual-band absorbers by ribbon/disk array[J]. Optical and Quantum Electronics,2019,51(6):167.

[13] 苏百宪,黄稳稳. 大数据视域下计算机信息安全及防护方法探析[J]. 网络安全技术与应用,2020(3):2-3.

[14] 陶　韬. 大数据视角下的济南交通治理研究[D]. 济南:山东大学,2019.