本文引用格式：张红金.基于云平台环境下的数据信息安全探究[J].自动化与信息工程,2023,44(2):48-51;58.
ZHANG Hongjin. Research on data information security based on cloud platform[J]. Automation & Information Engineering, 2023,44(2):48-51;58.

基于云平台环境下的数据信息安全探究

张红金
（工业和信息化部电子第五研究所/
基础软硬件性能与可靠性测评工业和信息化部重点实验室，广东 广州 510610）

摘要：随着网络技术的高速发展，数据信息呈爆发式增长，在带给人们诸多便利和商业机遇的同时，也增添了更大的数据信息安全风险，既有的安全防护技术已无法完全满足现阶段的安全需求，尤其是云平台时代，需要探究安全性更高的防护策略。该文基于入侵检测技术，提出容忍入侵检测的技术概念，在容忍入侵检测模型中增添容忍入侵单元，设计容忍入侵改进方案，使系统遭受攻击时，仍能继续提供部分或全部服务，这对构建云平台时代数据信息的安全机制，具有一定的指导意义。

关键词：云平台；数据信息安全；入侵检测技术；容忍入侵检测

中图分类号：TP393.4　　**文献标志码：**A　　**文章编号：**1674-2605(2023)02-0009-05

DOI：10.3969/j.issn.1674-2605.2023.02.009

Research on Data Information Security Based on Cloud Platform Environment

ZHANG Hongjin
(The 5th Electronics Research Institute of the Ministry of Information Industry of China / The Ministry of Industry and Information Technology Key Laboratory of Performance and Reliability Testing and Evaluation for Basic Software and Hardware, Guangzhou 510610, China)

Abstract: With the rapid development of network technology, data information is growing explosively, bringing people many conveniences and business opportunities, but also adding greater data information security risks. Existing security protection technologies can no longer fully meet the current security needs, especially in the era of cloud platforms. It is necessary to explore higher security protection strategies. This article proposes the concept of tolerant intrusion detection based on intrusion detection technology, adds tolerant intrusion units to the tolerant intrusion detection model, and designs an improvement plan for tolerant intrusion, so that when the system is attacked, it can still provide some or all services. This has certain guiding significance for building a security mechanism for real-time data information on cloud platforms.

Keywords: cloud platform; data information security; intrusion detection technology; tolerance intrusion detection

0 引言

随着网络技术的高速发展，大量的数据信息给人们生活、工作带来较大的影响，如新冠肺炎疫情防控期间，疫苗接种、核酸检测记录等数据信息为全面科学防疫工作贡献巨大。但共享资源在网络上日趋扩大的开放性，为机密信息与个人隐私信息的泄露、黑客攻击、计算机病毒等安全问题带来更多风险，也为网络风险管理带来更大的挑战。同时，由于数据信息类型多样，既有纯文本、图形图像信息，又有音频视频等信息；既有结构化的信息，也有非结构化的信息，这也给数据信息的存储及管理造成了一定程度的混乱，甚至可能引发网络的安全漏洞等风险。为了充分保障数据信息的安全性、完整性，目前采取的安全防

AUTOMATION & INFORMATION ENGINEERING

护措施主要有加密、认证、授权、签名以及防火墙等技术。虽然可通过多种预防措施尽可能地避免外部风险，但操作系统、数据库、信息系统等本身存在的漏洞或缺陷，给网络系统被入侵、被病毒感染增加一定的风险。

为保障数据信息的安全，本文引入容忍入侵技术。当数据信息遭受入侵时，采取容忍入侵策略达到容忍入侵的目的，避免数据信息失效。

1 云平台的涵义

云平台目前尚未有统一或标准的定义。大多数研究人员认为，云平台是基于网络提供的相关数据信息，采用虚拟技术，由软、硬件搭建而成的构架，采用整合分布式计算资源形成协同工作的计算模式，为用户提供所需服务[1]。在云平台环境下，用户根据自身需要向云计算供应商提出需求申请并付费，可获得自身所需的计算、数据信息等服务。云平台的主要功能包括：1） 接口登录功能，用户可以正常登录云平台；2） 申请响应功能，针对用户的需求申请，快速做出响应，并为用户提供资源库中对应的可用资源；3）角色响应功能，在门户网站界面，通过角色 Web 模式对用户需求自动响应；4） 监视功能，实时在线监视资源的使用状况；5） 编辑功能，用户既可根据自身需要更改操作系统、增添应用软件等，还可设置服务器数量、配置虚拟机资源等。云平台管理架构如图 1 所示。

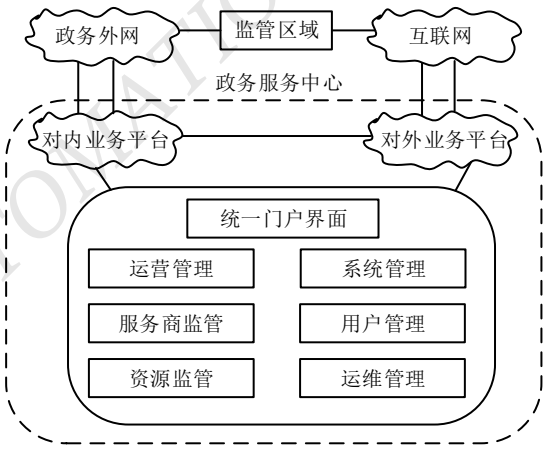

图 1 云平台管理架构

云平台管理是云平台管理内外业务的核心部分，具有监管、调度、运维等功能，由运营管理、系统管理、服务商监管、用户管理、资源监管、运维管理等 6 大功能模块组成。其中，资源监管模块较为重要，负责管理云平台资源的配置、运行、报警及故障分析、虚拟机的动态分配等。

2 云平台环境下的数据信息安全

目前，云计算、大数据、物联网等技术已成为学术界、产业界研究的热点，尤其是大数据的广泛应用，对信息技术及产业发展产生不可估量的影响[2-4]。另外，频繁发生的网络攻击事件，也使人们的关注点集中到网络信息安全上，只有保障大数据环境下的网络安全，才能避免网络数据免受侵害[5]。

2.1 数据信息安全防护

数据信息安全集中体现在数据信息泄漏和数据信息破坏 2 个层面。其中，数据信息泄漏是指未经授权的用户非法访问、截取授权范围外的数据信息；数据信息破坏分为有意和无意 2 种情况，有意破坏是指非法操作破坏或主动攻击，无意破坏是指数据信息使用过程中感染了病毒，对数据进行无意的修改、删减等操作，严重影响数据的一致性、正确性等[6-7]。数据信息安全就是保护数据信息的机密性、完整性、可用性等，可归纳为 3 个发展阶段：1） 防御技术阶段，主要包括防火墙、密钥、控制访问、认证等技术保护策略；2） 入侵检测阶段，主要包括日志和模式匹配保护策略；3） 容忍入侵检测阶段，经过前两个阶段的防护后，在发生入侵的情况下，系统或网络仍能继续提供部分甚至全部的服务。安全防御的 3 个发展阶段如图 2 所示。

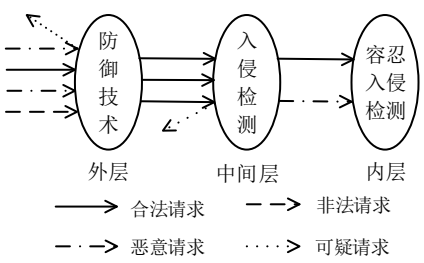

图 2 安全防御的 3 个发展阶段

AUTOMATION & INFORMATION ENGINEERING

2.2 安全防御策略

云平台环境下，数据信息的安全防御策略有：1）定期或随机对系统进行扫描杀毒，发现漏洞立即修补并查杀病毒；2） 完善网络安全、主机系统安全、信息安全等计算机安全体系；3） 建立完善的访问控制机制，用户仅能在自己的访问权限内使用、操作数据信息；4） 为防止计算机系统、网络故障等突发事件造成数据丢失，用户需及时备份数据，且重要数据要加密处理；5） 主动防范网络病毒，实时在线监测网络。基于上述安全防御策略，安装最新版本的杀毒软件，建立良好的防御体系，对网络病毒实行预先防御措施。但即使安装了杀毒软件，也不可能完全避免云平台网络的病毒入侵行为，这仅是数据信息的首道安全防线。

2.3 防火墙功能

防火墙布置于内网与外网之间，在网络连接处设置安全控制点，对进、出入内网的服务与访问实行审计和控制，保护内网免受外网非法入侵[8-9]。防火墙功能示意图如图 3 所示。

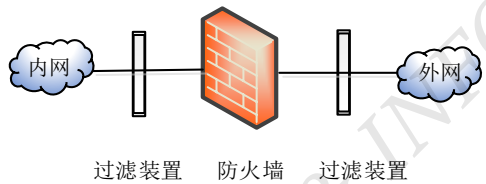

图 3 防火墙功能示意图

防火墙具有访问控制、记录与统计网络数据信息、禁止数据非法使用、保护脆弱以及执行策略等功能；其既能监控所有的信息访问与通信，还能通过配置策略设置对应的保护级别，切实保障系统安全。

2.4 入侵检测

入侵检测是指搜集网络系统、服务器、主机中可疑的访问数据，根据一定规则判断这些数据是否存在违反安全协议的行为；是防火墙的有益补充，协助防火墙进一步增强网络系统的安全管理。

3 入侵检测技术分类

根据入侵行为的特征，可将入侵检测技术按检测技术、检测数据来源 2 个维度进行分类。

按检测技术可分为异常入侵检测和模式匹配检测。1） 异常入侵检测技术主要通过入侵事件波及的范围、历史档案、各种活动状况等，判断入侵事件是否属于正常范畴。若发现入侵事件异于正常范畴，如网络流量异常，则初步判断这一活动可能属于入侵行为。该检测技术的局限性在于很难确保事件范围与历史档案一致，容易被误认为异常事件。2） 模式匹配检测技术用特定模式表示入侵行为，并与正常模式匹配比较。若不匹配，可能被认定为入侵事件。该检测技术的局限性主要体现在较难设计科学的匹配模式。

按检测数据来源可分为基于主机入侵检测、基于网络入侵检测、基于分布式入侵检测 3 类。1） 基于主机入侵检测，通过分析主机的审计日志，监视主机的网络及其连接，一旦发现与日志不一致的可疑状况，入侵检测系统立即采取防护措施。2） 基于网络入侵检测，检测经过网络的数据信息流与数据包，包括系统中流过不同网段的数据信息流与数据包，对任何可疑的数据包进行分析、判断以及处理等。3） 基于分布式入侵检测，将基于主机入侵检测和基于网络入侵检测有效结合，组建一种新的交叉检测技术，既能根据审计日志发现入侵行为，又能从网络中的数据信息流与数据包检测出入侵信息[10]。上述 3 种入侵检测技术比较如表 1 所示。

表 1 3 种入侵检测技术比较

比较内容	入侵检测数据来源分类		
	基于主机入侵检测	基于网络入侵检测	基于分布式入侵检测
检测范围	主机	特定设置网段	整体包括服务器
检测对象	审计日志	数据信息流、数据包	多台服务器
操作系统	依赖主机	不依赖主机	依赖服务器
硬件布置	一台主机	不同主机	多台主机
系统开销	大	小	很小

一般情况下，基于网络入侵检测的误报率偏高，而基于主机入侵检测的误报率较低，主要原因是主机

AUTOMATION & INFORMATION ENGINEERING

上的指令序列比网络上的信息流简单。即使系统发生故障，基于网络入侵检测也不会影响系统的正常运行。

4 容忍入侵技术

容忍入侵是指网络或系统在受到入侵攻击或发生报错时，其部分功能甚至全部功能仍可继续运行、提供服务。需要说明的是，容忍系统中原有的脆弱点并不会完全修复，受影响功能的性能会有一定程度地下降。基于容忍入侵检测模型的架构体系如图4所示。

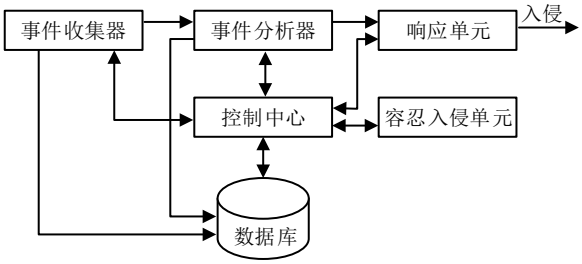

图 4 基于容忍入侵检测模型的架构体系

1）事件收集器，收集信息但不处理信息。首先，收集服务器、网络中的数据信息；然后，将收集的数据信息整理归类，转换为既定模式；最后，按规定格式发送给事件分析器。事件收集器与外部数据直接交互，在一定程度上起到了缓冲作用。

2） 事件分析器，利用算法分析事件收集器收集的数据信息，并将分析、处理的结果发送给响应单元。同时对攻击事件做出响应。

3） 数据库，主要存储事件收集器收集的数据信息与事件分析器分析的结果信息。数据信息分析采用以关系数据库为主的模式，既包括结构化的数据，也包括半结构化的数据，均使用结构化语言形式描述，最大程度地保证数据信息安全。

4） 控制中心，主要负责系统审计和系统监控等功能，还可提供收集网络、主机和状态信息的服务以及策略处理服务[11]。

5） 响应单元，当主机、网络出现异常事件时，根据处理策略做出相应的响应，把其他未记录到日志中的数据信息发送给容忍入侵单元处理，控制中心发出报警指令，监管系统执行报警指令。

6）容忍入侵单元，入侵数据进入容忍入侵单元，会对系统发起攻击，容忍入侵单元把需要保护的系统和数据进行还原甚至重构，将攻击节点转移到安全状态，即使受到攻击也能持续提供服务，其工作原理如图5所示。

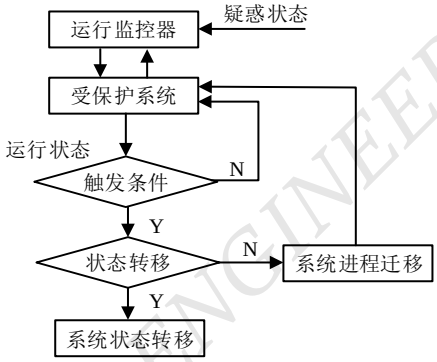

图 5 容忍入侵单元工作原理

运行监控器实时监控各关键部件的运行状态，如遇可疑情况，立即采取对应的安全管理策略，未达到触发条件前，继续完成既定的服务；达到触发条件立即进入转移状态。系统在算法的控制下转移到对应的状态，达到恢复正常状态的目的。

容忍入侵技术的优势：1） 更有效防护并阻止数据信息被攻击；2） 可以检测出攻击事件并能预估其造成的破坏程度；3） 一旦遭受攻击，可充分保障且能恢复数据信息中的关键部分。

5 结束语

随着互联网的高速发展，云平台中的数据信息量急剧陡增，增加了数据信息泄露的风险，同时也给网络恶意攻击提供了可乘之机[12-13]。目前，云计算已广泛应用于人们工作与生活的多个方面。云平台环境下，诸多的数据信息具有一定的关联性。如果网络信息安全防护措施不完善，将严重影响整个网络数据信息的安全。为此，需要加强网络信息安全的防护，采取多种防护措施，确保网络数据信息的安全。本文研究在网络攻击方面有一定的进展和成效，但在其他安全方面还需要进一步完善预防手段，确保云平台中数据信息在复杂的网络环境中更加安全。

（下转第 58 页）

AUTOMATION & INFORMATION ENGINEERING

Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017,40(4):834-848.
[20] 杨兵,刘晓芳,张纠.基于深度特征聚合网络的医学图像分割[J].计算机工程,2021,47(4):187-196.
[21] HU Yueyu, MA Zhan, YANG Wenhan, et al. Learning end-to-end lossy image compression: a benchmark[J]. IEEE Trans Pattern Anal Mach Intell, 2021.
[22] SONG Myungseo, CHOI Jinyoung, HAN Bohyung. Variable--rate deep image compression through spatially-adaptive feature transform[C]. International Conference on Computer Vision, Virtual Event, Montreal, QC, Canada, 2021:2360-2369.
[23] ISLAM K, DANG L M, LEE S, et al. Image compression with recurrent neural network and generalized divisive normalization[C]//CVPR, 2021:1875-1879.
[24] WANG X, YU K, DONG C, et al. Recovering realistic texture in image super-resolution by deep spatial feature transform [C]//CVPR, 2018:606-615.
[25] SZEGEDY C, VANHOUCKE V, IOFFE S, et al. Rethinking the inception architecture for computer vision[C]//CVPR, 2016:2818-2826.

作者简介：

张娅玲，女，1997 年生，硕士研究生，主要研究方向：信号处理。E-mail: 2635145995@qq.com

周松斌（第一通信作者），男，1978 年生，博士研究生，研究员，主要研究方向：智能传感。E-mail: sb.zhou@giim.ac.cn

庞锟锟，男，1991 年生，博士研究生，主要研究方向：机器学习。E-mail: kk.pang@giim.ac.cn

廖奕校，男，1992 年生，博士研究生，主要研究方向：装备故障诊断与智能运维。E-mail: yx.liao@giim.ac.cn

袁飞，男，1984 年生，博士研究生，讲师，主要研究方向：智能感知、智能数据处理。E-mail: eric_f_y@foxmail.com

张寿明（第二通信作者），男，1966 年生，博士研究生，教授，主要研究方向：复杂工业过程控制系统。E-mail: 1411834974@qq.com

（上接第 51 页）

参考文献

[1] 段昌淼.数据云平台技术研究与建设探讨[J].网络安全与信息化,2022(11):62-65.
[2] 慕慧娟,郑云林,塔依尔·斯拉甫力.智慧停车场在线计量云平台分析与设计研究[J].中国测试,2021,47(4):124-129.
[3] 李文迪,陈华伟,伍权,等.设备上云技术研究现状与展望[J].机床与液压,2020,48(15):194-198.
[4] 刘小梅,唐鑫,杨舒婷,等.基于 Reed-Solomon 编码的抗边信道攻击云数据安全去重方法[J].信息安全学报,2022,7(6):80-93.
[5] 张红金,刘维.国产云平台安全体系策略探究[J].自动化与信息工程,2022,43(2):23-28.
[6] 荣喜丰.云计算网络环境下的信息安全研究[J].网络安全技术与应用,2021(7):83-84.
[7] 李慧芹,吕静贤,王慧,等.网络监听技术下的网络安全平台设计[J].机电工程技术,2022,51(8):153-155;244.
[8] 刘隐.云计算网络环境下的信息安全问题探讨[J].电脑知识与技术,2021,17(18):64-65.
[9] 赵宏,常有康,王伟杰.深度神经网络的对抗攻击及防御方法综述[J].计算机科学,2022,49(S2):662-672.
[10] 张勇,郭骏,刘金波,等.调控云平台 IaaS 层技术架构设计和关键技术[J].电力系统自动化,2021,45(2):114-121.
[11] 齐祥柏,陈青,赵洪岗.工业控制系统信息安全问题探讨[J].机电工程技术,2021,50(12):180-182.
[12] 王承明,白连万,王健,等.基于云平台的计算机公共实验教学中心建设的研究与实践[J].实验技术与管理,2020,37(11):269-272.
[13] 谈永奇,王换换,阳媛,等.基于智能化集成设备的医院大数据信息化云测试系统设计[J].计算机测量与控制,2020,28(8):98-101.

作者简介：

张红金，男，1976 年生，本科，高级工程师，信息系统项目管理师，主要研究方向：软件测试、信息系统安全研究、科研项目管理及质量管理。E-mail: zhanghongjin@ceprei.com

AUTOMATION & INFORMATION ENGINEERING