专题：内生安全

基于拟态架构的内生安全云数据中心关键技术和实现方法

张帆[1]，谢光伟[2]，郭威[1]，扈红超[1]，张汝云[3]，刘文彦[1]
（1. 国家数字交换系统工程技术研究中心，河南 郑州 450002;
2. 复旦大学计算机科学技术学院，上海 201203；3. 之江实验室，浙江 杭州 311121）

摘　要：云数据中心是新一代信息基础设施的代表，其安全问题也成为近年来备受关注的焦点，具有重要的意义。首先，在对现有云安全形势分析的基础上，通过新兴的内生安全概念探索云数据中心的安全架构、关键技术和实现方法，期望利用拟态构造设计解决现有防护手段难以处理的漏洞、后门等内生安全问题。其次，提出了一种云数据中心内生安全架构与相关关键技术实现构想，同时给出了现有云平台系统拟态化改造的模式与技术趋势。未来，基于拟态架构的内生安全云数据中心或将为新一代信息基础设施建设提供有效的安全解决方案，进而加速云化服务模式的应用与推广。

关键词：内生安全；云数据中心；拟态构造；拟态化改造模式与趋势
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000－0801.2021056

Key technologies and implementation methods of endogenous safety and security cloud data center based on mimic architecture

ZHANG Fan[1], XIE Guangwei[1], GUO Wei[2], HU Hongchao[1], ZHANG Ruyun[3], LIU Wenyan[1]
1. China National Digital Switching System Engineering&Technological R&D Center, Zhengzhou 450002, China
2. School of Computer Science, Fudan University, Shanghai 201203, China
3. Zhejiang Lab, Hangzhou 311121, China

Abstract: Cloud data center is the representative of the new generation of information infrastructure, and its security has become the focus of attention in recent years, which is of great significance. Based on the analysis of the current cloud security situation, the security architecture, key technologies, and implementation methods of the cloud data center through the emerging concept of endogenous security were explored, hoping to use the mimic structure to solve the endogenous safety and security problems such as vulnerabilities and backdoors that were difficult to deal with by the existing means. Moreover, the endogenous security architecture of cloud data centers and related key technologies were proposed, with the mode and trend of mimic transformation. In the future, endogenous safety and security cloud data centers will provide practical solutions for the construction of a new generation of information in-

收稿日期：2021−02−01；修回日期：2021−03−15
基金项目：国家自然科学基金创新研究群体项目“网络空间拟态防御基础理论研究”(No. 61521003)；之江实验室重点项目“面向工业互联网的拟态分布式大数据存储”
Foundation Items: The National Natural Science Foundation of China for Innovative Research Groups “Research on the Basic Theory of Mimic Defense in Cyberspace” (No.61521003), Key Project of Zhejiang Laboratory “Mimic Distributed Big Data Storage for Industrial Internet”

frastructure, which may accelerate the technology application and promotion of the cloud service model.

Key words: endogenous safety and security, cloud data center, mimic structure, mode and trend of mimic transformation

1 引言

近年来，云计算技术的迅速崛起推动了服务模式与应用架构的变革重构，互联网业务的云化已成为主流趋势，得到了学术界和产业界的广泛关注[1]。然而，随着云计算技术应用的逐渐普及，其系统平台与信息管理等方面的安全问题也日益凸显[2]。根据近几年国家信息安全漏洞共享平台（CNVD）收录的相关漏洞的统计分析可知，与云及虚拟化相关的漏洞数量和危害等级正在不断升级[3]；另一方面，从每年产业界爆出的各类安全事件来看，大量云数据泄露、云设施服务中断、用户权限失效等问题，带来了不计其数的经济损失。

云数据中心是云计算业务服务的承载实体，也是安全防护聚焦的重点方向。但是，现有云数据中心的安全手段大多继承和沿用传统网络防护方法[4]，主要依赖于攻击先验知识的检测判别、基于边界“外挂式”的隔离阻断或“后知后觉”的补丁式安全技术，无法有效应对云环境下新的攻击模式，更难以解决因软/硬件缺陷、漏洞后门等内生安全问题所引发的未知威胁。当前，云环境下复杂严峻的安全问题已经成为制约应用与服务市场发展壮大的“达摩克里斯之剑”[5]。

值得关注的是，内生安全概念的逐渐兴起，使我们对以云数据中心为代表的新一代信息基础设施安全内涵进行了重新审视。从哲学意义上说，“世上万物有利必有弊”的对立统一关系，决定了云信息系统的功能在设计和实现时必然存在两面性，其负面性应用会产生内生安全问题的潜在影响。而想要抑制系统的内生安全问题，不能依赖于攻击者的先验知识特征或外挂式的传统安全技术，需要有效利用系统自身架构、功能和运行机制等内源性效应获得安全功能[6]。前期，相关团队在 6G 网络[7]、新型网络[8]、交换机[9]等领域的探索已验证了面向内生安全解决方案的有效性[10]，值得我们进一步延拓至云安全领域开展研究。

2 云数据中心内生安全分析

当前，云数据中心所暴露的安全威胁众多，大致包含的种类有：数据的泄露、篡改和丢失，应用权限控制异常、API 安全、账户劫持、恶意内部人员攻击、APT 攻击、拒绝服务攻击等。将上述问题根据攻击目标和云数据中心架构对应，基本可以归纳为图 1 所示表述方式。

不难发现，云数据中心所涉及的安全威胁在方法内容上与传统网络安全威胁大相径庭，只是在目标对象及渗透链路上更为丰富，攻击者可以基于云平台层面对应用业务及相关软/硬件发难，这使得其安全状态进一步恶化。如图 1 所示，简单来说，云数据中心的攻击方法是在传统的系统架构下引入了云平台新的攻击层面及其对应的新型攻击方法。而这些攻击方式手段看似繁杂，其实大多绕不开信息系统中存在的设计或实现的漏洞后门，即前文提到的内生安全问题。

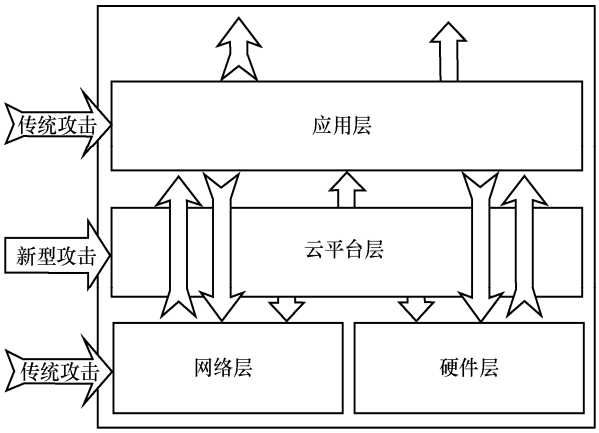


图 1 攻击链路示意图

2009 年，VMware 虚拟化软件 MAC 版本爆出严重的安全漏洞，攻击者基于该漏洞可通过 Windows 虚拟机在其 MAC 主机上直接执行恶意代码，是一种代表性的基于 API 的向下渗透攻击；2012 年，仅 XEN Hypervisor 4.1.4 版本就修复了 18 个关键漏洞，随后类似的 GAE（Google App engine）漏洞也被发现，攻击者可以利用它们逃逸虚拟机的隔离和安全保护措施，对系统平台实施越权控制；2016 年，QEMU 组件与 CloudStack SAML 组件也爆出诸多问题，攻击者可以基于其漏洞绕过身份验证机制；2017 年，OpenStack Glance Newton 组件也被发现存在服务器端的安全限制绕过漏洞的问题。通过上述安全事件，可以预见由云平台内生安全问题引发的各类威胁是难以避免的，将是安全人员首要面对的难题。

在安全方案上，目前业界主流还是集中对云虚拟主机、云应用以及云系统网络进行安全防护，如防病毒工具、异常行为检测、网络访问隔离、数据库审计、防火墙、虚拟 WAF 等。整个思路与体系的构建仍然没有脱离基于先验知识的传统被动式防御，难以检测和防御云平台自身的未知漏洞和攻击，例如，攻击者利用云平台本身的堆栈溢出、格式化字符串漏洞等绕过检测和审计，释放后再运用混淆、提权、API 误用等劫持软件等执行流程导致云计算环境被劫持或者信息泄露。而相较于传统信息系统，云数据中心的新型服务模式更加容易遭受内生安全威胁的影响。一方面，云服务实例的单一同质性使得系统平台更容易受到攻击；另一方面，云上数据和计算资源集中管理会导致攻击目标集中，信息跨域传递也会导致攻击目标的加速暴露；技术耦合度高、集成软件繁多也使得系统受攻击面更广，传统防护方法更加难以生效。

以此来看，当前云数据中心安全手段很难全面应对系统的内生安全问题，需要研究者另辟蹊径，借助内生安全的体制机制及方法改造自身架构，发挥内源安全功能效应破解当前问题。

3　云数据中心内生安全架构与关键技术

近年来，内生安全理论得到了逐渐完善与广泛应用，其核心解决方法——拟态防御的有效性已经得到了充分验证。对于以漏洞、后门为代表的内生安全问题，拟态防御通过动态异构冗余（dynamic heterogeneous redundancy，DHR）构造对系统结构进行内源性安全赋能[11]。首先，基于多样性构建异构冗余的执行空间，各执行空间相互独立承载完整的目标对象功能，作为拟态架构的基础条件。即使单一空间存在协议逻辑实现的漏洞后门，也难以干扰其他异构空间的正常运行；然后，利用分发－裁决机制对各个执行空间的运行处理结果进行判定，输出逻辑一致的处理结果，屏蔽和感知逻辑非一致结果；最后，利用反馈与动态调度机制对感知到的异常进行处理，从而规避攻击和清洗还原系统，达到安全防御的效果。与传统安全手段相比，拟态架构并没有增添知识库、检测机等外挂式的防护环节，而是通过对系统自身的内在架构改造使其具备了抵御漏洞、后门的安全功能，因此为云数据中心的内生安全问题提供了有效解决思路。

3.1　云数据中心内生安全架构

基于拟态防御 DHR 架构可以对云数据中心进行拟态构造设计，内生安全逻辑架构如图 2 所示，从逻辑上分为以下几个部分。

基础设施层：包括多种异构的物理服务器（x86 和 ARM 或其他架构），形成计算虚拟资源池，为上层拟态 SaaS 应用提供异构容器资源，拟态存储为 SaaS 应用提供安全的存储服务，基础设施层接受拟态云管理器的管理和调度，在不同节点上创建拟态 SaaS 应用执行体。

异构网络交换层：作为通信层主要负责不同层次间的通信，包括外部网络、业务网络和管理网络，负责不同系统的连接，其中外部用户通过外部网络访问代理服务，拟态括号系统中的代理

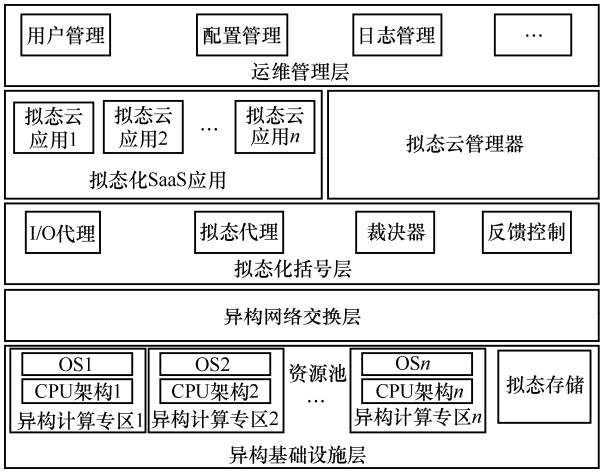


图 2　云数据中心内生安全逻辑架构

通过业务网络访问 SaaS 应用，拟态括号系统中的裁决器通过业务网络接收位于基础设施不同节点上的不同 SaaS 应用执行体的响应。管理网络负责基础设施间的互联，管理员通过管理网络基于拟态云管理器管理底层资源池，并对其他组件进行运维管理，同时管理网络负责拟态括号系统和拟态云管理器的互连互通。

拟态云管理层：提供拟态化的云管理系统，包括代理（转发资源调度等云操作管理方面的请求）、多个异构云管理系统和裁决器（裁决不同云管理系统对请求的处理结果（含配置信息），发送至基础设施进行实际部署），对底层资源进行管理，接受管理员及租户的请求创建拟态化 SaaS 应用，并对其进行生命周期管理。同时，其中的反馈控制模块根据运行情况决策实现对在线容器执行体的策略性动态轮换控制。

SaaS 应用层：基于生成的拟态化 SaaS 应用容器对外提供 SaaS 服务，包括代理、执行体和裁决器，执行体由底层不同区域的容器承载、代理和裁决器根据应用类型的不同分别设计与实现，同时为了增强其安全性，可以将代理和裁决器单独实现，如硬件形式或基于专门的服务器设计实现，不在底层虚拟化资源池中承载，通过业务网络对外提供服务。

运维管理层：基于管理网络进行运维用户管理（非 SaaS 用户），进行各设备的配置管理，负责处理拟态化 SaaS 应用的部署请求并通过调用拟态云管理器的 API 实现在不同节点上的异构多样化部署，监控系统各模块的整体运行情况，进行整体的态势感知展示，包括拟态 SaaS 应用的运行展示，此外，运维管理还需要将监控分析结果反馈至拟态云管理器中的反馈控制模块辅助决策。

云数据中心内生安全架构通过各个层次的联动工作，实现整个云数据中心业务应用的拟态化工作流程，从而产业内生性的安全效应。同时，还引入了拟态存储、拟态云管、异构化网络交换等具有内生安全功能的系统组件，保证了其核心环节的安全性与可靠性。

3.2　云数据中心内生安全关键技术

云数据中心内生安全架构的设计提供了系统构建的骨架，然而想要整个云系统最终做到正常运转，则需要进一步研究云数据中心内生安全的具体实现。尤其是结合云计算业务处理的多样化、灵活迁移等特点，形成适用于其应用场景的关键技术。本文着重选取拟态表决、业务迁移、数据同步 3 个重要处理环节，探讨云数据中心内生安全的关键技术实现。

3.2.1　拟态表决技术

由于云平台上的业务多样性，其正常的逻辑结果也通常会表现出不一致特点，决定了针对云主机难以基于结果进行表决。这里给出一种基于过程结果的拟态表决方法，通过对过程性结果进行取证分析，再配合基于负反馈机制对异常执行体实施自愈修复操作。

方法的核心思路是指拟态系统需要对执行体“过程数据和过程要素资源”进行监控，通过表决发现被攻击的执行体。其中，“过程数据”包括执行体的进程状态数据、内存数据、网络状态数据、注册表状态数据等运行过程中的实时状态数据；“过程要素资源”包括执行体的可执行文件、配置文件、日志文件等运行过程中的相关文件。

在表决的过程中，具体的过程数据和过程要素资源需要构建适合应用场景的集合。在执行体正常运行时，通过实时对比过程结果内容，判断该执行体是否被攻击。基于过程要素的多维度表决方法可以扩大拟态表决的范围，实时进行拟态表决，更加高效地发现异常执行体。

图 3 为基于过程结果的拟态表决示意图，主要包括云集群、虚拟云主机和表决器。表决器通过对设定的“过程要素”进行拟态表决发现异常运行的云主机。若发现存在异常，将进行云平台的自愈修复流程。

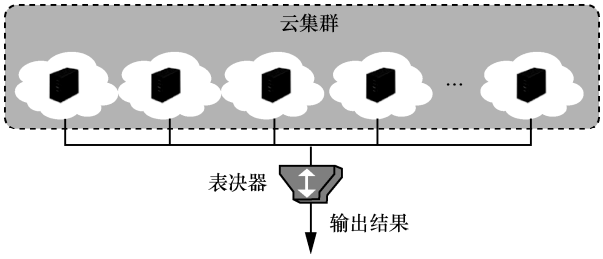


图 3　拟态表决示意图

图 4 为拟态表决的算法流程。控制器策略性地发出表决指令，表决器依据特定的表决算法，对多维度内容进行表决，若发现某执行体出现异常，将首先完成云上虚拟云主机的数据同步和业务迁移，随后完成异常云主机的下线和自愈修复操作。

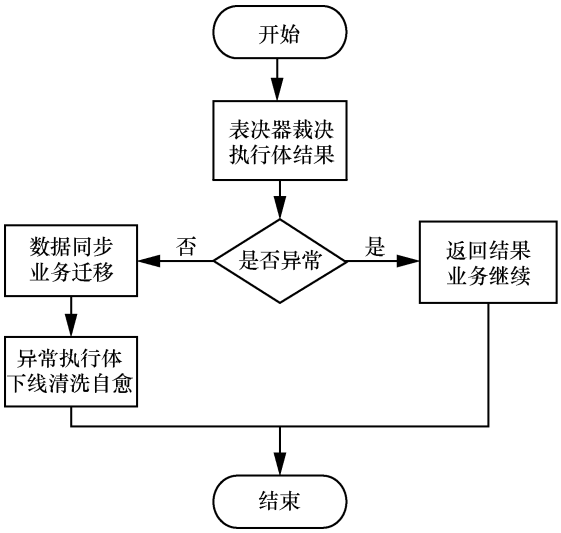


图 4　基于过程结果的拟态表决流程

3.2.2　业务迁移技术

由于拟态架构需要对异常的执行空间进行修复，因此需要良好的业务迁移技术支持。业务迁移的核心是实现虚拟云主机间在异构云之间的迁移，

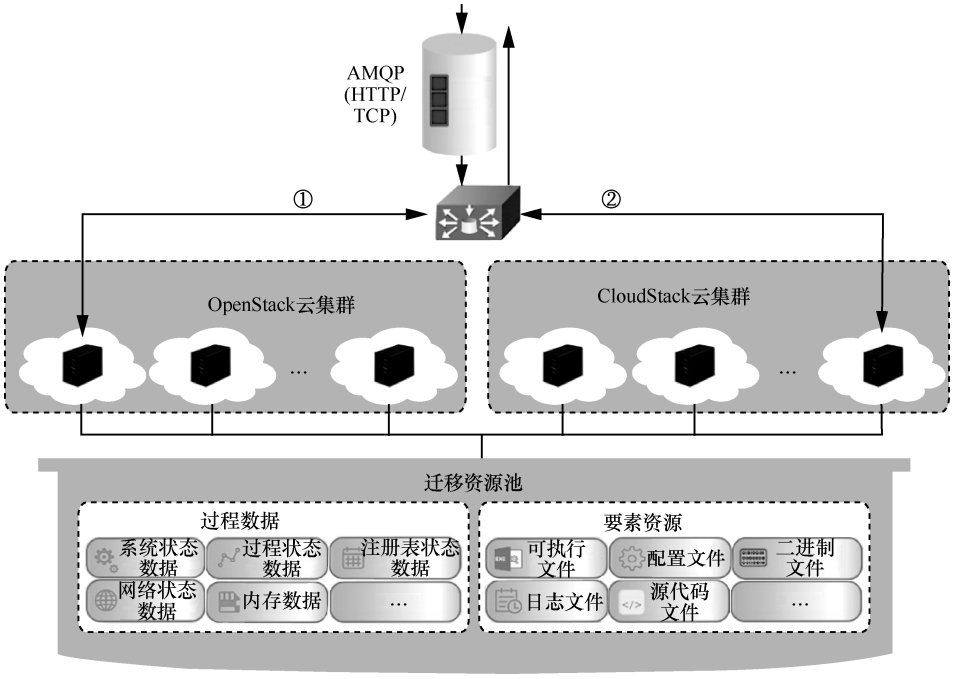


图 5　业务迁移示意图

同时还要保持业务不中断，这里给出一种基于缓冲池技术，在跨平台异构云间实现业务平滑迁移。

业务迁移示意图如图 5 所示，业务数据经过高级消息队列协议（advanced message queuing protocol，AMQP）缓冲池到达分发器，分发器依据当前策略对业务数据流进行定向转发。为提高系统的运行效率，流入数据必须经过缓冲池，而流出数据可不经过缓冲池。同时，在云发生异常时，由分发器完成数据链路由 1 切换到 2。

虚拟云主机业务迁移流程如图 6 所示，用户请求通过高级消息队列协议（AMQP）经由分发器发送到某台虚拟云主机，对过程数据和要素资源组合内容进行表决。若当前虚拟云主机出现异常，则迁移整个过程数据和业务，并将业务平滑迁移至异构虚拟云主机。同时，异常虚拟云主机下线自愈。

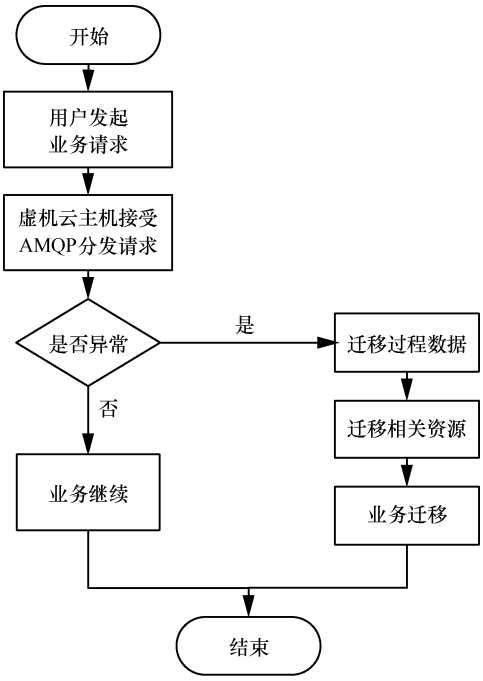


图 6　虚拟云主机业务迁移流程

虚拟云主机切换的流程如图 7 所示，当在线虚拟云主机所在的执行空间出现异常时，控制器发出虚拟云主机切换命令。若当前异构云集群中存在可用的虚拟云主机，则将业务数据及业务迁移至虚拟云主机，原虚拟云主机下线自愈修复。

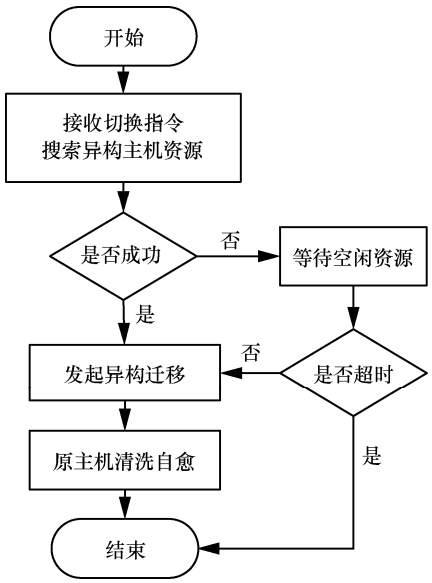


图 7　虚拟云主机切换流程

3.2.3　数据同步技术

为了更好地恢复补充拟态架构中的异构资源池，需要将异常的执行空间进行数据同步恢复，保证其进行正常的工作状态。虚拟云主机的数据实时同步可以通过多种方式实现，大致分为静态迁移（或称冷迁移）和动态迁移（或称热迁移）。冷迁移因为需要虚拟云主机在关机或暂停的情况下从一朵云迁移到另一朵云中。所以，从用户角度看有一段明确的服务停止时间。异构云平台所支持的静态文件格式对比见表 1。对比可知，在当前业界对于镜像文件，在多种异构云管理平台下，都进行了很好的兼容性支持，为冷迁移提供了技术支撑。同时，为了提升迁移效率，业界普遍采用普通快照加增量快照的方式完成镜像文件的生成。

表 1　云平台所支持的镜像文件对比

镜像文件/云平台	OpenStack	CloudStack
qcow2	支持	支持
raw	支持	支持
img	支持	支持
vdi	支持	支持
vmdk	支持	支持
vpc	支持	支持

而对于一个业务服务系统来说，热迁移是拟态架构实现中更加值得关注的研究点。热迁移是在虚拟云主机不停机的情况下完成的，将一个虚拟云主机从一朵云迁移到另一朵云。

目前热迁移有共享存储的动态迁移和本地存储的动态迁移两种方案。以共享存储为例，大多数虚拟化软件如 KVM 和 XEN 都支持共享存储，如 NFS（网络文件系统）。那么，即可利用 NFS 在虚拟云主机间共享数据，动态迁移时直接将虚拟机镜像迁移到其他云中相同的目录结构处放置即可。虚拟云主机同步的模块示意图如图 8 所示。

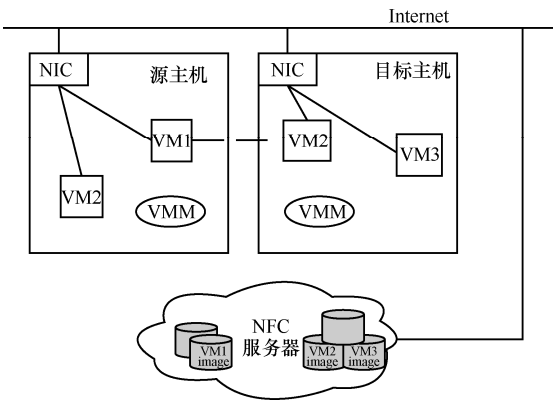


图 8　虚拟云主机同步的模块示意图

在利用网络传输解决动态同步问题时，所有虚拟云主机间建立 TCP 连接，通过网络传输或者删除文件。由于虚拟云主机数据同步的时效性要求，各物理设备间的网络连接带宽要尽量得到保证。

基于共享存储的实时迁移内容如图 9 所示，当一台虚拟云主机需要进行数据同步时，首先将动态过程数据和静态要素资源进行文件化处理；处理后的文件存放在拟态存储服务器中；最后，在异构云上的虚拟云主机利用共享文件进行还原。为了确保文件的安全，可以引入拟态存储系统放置共享文件数据。

热迁移下实现动态数据同步的过程如图 10 所示。首先，控制器发出数据迁移的命令开始数据动态迁移，动态数据迁移器从源虚拟云主机中取出相关数据形成文件；然后，将数据传入目标虚拟云主机；最后，源虚拟云主机完成下线自愈操作。其中，目标虚拟云主机在完成数据输入前需要无业务在线运行。

4　云数据中心拟态化改造模式与未来趋势

基于前文所述的云数据中心架构与关键技术，未来云数据中心拟态化改造中可能存在 3 种模式。

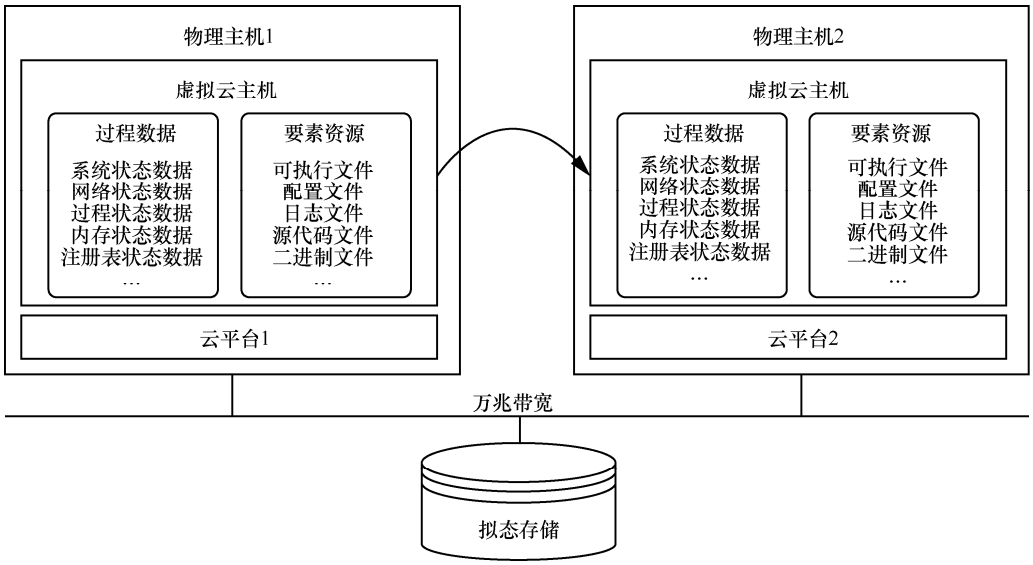


图 9　基于共享存储的实时迁移内容

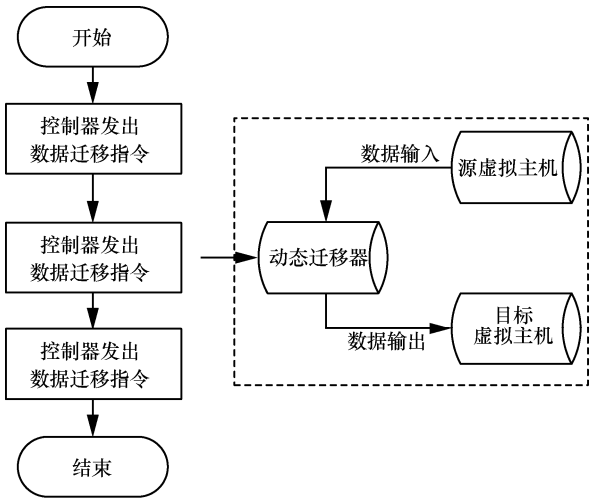


图 10　动态数据同步流程

模式 1：对信息技术产品处理流程的关键部位或模块进行异构化处理，设置拟态括号及配置相关的软/硬资源，从而尽可能减少功能性能、成本等方面的开销，如图 11 所示。

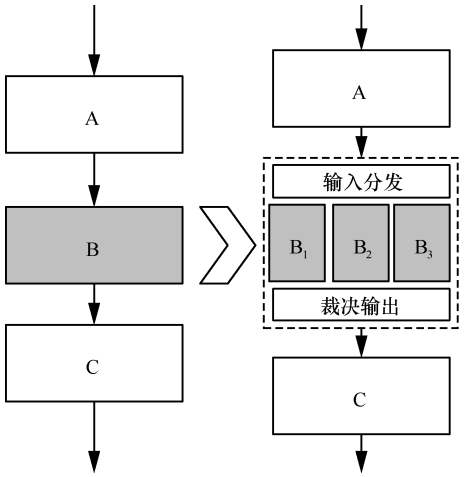


图 11　面向关键部位或模块的升级改造模式

适用场景：对系统关键部位或模块进行局部的拟态化改造需要清楚该部分的功能逻辑与接口，因此该模式比较适合于代码可控的自有产品，比如云计算开源社区发布的各类软件。

模式 2：针对某种应用技术产品的功能性能以及技术架构，在核心部位设置拟态输入和裁决部件，并直接配置相应的 COTS 级软/硬构件构成拟态化子系统，如图 12 所示。

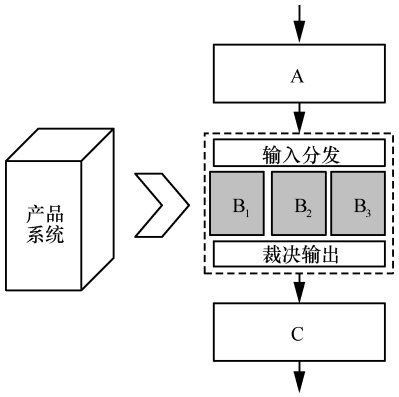


图 12　面向完整软硬中间件的集成开发模式

适用场景：在更多的情况下，云应用的业务提供商并不希望公开自己的代码，对此可以采取模式 2 直接将第三方产品作为独立的执行体集成到拟态化系统中。

模式 3：直接面向业务协议进行拟态化改造，在目标服务应用的输入/输出接口增加分发、裁决及反馈调度等机制即可，如图 13 所示。

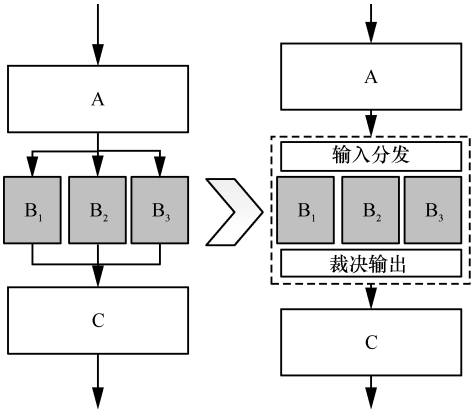


图 13　面向业务协议的升级改造模式

适用场景：在云数据中心环境下为了保证可靠性和可用性，在管理或应用业务中类似资源分配、数据存储等环节都具有分布、冗余、动态的特性时，则适合使用该模式进行改造。

对于云技术内生安全的发展而言，未来趋势大致包括 3 点。

首先，加快云数据中心内生安全基础软/硬件研发。现有拟态设备大多以 COTS 级软硬件直接作为多样化的异构执行体，未能深入模块或流程

级开展拟态化改造。对于云数据中心而言，其更大的场景规模和更高的应用需求都决定了必须开展内生安全设计语言、工具链、工具库等研发，从而增强云业务系统与内生安全组件的耦合度，才能更好地释放内生安全效应。

第二，进一步完善关键基础组件的研发。内生安全云数据中心除了对云业务本身的拟态化改造研究，还需要安全可信的存储系统、网络设备设施、云管平台等各种系统组件的支撑。因此，需要同步突破云管平台、云组件、分布式存储系统等关键环节的内生安全技术攻关，才能更好地支持推动内生安全云数据中心的新一代信息基础设施建设。

最后，面向云数据中心构建开源开放的内生安全技术研发、测试、评估等生态链。一方面能够更好地丰富软硬生态的多样化发展，为内生安全技术研究与实现提供基础环境；另一方面，也能更好地推动内生安全云数据中心的落地与良性迭代发展，促进系统与核心技术的实用性提升。

5　结束语

当前，云系统安全与应用安全已经成为了备受关注的焦点问题。本文从近年来频繁曝光的云系统漏洞及安全事件出发，着重分析和探讨了其内生安全问题及威胁根源；然后，结合最新的内生安全理论与技术思路，给出了一种典型的云安全架构及其相关技术内容，阐述了内生安全的生效机理与过程；进一步地，对后续内生安全技术发展与云内生安全未来趋势进行了分析阐述。

未来，云安全领域的从业者和研究者应着眼于网络安全技术研发从“外挂式”向“内生性”转变的技术变革，才能更好地推进“新基建”信息技术产业升级演进，催生网络信息服务与应用发展新业态。而其中，基于内生安全的新型云服务模式或将成为“新基建+新安全”“双轮驱动”的应用发展机遇，研发内生安全云系统平台，构建内生安全云应用服务生态等，将是筑牢云技术产业的发展基础，是助力我国数字经济繁荣发展的重要方向。

参考文献：

[1] MAJUMDAR S, MADI T, JARRAYA Y, et al. Cloud security auditing: major approaches and existing challenges[C]//Integer Programming and Combinatorial Optimization. [S.l.: s.n.], 2019: 61-77.

[2] EL-ATTY A, SAIED M, KOLHAR, et al. Cloud data auditing techniques with a focus on privacy and security[J]. IEEE Security & Privacy, 2017, 15(1): 42-51.

[3] DAVE D, MERULIYA N, GAJJAR T D, et al. Cloud security issues and challenges[J]. Big Data Analytics, 2018: 499-514.

[4] 俞能海, 郝卓, 徐甲甲, 等. 云安全研究进展综述[J]. 电子学报, 2013, 41(2): 371-381.
YU N H, HAO Z, XU J J, et al. Review of cloud computing security[J]. Acta Electronica Sinica, 2013, 41(2): 371-381.

[5] 陈钟, 孟宏伟, 关志. 未来互联网体系结构中的内生安全研究[J]. 信息安全学报, 2016, 1(2): 10-13.
CHEN Z, MENG H W, GUAN Z. Research on intrinsic security in future internet architecture[J]. Journal of Cyber Security, 2016, 1(2): 10-13.

[6] 邬江兴. 网络空间内生安全——拟态防御与广义鲁棒控制[M]. 北京: 科学出版社. 2020.
WU J X. Endogenous security in cyberspace -- mimic defense and generalized robust control[M]. Beijing: Science Press, 2020.

[7] 刘杨, 彭木根. 6G 内生安全: 体系结构与关键技术[J]. 电信科学, 2020, 36(1): 11-20.
LIU Y, PENG M G. 6G endogenous security: architecture and key technologies[J]. Telecommunications Science, 2020, 36(1): 11-20.

[8] 江伟玉, 刘冰洋, 王闯. 内生安全网络架构[J]. 电信科学, 2019, 35(9): 26-34.
JIANG W Y, LIU B Y, WANG C. Network architecture with intrinsic security[J]. Telecommunications Science, 2019, 35(9): 26-34.

[9] 宋克, 刘勤让, 魏帅, 等. 基于拟态防御的以太网交换机内生安全体系结构[J]. 通信学报, 2020, 41(5): 22-30.
SONE K, LIU Q R, WEI S, et al. Endogenous security architecture of ethernet switch based on mimic defense[J]. Journal on Communications, 2020, 41(5): 22-30.

[10] 普黎明, 刘树新, 丁瑞浩, 等. 面向拟态云服务的异构执行体调度算法[J]. 通信学报, 2020(3): 17-24.
PU L M, LIU S X, DING R H, et al. Heterogeneous executor scheduling algorithm for mimic cloud service[J]. Journal on Communications, 2020(3): 17-24.

[11] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1-10.

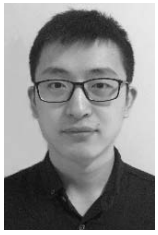
[作者简介]

张帆（1981− ），男，博士，国家数字交换系统工程技术研究中心副研究员、硕士生导师，主要研究方向为主动防御、芯片设计技术、高性能计算。

扈红超（1982− ），男，博士，国家数字交换系统工程技术研究中心副研究员、研究室主任，主要研究方向为云计算、内生安全技术。

谢光伟（1981− ），男，博士，复旦大学高级工程师，主要研究方向为拟态防御、拟态计算和数据科学与工程。

张汝云（1973− ），男，博士，之江实验室工业互联网研究中心研究员、副主任，主要研究方向为工业互联网内生安全、新型网络架构、工业网络计算等。



郭威（1990− ），男，博士，国家数字交换系统工程技术研究中心助理研究员，主要研究方向为主动防御、网络体系结构、分布式存储系统。

刘文彦（1986− ），男，博士，国家数字交换系统工程技术研究中心讲师，主要研究方向为网络空间主动防御技术、云计算安全技术。