基于私有云平台的网络安全防护措施

黄 浩

（中通服网盈科技有限公司 南京 210000）

摘 要 由于信息网络的高速发展，云计算服务在各类私有云平台中得到了广泛的应用，但作为一种可定制的、私有的计算环境，如何保障各类数据的安全性，加强网络安全防护，成为亟待解决的问题。文中简要说明了私有云平台的概念及发展现状，并基于对网络安全威胁的分析，提出了具体的防护措施，以期能为相关人员提供参考。

关键词： 私有云平台；网络安全；防护措施

中图分类号 TN915.08

Network Security Protection Measures Based on Private Cloud Platform

HUANG Hao

（ZTO Service Netying Technology Co.，Ltd.，Nanjing 210000，China）

Abstract Due to the rapid development of information networks, cloud computing services have been widely used in various private cloud platforms. However, as a customizable and private computing environment, how to ensure the security of various data and strengthen cyber security protection has become an urgent issue to be solved. This paper briefly explains the concept and development status of private cloud platforms, and based on the analysis of cyber security threats, puts forward specific protection measures, in order to provide reference for relevant personnel.

Key words Private cloud platform，Network security，Protective measure

0 引言

随着“数字经济”与“大数据”的快速发展，私有云平台逐渐成为广大政企部门部署云解决方案的必要工具。私有云平台虽然在成本控制、资源利用等方面提供了诸多便利，但也面临着复杂的网络安全挑战[1]。作为关键数据的储存与处理中心，私有云平台的安全性会直接决定客户信任度、数据完整性以及业务连续性。因此，掌握私有云平台中可能存在的网络安全威胁，并构建高效、全面的防护措施，显得尤为重要。

1 私有云平台的概念及发展现状

1.1 私有云平台的概念

私有云平台是指由某一组织机构自行创建和维护的云计算环境。与公共云平台相比，私有云平台并不面向大众，只针对特定的组织机构，为其特定的技术、业务等需求而服务。

私有云平台可以被配置在主机托管场所、数据中心等区域，主要属性是专有资源，且具有 3 个层次的云计算体系架构，分别是软件即服务（SaaS）、平台即服务（PaaS）以及基础设施即服务（Iaas）[2]。

1.2 私有云平台的发展现状

目前，我国私有云平台的发展方向由消费互联网转向了工业互联网，而上云企业不断增加，对传统企业的影响不断扩大。随着“智慧城市”“数字政务”等的深入发展，能源、医疗、交通、政务等领域均呈现出快速发展的趋势，促进了更多的私有云平台的构建，使得私有云平台迈入了快速成长的阶段。据信通院统计，2023 年我国私有云平台市场规模为 6 165 亿元，预计 2027 年将突破 20 000 亿元，年市场增长率超过 30%。虽然私有云平台拥有众多优点，但其仍面临着严峻的网络安全威胁。其中，各大供应商纷纷采用微服务体系结构、自动化工具等技术，不断提高了私有云平台的可靠性与安全性，但仍然任重而道远[3]。

2 基于私有云平台的网络安全威胁分析

2.1 常见的安全威胁

（1）分布式拒绝服务攻击。利用来自不同来源的海量请求，使私有云平台无法正常工作。（2）恶意程序和勒索软件。这些程序与软件能未经许可地进入或利用私有云平台资源，并对重要数据予以加密，通过设置密钥索要费用。（3）侧信道攻击。在物理层，部分攻击者并不会直接攻击，而是通过虚拟机获取数据，是一种持续性安全风险。（4）虚拟化漏

作者简介：黄浩（1979—），本科，助理工程师，研究方向为电子信息工程。

洞。私有云平台的软、硬件可能存在缺陷，导致黑客可以通过其展开非法访问，严重影响私有云平台的安全性。(5)错误配置。错误配置会让黑客有机会获取访问权限，如打开多余的网络端口或进行未经认证的服务，造成数据泄露或其他安全事故。(6)过度授权。当应用程序或用户获得了过多的权限时，私有云平台就会变成一个可以被攻击的平台，或被恶意软件利用。(7)内部威胁。不怀好意的第三者或内部人员可能会窃取、破坏数据[4]。

2.2 特殊安全威胁

(1)数据集中化风险。私有云平台一般采取集中储存的方式，但其可能成为黑客的攻击对象，非授权的内部使用者也可能会企图获取存储在私有云平台中的机密数据。(2)虚拟机逃逸。虚拟机逃逸是指黑客从一台虚拟机向另一台服务器发起攻击。在虚拟环境中，黑客可以悄无声息进入物理服务器，从而对其他虚拟机构成威胁。(3)资源池攻击。私有云平台的资源通常会被各种业务部门共享，这导致攻击者可以通过对某个资源池内的某个程序实施攻击，从而对私有云平台内的全部程序产生影响。(4)API和界面漏洞。用于私有云平台的API和界面都会存在一些安全性问题，如非加密API通信可能会被监听，导致数据被篡改或泄漏。

3 基于私有云平台的网络安全防护技术

3.1 数据完整性验证协议

传统数据完整性验证协议多采用访问的方式，如数据库存储系统、海量存储系统以及在线存储系统等，导致服务器负载升高，浪费网络带宽[5]。也可采用应答的方式，即客户端向某个特定的区块发起一个请求，然后由服务端产生一个完整性证据，再由客户端进行判定，整体成本较高。本文立足于PDP模型，提出了一种适用于私有云平台的数据完整性验证(PCS-DIV)协议，主要方案如下。当客户端将校验标签、数据文件上载至专用的私有云平台服务器后，该服务端会对特定数据予以抽样检验，并将检验结果反馈给客户端，使客户端能对该数据进行完整的判定。另外，该算法还具备一定的自适应能力，能确保小文件检索的正确性；对于大文件，则通过检验某些数据块，使其保持完整性，降低系统负载及带宽开销。

在参照Google文件系统的基础上，可以将私有云平台划分为5种类型，即储存服务器(R1，R2，R3……)、接口服务器R0、监控服务器R'、主服务器R以及客户端W。客户端W若想将某个文件储存在私有云平台中，可以与接口服务器R0交互，简化客户端执行流程。主服务器R作为私有云平台的枢纽，不仅可以控制所有储存资源的调度与分配，还能保存所有用户的储存信息。如此，可以实现数据流与控制流的分离，使主服务器R和接口服务器R0之间只有控制流，不存在数据流，以降低负载，让数据在多个储存服务器(R1，R2，R3)中进行传输。

R0需先与W互相认证，获取密钥，然后由W生成校验的私钥，通过对待上传数据块生成标签，并向R0申请访问私有云平台，R0告知主服务器R，结合R'反馈，将状态信息表分配给R1、R2、R3。其中，由W生成校验挑战，主服务器R根据储存信息将校验标签发送至R0，再反馈给W；W按照私钥判断数据是否完整。算法设计主要包括Key、Tag、Proof和Verify，具体如下。

算法1 Key

$(N, sk) \leftarrow Key(1^k)$/*生成用于文件校验的参数*/ *Generaleparameters N，e，dmeettheconditonsof RSA assumption*；

算法2 Tay

$(T_0, T_2 \cdots T_{n-1}) \leftarrow \frac{Tag(pk, sk, m)}{}$ *为每个文件块生成标签块 *for(j=0；j≤0-1；j++)；$\left\{ w_j = r*(j+1);\ T_i = \left[h\left(w_j \cdot m_j \right) \right]^e mod\ N \right\}$；*Output* $(T_0, T_2 \cdots T_{n-1})$；

算法3 Proof

V←Proof $(m_{ik}^{ak} modN, T_{ik}, pk)$/*生成文件校验的证据*/*for*$(k=1; k \leqslant u; k++)$；$\left\{ i_k = a_{b_{r_{K3}(k)}};\ a_k = f_{K4}(k) mod\ N \right\}$；*Output V*=$(T, P)$；

算法4 Verify

'$\{$"*success*"，"*failure*"$\}$←*Verify*$(N, sh, u, K3, K4, V)$/* 对证据进行验证*/

$t = T^d mod\ N$；

For$(k=1; k \leqslant u; k++)$；

$\left\{ W_{ik} = r*ik;\ t = \frac{t}{h(W_{ik})} mod\ N \right\}$；

if$h(t)=P$

Out"*success*"

slse Output"*failure*"

3.2 分布式文件系统

文件系统的实质是一个软件，它负责为用户建立文件，存入、读出、修改文件的存取，并能在用户不再使用时撤销文件。由于分布式文件系统设置在互联网上，比一般的硬盘文件系统更加复杂[6]。例如，如何在保证网络安全运行的前提下，保证网络中的节点不会失效或数据不会丢失，就变得十分困难。本文应用分布式文件系统，针对文件小、数据多的需求，展开了分布式文件系统优化，使之满足如下条件。(1)空间提升。上传文件将实施分布式储存，如果存在空间不足的情况，则单加硬盘或服务器即可。(2)高可靠性。能实现数据完整性校验、智能副本存放等。(3)均衡负载。在其他服务器中进行上传、下载，不和主服务器争夺带宽，降低安全隐患。

3.3 ID特征码设计与数据分片

在现实生活中，企业存在很多部门，且每个部门都有很

多用户，每个用户拥有多个文档，而每个文档都与多个文档数据块相对应。ID特征码可以使各部门与区域互相对应，各用户在登记时产生一个使用者ID（假定为i_j，i为该部门ID，j为该用户的登记号码），这个ID会按照登记的时间顺序自动增加1，第1名使用者的编码是1。各用户的文件ID（以i_j_k表示）中的i_j为用户ID，k表示该文件的编码。各文件块会被分割成若干个区块，如技术部门ID是2，技术部门的第44名用户的第9个文件被划分为p个区块，则区块ID为2_44_9_p。

如果这个区域内存在失效节点，则按照索引表格将其保存为0的内存节点ID；如果将包含文件的子模块保存在失效节点上，则可以将其作为内存的子模块进行随机保存。数据分片可以随意设置区块的大小，以1M为单元划分，小于1M的也被视为一块，当用户下载某个文件时，需向接口服务器发出请求，然后由接口服务器向主机服务器发送请求，并由主机服务器通过文件ID从数据库中找出这个文件的储存节点地址、块信息，然后将其返回接口服务器，最后由接口服务器将其返回给用户，并将各文件块集成为一个整体的文件。

3.4 加强网络边界防护

（1）网络访问控制。在私有云平台下，基于数据中心的数据访问控制机制是实现用户数据安全保护的重要手段，需要改善网络访问控制方式，定制并执行访问控制规则，以处理不同的实体在云端的互动方式。角色访问控制（RBAC）提供了一种全新的架构，可以为用户赋予不同的角色，这种角色往往是相应的职位，如业务分析师、开发人员、系统管理人员等。在RBAC的基础上，可以为某个角色赋予相应的权限。

（2）入侵检测系统。私有云平台可以结合入侵探测体系与网络安全防护技术，以监测和应对可能出现的攻击行为。入侵检测系统提供了一个全新的视角，使其能识别危险并作出反应，从不同的角度来应对不同的安全威胁。例如，当一个系统侦测到来自某个特殊来源的大量请求时，这个动作就会被标记为泛洪攻击。

（3）强密码机制。在私有云平台中，强密码机制是保障其安全性的关键，因此需要建立并使用一个强有力的密码，如包含特殊符号、数字以及字母，且长度应足够长，以增加解密的困难。同时，需定期修改密码，避免密码被推测或泄漏。

（4）加密敏感数据。私有云平台中储存着大量的数据，包括业务数据、用户信息等，如何保证数据的安全性非常重要。可以利用密码学原理来加密重要信息，并保证其在储存、传输时的机密性。除被授权的用户外，任何人都不可以对其进行访问或加密，以减少数据泄漏的危险。

（5）使用虚拟局域网进行网络隔离。当多个业务或服务同时存在于一个物理环境中时，虚拟局域网（VLAN）技术可以有效地实现对多个业务或服务的分离，将网络从一个逻辑层次上划分成若干个单独的广播域，保证数据流在一个特殊的逻辑网中进行，而不会和其他网络发生交叉，提高网络的安全性。

4 结语

私有云平台具有强大的数据管理能力，但并不完全安全，因此有必要加强网络安全防护措施，使用数据完整性验证协议、分布式文件系统、加强网络边界防护等措施，不断健全私有云平台的安全体系，为用户提供安全保障，实现更全面的安全防护。

参考文献

[1] 肖伟钢.基于私有云平台的网络安全防护策略研究[J].中国新通信，2024，26(6)：54-56，223.

[2] 王逸鹤，吉梁，李东.面向企业私有云的网络安全能力模型研究[J].网络安全和信息化，2023(5)：36-39.

[3] 汪刚.基于私有云区块链的农业网络安全系统设计[J].农机化研究，2023，45(12)：235-239.

[4] 周弘.私有云网络安全风险分析及安全防护策略[J].长江信息通信，2022，35(10)：143-144，147.

[5] 米捷，张凌超，高彦伟，等.基于私有云安全防护的网络密文数据防泄露方法[J].河南工程学院学报(自然科学版)，2022，34(3)：48-53.

[6] 童瀛，周宇，姚焕章，等.面向私有云的虚拟化网络密文数据防泄漏模型设计[J].西安工程大学学报，2022，36(1)：129-135.