

# 大数据环境下密码资源池多租户安全隔离研究

高秀武,刘文丽,高恒振,刘明达  
(江南计算技术研究所,江苏 无锡 214083)

**摘要:**大数据与云计算的快速发展,共同创造了一种数据规模极大、计算存储高效、资源共享的大数据环境。大数据环境下隐私数据保护、多租户模式等对密码服务的需求发生改变,促使密码技术向“密码资源池化”发展。在研究了大数据环境下密码资源池组成结构与应用场景的基础上,分析了大数据环境下多租户密码服务整个生命周期的安全隔离需求,同时研究了 OpenFlow 软件定义网络技术以及 VxLAN 网络虚拟化技术。针对大数据环境下密码资源池多租户密码服务安全隔离问题,提出一种将密码服务请求与密码任务执行相分离的服务机制,基于 VxLAN 技术实现网络隔离的密码资源池多租户安全隔离模型,实现租户密码资源与租户业务环境同属于一个安全域,从而确保大数据环境下密码资源池多租户密码服务的安全隔离。

**关键词:**大数据环境;密码资源池;多租户隔离;VxLAN

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2018)09-0127-05

**doi:**10.3969/j.issn.1673-629X.2018.09.026

## Research on Multi-tenant Security Isolation of Cryptographic Resource Pool in Big Data Environment

GAO Xiu-wu, LIU Wen-li, GAO Heng-zhen, LIU Ming-da  
(Jiangnan Institute of Computing Technology, Wuxi 214083, China)

**Abstract:** The rapid development of big data and cloud computing has jointly created a kind of big data environment with large data scale, efficient computing storage and resource sharing. In the big data environment, privacy data protection, multi-tenant and other issues change the cryptographic service requirements, which promotes the development of password technology to “cryptographic resource pool”. Based on the study of the structure and application scenarios of the resource pool under the large data environment, we analyze the security isolation requirements of the multi-tenant cryptographic service. At the same time we study the OpenFlow software definition network technology and the VxLAN network virtualization technology. Aiming at the security isolation of the multi-tenant cryptographic service of the cryptographic resource pool in the big data environment, we put forward a service mechanism of separating cryptographic service request and cryptographic task execution and realize a multi-tenant network isolation model of cryptographic resource pool based on VxLAN technology to achieve network isolation. The implementation of tenant cryptographic resource and tenant working environment belongs to the same security domain, ensuring security isolation of multi-tenant cryptographic service in the big data environment.

**Key words:** big data environment; cryptographic resource pool; multi-tenant isolation; VxLAN

## 0 引言

大数据<sup>[1-2]</sup>与云计算<sup>[3]</sup>技术的不断发展,共同创造了一种数据规模极大、计算存储高效、资源共享的大数据环境。大数据环境为大数据的挖掘分析提供了高效灵活的存储计算分析能力,不断从海量数据集中获取新的知识和创造新的价值。大数据环境不断创造价值的同时也带来了许多安全挑战<sup>[4-5]</sup>,计算存储资源

的共享使得传统的安全边界变得模糊,数据安全难以得到保证。而密码技术提供的数据加解密、数据完整性、认证、访问控制等密码服务,能够有效地为传统应用系统提供安全保障。但大数据环境是大数据技术与云计算技术融合而成的,一般基于云平台搭建,具有数据量庞大、数据类型多样化、应用系统动态接入与资源按需自动化部署、多租户资源共享等新特征。现有的

**收稿日期:**2017-09-08

**修回日期:**2018-01-05

**网络出版时间:**2018-05-16

**基金项目:**国家重点研发计划战略高技术重点专项(17-H863-01-ZT-004-009-01);国家自然科学基金(91430214)

**作者简介:**高秀武(1992-),男,硕士,研究方向为大数据安全、云计算安全、密码技术;刘文丽,硕士,高级工程师,研究方向为大数据安全、云计算安全、密码技术。

**网络出版地址:** <http://cnki.net/kcms/detail/61.1450.TP.20180515.1651.030.html>

密码服务系统无法在大数据环境中高效的服务能力与资源利用率最大化两者之间达到平衡,并提供安全的密码服务。

面对大数据环境新的密码服务需求,文献[6]提出一种通用的高性能密码服务系统模型,通过统一的服务接口设计相应的密码服务资源调度算法,实现不同密码机密码资源的统一管理,解决了密码资源的动态分配与管理,有效提高了系统的可移植性,满足互联网在线应用对密码机的性能需求。文献[7-8]基于虚拟化技术构建了密码服务系统,提高了密码资源的利用率,解决了虚拟化环境中的密码服务问题。文献[9]针对云计算环境下业务应用系统大容量、可靠的、云密码服务系统的需求,提出密码资源池对云中密钥与密码设备实现统一全生命周期的安全管理,通过硬件虚拟化技术为多个应用系统提供高速、可靠、可扩展的密码运算服务。

综上,目前的密码服务研究侧重于解决高效的密码服务与密码资源利用率最大化问题,并没有对密码服务自身安全进行深入研究。文中提出将密码服务请求与密码任务执行相分离机制,基于 VxLAN 技术对大数据环境中多租户模式的密码服务进行网络隔离,提高密码服务自身的安全性。

## 1 大数据环境密码资源池与多租户网络隔离技术分析

云计算技术通过聚合大量的计算、存储、网络以及软件等资源,基于虚拟化技术为租户提供所需的服务,把云计算提供的各类服务所需要的资源集合看成一个巨大的“资源池”<sup>[10]</sup>。云计算资源池具有高可靠性、通用性、动态弹性、虚拟化以及低成本等优点,能够供租户在任意位置通过网络访问并按需获取服务,提高了资源的利用率。

大数据环境中面临的高性能、多租户、动态弹性等密码服务新需求,也可以采用“资源池”的模式进行解决。大数据密码资源池是指对大数据环境中密钥和密码设备实现统一全生命周期的安全管理,通过虚拟化技术为多租户提供高速、可靠、可扩展的密码运算服务,实现密码资源的共享,有效提高密码资源的利用率。

在大数据环境应用场景中,密码资源池根据租户密码服务需求为其分配密码资源,并创建租户虚拟密码机供租户进行密码服务访问。租户虚拟密码机负责密码服务请求认证与任务的分配,密码资源池负责维护租户虚拟密码机与密码资源之间的映射关系,从而为租户提供高性能、多样化的密码服务。

## 2 多租户网络隔离相关技术分析

大数据环境下多租户共享密码资源,如何实现租户的密码服务网络隔离,是密码资源池研究的关键之一。传统网络隔离通过交换机划分 VLAN 来实现,但由于 VLAN ID 只有 12 比特,最多只有 4 094 个虚拟子网,难以满足大数据环境中大量的租户网络需求。其次交换机 VLAN 划分配置的不灵活性,很难匹配大数据环境下资源动态按需分配的特征。随着网络虚拟化的不断发展,软件定义网络 (software defined networking, SDN<sup>[11]</sup>) 的出现为新一代网络架构提供了技术方向。基于 SDN 思想的 OpenFlow 技术,可以实现网络资源的按需服务与动态配置。同时利用 VxLAN 网络隔离技术,将类似于 VLAN ID 的隔离标识位扩展到 24 位,可支持高达 16 M 的租户隔离,能够很好地满足大数据环境下多租户的网络隔离需求。

### 2.1 OpenFlow 技术

OpenFlow 技术是 SDN 网络架构的一个具体实现,其核心思想是将传统网络设备中控制逻辑与数据转发逻辑相分离,形成两个相对独立的模块。如图 1 所示,OpenFlow 架构主要由 OpenFlow 控制器、OpenFlow 交换机与 OpenFlow 协议组成,控制器与交换机之间通过 OpenFlow 协议来实现安全通信<sup>[12-13]</sup>。交换机与控制器进行通信之后,控制器拥有了整个网络的交换机信息,并通过链路发现协议 (LLDP) 获取网络的链路信息,从而控制器组成了整个网络拓扑结构。控制器将流表安装在交换机上,交换机根据流表规则对数据包进行转发。当交换机收到无法处理的数据包,交换机通过 packet-in 操作反馈给控制器,控制器根据具体的需求生成流表并下发到交换机,对交换机的转发策略进行修改,从而对网络进行相应的管理与控制。

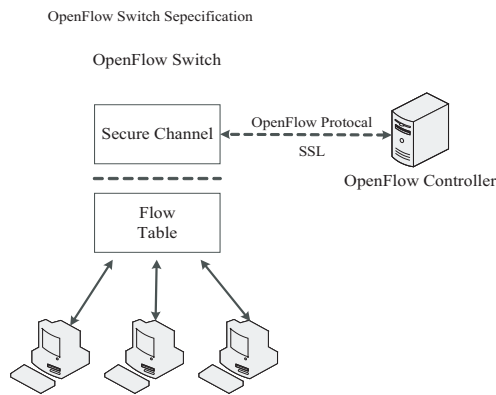


图 1 OpenFlow 架构

### 2.2 VxLAN 网络隔离模型

VxLAN<sup>[14-16]</sup> 是一种将以太网报文封装成 UDP 报文进行隧道传输的数据转发模式,是 Overlay 网络技术领域提出的一种较为成熟的技术方案。Overlay 网

络在不改变原有网络架构的基础上叠加虚拟化技术模式,将原始二层报文通过添加新的报文头叠加封装成为新的数据包。而这种新的数据包仍然是 IP 数据包格式,可以在现有成熟的 IP 网络上进行传输,不必对现有网络架构做出大的改动。VxLAN 数据报文格式如图 2 所示,其中 VxLAN 头里包含 24 比特的标识位 VNI,用于区分不同的 VxLAN,只有相同 VxLAN 的虚拟机之间才能相互通信。

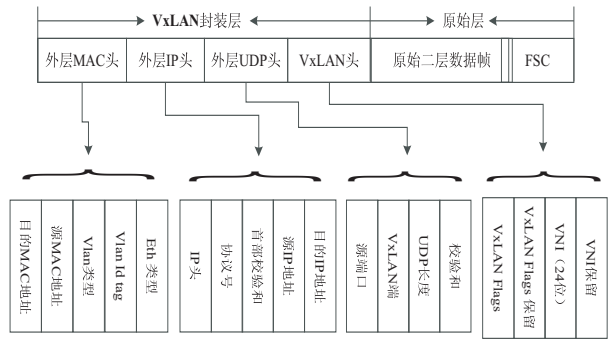


图 2 VxLAN 报文格式

VxLAN 数据包的 VxLAN 号识别、VxLAN 封装与解封、VxLAN 报文转发等相关处理都是在 VTEP 上进行的。VTEP 既可以在虚拟机终端实现,也可以在虚拟机连接的交换中实现,VxLAN 网络模型如图 3 所示。在 VxLAN 网络中虚拟机发送报文,首先由虚拟机连接的交换机判断报文目的虚拟机是否是在同一服务器的虚拟机,若是根据转发规则在服务器内转发;若报文目的虚拟机不是同一个服务器的虚拟机,则将报文转发给 VTEP,由 VTEP 进行封装,然后转发到核心网络中,通过核心网络中的 VxLAN 隧道转发到对端 VTEP,在对端 VTEP 中对 VxLAN 报文解封后发送到目的虚拟机。

VxLAN 技术使用成熟的 IP 网络作为传输隧道,利用标准的 UDP 协议进行报文传输,对现有的网络设

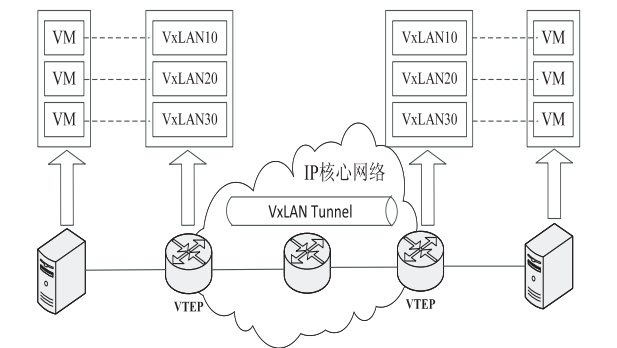


图 3 VxLAN 网络模型

备与网络架构几乎不做改动,实现简单且成本低。VxLAN 提供 4K 的网络隔离标识,能够很好地满足大数据环境中大量租户网络隔离的需求。其次,VxLAN 技术在云计算的多租户网络隔离上取得了很好的实现,完全满足当前云计算数据中心的网络隔离需求,对大数据环境密码资源池多租户网络隔离具有很好的借鉴意义。

3 密码资源池密码服务安全隔离分析

3.1 密码资源池密码服务安全需求分析

大数据环境下密码资源池对密码资源进行统一全生命周期的管理,为租户提供高性能、多样化的密码服务,从而为租户业务环境提供安全保障。密码服务为租户环境提供安全保护,其自身的安全是租户业务环境安全的根本之源。因此在多租户模式下密码资源池需要实现密码服务整个生命周期的安全隔离,从而确保密码服务的自身安全。大数据环境下的密码资源池将租户的密码资源与租户业务环境构建在同一安全域,租户业务环境应用只能访问属于自己的密码资源,密码服务不能跨安全域进行访问,实现密码服务的安全隔离。大数据环境下密码资源池多租户密码安全隔离逻辑视图如图 4 所示。

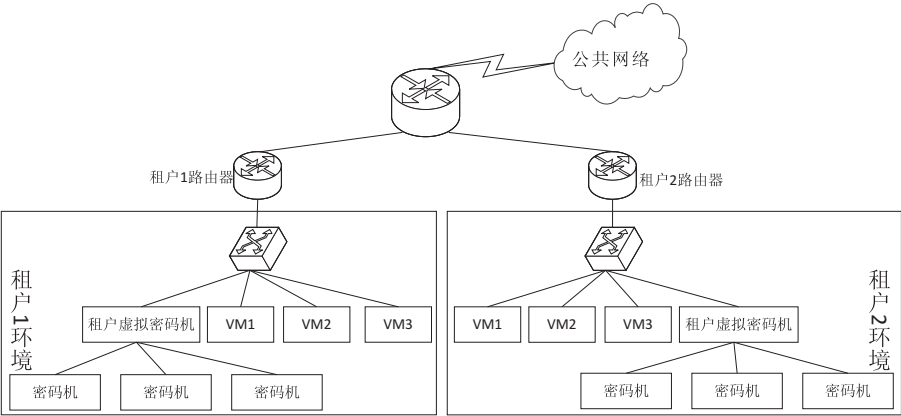


图 4 密码资源池多租户逻辑视图

大数据环境下密码资源池根据租户密码服务需求为其分配密码资源,然后基于虚拟化技术为租户创建一个高性能的租户虚拟密码机,密码资源池负责维护

租户虚拟密码机与密码资源之间的映射关系,租户只需访问租户虚拟密码机即可获得密码服务。因此,在密码资源池的工作原理下,密码服务整个生命周期可



以分为密码服务请求与密码任务执行两个阶段。密码服务请求阶段负责密码服务请求认证与密码任务的调度分配工作,主要在租户虚拟密码机上完成;密码任务执行阶段负责密码任务具体密码计算与计算结果反馈,主要在密码机上完成。因此,大数据环境下密码资源池的密码服务自身安全可以从这两阶段进行分析研究。

### 3.2 密码服务请求阶段安全隔离分析

密码机在传统应用系统中使用时,应用系统服务器独享密码设备,服务器与密码机在同一个安全域中进行网络互联。所有密码服务请求由服务器发起,密码机进行密码计算并给服务器反馈计算结果,从而为应用系统提供安全保障。密码机在应用系统的安全域中使用,密码机抽象密码操作细节向上提供密码服务接口供应用系统调用,密码服务整个生命周期具有很高的安全性。因此,在大数据环境多租户模式下,密码资源池通过虚拟化技术根据租户需求分配一个高性能的租户虚拟密码机,租户虚拟密码机负责密码服务请求以及密码任务的分配工作,保留了租户应用与租户虚拟密码机在同一个安全域中的特性,确保租户密码服务请求阶段的相互隔离。

### 3.3 密码任务执行阶段安全隔离分析

大数据环境下密码资源池密码任务执行阶段的安全隔离主要包括租户虚拟密码机与密码机之间数据传输通道的安全隔离以及密码机内密码运算环境的安全隔离。目前大数据环境常用密码设备有服务器密码机与云密码机,云密码机基于虚拟化技术可以在一台实体密码机虚拟出多台虚拟密码机。服务器密码机通过提供 API 对外服务,屏蔽密码运算具体细节,保证密码运算环境安全。对于密码资源池的服务器密码机的密码任务安全隔离,只需确保租户的整个生命周期之内只对所属租户提供密码服务,即不允许许多租户在同一个时间段内共享密码机,从而保证租户密码任务执行阶段的安全隔离。而对于云密码机,租户虚拟密码机到虚拟密码机共享物理传输通道,需要构建虚拟的安全域边界,实现租户虚拟密码机到虚拟密码机数据传输通道的相互隔离;其次多个虚拟密码机共享云密码机硬件资源,云密码机需确保不同租户的虚拟密码机密码任务运算环境的安全隔离,从而确保租户密码任务执行阶段的安全隔离。

## 4 基于 VxLAN 的密码资源池多租户安全隔离模型

由上节密码资源池密码服务安全隔离需求分析可知,大数据环境下的密码资源服务应能与租户环境构建在同一虚拟安全域中,通过虚拟安全域边界防护可

达到与物理安全域相同的数据保护和隔离效果,使租户相信自己申请的密码资源独自占有,其他租户无法访问,实现大数据环境密码资源池多租户模式下的密码服务安全隔离。文中提出基于 VxLAN 技术对大数据环境密码资源池多租户进行安全域划分,其安全隔离模型如图 5 所示。

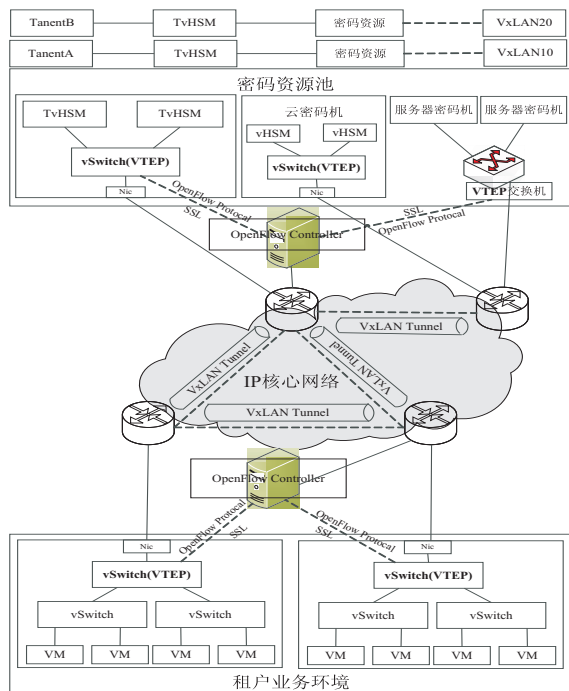


图 5 大数据环境密码资源池多租户隔离模型

该模型主要包括三个方面:

#### (1) 密码资源池密码服务机制。

在大数据环境应用场景中,密码资源池根据租户密码服务需求为租户分配密码资源,创建租户虚拟密码机供租户密码服务访问,密码资源池负责维护租户虚拟密码机与密码设备之间的映射关系,租户虚拟密码机负责租户密码服务请求处理以及密码任务的分配。租户业务环境所有的密码服务访问都由租户虚拟密码机处理,将密码服务请求与密码任务执行隔离,租户不与密码设备直接交互,提高了密码资源的安全性。

#### (2) 基于 OpenFlow 的 VxLAN 网络实现。

大数据环境下基于 OpenFlow 技术进行网络控制管理,交换机根据 OpenFlow 控制器下发的流表进行数据报文转发。在 OpenFlow 网络中,当交换机接收到一个新的数据包,会将数据包通过 packet-in 反馈给 OpenFlow 控制器,OpenFlow 控制器就可以很方便地学习全局的 MAC 地址与 VxLAN 网络的 VTEP IP 地址。控制器中维护着 MAC 地址表与 VTEP IP 映射关系表,MAC 地址表记录 OpenFlow 控制器管理的 vSwitch 端口与虚拟机 MAC 地址的映射关系,VTEP IP 映射关系表则记录 VNI 号、MAC 地址以及 VTEP IP 的映射关系。Open Flow 控制器通过 MAC 地址表与 VTEP IP 映射表

信息为管理的交换机下发相关数据转发流表,从而实现对 VxLAN 网络的控制。VTEP IP 映射表是 VxLAN 网络隔离的基础,其映射关系如表 1 所示。由 VTEP-IP 映射表可以通过 VNI 判断数据报文发送端与目的端是否属于同一个 VxLAN,同时用于封装 VxLAN 数据报文时添加外层 IP 地址。

表 1 VTEP-IP 映射表

VNI	MAC 地址	VTEP IP
000001	74-27-EA-A0-B7-83	192.168.100.1
000001	00-50-56-88-49-1F	192.168.100.2
...	...	...
FFFFFF	0A-57-3B-6E-F1-20	192.168.200.3

在 OpenFlow 控制器学习到 MAC 地址表与 VTEP IP 映射关系表信息后,将相关转发流表下发到控制的交换机,交换机便可以根据流表规则进行数据报文的转发。VxLAN 网络的转发流程如图 6 所示。

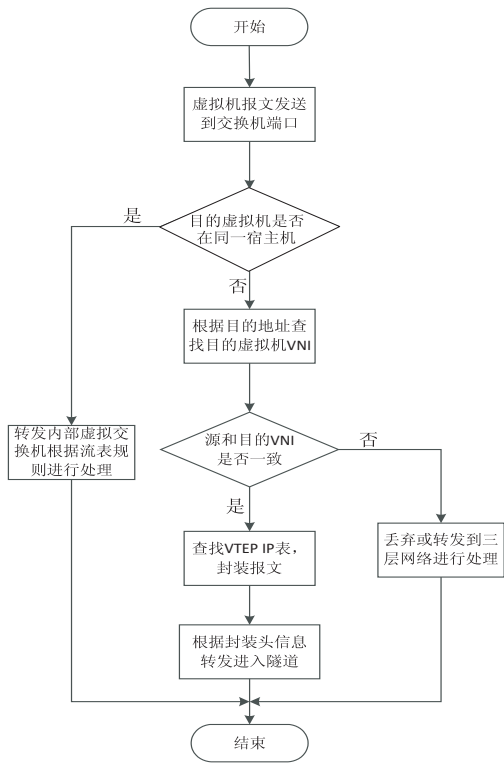


图 6 VxLAN 网络数据报文转发流程

虚拟机报文发送到 VTEP 交换机,交换机判断报文的目的虚拟机是否与源虚拟机在同一宿主机,若是则转发给内部虚拟交换机根据流表进行转发处理。若不是,则根据目的地址查询所属 VNI 号,并判断源端虚拟机是否是一个 VxLAN。若不属于同一个 VxLAN,则丢弃数据报文或转发到三层网络进行处理;若属于同一个 VxLAN,则查询对端 VTEP IP 地址进行封装并转发进入隧道传输。因此,可以很好地实现同一个 VxLAN 的设备进行网络互通,属于不同 VxLAN 的设备之间进行隔离。

(3)基于 VxLAN 构建大数据环境下密码资源池租户虚拟安全域环境。

大数据环境下密码资源池租户环境包括租户业务环境、租户虚拟密码机以及租户密码资源。基于 OpenFlow 实现的 VxLAN 网络虚拟化技术,可以很容易地构建大数据环境密码资源池租户虚拟安全域环境。在租户业务环境、租户虚拟密码机以及云密码机的宿主主机上安装带有 VTEP 功能的 Open vSwitch(虚拟交换机),服务器密码机连接到实现了 VTEP 功能的实体交换机,实现 VxLAN 数据包的封装、解析以及转发功能。租户通过大数据云平台网络服务规划自己的虚拟网络,将租户业务环境的所有虚拟机、租户虚拟密码机以及密码资源连接到同一个子网中。OpenFlow 控制器通过管理的网络设备能够及时获取用户虚拟网络信息,VxLAN 自动在物理网络上建立 VxLAN 隧道,为租户虚拟网络设置网络边界,实现同一租户虚拟机与密码资源之间的互联互通,不同租户虚拟机与密码资源之间的网络隔离,为多租户创建相互隔离的虚拟安全域环境,从而确保大数据环境下密码资源池多租户密码服务的安全隔离。

5 结束语

文中对大数据环境下密码资源池多租户密码服务安全隔离需求进行分析,研究了 OpenFlow 软件定义网络技术以及 VxLAN 网络虚拟化技术。针对大数据环境密码资源池多租户密码服务网络隔离问题,提出一种将密码服务请求与密码任务执行相分离的服务机制,基于 VxLAN 技术实现网络隔离的密码资源池多租户安全隔离模型,很好地解决了大数据环境下密码资源池多租户密码服务安全隔离问题。

参考文献:

[1] 孟小峰,慈 祥. 大数据管理:概念、技术与挑战[J]. 计算机研究与发展,2013,50(1):146-169.

[2] 马立川,裴庆祺,冷 昊,等. 大数据安全研究概述[J]. 无线电通信技术,2015,41(1):1-7.

[3] 林 闯,苏文博,孟 坤,等. 云计算安全:架构、机制与模型评价[J]. 计算机学报,2016,36(9):1765-1784.

[4] DEMCHENKO Y,ZHAO Zhiming,GROSSO P,et al. Addressing big data challenges for scientific data infrastructure[C]// 4th IEEE international conference on cloud computing technology and science. Taipei,Taiwan:IEEE,2013:614-617.

[5] SALLEH K A,JANCZEWSKI L. Technological,organizational and environmental security and privacy issues of big data:a literature review[J]. Procedia Computer Science,2016,100:19-28.

表3 7次实验预测结果

PH	温度 /℃	装液 量/ml	转速	接种 量	种龄	发酵 时间	桑黄产量 /(μg/ml)	迭代 次数
6	29	100	150	12%	7	8	2164	39
6	28	901	150	12%	8	11	2204	31
6	30	90	150	12%	7	12	2121	208
6	30	90	141	9%	8	8	2045	430
6	28	90	150	12%	8	11	2204	52
6	29	100	150	12%	9	11	2207	44
6	29	100	150	12%	8	8	2171	56

4 结束语

利用桑黄实验数据作为载体,提出了一种利用计算机技术处理生物实验数据的方法。实验结果表明,模型预测的最优条件与生物实验结果一致,证明该方法对培养条件优化具有良好的可预测性。机器学习与数据挖掘的算法在处理大量数的生物数据具有独特优势,是生物信息学潜在的发展方向<sup>[16-17]</sup>。

参考文献:

[1] 王勇献,王正华.生物信息学导论[M].北京:清华大学出版社,2011.

[2] LAVECCHIA A. Machine-learning approaches in drug discovery: methods and applications[J]. Drug Discovery Today,2015,20(3):318-331.

[3] 张梅,潘大仁,周以飞,等. BP神经网络结合正交试验法优选锦锈杜鹃黄酮的提取工艺[J]. 信阳师范学院学报:自然科学版,2011,24(2):261-264.

[4] KHAOUANE L,SI-MOUSSA C,HANINI S,et al. Optimization of culture conditions for the production of Pleuromutilin from Pleurotus Mutilus, using a hybrid method based on central composite design, neural network, and particle swarm optimization[J]. Biotechnology & Bioprocess Engineering, 2012,17(5):1048-1054.

[5] TSAI M F,YU S S. Data mining for bioinformatics: design

with oversampling and performance evaluation[J]. Journal of Medical & Biological Engineering,2015,35(6):775-782.

[6] BAZZAN A L C. Agents and data mining in bioinformatics: joining data gathering and automatic annotation with classification and distributed clustering[M]//Agents and data mining interaction. [s. l.]:Springer-Verlag,2009:3-20.

[7] SAEB A,DAVID S K,RUBEAN K A. Comparative analysis of data mining tools and classification techniques using WEKA in medical bioinformatics[J]. Computer Engineering & Intelligent Systems,2013,4(13):11-17.

[8] LI Zhongwei,XIN Yuezheng,WANG Xun,et al. Optimization to the culture conditions for phellinus production with regression analysis and gene-set based genetic algorithm[J]. Biomed Research International,2016,8(1):1-7.

[9] 刘伟. 药用菌桑黄代代谢黄酮的调控研究[D]. 青岛:中国石油大学(华东),2012.

[10] COHEN G,HILARIO M,SAX H,et al. Learning from imbalanced data in surveillance of nosocomial infection[J]. Artificial Intelligence in Medicine,2006,37(1):7-18.

[11] 梁循. 数据挖掘:建模、算法、应用和系统[J]. 计算机技术与发展,2006,16(1):1-4.

[12] 王崇骏,于汶滢,陈兆乾,等. 一种基于遗传算法的BP神经网络算法及其应用[J]. 南京大学学报:自然科学版,2003,39(5):459-466.

[13] 徐远芳,周旻,郑华. 基于MATLAB的BP神经网络实现研究[J]. 微型电脑应用,2006,22(8):41-44.

[14] 赵志鹏,董红斌. 一种新的基于遗传操作的改进型遗传算法[J]. 计算机应用与软件,2008,25(1):235-237.

[15] MARDLE S,PASCOE S. An overview of genetic algorithms for the solution of optimisation problems[J]. Cheminform, 2007,26(16):1785-1790.

[16] WANG Xun,SONG Tao,GONG Faming,et al. On the computational power of spiking neural P systems with self-organization[J]. Scientific Reports,2016,6(1):24-27.

[17] 张方舟,高晓松. 基于条件函数依赖的挖掘算法研究[J]. 计算机技术与发展,2015,19(5):56-59.

(上接第131页)

[6] 寇文龙,陈莉君. 通用高性能密码服务系统模型[J]. 微电子学与计算机,2016,33(10):87-90.

[7] 林璟铨. 一种基于虚拟化环境中提供密码服务的方法和系统:中国,104461678[P]. 2015-03-25.

[8] 李国,蔡成杭,马晓艳,等. 一种基于宿主机的密码机及密码运算实现方法:中国,105871540[P]. 2016-08-17.

[9] 张晏,岑荣伟,沈宇超,等. 云计算环境下密码服务资源池的应用[J]. 信息安全研究,2016,2(6):558-561.

[10] 涂俊. 云计算—安全资源池化[J]. 信息通信,2017(4):119-120.

[11] KREUTZ D,RAMOS F M V,VERISSIMO P E,et al. Software-defined networking: a comprehensive survey[J]. Proceeding of the IEEE,2015,103(1):10-13.

[12] ROTHSCHILD N,ARRAR N,UHLIG S,et al. OFLOPS: an open

framework for OpenFlow switch evaluation[C]//Proceedings of the 13th international conference on passive and active measurement. [s. l.]:[s. n.],2012:85-95.

[13] LARA A,KOLASANI A,RAMAMURTHY B. Network innovation using OpenFlow: a survey[J]. IEEE Communications Surveys & Tutorials,2014,16(1):493-512.

[14] 齐保社. 面向数据中心的 VXLAN 系统设计与实现[D]. 南京:南京大学,2017.

[15] PAUL S,JAIN R,SAMAKA M,et al. Application delivery in multi-cloud environments using software defined networking[J]. Computer Networks,2014,68(11):166-186.

[16] VARADHARAJAN V,TUPAKULA U. Trust enhanced security for cloud environment[C]//IEEE international conference on trust, security and privacy in computing and communications. [s. l.]:IEEE,2012:145-152.