RSA 加密算法在私有云平台中的应用

余丽萍,朱 亮*,雷婷婷
(郑州轻工业大学,河南 郑州 450001)

摘要:全球计算机网络以及云计算平台智能化的不断普及,尤其是基于 SSL 协议的迭代升级和快速蔓延,促使数据信息安全在日常开发应用体系中变得尤为重要。传统云计算平台采用 CA 加密证书保证数据传输安全,文章提出一种基于 RSA 加密算法的私有云平台架构,使用基于 SpringBoot 框架快速搭建私有云平台,形成对私有云网络传输安全、高性能、高可用的一套解决方案。最后,通过搭建原型系统,对系统进行功能测试和性能测试。实验证明,文章提出的私有云平台架构比传统的私有云平台具有更高的下载速度,下载速度可达每秒百兆级别。

关键词:私有云平台;RSA 算法;SSL 协议;CA 证书
中图分类号:TP301.6 **文献标志码**:A

0 引言

伴随着云计算时代的来临,全球云盘市场将受到更大的安全挑战。5G、云计算技术推动了云盘行业的快速发展,据数据统计,2020 年中国云计算(Infrastructure as a Service,IaaS)市场规模约达 895 亿元。市场发展日趋成熟,配套设施不断完善。以云计算为基础的云盘服务也不断发展,5G 技术的高速率传播特性能够优化云盘体验,驱动云盘市场发展[1]。个人云盘使得用户的应用场景丰富化,并提升用户的工作、生活效率。个人云盘将进一步取代个人计算机(Personal Computer, PC)的核心地位,成为人们工作和生活的主要工具[2]。此外,个人云盘与智慧家居、5G 生活、虚拟现实(Virtual Reality, VR)技术等相结合,极大地改变了用户的生活方式,打造了一个智能化的人类文明社会。企业云盘的投入使用能促进企业数字经济的发展,提高企业的工作效率,为企业带来丰富的云上资源,促进企业高质量发展。云存储系统能够解决当前普遍存在的数据资源安全存储、便捷快速共享等问题,使内容安全性得到保障[3-4]。

本文主要设计了一套私有云平台的总体构建方案,提出了基于(Rivest-Shamir-Adleman, RSA)加密算法的私有云平台架构,并通过响应速度、并发压力、文件下载速度 3 个方面对私有云平台的性能进行了测试。

1 相关工作

1.1 国内研究现状

国内个人云盘行业主要以免费的网盘服务吸引用户并培育市场,2011 年广州市政府提倡建设智慧城市,国内三大运营商快速开发自己的私有云存储空间。例如:中国联通 2012 年推出的“悦云”、中国电信 2013 年推出的“天翼云”、中国移动 2014 年推出的“彩云”。为了推进上云时代的到来,三大运营商决定无论使用哪个运营商的电话号码都可以进行注册、登录,极大地方便了广大用户对私有云平台的使用。直到 2016 年的关停潮,其他的云盘厂商开始积极尝试探索新的商业模式,逐渐发展为以付费为主的云平台服务,用户如果想使用云存储空间的额外大小和下载速度,需要付费才能全速下载。截至 2021 年,中国个人云盘市场交易规模预计达 24 亿元,同比增长 42%[6]。随着疫情的到来,从 2020 年起企业逐渐支持线上办公,上班群体的需求逐渐增大,用户不仅需要在家里进行移动办公,而且还要做到文件数据同步到公司数据库,激发了云盘市场的增量化以及对私有云平台的迫切需求。截至 2021 年 1 月,百度网盘约占市场份额比的 85%,行业已经趋显寡头化,但是随着个人云盘行业的活跃用户在波动中缓慢扩大,阿里云盘快速兴起,同时也出现了其他各式各样的私有云平台。

基金项目:国家自然科学基金;项目名称:位置信息共享下面向智能服务推荐的隐私保护方法研究;项目编号:61902361。
作者简介:余丽萍(1984—),女,河南平顶山人,中级实验师,硕士;研究方向:服务计算,隐私保护。
*通信作者:朱亮(1987—),男,河南焦作人,讲师,博士;研究方向:智能推荐,隐私保护。

1.2 国外研究现状

2002 年 RapidShare 成立,它是全球最早的网盘产品。2007 年开始转型为云盘企业,使用企业级用户超过 2 000 万。美国凭借其较先进的信息技术,最早提出“云文件”的研究概念。谷歌在 2006 年已经提出云计算的概念,之后主流的 IT 厂家均推进了云计算和私有云平台的服务和应用,例如:Google 的 Cloud Storage 云盘,亚马逊的简单储存服务(Amazon Simple Storage Service, Amazon S3),EMC 的 EMC Atmos 云存储平台,微软云存储 skydrive,IBM 企业级的云计算技术和服务组合 IBM SmartCloud[5]。2020 年以来,私有云平台市场的用户量呈指数型快速增长,推动了全球私有云市场规模的发展。面对庞大的市场需求,大型的互联网企业纷纷推出自己的云存储产品类型,而作为更具功能性的私有云存储将成为未来云存储的主流模式。

综上所述,5G 信息时代的到来,私有云平台厂商加大力度推陈出新。未来的私有云平台将伴随着人工智能、大数据等新兴技术的出现而快速发展,云上文件将像现在的电脑文件一样,实现随时可取、随地可存。

2 总体架构

私有云平台的主要模块包括:Nginx 服务模块、Tomcat 服务模块以及 DNS 服务模块。Nginx 服务主要是云服务的反向代理,保证服务器域名或 IP 地址到 Tomcat 服务的映射关系,不参与应用提供服务的同时还可以抵御大部分的网络攻击和非法请求;Tomcat 服务主要是为应用提供服务,保证私有云系统能在 Tomcat 服务上正常、稳定地运行;DNS 服务主要是域名解析,通过域名访问请求解析出对应的 IP 地址,实现网络域名通信的正常访问。

为了搭建私有云平台,本文在业务逻辑上采用 MVC 分层架构。在网络通信上采用 B/S 架构,当应用服务需要更新或者扩展时,它可以在不需要停服更新的情况下处理系统维护,实现无缝替换部署上线,私有云平台的总体架构如图 1 所示。

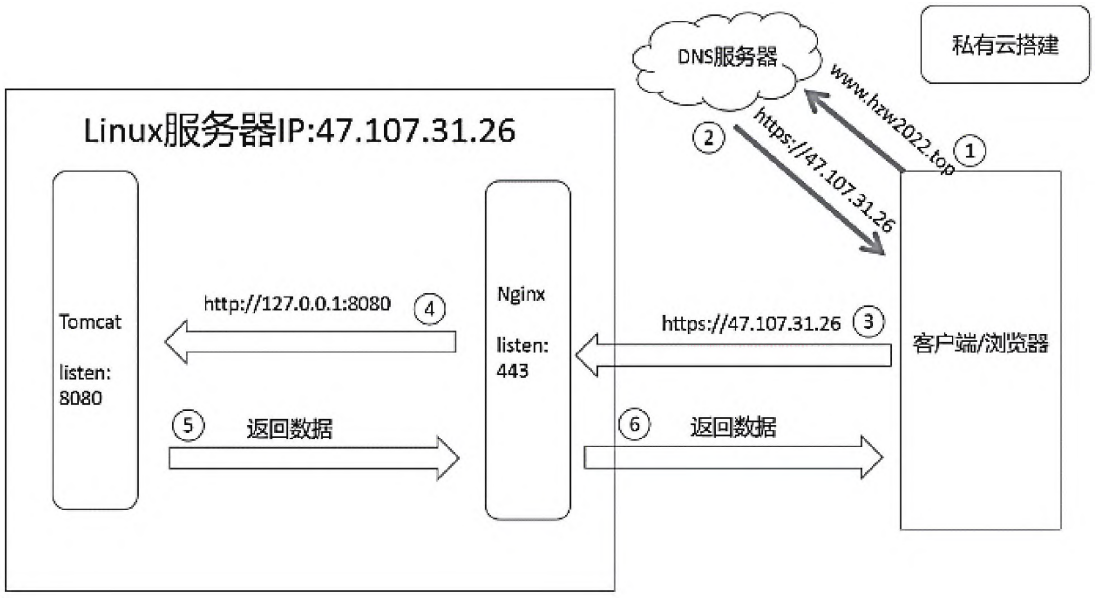

图 1 私有云平台的总体架构

在图 1 中,数据请求访问的流程如下:

(1)通过 https://www.hzw2022.top 域名访问,DNS 云解析服务器首先查找对应的 IP 服务主机,完成域名解析;

(2)当 DNS 云解析服务器找到 IP 服务主机时,返回 IP 服务主机的地址;

(3)浏览器根据 IP 主机服务地址发送请求,端口为 443(浏览器 HTTPS 的默认端口);

(4)服务器主机(47.107.31.26)收到请求后,处理来自 443 端口的所有请求并转发,根据请求转发给 http://127.0.0.1:8080;

(5)Tomcat 服务收到来自 Nginx 的 HTTP 请求,处理并响应,返回响应数据;

(6)Nginx 收到来自 Tomcat 的响应数据,再次转发数据到客户端,完成数据请求。

3 RSA 加密算法

3.1 OpenSSL 工具生成 CA 证书

CA 证书是相关权威机构颁发的数字签名证书,签名证书上有颁发的机构,SSL 协议涵盖了许多加密需求。也可以使用 Linux 系统中的 OpenSSL 工具生

成 CA 证书,但是会显示此链接不是安全连接。

在 Linux 环境中生成 CA 证书过程如下:

(1)安装 OpenSSL 工具;

(2)生成 CA 证书。

CA 证书添加方法:安装以上命令生成的 CA 证书,在/usr/local/nginx/conf 文件夹下会有 3 个文件,分别是 server. crt、server. key 和 server. csr 3 个文件(其中的 server. crt 也可以是 server. pem),其中 server. crt 文件是证书,其中包含了公钥,server. key 文件是私钥。

3.2 CA 证书的使用

CA 证书用于 Nginx 代理服务,在数据传输时进行加密。由于本文所设计的架构中,Nginx 服务和 Tomcat 服务处于同一个服务器,故在 Nginx 和对外互联网连接的接口上添加了 SSL 协议,而在 Linux 本机内部没有使用 SSL 协议。同时,Nginx 与代理器端也进行了数据传输加密,和 CA 证书添加方法类似,只需在 nginx. conf 配置文件中添加 proxy_ssl_certificate 和 proxy_ssl_certificate_key,具体流程如图 2 所示。

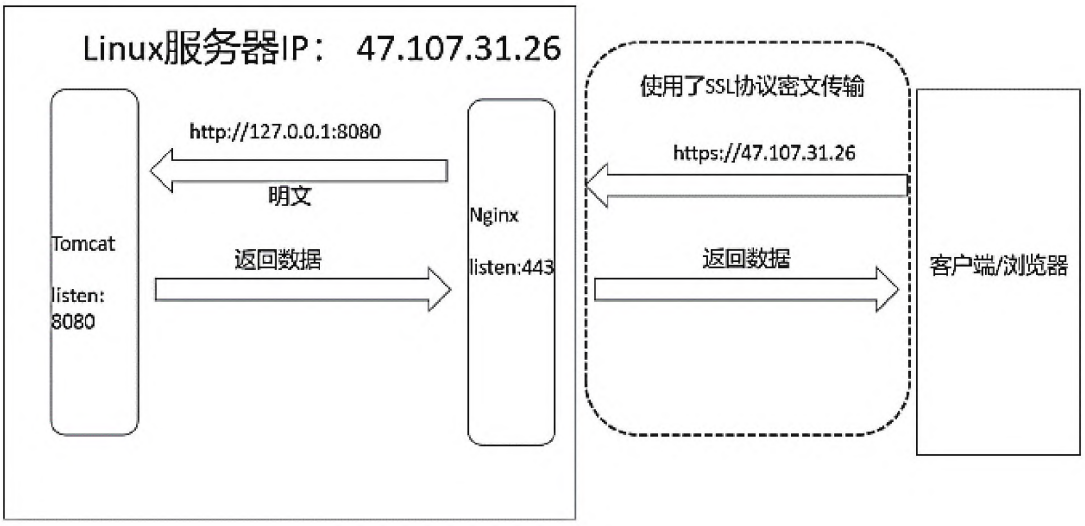

图 2 SSL 协议数据传输流程

4 平台实现

本文的数据库设计分为 MySQL 数据库和 H2 数据库。MySQL 数据库主要存放用户信息、密码信息相关的表。用户使用云数据库时,可以实现按需付费、弹性扩容、动态升级等功能。根据数据库功能数据设计要求,为了满足数据的存储效率和数据表的信息完整性,本文所设计的表数据库满足第一范式、第二范式、第三范式的设计模式[7]。考虑到安全问题,用户密码表采用了 MD5 加密的方式,实际上存放的是前端 MD5 算法加密后的 64 位字符串。对于云存储文件,用户可以自定义文件分类,例如:依据个人的喜好或者需求来分类。分类的基本原则是用户能够方便管理和查找文件资料[8]。

在数据传输安全方面,本文采用 CA 证书,使用 HTTPS 传输协议,保障数据传输安全,避免用户数据在传输过程中出现被不法分子窃取、篡改等情况。除此之外,系统本身还涉及预防网络攻击的安全防护功能,例如:常见的 DDOS 攻击,通过大规模互联网访问请求目标主机服务器,造成网络拥堵、CPU 阻塞等现象,以达到使服务器出现宕机或者对外拒绝访问的目的。对于 DDOS 攻击,只需在 Nginx 上限制同一个 IP 请求访问的次数,同一个 IP 地址发出的请求每秒允许 2 个,按照正常人的手速,刷新一个网页的速度基本在每秒 2~3 次左右,如果超出这个频率将可能是代码发出的请求。Nginx 任务是当同一个 IP 的请求每秒大于 2 时,将不再接收这一秒内的其他请求。

对于内存而言,每个连接数分别对应一个 read_event 和一个 write_event。每个连接数占用 232 字节,2 个事件总占 96 字节,那么一个连接占用 328 字节,通过数学公式算出 100 000 个连接数大概占用 31 MB = 100 000×328/1 024/1 024,这只是 Nginx 启动时,connections 连接数所占用的 Nginx,现在的计算机内存已经达到至少 4GB、8GB,进程的最大可打开文件数取决于本机操作系统。文中使用的单核 Linux 系统进程最大可打开文件数为 65 535,而实际在代理服务器中 Nginx 最大并发数为 worker_processes×worker_connections/2。

5 性能测试

系统测试采用响应速度测试和并发压力测试,响应速度测试是保证在全国各地都能访问到私有云平

台,不会出现由于地理位置原因而影响私有云平台使用的情况,压力测试是保证私有云平台服务的稳定性,能够承受并处理大量并发请求。

5.1 响应速度测试

本部分使用 https://www.17ce.com 网站测试,该工具的特点是在全国各地都有测试请求服务器,帮助用户做请求访问测试,同时生成测试数据分析表。生成的数据分析表如图 3 所示,由于本文实验部分购买的服务器处在华南地区的深圳,因此网速较好的地方集中在华南地区。

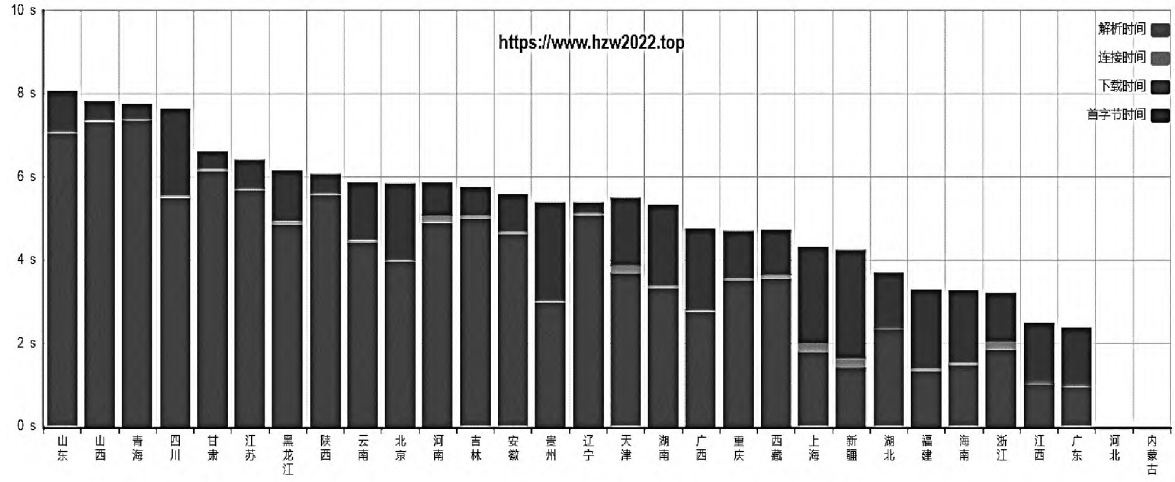

图 3 测试数据分析

5.2 压力测试

本部分使用 ApiPost 测试工具 ApiPost 可以模拟 POST、GET、PUT 等常见 HTTP 请求,直接生成并导出接口文档的 API 文档,测试发出的所有请求中完成响应的次数百分比,同时显示请求失败时的位置。在 ApiPost 工具中选择测试,本次测试为 10 个进程,每个进程请求 10 次,共计 100 个请求,测试结果通过。

此外,本文对文件下载速度也做了测试,由于云服务器的带宽有限,不能完全测试出私有云的下载速度,因此只能在单机上测试文件下载速度。在单机上运行私有云平台,提前上传一个 1 452 MB 的电影,默认下载工具是迅雷,下载速度可以达到 224 MB/s,相当于 1 792 MB 带宽的下载速度。

6 结语

云存储系统虽然能够实现数据的云上存储,但是在数据的安全性以及下载速度等方面存在缺陷,数据资源安全存储及快速共享成为影响用户隐私安全及系统可靠性的主要因素。本文提出了一种基于 RSA 加密算法的私有云平台架构,使用基于 SpringBoot 框架快速搭建私有云平台,形成对私有云网络传输安全、高性能、高可用的一套解决方案,通过搭建原型系统及测试,验证了本文提出的私有云平台架构比传统的私有云平台具有更高下载速度,下载速度可达每秒百兆级别。

参考文献

[1]王煜,朱明,夏演. 非对称加密算法在身份认证中的应用研究[J]. 计算机技术与发展,2020(1):94-98.
[2]孙建刚,高颖,杨庆甫,等. 私有云平台数据云上云下备份体系设计[J]. 现代计算机,2023(2):1-5.
[3]李艳红. 大数据背景下云存储数据安全研究[J]. 网络安全技术与应用,2022(9):70-71.
[4]BINANDA S,AKANKSHA D,SUSHMITA R. Secure cloud storage with data dynamics using secure network coding techniques[J]. IEEE Transactions on Cloud Computing,2022(3):2090-2101.
[5]陈晓丹,庞双龙,曾德生,等. Ceph 存储系统在云计算环境中的应用[J]. 电子技术,2020(8):40-42.
[6]李军,劳凤丹,邹仁明. 校园网云盘系统构建研究[J]. 通信学报,2013(增刊 2):1-5.
[7]卫孝贤,刘文欣,蔡鹏. 多主云数据库的全局事务日志[J]. 华东师范大学学报(自然科学版),2020(5):10-20.
[8]王小平,张海云. 实现私有云盘数据同步[J]. 网络安全和信息化,2017(6):83-84.

(编辑 王雪芬)

(下转第 105 页)

科技风,2022(16):105-107.
[2]马丽,高敬礼,周改云. 融合 OBE+BOPPPS 的软件工程线上教学设计与实施[J]. 电脑知识与技术,2021(6):10-12.
[3]闫秀静,刘瑛,许丹凌,等. 基于课程思政理念的云班课联合 BOPPPS 医学生英语教学模式构建[J]. 中国中医药现代远程教育,2023(8):12-15.
[4]徐暄,马乃荣. 基于“云班课”的 BOPPPS 教学模式在园艺植物病虫害防治课程中的应用[J]. 现代园艺,2022(7):167-169.
[5]王英让. 基于“互联网+BOPPPS”混合教学模型的教学设计[J]. 电脑知识与技术,2021(3):170-172.
[6]熊琦. 基于 BOPPPS 的《软件工程》课程教学设计的研究[J]. 中国新通信,2022(21):122-124.

(编辑　王雪芬)

Exploration of “Software Engineering” course teaching mode based on mosoteach and BOPPPS

Fan Yongquan, Xie Chunzhi, Du Yajun
(School of Computer & Software Engineering, Xihua University, Chengdu 610039, China)

Abstract: In order to promote the achievement of teaching goals and strengthen students' ability training, explore the application of BOPPPS teaching mode based on mosoteach in the teaching of “Software Engineering”. Through a series of links such as clarifying the teaching objectives of the course, establishing teaching cases, using case-driven teaching methods, introducing multiple teaching methods, and improving assessment methods, the teaching reform of “Software Engineering” courses is explored, and corresponding improvement measures are proposed. Practice shows that this teaching method effectively cultivates students' ability to analyze and design systems.
Key words: “Software Engineering”; teaching reform; mosoteach; BOPPPS

(上接第 93 页)

Application of RSA encryption algorithm in private cloud platform

Yu Liping, Zhu Liang*, Lei Tingting
(Zhengzhou University of Light Technology, Zhengzhou 450001, China)

Abstract: With the continuous popularization of global computer network and cloud computing platform products, especially the iterative upgrade and rapid spread of SSL protocol algorithm based on network, data information security is particularly important in daily development and application system. Traditional cloud computing platform products use CA encryption certificate to ensure data transmission security. This paper proposes a private cloud platform architecture based on RSA encryption algorithm, using the SpringBoot framework to quickly build a private cloud platform, forming a set of solutions for private cloud network transmission security, high performance and high availability. Finally, by building a prototype system, functional test and performance test of the system, it is proved that the private cloud platform architecture proposed in this paper has higher download speed than the traditional private cloud platform, and the download speed can reach 100 megabits per second.
Key words: private cloud platform; RSA algorithm; SSL protocol; CA certificate