

一种基于网格的教育资源管理模型^{*})

董晓华^{1,2} 李 季¹ 吴中福¹ 邓 伟¹

(重庆大学计算机学院 重庆 400044)¹ (重庆大学经济与工商管理学院 重庆 400044)²

摘要 数据网格由于其在跨组织资源的协调共享等问题解决上的优越性,成为了广域教育资源库的首选平台。本文首先提出了适合我国教育资源管理的基于网格平台的分层模型,并针对教育资源网格的特点提出了一种教育资源管理的综合安全解决方案。实验表明,分层结构和安全体系是可行的,具有较好的有效性和可扩展性。

关键词 数据网格,教育资源管理,网络安全

A Grid-based Education Resources Mangement Model

DONG Xiao-Hua^{1,2} LI Ji¹ WU Zhong-Fu¹ DENG Wei¹

(Department of Computer Science and Technology, Chongqing University, Chongqing 400044)¹

(The College of Economics & Business Administration, Chongqing University, Chongqing 400044)²

Abstract Because of the advantage to resolve the matters of different organization resources and co-share, data grid becomes the first flat of wide area education resources. In this paper, a suitable tier model for education resource management based grid is proposed firstly, and according to the features of education resource grid, a integrated security architecture is proposed too. The experiment results show that tier model and security architecture are feasible, effective and extensible.

Keywords Data grid, Education resource management, Grid security

1. 引言

经过多年的发展,目前全国所有高校和几乎所有城市中小学都连接并网,教育资源建设也取得了长足的进步,但教育资源管理模式(Education Resource Management Model, ERMM)还停留在以前的网络形式,存储在分散的不同组织结构中的数据库中,因此存在很多突出的问题,如资源总体缺乏、重复建设、缺乏统筹规划、难以共享等。在国家发改委的下一代互联网示范工程(CNGI)中,建设开放式教育网络是构建终身学习体系的重要组成部分,而配套的远程教育资源建设是其主要内容^[1]。远程教育资源分为媒体素材、题库、案例、课件与网络课件、网络课程等,它们往往是海量的,且分布在不同地域的异构存储系统上。为了向用户透明地提供一套高效的资源共享、存储管理机制,数据网格成为一种最理想的选择^[2]。

考虑到目前 CNGI 资源管理系统的现状和可扩展性的要求,结合网络技术的发展前沿——网格技术,本文首先提出了基于数据网格技术的分层管理模型来满足资源元目录的集中式管理的需要,然后针对 CNGI 数据网格,提出了一种教育资源网格安全的综合解决方案——教育资源管理安全体系(Education Resources Management Security Architecture, ERMSA),解决了数据网格的安全问题,并在我校的搭建的 CROWN 网格平台上进行了实验分析,结果表明分层管理结构及安全体系是可行的。

2 数据网格简介

目前系统需要的高性能、大规模的数据管理、访问和存储的支持给数据管理和存储体系结构带来了巨大的挑战。传统的基于集中式的存储管理结构已不能适应这种大规模数据密

模型应用的复杂性和性能要求。因此必须通过开发专门的存储管理体系结构来对这些广域分布的资源 and 数据进行管理和协同工作。数据网格(Data Grid)就是根据这种需求,提出的一种数据管理和存储架构。数据网格的概念来自网格(Grid)^[3]。它是网格技术在数据管理方面的应用和实现。即是为了建立网格环境下,透明访问异构数据资源的新的体系结构。数据网格可以理解为是应用程序、用户等同底层存储系统之间的中间件。它对应用程序提供一致的管理和使用存储系统的界面。对用户屏蔽广域操作的复杂性和广域网络上存储系统的异构性。当前,在分布式、异构、海量数据管理上采用数据网格已经成为国内国际的发展趋势。

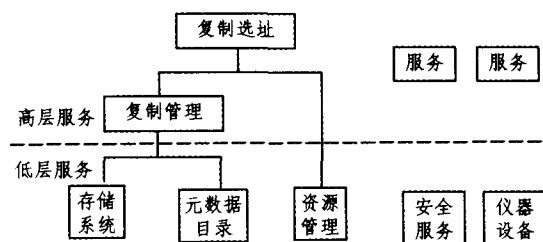


图 1 数据网格的结构和主要服务

数据网格的基本服务已由国际的 Data Grid Group 制定并由 Globus Toolkit Version 4.0^[4]实现(如图1),但是对于上层的各种服务必须根据不同的应用领域加以专门的研究并根据系统的需求实现。

在图1中,存储系统对应于各种数据库和文件系统。元数据是将网格中的数据和文件按照数据网格标准 WSRF^[5] 进行描述并加上物理存放位置的信息(类似于文件描述和索引),元数据目录包括系统中所有的元数据信息。复制管理和复制选址用于网格中文件副本的放置、维护和管理,主要目的

*)基金项目:国家发改委基金项目(CNG1-04-15-3A)。董晓华 讲师,博士生,研究方向为网络技术、远程教育;李 季 讲师,博士;吴中福 教授,博导,主要研究方向为远程教育、网络技术。

是复制常用资源以利于广域中减少网络延迟和网络负载。安全服务提供基本的安全服务接口。

3 基于数据网格的教育资源管理

通过在已有的教学资源系统上建立数据网格,可以屏蔽下层操作系统、数据库系统及不同 Web 服务的差异,给用户提供一个基于 Internet 的统一接口,从而达到整合优质教育资源,便于远程用户访问的目的。而且,我国教育资源的地域分布很广,面向的用户众多,网络延迟也比较大,只有基于数据网格进行研究和开发,才能真正实现分布式、异构资源的透明共享。

基于数据网格的教育资源管理系统的系统模型示意图如图 2。

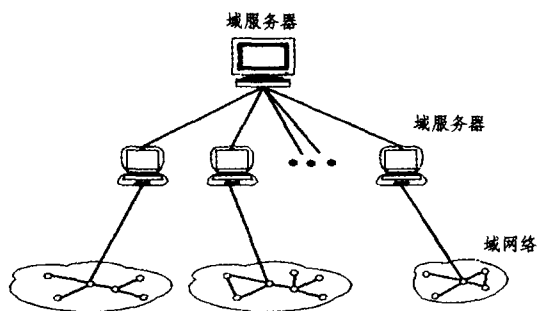


图2 一个3层的域管理机构

在图2中,每个局部网络有一域服务器,负责该域的教学资源管理,高层域服务器应有较大的存储能力。每个域内的拓扑可以为树形或者其它的无向连通图拓扑。每层内的结点根据地理位置、网络延迟等因素形成彼此不重合的域,域与域之间没有连接,域内通过其域管理结点与上一层联系。域网络中一个结点可对应于下层中的一个域管理结点,由此可以根据实际情况增加域管理的机构的层次。当一个结点加入域后向域服务器注册自己的资源,当自身资源发生更改或退出域都应该通知域服务器。域服务器定期将本地的元数据目录传递到上级域服务器。

这种分层管理的拓扑结构非常适合当前的教育资源整合。因为 CNGI 项目的第一步试点将在清华、北大、上海交大、重大等 12 所高校开展,所以这些高校将成为顶层域结点,顶层域的管理结点可以设在北京或者上海。每所高校建立自己的域管理结点,管理其域内的元数据目录和信息,还可根据实际情况向下建立更多的域。而且,这种分层管理的拓扑在资源的分布式存储的条件下实现了目录的集中统一管理,这样便于对资源进行组织和管理,从而有利于查询和复制等其它应用。

4 远程教育资源管理的安全体系结构

4.1 远程教育资源管理的安全需求

远程教育资源包括媒体素材、题库、案例、课件与网络课件、网络课程等,为了让这些资源能充分有效地得到利用,安全和隐私问题是一个重要因素^[6]。目前教育资源管理的安全和隐私研究主要包括如下几个方面:认证和授权、数据完整性、隐私保数字版权保护和交互过程保护^[7]。

1) 认证和授权能够防止非法用户访问系统,并且确保合法用户只能在其权限允许的范围内执行操作,目前大多数系统都采用基于用户名/口令方式的用户认证。

2) 数据完整性能够防止数据或程序在分发的过程中被非法读取、篡改,通常采用数据加密和数据签名来保证数据完整

性。

3) 隐私保护保证系统的行为不会侵犯用户的隐私权,从而避免触犯法律法规问题。隐私保护涉及两方面,一是提供资源的作者,包括有作者的个人信息、发布权限信息等,以及用户的私有资源;另一方面是资源的访问者,包括的信息有个人信息、用户行为和学习能力等。

4) 数字版权保护指的是网上发布资源的版权保护。数字化给学习资源的存储和传播带来了极大的方便,同时也给版权保护带来了很大的挑战,数字签名、数字水印等技术只能够帮助确定数字资源的所有权,不能够防止拷贝。避免数字资源被非法复制与传播的研究虽然取得了一些进展,但目前还没有有效解决的方法。

5) 交互过程保护是指在使用资源时的交互行为保护。一方面通过数据加密、数据签名保证交互信息不会被非法读取或篡改;另一方面,要保证交互过程的畅通,防止因为拒绝服务攻击导致系统可用性的降低。

4.2 远程教育资源管理的安全体系结构

根据数据网格的分布式和动态性特征,结合远程教育数据网格的体系结构,我们提出了一种教育资源管理安全体系(ERMSA),覆盖了系统体系结构的每个层次,如图3。在该模型中,根据远程教育数据网格的每一层次的特点,分别采用了统一入口、单一登录、访问授权、安全令牌以及 WS-Security(消息加密与签名)等技术。

1. 用户接口层

在用户接口层,采用 portal 和 rich client 实现用户使用教育资源系统的统一入口,用户从统一入口登录后,系统自动将其定向到归属节点,这样就实现了网格异构资源操作的透明性。为了防止用户敏感数据在传输过程中被窃听,客户端采用 HTTPS 方式与 Web 服务器交互。HTTPS 协议是 HTTP 协议的安全版本,主要提供认证和加密通信,它使用 SSL(Security Socket Layer)或 TLS(Transport Layer security)对回话进行加密,从而确保数据不被窃听。

2. 业务层

在业务层,通过认证和授权,确保只有合法用户才能使用该系统,并且保证用户的操作不会超越系统授予的权限。网格环境允许用户访问分布在虚拟组织中不同网络节点上的资源,用户在访问任何网络节点资源时都需要进行身份认证,这里通过单一登录避免用户在使用系统的过程中多次输入认证凭据。单一登录过程中,当用户通过身份认证后,入口节点首先利用归属节点的加密密钥对用户身份票据进行加密,然后颁发给用户,并把该票据作为 URL 的查询字符串随重定向指令发送到用户的归属节点。

基于角色的访问授权是在身份认证的基础上进一步保障系统安全。身份认证只能证明用户是否为合法用户,不能确定用户的操作权限。访问授权可根据系统预先设定的策略,提供用户能够执行系统允许的最小操作权限。角色授权策略在用户登录后随用户身份票据一并重定向到归属节点。

3. 网格中间件层

网格中间件层是实现教育资源管理的主要功能模块。在本层中,从两个层面增强了系统的安全性:机密通信和安全令牌服务。机密通信通过消息加密和消息签名机制提供了消息级的安全性,保证信息的传递过程中的安全性,它是基于开发标准的,包括 WS-Security、XML-Encryption、XML-Signature 等;安全令牌服务提供网格节点相互认证和机密通信所需的安全令牌,以及通过动态密钥生成和安全密钥交换保证虚拟组织中的共享不会被虚拟组织外的非授权用户使用,即体现

在两个方面:一是在网格不同节点操作时验证调用节点的合法性,二是对网格节点之间传输的数据进行数字签名和加密,

X.509 证书、Kerberos 票据、用户名/口令等都可以用于安全令牌。

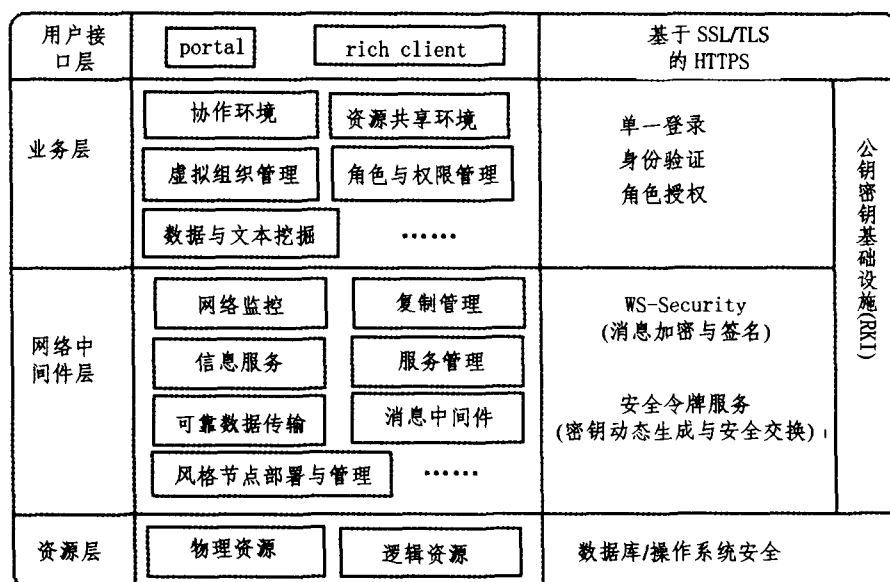


图 3 基于网格的教育资源管理安全体系结构(ERMSA)

4. 资源层

资源层包括有物理资源和逻辑资源。该层的安全策略主要依靠本地系统平台提供的安全性,如操作系统的安全措施、数据库的安全措施以及网络安全措施等。

5 实验结果及分析

在本研究小组的 CNGI 综合实验室中,搭建了 CROWN 网格平台,我们按照论文提出的教育资源管理的分层结构和网络安全体系模拟进行了资源的管理仿真。在网格平台中,有 200 个域网络,每一个域中包括了 500 个实体,实体中包括了 good entities,也存在 bad entities,其中 bad entities 约占实体总数的 25%。

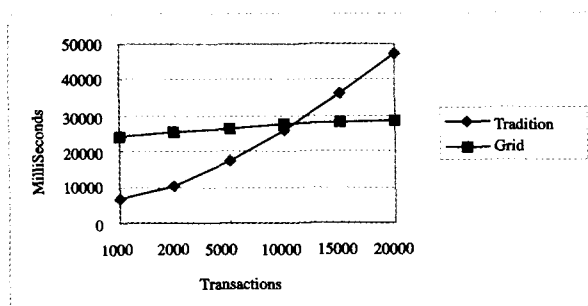


图 4 传统模式和 Grid 环境的运行效率

首先,我们通过实验验证教育资源管理的分层模型的有效性,在这里,把每一次对资源管理的操作称为一次事务(Transaction)。我们通过在模拟平台上的操作和在传统数据库和文件管理模式上资源管理实验的对比发现,在处理事务较少和存储资源较少的时候,传统模式的效率较高,随着处理事务及存储资源的增加,传统模式的时间复杂度明显增加,而网格平台中的处理模式逐步趋于平衡,如图 4。

然后,我们在网格环境的模拟实验中加入 bad entities,通过实体运行 Transactions 的可靠性发现,采用本文中提出的 ERMSA 综合解决方案,安全性比其它方式的安全解决方案的可靠性明显要高,如图 5。

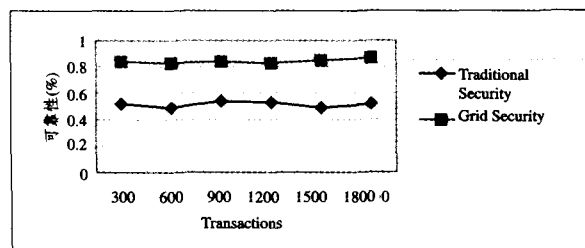


图 5 采用 ERMSA 的事务处理可靠性

结束语 网格技术是当今技术的一个研究热点,但通过网格技术解决广域网络的教育资源管理还没有成熟的模式。本文采用数据网格技术来解决远程教育中的资源整合和共享问题,提出了基于网格平台的一种解决异构网络资源管理的分层体系,并结合教育资源管理的特点,在此分层体系结构之上提出了一种教育资源安全管理的综合解决方案—ERMSA,在 CROWN 网格平台上通过实验表明,本文提出的教育资源管理的分层模型和 ERMSA 是可行的,并具有一定的实用性。

通过实验也发现,采用本文提出的 ERMSA,尽管其可靠性比网络环境下的安全措施要高得多,但还不是非常理想。因此,下一步工作将针对在不影响运行效率的基础如何提高教育资源网络运行的可靠性进行研究。

参考文献

- 郭惠珍, 张小可, 李平. 现代远程教育专家访谈-技术篇. 中国远程教育, 2000, 8(163): 5~10
- Reklaitis V. Towards e-learning application architecture based on GLOBUS framework. www.w3c.rl.ac.uk
- Foster I, Kesselman C, Tuecke S. The Anatomy of Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications, 2001, 15(3)
- Foster I, Kesselman C. The Grid: Blueprint for a New Computing Infrastructure(2nd Edition). Morgan Kaufmann, 2004
- http://www.globus.org/wsrf/
- Lin N H. Security and Privacy Technologies for Distance Education Application. In: Proceedings of the 18th International Conference on Advanced Information Networking and Application, 2004
- 许骏, 史美林. 网格计算与 e-Learning Grid—体系结构·关键技术·示范应用. 科学出版社, 2005