基于OGC规范的空间信息网格安全体系研究

雷星松[1,2] 李国庆[1] 于文洋[1] 解吉波[1] 胡 霞[2]

(中国科学院对地观测与数字地球科学中心 北京 100094)[1] (中国科学院研究生院 北京 100049)[2]

摘 要 网格技术在空间资源共享上起到了很大的作用,海量遥感数据、复杂的测量数据、专业的地学软件、科学的计算模型等数据和计算资源通过服务化技术,在网格环境能够提供一体化、按需服务。为了保证资源所有者的控制权和资源的私有性以及用户的隐私,需要设计一个完整的安全体系来从资源层、传输层、服务层、应用层等各个级别保证安全,同时要尊重网格节点的自治性和网格服务的整体性。本研究能够为跨区域、跨组织的数据和计算资源网格化共享的安全方案提供借鉴作用。

关键词 网格计算,安全体系,空间信息,数据资源,计算资源

中图法分类号 TP393 **文献标识码** A

Research on Security Framework of OGC-based Spatial Information Grid

LEI Xing-song[1,2] LI Guo-qing[1] YU Wen-yang[1] XIE Ji-bo[1] HU Xia[2]

(Center of Earth Observation and Digital Earth, Chinese Academy of Sciences, Beijing 100094, China)[1]

(Graduate University of Chinese Academy of Sciences, Beijing 100049, China)[2]

Abstract Grid technology has been used widely in spatial resource sharing. Many kinds of resources (such as large amount of remote sensing images, complex observation data and professional geographical software) can be integrally accessed on Internet on demand through grid environment. In order to protect the owner's right, resource's security and user's privacy, the security framework is needed. The framework should be comprehensive enough to cover the resource layer, service layer, transport layer, application layer etc. Meanwhile, the framework should keep each node of the grid themselves. This research could give advice to those applications which are cross regions, cross organizations and share the resource through services.

Keywords Grid computing, Security framework, Spatial information, Data resource, Computational resource

空间信息网格的出现,能够满足科学工作者对数据资源的全球化、多中心、多要素、信息化的要求,也能满足对计算资源的专业化、自动化、高性能、简单化的要求,从而实现资源共享和互操作。实践证明,空间信息网格在我国灾害应急[1]、数据共享、科学计算[12]等领域具有重要的作用。

安全是空间信息共享的重要因素,也是网格计算从一开始就遇到的主要问题,被认为是网格计算最大的挑战[2]。一方面,数据具有私有性,数据所有者的权益必须得到保证,有的数据还具有国防意义;另一方面,数据使用者也需要保护自身的隐私和安全,需要安全体系保证安全。

一般来说,网格对于安全性有以下几个基本要求:保证网格实体之间的通信是安全的、防止篡改的,这些网格实体包括用户、资源和程序;网格用户在多个资源之间使用单点登录的能力;从一个实体到另一个实体的权限委托,用于委托代理的操作;参与组织中安全机制方面的互操作性[9]。

国内外对网格体系的安全展开了深入研究,大多研究围绕网格计算安全应用层展开。Vivas 等人通过代理和组件的方式,提出了基于工作流的网格安全框架[3]。该安全框架探讨了代理机制,提出了授权推和拉两种模式。Nagaratam 等人探讨了 OGSA(开放网格服务架构)框架下网格安全架构,用安全组件的方式探讨了各个层次的安全问题[5],安全组件可以保证安全。Shuying Wang 等提出了基于代理机制的网络服务工作流模型[6],它通过代理能够实现 Web Service 的聚合,在执行过程中带着执行者的角色。IBM 公司研究人员和 Ian Foster 等还提出了 OGSA 的安全架构[7],其定义了网格体系的安全问题和解决方案,是很好的手册。

然而空间信息领域的网格技术和安全框架不成熟,大多利用中间件进行开发。本文在国家 863 基金项目的支持下完成了空间信息网格项目——基于 OGC 规范的空间信息网格体系,结合具体实施过程中的论证方案和国内外研究现状,提出了空间信息网格安全体系,并通过程序实现了数据和算法资源的共享,进而实现了安全框架。

到稿日期:2011-10-08 返修日期:2011-11-25 本文受数字地球科学平台重大项目——数字地球系统的信息学研究,国家 973 项目(2009CB723906),国家 863 项目——星机地立体组网协同观测关键技术资助。

雷星松(1987—),男,硕士生,主要研究方向为网格计算与并行计算,E-mail:leixingsong@gmail.com;**李国庆** 男,博士,研究员,主要研究方向为网格计算、数据共享;**于文洋** 男,副研究员,主要研究方向为云计算、网格计算;**解吉波** 男,副研究员,主要研究方向为数据服务;**胡 霞** 女,硕士生,主要研究方向为空间数据挖掘、混合像元分解、空间信息算法。

1 基于OGC规范的空间信息网格体系结构

网格环境可以依赖网格中间件(如Globus,gLite等)实现,然而面向中间件编程导致了网格系统过分复杂,性能和扩展性受到中间件制约,部分功能应该在其他层实现[4]。从安全角度考虑,基于中间件的网格体系需要依赖中间件,其过于复杂且耦合程度高[13],无法与既有业务的安全系统方便地整合,因此,本文不采用基于中间件的网格环境,而采用基于开放标准的空间信息网格体系[9],如图1所示。

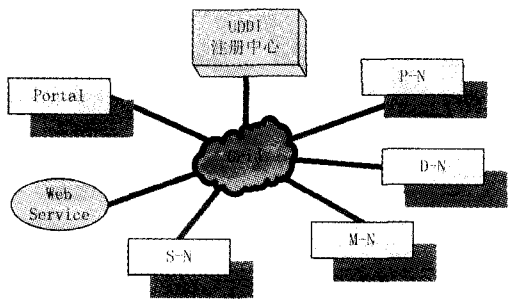

图1 基于OGC规范的空间信息网格平台体系结构

如图1所示,空间信息网格由如下节点组成:空间数据处理网格节点(P-N,Processing Grid Entity Node)、空间数据服务网格节点(D-N,Data Service Grid Entity Node)、空间数据显示网格节点(M-N,Mapping Grid Entity Node)、空间数据安全网格节点(S-N,Security Grid Entity Node)。在此基础上,各个节点内部自治,外部提供标准化接口。

通过增强网格节点,空间网格体系可以兼顾不同组织的私有性。其中,数据节点主要进行数据缓存和共享,计算节点主要进行算法的发布与共享;显示节点提供数据的可视化显示;安全节点提供必要的安全服务,保证网格共享体系的安全。可以看出,安全系统是空间信息网格平台的重要组成部分,需要整合整个网格系统实现资源共享,同时保护资源和用户的安全,对该系统的研究,也有助于网格技术在资源共享上的推广。

2 空间信息网格安全体系设计

基于OGC规范的空间信息网格体系能够实现数据和计算资源的共享。为了保护共享过程中资产和信息的安全,需要建立安全基础设施;同时需要在资源层、服务层、应用层等多层次进行安全保证[15],结合认证、授权、记账等手段来保证数据和计算资源共享过程的安全。整个安全框架如图2所示。

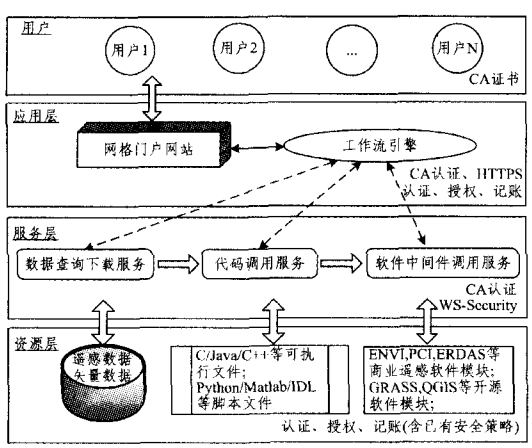

图2 网格安全体系架构

如图2所示,资源层的数据可以是数据资源和算法资源,这些资源提供者的所有安全措施,很多是运行时的安全系统,需要很好地兼容。服务层是资源在网格中的共享方式,通过标准服务化,使得资源的共享更加灵活。应用层是网格的入口,也是网格系统各个资源聚合的地方,需要更加综合地考虑安全。用户使用过程需要受到保护。为了保证整个体系的安全,需要建立安全基础设施。下面将自底向上地介绍安全体系的详细内容。

2.1 安全基础设施搭建

安全基础设施是安全框架的基础,通常包含以下内容:证书、密钥、硬件加密装置、软件加密解密代码、认证代理等。安全等级越高,需要的基础设施越复杂,一般安全体系证书和加密算法是必需的。

通过搭建CA中心,可以为用户、服务容器签发证书来搭建HTTPS的链接,同时保证用户和服务器的有效性。另外,CA中心通过提供认证代理,公布有效用户和过期用户,供各节点管理自己的信任用户列表。CA证书中心的实现可采用OpenSSL,利用shell脚本或API实现自动生成密钥和证书,并提供证书查询接口供认证程序调用。

另外,安全基础设施还包括加密、解密代码,供程序调用,以实现信息加密和解密自动化操作。

2.2 资源层安全

2.2.1 数据资源安全

由于数据量大、数据产生速度快,因此空间数据资源共享一般采用FTP协议。为了增加安全特性,本文的架构使用扩展的FTPS协议进行安全传输控制,从以下3个方面考虑:认证、访问控制、记账。

首先,需要认证用户。FTPS协议能够通过用户名和密码的方式进行认证,由于SSL加密,因此认证过程也是加密的,整个过程如图3所示。通过实现FTP服务器动态创建用户的临时账户,并通过缓存服务器进行临时分发服务,可以保证安全。

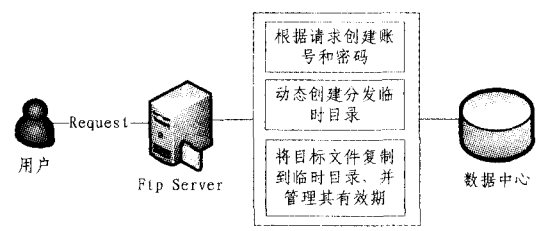

图3 FTP安全认证

其次,访问控制根据不同需求采取不同的访问控制策略。比较通用的做法是基于用户角色的控制、基于资源的访问列表。这些方式对于生产速度很快的遥感数据,不是很有效。由于网格资源种类多、变化大,因此采用分级访问控制策略(lattice-based access control,LBAC);数据资源按照价值和共享策略进行分级(0~9),级别越高,数据的权限要求越高;用户在节点也进行分级(0~9),根据用户购买的权限和能够获取的权限,设置用户级别。当且仅当用户级别大于数据级别时,用户才能够访问该数据。

再次,为了对数据的使用过程进行审计,需要对用户使用资源情况进行审计,建立完善的日志系统,记录下用户访问和下载数据的情况,以便资源所有者审计。记录如表1所列的字段信息就可以满足需求。

表 1　数据资源记账系统样表

用户	文件信息	时间	地点	次数	备注
user1	file1	12:12	TJ	2	
user2	file2	13:13	BJ	1	

通过这个记账系统，用户访问资源的情况就能够被记录下来，如果资源是收费的，还可以对用户进行费用收取。

2.2.2　计算资源安全

计算资源是可执行程序，保证计算资源安全需要保证算法不会被恶意执行。由于计算资源的调度是通过 Web Service 进行的，根据 WPS 规范，每一个处理功能都可以被控制。对计算资源需要保证以下几个方面的安全：认证授权、输入输出校验、记账，如图 4 所示。

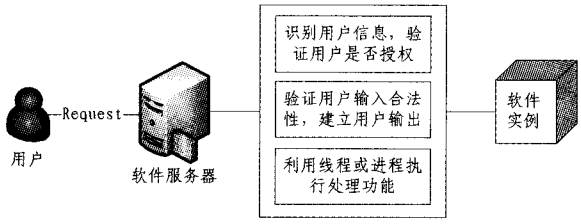

图 4　计算资源需要解决的安全问题

其中，输入输出是保证算法执行过程不会有恶意数据和代码的基础。另外，需要特别关注文件读写、数据库读写、用户输入输出等模块的安全漏洞，保证软件没有安全漏洞。

记账系统和数据资源一样，采取分级管理方式，不同的计算节点可以采用一套安全体系，又可以根据自身的设置分配给不同的用户，满足了多种需求。

对于用户上传的程序，需要严格控制安全[10]，防止病毒或木马的上传。本安全体系引入 sandbox 机制，通过隔离用户上传的应用程序限制其使用的数据、网络和硬件资源，以保障系统的安全。另外，需要将用户上传服务器与其他业务机隔离开来，将风险降低到最低。访问方式如图 5 所示。

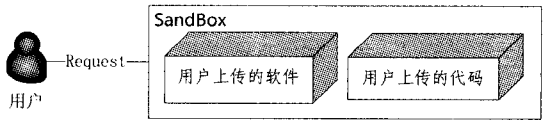

图 5　沙箱保护用户上传的程序

图 5 中用户上传的程序，通过沙箱机制实现了隔离，可以防止恶意程序和意外执行发生。

2.2.3　集成到已有安全系统

网格技术下资源共享方式发生了变化。为了不影响已有的业务系统正常运行，需要将网格系统的安全框架与单位既有安全系统集成。

空间信息的拥有者大多通过分发系统对外服务，例如通过 ACL 控制用户授权信息、通过传真方式进行业务操作等，不同单位会有所不同。

为了让网格安全系统集成到已有的安全系统，又不至于破坏原有安全系统，需要进行适应，通过适配器模式，实现网格安全系统与已有安全系统的转换，从而通过已有的安全系统访问资源。

认证信息通过代理机制可以很好地实现集成，授权策略需要进行保证，尤其是在网格化环境中，需要通过程序自动实现。一般来说，既有安全系统可能具有如下授权策略：访问控制列表、基于内容的访问策略、基于角色的访问控制等。LBAC 经过转换，可以灵活地变成访问控制列表。

如果用户权限高于文件权限，则将用户加入该文件的访问控制列表；如果是基于内容的访问策略，则需要将符合要求的用户加入到内容中，给用户访问的权利；如果是基于角色的访问控制，则将资源按照等级分组，然后将用户按照角色分组，将 LBAC 转换为访问控制列表。

通过转换，LBAC 不仅适应了网格中工作流跨域跨资源的特性，也适应了各单位保持已有财产的要求。

2.3　服务层安全

由于服务访问容易，为了保护服务对应的计算资源和数据资源的安全，需要进行认证、授权和记账，同时需要对传输过程进行加密。W3C 为保护 Web Service 级别的安全，提出了 WS-Security 标准，该标准通过对消息体的加密，可以保证服务级别的安全。OGC 规范提出的 WPS 尚未纳入 W3C 规范，无法直接使用 WS-Security，另外 OGC 组织正在研发安全标准[8]，但尚未完成。

目前，有两种方案可以解决服务层的安全：基于 HTTPS 的传输加密、基于 WSS 的加密访问。

(1)HTTPS 保证服务在访问和相应过程中是密文。WPS 实质上是基于 HTTP 协议，只不过消息体有一定的语义，通过 HTTPS 使得整个传输的内容都加密，自然能够保证安全。由于 WPS 主要传递的是控制流信息，因此数据量不大，使用 HTTPS，不至于带来太多的速度延迟。

(2)52North 组织提出了 WSS，其通过提供安全认证策略和加密规范，实现 OGC 服务请求过程和请求内容的加密，增强 OGC 服务的安全[5]。有的应用针对 OGC 规范进行了开发[14]。然而，由于 52North 需要修改服务并依赖其中间件，且不是 OGC 规范，本系统不采用此方法。

另外，OGC 组织正在制定安全规范，目前尚未发布版本，预计将在不久提供一个新的规范。

2.4　应用层安全

网格计算使得多种数据资源和计算资源的协同变得容易，也可以极大地丰富应用层。通过网格 portal，用户可以通过网页访问分布在各地的数据和计算资源，这给用户带来了方便。应用层安全是与用户打交道的安全，通过聚合各种空间服务来保证用户服务过程中的安全。因此，应用层需要通过认证、授权、记账等方式保证 portal 应用的安全。

应用层需要汇聚不同区域、不同组织、不同类型的服务，这些服务通过工作流方式进行组织。在工作流执行过程中，为了保证稳定性和健壮性，需要添加动态发现机制和策略，因此安全机制需要动态性。下面从认证、授权、记账 3 个方面探讨应用层的安全。

2.4.1　应用层认证安全

认证可以有多种方式，基于用户名/密码方式的认证是最简单的方式；利用 https 和 CA 进行高级别认证是一种较复杂的方式，两者结合就更加复杂了。

另外，为了避免 Denial of Service 的攻击，可以加入 Client Puzzle Protocal，即一种可能的 Client Puzzle 解决方案[6]。用户的请求加上一个带时间戳的密码，组成一个谜语，用户需要进行解答才能够继续访问。

上述几种认证方法综合起来就构成了如图 6 所示的安全措施。通过用户名密码匹配、基于 HTTPS 证书验证、Client Puzzle 能够实现安全认证。

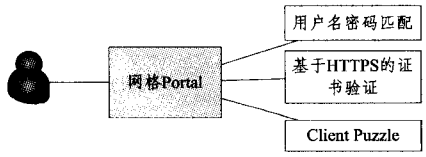

图 6　portal 安全逻辑

图 6 中用户的请求将经过用户名密码匹配、证书认证、HTTPS 加密、Client Puzzle 等技术保证认证安全。

2.4.2　应用层授权安全

应用层主要汇聚的是数据和计算服务，因此需要考虑数据和计算资源的安全。另外，应用层通过组织工作流，实现各个服务的协同，因此工作流级别的授权也是比较复杂的。

在资源级别已经有授权控制。对于 portal 来说，对用户服务的不是资源本身，而是访问资源的各个服务组成的工作流。工作流在创建的时候，就根据资源的安全等级计算出了安全等级，应用的安全等级计算公式如下。

$$F(wf)=\max\{f(r_1),f(r_2),f(r_3),\cdots,f(r_n)\}$$

式中，$F(wf)$代表工作流的安全级别，$f(r_n)$代表第 n 个资源的安全等级，工作流的安全等级为资源安全等级的最大值，即安全要求最高的资源决定了工作流的安全等级。

值得说明的是，数据服务的安全等级没有反映在工作流的安全等级中。实际上，WPS 的数据查询和下载操作可以认为是安全级别最低的操作，能够查询和下载的内容是具有强安全约束的，因此，每个人能够访问的数据资源都不是相同的。

2.4.3　应用层记账

记账是保护资源使用情况，防止用户恶意使用资源，同时可以进行收费等活动。对于网格 portal，由于用户经常使用，因此发生的交互很多，必须建立一个合理的记账系统，以保障资源的安全。

网格 portal 记账系统主要是针对用户使用工作流情况记账，因此需要包含以下信息：用户信息、工作流信息、时间、地点、事情情况、备注，如表 2 所列。

表 2　网格应用记账系统样表

用户	工作流信息	时间	地点	次数
user1	WF_ImageMerge	15:20	BJ	3
user2	WF_ImageRotate	15:20	BJ	3

表 2 中的工作流信息包含下载的数据量、使用的算法数、消耗的 CPU 和内存量等信息。如果网格 portal 包含付费内容，记账系统需要整合购物车功能，并提供支付过程的记录。记账系统是系统自查必需的组件，也是服务使用情况的查询组件。

2.5　网格体系必须解决的安全问题

通过前面的论述，网格资源共享的安全得到了保证，然而，跨域是网格的重要特点，需要涉及不同国家和地区的多个资源拥有者。由于政策和技术的限制，无法通过一种安全策略加以解决，因此需要解决多虚拟组织、多层次安全策略交换、多用户使用等网格必须解决的安全问题。

2.5.1　多虚拟组织单点登录

如果用户使用资源过程中需要频繁登录，必将导致可用性减低，甚至无法使用。单点登录解决方案不仅提高了网格资源使用效率，而且改善了用户体验。为了实现单点登录，需要做到以下几点：资源所有者对资源拥有控制权，用户可以方便使用不同资源，用户个人信息能够在需要的时候出现。

网格安全体系中采用安全代理技术并通过 OAuth 实现。安全代理负责保存用户登录信息和实效信息。为了保证安全信息的保密，用户信息是加密存储的。资源所有者通过安全代理取得用户信息，再将其和自身的安全认证策略结合(详见 2.5.2 节多层次安全策略交换)。如果需要与既有业务系统交互，则将策略做一个映射，将其转换为可用的安全框架。

2.5.2　多层次安全策略交换

安全策略交换涉及两个方面，即网格 portal 管理策略如何与网格节点的管理策略交换、网格节点的管理策略如何与资源所有者的既有业务系统的安全策略交换。portal 和网格节点的安全框架都基于分级安全框架。网格 portal 提供用户查询 service 供其他节点查询，新用户注册到网格 portal 之后，网格 portal 通知其他节点，其他节点接到通知后，调用 portal 的查询 service 获得基本的信息，并生成相应的节点访问密码，再通知到网格 portal 将需要的信息提取过来，整个过程均对重要信息进行加密。

2.5.3　多用户隐私保护

随着网格节点和用户数量的增多，用户信息传递逐渐增加，需要考虑保护用户的隐私。通过如下措施，可以在一定程度上保证用户的隐私。

(1) 制定完善的管理制度。只有限制资源访问、尽可能少地将敏感资源暴露出去，才能够保证用户的隐私。

(2) 用户的私密信息需要加密存储：密码用 MD5 等不可逆方式加密，证件号码通过对称加密方式存储。

(3) 用户访问记录不宜保存过长。除非特别需要，不要长久保存用户访问记录。

(4) 需要提供一种清除信息的方式，供用户请求删除，用户对自己的信息有控制权。

(5) 遵守其他保护用户隐私的方式，如法律、政策、服务商解决方案等。

3　空间信息网格安全体系实现和验证

本文依托的空间信息网格项目利用网格技术实现了数百 GB 数据和数百个算法资源的协同共享，整合的数据和计算资源如表 3 所列。

表 3　项目整合的数据和计算资源

资源类别	资源内容
数据资源	(1) HDF/GeoTiff/img 等栅格影像 (2) shapefile/kml 等矢量数据
计算资源	(1) MPI 并行算法 (2) Java 类、DLL、可执行程序 (3) Python 可执行脚本 (4) ENVI 模块(IDL 二次开发)

表 3 的资源被部署在跨 3 个行政区域的 6 个子节点中，这些网格节点组成的网格体系，实现了各单位资源的协同和共享，其中的一个网格节点作为中心节点，提供网格系统管理

(下转第 23 页)

tions (ICC'08). Beijing, China, May 2008: 19-23
[9] Zhang C, Lin X, Lu R, et al. An Efficient Message Authentication Scheme for Vehicular Communications[J]. IEEE Transactions on Vehicular Technology, 2008, 57(6): 3357-3568
[10] Xi Y, Sha K, Shi W, et al. Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks[C]// Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07). 2008: 344-351
[11] Mak T K, Laberteaux K P, Sengupta R. A Multi-Channel VANET Providing Concurrent Safety and Commercial Services[C]// Proceedings of 2nd ACM International Workshop on Vehicular Ad Hoc Networks. Cologne, Germany, Sep. 2005: 1-9
[12] Raya M, Hubaux J P. The security of vehicular ad hoc networks [C]//3rd ACM workshop on Security of ad hoc and sensor networks. 2005: 11-21
[13] Xu Q, Mak T, Ko J, et al. Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages[J]. IEEE Transactions on Vehicular Technology, 2007, 56(2): 499-518
[14] Xiong Hu, Qin Zhi-guang, Li Fa-gen. Secure Vehicle-to-roadside Communication Protocol Using Certificate-based Cryptosystem [J]. IETE Technical Review, 2010, 27(3): 214-219
[15] Boneh D, Lynn B, Shacham H. Short Signature from the Weil Paring[C]//Proceeding of Asiacrypt '01. LNCS 2248, Springer-Verlag, 2001: 514-532
[16] Barreto P S L M, et al. Efficient and Provably Secure Identity-based Signature and Signcryption from Bilinear Maps[C]//Proceeding of Asiacrypt '05. LNCS 3788, Springer-Verlag, 2005: 515-532
[17] Dai W. Crypto++5. 2. 1Benchmarks[EB/OL]. http://www.eskimo.com/ weidai/bench-marks.html, 2004
[18] Zhang Y, Liu W, Fang Y. Securing mobile Ad Hoc networks with certificateless public keys[J]. IEEE Trans. Depend. & Secur. Comput., 2006, 3(4): 386-399
[19] Ren K, Lou W, Zeng K, et al. On broadcast authentication in wireless sensornetworks[J]. IEEE Trans. on Wireless Commun., 2007, 6(11): 4136-4144

(上接第 8 页)

功能。通过采用本文档的安全体系，并搭建 CA 中心，保证了网格节点的通信和中心节点的用户服务过程的安全，实现了资源的安全共享。项目采用 B/S 架构，建立了网格用户服务 portal，使得计算资源和数据资源很方便地被用户查询和使用。项目的部分用户界面如图 7 所示。

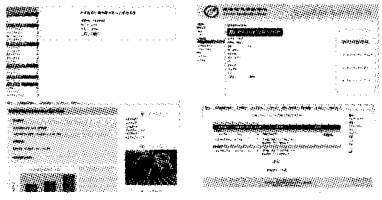

图 7 项目部分界面效果图

通过本项目的实践，验证了网格安全基础设施的重要作用。CA 中心的可用性、加密算法的保密性决定了整个安全框架的基石；应用层的认证、授权、记账系统，也决定了资源使用过程的安全。通过对各单位已有安全系统的整合，使网格系统更好地实现资源共享。从用户使用的便利性和资源共享的有效性角度来看，网格系统和安全体系很好地发挥了作用。

结束语 本文探讨了空间信息网格系统的安全体系，通过资源层保证、传输层加密、应用层保障，才能构建一个安全的系统。通过本文探讨，给出了网格环境中数据和计算资源共享的安全策略——基于 HTTPS 和 CA 认证、基于 LBAC 的授权、网格记账系统。通过采用符合 OGC 规范的 Web 服务，使得各个资源的共享方式松耦合，保证了资源使用过程的安全性。另外，网格安全体系的实现过程也是安全体系的一次检验。

今后将进一步跟进国际标准，研究如何将 WS-Security 加入到空间信息网格体系中；另外，网格资源与已有业务之间交换安全策略的方式还需要经过不断实践，根据具体情况找到更好的解决方案。

参 考 文 献

[1] 李国庆，刘定生，于文洋，等. 基于网格技术的汶川地震国际数据共享环境[J]. e-Science, 2008(02)
[2] Humphrey H, Thompson M R, Jackson H R. Security for grids [J]. Proceedings of the IEEE, 2005, 93(3): 644-652
[3] Vivas J L, Fernadndez-Gago C, Lopez J, et al. A security framework for a workflow-based grid development platform[J]. Computer Standards & Interface, 2010, 32(5/6): 230-245
[4] Wang Li-zhe, von Laszewski G, Kunze M, et al. Provide Virtual Distributed Environments for Grid computing on demand[J]. Advances in Engineering Software, 2010, 41(2): 213-219
[5] Nagaratnam N, Janson P, Dayka J, et al. The Security Architecture for Open Grid Services[OL]. http://www.ggf.org/ogsa-sec-wg, July 2002
[6] Wang Shu-ying, Shen Wei-ming, Hao Qi. An agent-based Web Service workflow model for inter-enterprise collaboration[J]. Expert Systems with Application, 2006, 31(4)
[7] Nagaratnam N, Janson P, Dayka J. The Security Architecture for Open Grid Services[OL]. http://wwww.ggf.org/ogsa-sec-wg, 2002
[8] http://www.opengeospatial.org/projects/groups/securitydwg
[9] 张小溪. 基于 OGC 规范的空间信息网格平台构建技术研究[D]. 北京：中国科学院研究生院，2009
[10] 樊晓光，褚文奎，张凤鸣. 软件安全性研究综述[J]. 计算机科学，2011(5)
[11] Li Guo-qing, Liu Ding-sheng, Sun Yi. Grid Research on Desktop Type Software for Spatial Information Processing[J]. Verlag Berlin Heidelberg, 2005, 3516: 155-162
[12] 胡霞，雷星松. 基于时序的遥感影像混合像元分解模型的研究[C]//第十七届中国遥感大会摘要集. 2010
[13] Globus Security[OL]. http://www.globus.org/toolkit/docs/5.0/5.0.4/security/key/, 2011-10-02
[14] License D J. Permission-based access to OGC Web Services with 52°North[C]//FOSS4G 2010. Barcelona, Spain, September 2010
[15] Li Guo-qing, Li Chen-hui, Yu Wen-yang, et al. Security Accessing Model for Web Service based Geo-spatial Data Sharing Application[C]//3rd ISDE Digital Earth Summit. 2010(07)