LDAP在数字校园统一身份认证系统中的应用

贺玉明,李晋宏,唐 辉
(北方工业大学 信息工程学院,北京 100144)

摘 要:数字校园统一身份认证系统就是集成了多个应用系统的认证模块,所有应用系统都通过同一个认证模块进行认证和授权,从而避免了各应用系统维护多套用户名和密码。LDAP由于其跨平台性、高可读性和扩展性等,在数字校园的统一身份认证系统中得到了广泛的应用。在深入研究分析LDAP及其相关技术的基础上,设计并实现了数字校园中基于LDAP的统一身份管理,并且实现了新的目录信息录入接口,避免了命令行和LDIF文件录入的不方便性。

关键词:LDAP;统一身份认证;目录信息树;LDIF
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2011)05-0139-04

Application of LDAP in Uniform Identity Authentication of Digital Compus

HE Yu-ming, LI Jin-hong, TANG Hui
(College of Information Engineering, North China University of Technology, Beijing 100144, China)

Abstract: Digital Campus uniform identity authentication system integrates multiple applications of authentication module. All applications are authenticated and authorized by the same authentication module, which makes application systems avoid of maintaining multiple username and password. LDAP has been widely used in the uniform identity authentication system due to its cross-platform, high readability and expandability. Based on research of LDAP and related technologies deeply, design and implement digital campus uniform identity management. What's more, design new directory information input interface, which avoids of inconvenience of command line and LDIF file.

Key words: LDAP; uniform identity authentication; directory information tree; LDIF

0 引 言

随着网络以及数字化技术的不断发展与进步,数字化校园的建设越来越被各个高校所重视,数字校园是构建学校的数字化空间,具体解释请详见文献[1]。传统方式上,在高校各个相互独立的业务系统中,绝大多数都是需要用户提供登录的用户名和密码才能进行认证,进而实现访问控制和用户授权。这种相互独立的认证模型导致了同一用户必须记住多套用户名和密码,管理员也必须维护多个用户信息库,因此统一身份认证的登录系统受到了很大的欢迎。

统一身份认证[2]系统就是集成了传统方式上的多个应用系统的认证模块,将各个应用系统独立的认证模块有机地组织起来,且将原来分散的、无组织的用户认证信息进行统一的管理与维护,从而实现了一次登录便可访问其他各个应用系统,而不需要再次重新登录验证。这无疑给用户带来了方便性,使其不用再记忆多套用户名和密码。轻量级目录访问协议[3] LDAP (Lightweight Directory Access Protocol)可以构建复杂的分布式目录结构,能够对用户认证信息进行有效组织和管理,并提供高效安全的目录访问,因此LDAP在数字校园统一身份认证系统中得到了良好应用。

收稿日期:2010-10-13;**修回日期**:2011-01-17
基金项目:北京市人才强教深化计划高层次人才资助项目(PHR 20100509)
作者简介:贺玉明(1985-),女,河北唐山人,硕士研究生,主要研究方向为数据挖掘;李晋宏,教授,博士,主要研究方向为模糊专家系统、数据挖掘、商业智能等。

1 LDAP特点

LDAP[4-6]是由美国Michigan大学研发的,是一个得到广泛接受的目录访问方法,而且已经成为了开放的行业标准。由于LDAP目录服务器是运行在TCP/IP的上层,因此具有更好的跨平台性。LDAP是一种基于网络的数字目录,在LDAP中目录由条目(Entry)组成。存储的数据被组织成树形结构,类似于电话薄、地址薄和文件系统。

LDAP目录服务器是对读操作进行了专门优化的

特殊的数据库。与数据库相比，它查询速度快，支持分布式，以树状的层次结构来存储数据，安全机制也更加完善，但是相对增删改的速度比较慢，因此它的读性能要比写性能强很多。正是利用这一特点，完全适合于数字校园的统一身份认证系统，因为该系统主要是对用户输入的口令和密码进行查询验证和授权，进而决定是否允许登录，读操作是起决定性作用的，是整个数字校园系统运行性能的瓶颈。

2 统一身份认证原理

统一身份认证的思想就是多个独立的应用系统共享一个认证模块，用户要登录各个应用系统前必须通过这个统一的认证模块的授权。当用户通过这个认证模块的认证后，则可以访问其他各个应用系统，而不需要再次进行认证，也就是只进行一次认证，就能访问所有的应用系统。这无疑给用户带来了良好的方便性和交互性，通过一次登录就可以访问到他所能访问的全部资源，进行日常工作，提高了工作的效率。对管理者而言，也极大地提高了管理效率，管理者只需维护一套用户信息即可。

统一认证的过程如图 1 所示。

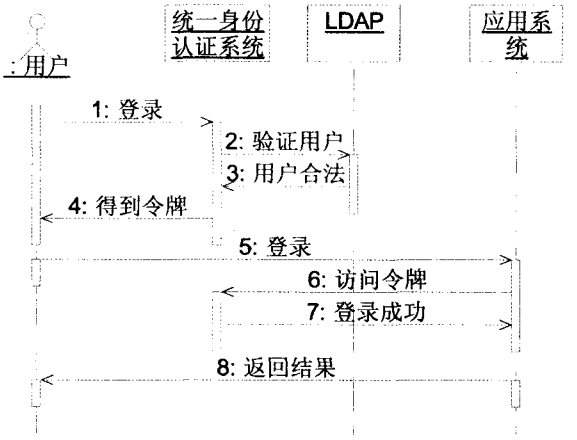

图 1 统一认证过程图

原理为：

1）用户登录统一身份认证模块，输入用户名和密码；

2）统一身份认证模块访问 LDAP 存储库，看是否存在该用户信息且合法；

3）验证合法后向统一身份认证模块返回结果；

4）统一身份认证模块向用户返回令牌；

5）用户登录应用系统且传递自己所拥有的令牌；

6）应用系统向统一身份认证系统检验令牌是否存在，如果存在则允许访问；

7）用户此时能够成功登录应用系统，且得到返回结果。

3 系统设计

3.1 总体结构

客户端通过访问 Web 浏览器，进入到统一身份认证系统中，输入用户名和密码，统一身份认证系统会向 LDAP 服务器发送请求进行认证，如果认证通过，则客户端拥有了访问权限，此时就可以访问各个应用系统。

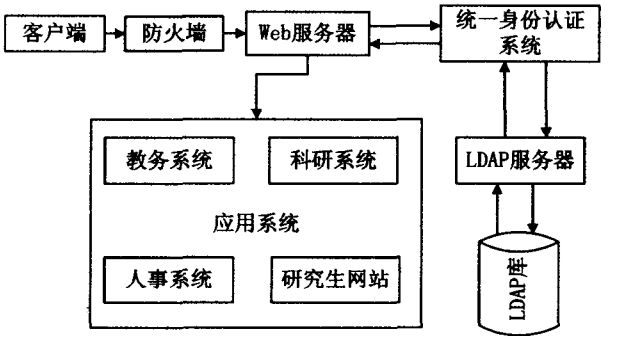

图 2 系统总体结构图

3.2 LDAP 类型定制与目录设计

LDAP[7~10] 目录服务器中信息是以条目的形式存在的，被组织成树状结构，类似于文件系统、电话薄、地址薄等。每一个条目都是通过一个唯一的标识 DN（Distinguished Name）来确定它在树形结构的位置，每一个 DN 都由几个元素组成，称之为相对 DN，即 RDN（Relative Distinguished Name）。这种树形结构组织构成了目录信息树，它提供了有效的服务层进行条目的过滤、严格的访问控制等。

统一身份认证系统的首要步骤就是要设计目录信息树，而目录信息树的条目是由对象类和属性决定的，因此目录信息树的设计要从属性和对象类开始，首先定义条目相应的对象类，然后定义每个对象类对应哪些属性。针对数字校园用户认证信息特点，分成了学生信息、教师信息和管理员信息三种，对应在目录服务器中建立了 studentClass、teacherClass 和 administratorClass 三个用户自定义类。

在 Sun DSEE（Sun Java System Directory Server Enterprise Edition）7.0 中，用户自定义属性和类放在目录服务器实例对应目录下的 schema 目录下的 99user.ldif 文件中，例如，对应学生信息的自定义属性（college，class，major）和对象类（studentClass）存储格式如下所示：

attributeTypes：（ college－oid NAME ´college´ SYNTAX 1.3.6.1.4.1.1466.115.121. 1.15 X－ORIGIN ´user defined´ ）

attributeTypes：（ class－oid NAME ´class´ SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 X－ORIGIN ´user defined´ ）

attributeTypes：（ major－oid NAME ´major´ SYN－

TAX 1.3.6.1.4.1.1466.115.121.1.15 X-ORIGIN 'user defined')

objectClasses: (studentClass-oid NAME 'studentClass' SUP top STRUCTURAL MUST (uid $ userPassword $ cn) MAY (college $ class $ major) X-ORIGIN 'user defined')

基于以上的属性和对象类,设计了如图 3 所示的目录信息树。在这个 LDAP 目录结构中,主要分成了三部分 ou = student、ou = teacher 以及 ou = administrator。dc = ncut、dc = edu、dc = cn 对普通教师和学生是不可见的,只有管理员才可操作。

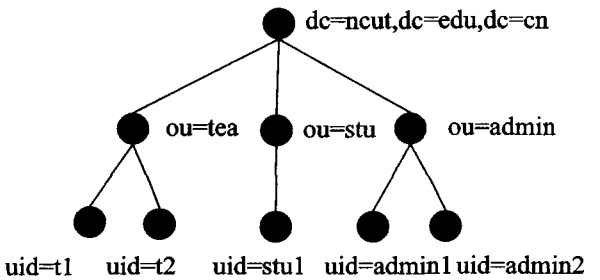

图 3　目录信息树结构

3.3　LDAP 功能模型

LDAP 功能模型[1]描述了如何对存储在 LDAP 中的数据进行操作,说明了如何使用 LDAP 协议本身对 LDAP 中的数据进行相关操作,主要有以下几类操作。

1)询问类。主要有搜索和比较两种,根据标准在指定范围内进行条目选择,这个标准通常称为过滤器。

2)更新类。主要有新增、删除、修改和修改条目 RDN 等操作。

3)验证类。主要有连接、断开和作废等操作。

4)其他操作。主要有 LDAP 协议提供的可扩展性操作等。

4　系统实现

4.1　LDAP 服务器安装

本系统采用的目录服务器是 Sun Java System Directory Server Enterprise Edition 7.0,为了提高 LDAP 服务器的响应速度,以及方便对 LDAP 的管理与维护,将 LDAP 部署到一个专门的 domain 域中。首先建立一个 domain 域,专门用来部署 LDAP 服务器。

>asadmin create-domain - u admin --portbase 5000 --profile cluster dsee-domain

在建好的域文件的配置文件 server.policy 结尾处加上如下配置:

```
// Permissions for Directory Service Control Center
grant codeBase "file: ${com.sun.aas.instanceRoot}/applications/j2ee-modules/dscc/-"
{
permission java.security.AllPermission;
};
```

然后转向安装文件所在目录执行以下命令:

>dsee_deploy install -i D:\Sun\dsee6

在 dsee6\dscc6\bin 目录执行以下命令:

>dsccsetup ads-create

4.2　与目录服务器建立连接

本系统利用 JDNI(Java Directory Naming Interface)操作 LDAP 目录服务器,JNDI 对外部应用程序提供了一个统一的接口,Java 应用程序即可通过 JNDI API 来操作 LDAP 目录服务器,而不必关心目录服务器内部实现的细节。LDAP[11,12]是运行在 TCP/IP 层,能够很好地支持 Web 应用程序,而且对读操作进行了专门的优化,使得读取的性能比关系数据库要好很多。

```
// 服务器地址
private String url = "ldap://域名:389";
    // 管理域的 dn
private String dn = "cn=Directory Manager";
  // 管理域的密码
private String pwd = "password";
  // 管理域的验证方式
private String type = "simple";
private String cfactory = "com.sun.jndi.ldap.LdapCtxFactory"。
```

4.3　功能模块

4.3.1　用户注册

对于目前 LDAP 目录服务器中还未存在账户的用户,通过注册模块添加自己的信息,需输入用户名、密码等基本信息,根据用户不同的角色,应按照 LDAP 条目对应的对象类定义的属性进行添加。

4.3.2　统一身份认证

当用户登录系统时,需输入用户名和密码,然后将用户输入的信息传给 LDAP 目录服务器,此时 LDAP 目录服务器会将用户名和密码与 LDAP 存储库中存在的信息进行匹配,如果匹配成功则可以通过认证。用户通过统一身份认证后,就可以进入统一登录的门户界面,进入数字校园门户中的各个应用系统。

4.3.3　修改密码

对于经过统一身份认证的用户,则可以进入密码修改页面进行密码的修改,存储在 LDAP 目录服务器中的密码都是经过加密算法加密的,即使是系统管理员也不知道用户密码的真实内容。

4.3.4　目录信息维护

目前目录信息录入方式有两种:命令行录入和通过 LDIF(LDAP Data Interchange Format)文件录入。命令行录入方式是最直接的一种,但对于大批量数据的

话工作量大、不方便。通过 LDIF 文件录入必须保证文件符合 LDIF 文件的格式要求,因此也具有不方便性。因此本系统设计并开发了目录信息维护的接口,提供了可以通过从数据库中或者从 Excel 文件中导入数据的用户界面,这给用户的操作带来了方便性和直观性。

5 结束语

用户的统一管理是数字化校园建设的基础和关键点,与传统的信息管理者数据库相比,LDAP 具有跨平台性、高校的读性能、支持分布式的目录信息维护、基于结构化的信息表示以及高可用性等逐渐被高校所接受,作为数字校园统一身份认证系统的用户信息存储库。

文中在对 LDAP 和统一身份认证深入研究的基础上,设计了目录信息树以及实现了对目录服务器的访问,并提供了一个基于 Web 的信息录入方式,进而实现了基于 LDAP 的数字校园统一身份认证系统。该系统作为数字校园建设的支柱,为其他各个系统提供了统一的认证和授权。

参考文献:

[1] 郑 凯,聂瑞华,梁卓明,等. 数字校园 ESB 技术的分析与实现[J]. 计算机技术与发展,2009,19(11):246-249.

[2] 李 翔,晁爱农,刘孟强. LDAP 的研究及其在统一身份认证系统中的应用[J]. 计算机应用, 2008,28(6):98-100.

[3] 李 涛,张 波,张晓鹏,等. 基于 LDAP 与 Struts 的数字校园门户统一身份申请系统[J]. 计算机应用与软件,2008,25(3):173-175.

[4] 关婷婷,陈性元,张 斌. 基于 XML 的数据表现格式在 LDAP 目录中的应用[J]. 计算机工程与设计,2006,27(22):4383-4386.

[5] 吴杰明,周 宁. 基于 LDAP 的信息共享平台研究与实现[J]. 计算机应用,2008,28(4):1042-1044.

[6] Qadeer M, Salim M, Sana A. Profile management and authentication using LDAP[C]// Proceedings of 2009 International Conference on Computer Engineering and Technology. [s. l.]:[s. n.],2009:247-251.

[7] Koutsonikola V, Vakali A, Mpalasas A, et al. A structure-based clustering on LDAP directory information[C]//Proceedings of the 17th International Symposium on Foundations of Intelligent Systems. [s. l.]:[s. n.],2008:121-130.

[8] Salim M, Akhtar M S, Qadeer M A. Data Retrieval and Security Using Lightweight Directory Access Protocol[C]// Proceedings of Second International Workshop on Knowledge Discovery and Data Mining. [s. l.]:[s. n.],2009:685-688.

[9] 肖琬蓉,杨生举. 基于 LDAP 的统一用户认证系统设计与实现[J]. 计算机科学,2008,35(5):298-300.

[10] 胡立春,武友新,张 烨,等. LDAP 环境下的统一用户管理系统的研究与实现[J]. 计算机工程与设计,2007,28(4):823-826.

[11] 常 潘,沈富可. 基于 LDAP 的校园网统一身份认证的实现[J]. 计算机工程,2007,33(5):281-284.

[12] Vasiliadis D C, Rizos G E. A Trusted Network Model Using the Lightweight Directory Access Protocol[C]//Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications. Athens, Greece:[s. n.], 2007:252-256.

(上接第 133 页)

像缓存区,对图像缓存区进行移动,实现了多地物的移动功能以及地物结点的捕捉功能。该方法已经在蓄滞洪区监测系统中得到了实际的工程应用,有效地提高了地图的制图精度。

参考文献:

[1] 薛 伟. MapObjects—地理信息系统程序设计[M]. 北京:国防工业出版社,2004:192-193.

[2] 李新召. 基于 COM 组件的 Shape 文件生成算法[J]. 矿山测量,2003(4):29-31.

[3] ESRI. Arcedit Users Guide: Interactive Graphics Editor[M]. California: Environmental Systems Research Institute,1998.

[4] 刘文宝,夏宗国,崔先国. GIS 结点捕捉的广义算法及误差传播模型[J]. 测绘学报,2001,30(2):140-147.

[5] 周安宁,沈成武. 对象模型与关系模型结合实现高效的对象系统[J]. 武汉理工大学学报(交通科学与工程版),2001,25(2):124-127.

[6] 蔡德利,郭庆丰,汪 春. 扩展 MapObjects 数据源的研究 I:将 Shapefiles 保存到 ADO. NET 数据集[J]. 计算机工程与设计,2006,27(9):1533-1536.

[7] Burroughp A, Mcdonnell R A. Principles of Geographical Information Systems[M]. Oxford: Oxford University Press, 1998.

[8] Jones C B. Geographical Information Systems and Computer Cartography[M]. Harlow: Long-man,1997:87-92.

[9] 吴 磊,黄先锋,舒 宁. GIS 大数据量编辑处理中快速捕捉的优化策略[J]. 武汉理工大学学报(交通科学与工程版),2005,29(2):316-318.

[10] 周迪民,段国云. 地理信息系统属性数据不确定性的研究[J]. 计算机技术与发展,2009,19(12):174-178.

[11] 杨建昌. GDI+高级编程[M]. 北京:清华大学出版社,2010:201-220.

[12] 徐正光,田 清,张利欣. 图像拼接方法探讨[J]. 微计算机信息,2006(10x):255-257.