基于数字证书的身份认证系统的设计与实现

李星宜,李陶深,崔 杰,葛志辉
(广西大学 计算机与电子信息学院,广西 南宁 530004)

摘 要:身份认证技术是能够对信息收发方进行真实身份鉴别的技术,是保护网络信息资源安全的第一道大门,在安全系统中的地位极其重要。提出了一种基于数字证书进行身份认证的方法,构建了身份认证系统模型方案,采用 OpenSSL 软件包,Ubuntu 作为服务器操作系统,Tomcat 作为 WEB 服务器软件,设计一个基于数字证书的身份认证系统,以网站登录注册系统为例实现身份认证。本系统由四大模块组成,有登录模块、注册模块、数据加密模块、数字证书处理模块,能够实现用户身份认证。系统模块实现结果表明,该系统安全可靠、易维护,具有良好的可扩展性。

关键词:数字证书;身份认证;OpenSSL;登录系统
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)12-0160-04

Design and Implementation of Identity Authentication System Based on Digital Certificate

LI Xing-yi, LI Tao-shen, CUI Jie, GE Zhi-hui
(School of Computer, Electronics and Information, Guangxi University, Nanning 530004, China)

Abstract: The identity authentication technology that can authenticate the identity of the sender and receiver is very important in the security system. As a first security guard, it is used to protect the network information resources. It puts forward the designing methods of the identity authentication system, constructs a model scheme and employs OpenSSL software package, Ubuntu as server operating system, Tomcat as web server software to design and implement a network identity authentication system based on digital certificate. Meanwhile an example which is a website login registration system is given to introduce how to implement identity authentication. This system which consists of four modules includes login module, registered module, data encryption module, digital certificate processing module. It can be used to identificate users who are using system. The system has good safety, easy maintenance and good expansibility.

Key words: digital certificate; identity authentication; OpenSSL; login system

0 引 言

随着 Internet 网络技术的飞速发展,电子商务、电子政务、企业内部网的信息管理、Internet 网络信息服务已获得广泛应用,由此许多重要的信息和机密的资料都存放在计算机或网络上。网络的开放性、交互性及其分布式特性使信息安全问题越来越受到人们的重视。身份认证对于保证信息只被合法授权用户获取和访问起着重要作用,因而建立强有力的身份认证机制成为系统安全的关键之一[1,2]。身份认证系统作为第一道关卡,可以给用户和系统提供较强的安全性能。

数字证书就是在网络中表明身份的数字"身份证",以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证,确保网上传递信息的机密性、完整性[3]。OpenSSL 开源软件包,由于其开源性使它得到众多的改进和完善,能够下载直接编译使用,也可以根据项目需求做二次开发。它主要包括三大模块:密码算法库模块、SSL 协议库模块以及应用程序模块。通过使用该软件包,生成符合 X.509 标准的数字证书。它提供的 CA 应用程序就是一个证书管理中心,实现证书签发的整个流程,同时有对证书管理的机制,从而实现了基于数字证书的网络身份认证功能[4,5]。文中使用 J2EE 网络编程技术、基于数字证书等安全技术设计并实现一个易扩展的安全的身份认证系统。

1 系统的总体设计

1.1 系统的总体框架结构

(1)从系统编程实现上考虑,本系统采用 MVC 三

收稿日期:2011-04-23;**修回日期**:2011-07-27
基金项目:广西自然科学基金重点项目(2010GXNSFD013037);广西科技创新能力与条件建设项目(09-007-05S018)
作者简介:李星宜(1985-),女,河北唐山人,硕士研究生,CCF 会员,主要从事信息安全、并行分布式计算技术研究;李陶深,博士,教授,CCF 高级会员,研究方向为网络信息安全、分布式数据库、网络路由算法、无线 Mesh 网络。

层架构设计,使结构更加清晰,系统易于扩展,如图 1 所示。

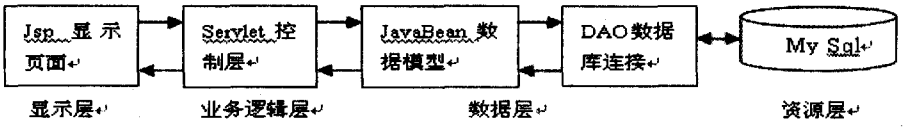

图 1　身份认证登录系统框架结构

其中数据层又细化为:JavaBean 数据模型层和 DAO 层。DAO(Data Access Object,数据访问对象)主要功能就是数据操作,提供多个原子性的 DAO 操作,如增加、修改、删除等,管理数据库的连接。

(2)从系统安全角度考虑,可以对整个系统分四层如图 2 所示。第一层是物理层,提供系统运行环境安全、网络安全以及系统安全策略等;第二层是服务层,一方面负责为用户提供各种系统功能,另一方面是安全认证基础设施,负责管理数字证书,实现身份认证服务;第三层为界面层,主要是安装数字证书的浏览器,提供对数字证书的使用的接口;第四层为应用层,用户使用数字证书进行身份认证,实现对应用系统访问[6,7]。

1.2　系统的网络拓扑结构设计

从图 3 中可以看出系统由多个应用服务器和一个用户认证服务器组成,用户可以通过客户端浏览器访问该系统。在访问系统时,用户需要使用自身的数字证书来通过身份认证服务器的验证,通过身份验证的用户才能获得使用系统的权限,不同的用户在访问系统时也会有着不同的权限;应用服务器负责为用户提供各种系统功能,身份认证服务器负责验证用户身份,管理用户数字证书是 CA 认证中心,提供认证服务[8~10]。

1.3　系统功能模块

身份认证系统可以分为前台和后台功能模块,如图 4 所示。

●前台功能需求说明:

1)注册功能:注册时合法用户输入的信息只有符合要求才允许其注册;信息经过后台处理,注册成功后,用户下载安装数字证书到浏览器。

2)登录功能:成功注册后,登录时用户需要输入正确的信息,同时提供用户数字证书。

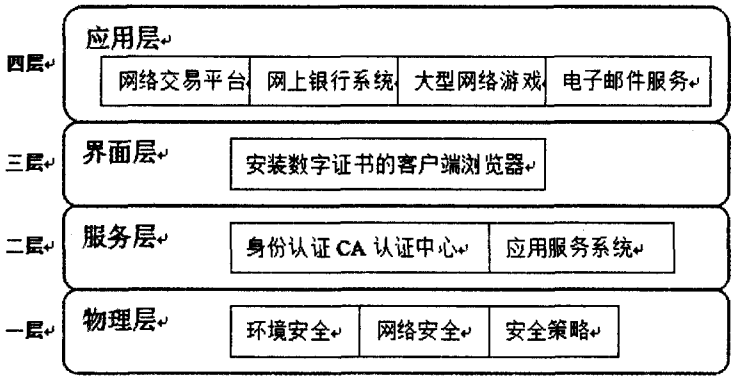

图 2　系统分层设计图

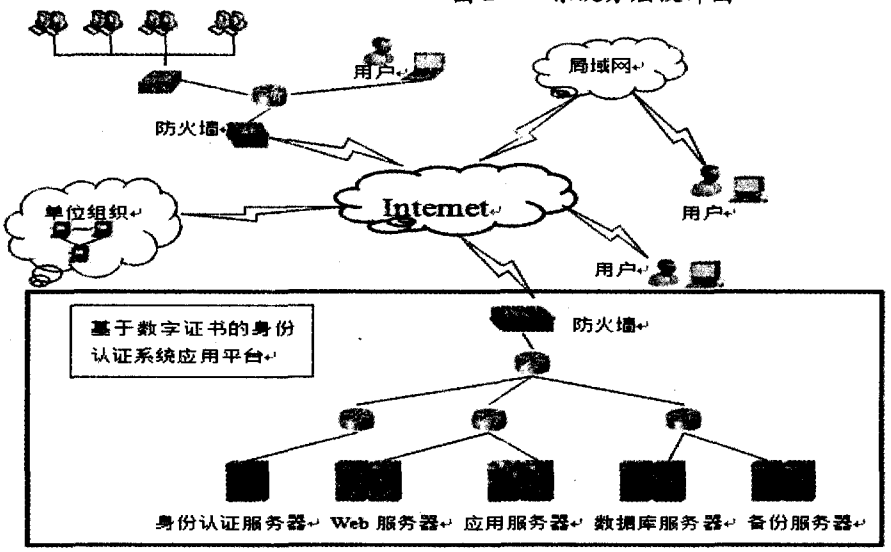

图 3　系统网络拓扑结构图

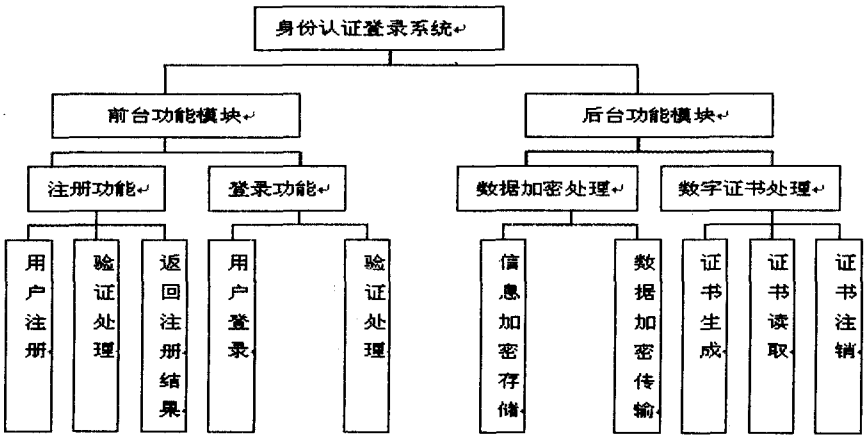

图 4　身份认证登录系统功能模块

●后台功能详细需求说明:

1)数据加密处理:为防止用户信息被泄密,用户注册信息的密码用MD5算法加密后存储到数据库中;用户在和服务器数据通讯时,数据加密传输,实现数据的加密传输。

2)数字证书处理:

(1)数字证书生成。使用Openssl生成,每一个注册用户有一个数字证书和密钥对(公钥和私钥),通过系统CA的认证后用户可以下载安装到用户的浏览器中,用于登录系统时候进行身份认证。

(2)数字证书读取。在用户登录时,身份认证服务器读取安装在浏览器的数字证书信息。

(3)数字证书注销。当用户数字证书不被信任时系统要对证书进行注销操作,被注销的数字证书写入数字证书注销列表文件中,然后发布。

1.4 身份认证流程

从总体上来看,身份认证流程分为三个步骤:

1、客户端用户选择自己的数字证书,并发送证书信息到认证服务器进行认证。

2、认证服务器对用户的证书进行认证,证书认证通过后,返回成功信息。

3、用户身份验证完成,登录到应用服务器获得所在权限范围内的数据信息。

2 系统主要功能模块设计与实现

根据本系统功能设计和流程,身份认证系统最主要的部分是数字证书的处理模块,它是整个系统的核心,实现该部分的功能其它的部分就可以随之解决。

该模块可以分两个部分:

其一,数字证书服务,该部分实现了数字证书的生成和管理;

其二,证书认证服务,对数字证书进行验证,实现统一的身份认证服务[11,12]。

2.1 数字证书服务

数字证书服务实现符合X.509标准的数字证书生成和CA认证中心数字证书发放功能。使用以C为开发语言的OpenSSL开源软件包,它包含庞大的指令和接口,实现一个CA认证中心,用来生成和管理数字证书。可在OpenSSL官网 http://www.openssl.org/source/下载编译直接使用,这里使用版本:openssl-1.0.0c。

第一步:建立CA。

在建立CA之前要进行一些准备工作,首先生成根目录gx-ca,其次生成证书数据库文件,在gx-ca根目录下创建index.txt,用来保存以后的证书信息;再次生成证书序列号文件;最后修改CA的配置文件openssl.cnf如下:

```
[ CA_default ]
dir   =c:\gx-ca      # 定义建立CA系统的根目录
certs   = $dir/certs   # 保存已经签发过的证书
crl_dir   = $dir/crl   #保存证书注销表文件
database = $dir/index.txt   #证书数据库文件
new_certs_dir = $dir/newcerts   # 新证书的默认保存目录
certificate = $dir/private/gx-ca.pem      # CA根证书
serial   = $dir/serial   # 当前证书序列号文件
crl   = $dir/gx-ca.crl   # 当前的证书注销表文件
private_key = $dir/private/gx-ca.key   # CA系统根证书的私钥文件
[gx_ca_dn]
commonName=gx ca   #CA根证书持有者的名字
stateOrProvinceName=guangxi   #CA根证书持有者的省份
countryName=CN   #CA根证书持有者的国家
emailAddress=wang123@163.com   #CA根证书持有者的邮箱
organizationName=GXU   #CA根证书持有者所属的组织
```

在上述准备工作即对CA系统的环境和配置文件修改完成后,就可以生成CA证书了:

1、首先建立一个CA的根私钥文件,使用RSA格式,2048位。格式如下:

```
openssl genrsa -des3 -out gx-ca.key 2048
```

2、利用建立的私钥,为CA自己建立一个自签名的根证书文件。格式如下:

```
openssl req -new -x509 -days 5000 -key gx-ca.key -out gx-ca.pem-outform PEM
```

查看证书:openssl x509-in gx-ca .pem -text -noout

第二步:签发用户证书。

1、生成用户证书的私钥文件:openssl genrsa -des3 -out client.key 2048。

2、OpenSSL生成用户证书时,不能直接生成证书,而是需要通过证书请求文件生成,因此现在来建立用户的证书请求文件。格式如下:

```
openssl req -new -key client.key -out client-req.pem-outform PEM
```

3、证书请求文件生成后,就可以使用CA的根证书、根私钥来对请求文件进行签名,生成客户端证书client.pem。格式如下:

opensslca -in client-req. csr -out client. pem -outform PEM -days 365 -CAserial serial

4、签发完成后,需要对证书文件 client. pem 和密钥文件 client. key 合并,并且使用 openssl 的 pkcs12 转换成浏览器可以识别的证书格式。格式如下:

openssl pkcs12 -export -in client. pem -inkey client. key -out client. pl12

到此,根 CA 为用户签发的证书 client. pl12 的过程结束,用户可以把该证书安装到用户浏览器中使用。

第三步,注销用户数字证书。

1、当用户没有权限访问本系统或者该用户数字证书不被信任,系统要对证书进行注销操作,被注销的证书写入 CRL(数字证书注销列表)文件中:openssl ca -revoke client. pem

2、证书被注销后还需要发布新的 CRL 文件:openssl ca -gencrl -out gx-ca. crl

3、查看 CRL 列表中数字证书注销的信息:

openssl crl-in gx-ca. crl-text-noout-keyfile gx-ca. key -cert gx-ca. pem

4、验证 CRL 列表的 CA 签名信息:openssl crl-in gx-ca. crl-noout-CAfile gx-ca. pem

2.2　证书认证服务

证书认证服务是在 CA 证书中心生成并颁发给用户数字证书后,并由用户把数字证书安装到浏览器中,当用户登录访问应用系统时候,身份认证系统会自动读取安装在浏览器证书文件,进行身份验证。证书认证服务流程如图 5 所示。

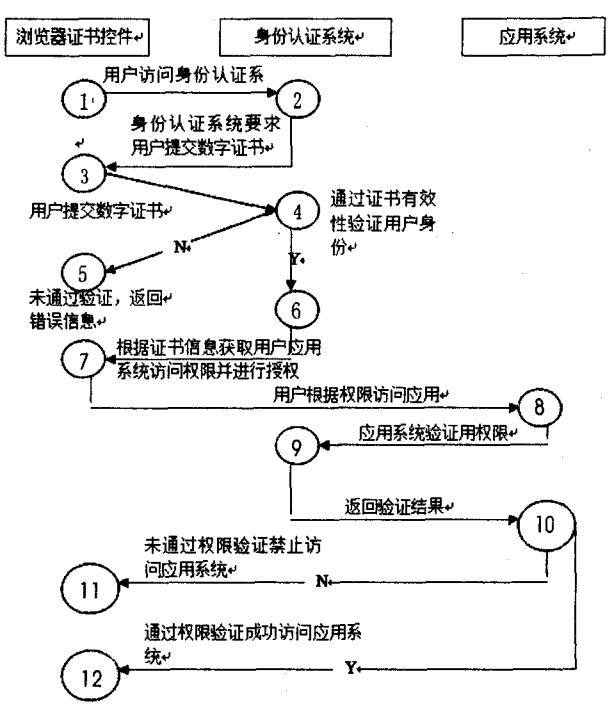

图 5　证书认证服务流程图

3　结束语

文中设计并实现了基于数字证书的网络身份认证系统。采用 JSP 技术、软件成熟架构、开源 OpenssL 软件包以及数字证书等安全技术实现了各个模块的功能[13,14]。身份认证登录系统作为第一道关卡,能够确保合法用户安全使用系统,系统模块实现的结果表明,成熟的系统架构更具有良好扩展性和易维护性,系统采用的技术路线和设计方法是有效和可行的。开发对安全性要求较高的项目中,该系统可以作为一个基础以此扩展。

参考文献:

[1] 管　军. 基于数字证书认证机制的应用研究[J]. 信息化研究,2010,36(3):35-39.

[2] 曹　望,尤志强. 基于数字证书的通用权限管理的设计与实现[J]. 计算机系统应用,2010,19(9):128-133.

[3] 贺　锋,王汝传. 一种基于 PKI 的 P2P 身份认证技术[J]. 计算机技术与发展,2009,19(10):181-184.

[4] 徐小平,尹颖禹. 基于数字签名的身份认证模型的一种方案[J]. 计算机技术与发展,2006,16(2):220-225.

[5] 李余库,张德运,张　勇. 身份认证机制研究及其安全性分析[J]. 计算机应用研究,2001,5(11):126-128.

[6] Park J S, Sandhu R. Binding identities and attributes using digitally signed certificates [C]//In:16th Annual Conference on Computer Security Applications. [s. l.]:[s. n.],2000.

[7] Zhu Junxuan, Wu Zhong. The Digital Signature Technology in E-commerce Systems[C]//Proceedings of the 2009 International Conference on Electronic Commerce and Business Intelligence. [s. l.]:[s. n.],2009.

[8] Lu Yang, Li Jiguo. Generic Construction of Certificate-Based Encryption in the Standard Model[C]// In: Second International Symposium on Electronic Commerce and Security. [s. l.]:[s. n.],2009.

[9] Chin-Ming Hsu. A group digital signature technique for authentication[C]//In:IEEE 37th Annual 2003 International Carnahan Conference on Security Technology. [s. l.]:[s. n.],2003.

[10] Peng Yinghui. The Application of PKCS#12 Digital Certificate in User Identity Authentication System[J]. IEEE Computer Society,2009,4(10):351-355.

[11] 吕格莉,王　东,戴　骥,等. 基于数字证书技术的增强型身份认证系统[J]. 计算机应用研究,2006,8(11):114-119.

[12] 彭英慧,刘海丰. 基于数字证书 X. 509 的身份认证系统的研究[J]. 计算机安全,2008(11):46-49.

[13] 李振捷,陈　雄,王　军. JSP 网站开发典型模块与实例精讲[M]. 北京:电子工业出版社,2006.

[14] 邓子云,肖　锋,谢英辉. 精通 J2EE 网络编程[M]. 北京:清华大学出版社,2007.