文章编号:2095-6134(2015)05-0682-07

云存储环境中的统一认证技术*

王 雷†, 王平建, 向 继

(中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093)

(2014 年 8 月 20 日收稿; 2015 年 1 月 30 日收修改稿)

Wang L, Wang P J, Xiang J. Unified authentication technology in cloud storage environment[J]. Journal of University of Chinese Academy of Sciences, 2015,32(5):682-688.

摘 要 深入研究云存储环境中的统一身份管理技术,并针对云存储环境中的用户认证和授权问题开展研究,提出一种新型的统一认证和身份管理云服务方案.该方案可以有效地为云计算环境中多个应用与云存储之间的数据访问提供安全保护.对该方案的原型系统进行了实现,验证了该方案的可行性和安全性.

关键词 云存储; 统一认证; 身份管理

中图分类号:TP309 **文献标志码**:A **doi**:10.7523/j.issn.2095-6134.2015.05.015

Unified authentication technology in cloud storage environment

WANG Lei, WANG Pingjian, XIANG Ji

(*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract We study the technology of unified identity management and the user authentication & authorization in the cloud storage environment. We propose a cloud service scheme for the unified authentication and identity management, which provides the security assurance when users enjoy the cloud storage and application services in the cloud environment.

Key words cloud storage; unified authentication; identity management

在普通计算环境中,用户需要经常性地访问已知的网络应用,然而,尽管这些网络应用需要能够对用户身份进行认证,用户却通常并不对访问的网络应用进行认证.在云存储环境中,用户往往会接触很多应用,并且用户选择和使用的应用总数将会持续增加,如何在满足不断增加的云应用对用户的认证需求的同时,减轻用户的登录代价是目前亟待解决的问题,即在不需要用户频繁地进行登录,并且不过多地向应用暴露用户隐私信息的前提下,实现用户对多个应用的访问.另外,组织内部在部署使用多个云应用来辅助办公时,如何为每个应用维护用户账号信息,如何实现统一的安全策略也是需要进一步研究的问题.

在使用现有的云存储[1]服务时,只有通过身份鉴别和执行操作权限验证的用户,才能利用云存储服务提供的接口,提交操作请求并完成后续

* 国家高技术研究发展(863)计划(2012AA013104,2013AA01A214)和中国科学院战略性先导专项(XDA06010702)资助

† 通信作者,E-mail:wanglei@iie.ac.cn

流程;否则,云服务将拒绝用户的操作请求. 云存储服务的访问控制过程,主要包括身份鉴别和权限验证,而不同的云存储服务商所使用的身份鉴别机制、权限验证机制又略有不同. 因此,目前还无法在多个云存储服务、云计算服务、云应用服务的提供商之间直接实现灵活的相互访问.

随着云存储技术的发展与各种云应用的普及,云存储环境中面临各种安全问题,其中,作为访问控制的第一道屏障,身份认证是最基本的安全需求. 然而,在云存储环境中,由于参与方之间没有传统应用模式中直接的相互认证,因此,需要以一种既适用于云计算环境又安全可靠的方式来鉴别彼此.

为解决云计算模式带来的对认证和鉴权技术的新挑战,我们提出一种新型的统一认证和身份管理云服务,以云服务的形式对用户、应用提供身份鉴别、权限判定、身份管理等多种功能,实现多应用之间用户的相互认证、云服务之间的相互访问,为云计算环境中多个应用与云存储之间的数据访问提供灵活而安全的保护.

1　现有云存储环境中的认证与授权技术

1.1　云存储中的身份鉴别

目前,典型的云存储服务有 Amazon S3[2]、Microsoft Windows Azure[3]和 Google Storage[4],我们对这 3 种典型的云存储服务进行了深入研究,对现有的认证与授权技术展开分析.

这 3 种主流的云存储服务均采用两层的方式组织存储,以 Amazon S3 为例,要求每个被存储的对象都存在一个具有唯一标识的桶(Bucket)中,桶在云存储中具有唯一的、不可重复的名称,且这个名称用于识别用户的账号、计费、实施访问控制等.

云存储服务以访问接口的形式,对用户提供数据上传、下载、编辑、删除等基本操作功能,例如 Amazon S3 提供 REST(Representational State Transfer)[5]和 SOAP(Simple Object Access Protocol)[6]2 个接口. 表 1 总结了 3 种典型云存储服务支持的服务接口以及官方为开发人员提供的客户端类库[7].

表 1　云存储服务接口对比[7]

Table 1　Comparison of the cloud storage service interface

云存储服务	接口类型	客户端类库
S3	REST 接口, SOAP 接口	Java、PHP、Ruby、Windows and. NET
Windows Azure	REST 接口	. Net Managed Library、Native Library
Google Storage	REST 接口	Python

Amazon S3、Windows Azure 和 Google Storage 这 3 种主流的云服务采用的用户身份鉴别方式,都是基于用户标识与访问密钥进行的:当用户请求云服务的访问操作时,需要调用云服务提供的接口生成请求数据包(含有用户标识、用户访问权限等),并利用访问密钥采用某种 HMAC[8]对请求数据包进行签名,同时将签名结果附加到请求数据包中,云存储服务在对签名进行验证通过后,方才处理请求数据.

这些主流云存储服务采用基于用户标识与访问密钥的鉴别方式,在某种程度上无法满足对安全性要求较高的应用场景,为了提高用户使用云存储服务的安全性,需要结合使用多因素认证机制,例如,在进行身份鉴别时,用户在提供标识与访问密钥的同时,还需要提供智能密码钥匙,从而采用非对称密码算法完成用户身份的鉴别.

1.2　云存储中的授权

文献[7]中指出,Google Storage 仅支持通过访问控制表进行授权,能够赋予的权限相对简单,包括读、写和完全控制;Amazon S3 和 Microsoft Windows Azure 的授权方式比较完善,并且存在较大差异. Amazon S3 和 Microsoft Windows Azure 的授权方式在安全性和灵活性上各有侧重,如果将二者结合,可以实现更好的授权方案.

本文提出的统一认证和身份管理云服务方案,为用户在云环境中的多个应用和云存储之间的数据访问提供了安全保护,有效结合身份管理、身份鉴别、授权、访问控制、审计等多方面的内容,可以有效提高云存储环境中数据访问的安全性.

2 统一认证和身份管理云服务设计

2.1 设计思路

3 种典型的云存储服务在实现身份鉴别、授权与访问控制功能方面,具有各自的特点. 但是通过对其功能及技术特点进行分析、比较,他们均缺少一种可以有效地为用户与多个云存储应用之间的交互提供灵活的、统一的身份认证与访问控制方式,从而减少用户在访问多个云存储应用时的认证次数、提高用户使用体验.

因此,为了满足用户在云存储环境中使用多种云服务带来的新的安全需求与认证挑战,同时减轻用户的登录负担,优化用户使用体验,促进云存储服务应用的发展,我们提出一种集中的、统一的身份认证与管理系统架构,为用户在多个云存储应用之间提供统一的身份鉴别机制,简化用户身份鉴别的流程.

统一认证是指,通过建立统一认证与身份管理系统,为机构的和授权各类业务系统提供通用支撑性的用户管理、身份认证管理,为用户提供方便的单点登录功能,并实现可靠访问控制. 统一认证与身份管理系统的建设将大大提高用户管理的高效性,降低后台管理人员的维护工作量,并通过共享的用户信息服务,将各业务系统有机的整合在一起,实现互联互通.

2.2 统一认证与身份管理系统架构

统一认证与身份管理系统的建立,对用户而言,登录所有业务系统都使用唯一的凭证(数字证书或用户名/口令),实现对多个系统的“单点登录、多点漫游”. 对管理者而言,可以为其提供统一、集中、有效的用户管理机制;建立统一的用户编码体系,实现用户的统一,实现和各业务系统一一对应,并在系统上线时实现各系统之间的平滑过渡;能够实现用户管理和授权;整合了现有各个业务系统的登录入口;实现业务管理与安全管理之间的分权管理;具备灵活和方便的使用模式.

与现有云存储使用的用户认证技术相比,统一认证与身份管理系统能够为云环境中的云应用服务和云存储之间的数据访问提供统一的用户身份认证、权限管理等功能,简化用户对繁杂登录口令的管理,使得用户在使用多个云应用、云存储服务时,仅需要登录、认证一次即可,无需多次登录;同时,将用户身份管理功能、部分访问控制功能从云应用中脱离出来,由统一认证与身份管理系统集中完成,简化管理员的管理工作,提高用户管理的效率.

统一认证与身份管理系统总体框架如图 1 所示:

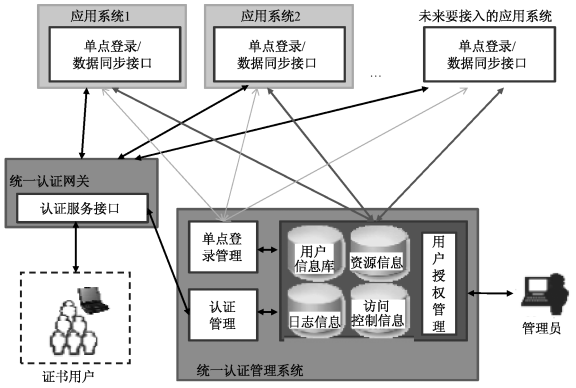

图 1 统一认证与身份管理系统总体框架图

Fig. 1 Framework of the unified authentication and identity management system

2.3 系统安全服务架构

统一认证与身份管理系统主要用于管理用户的身份和认证凭证(口令、数字证书),同时提供各个业务系统统一认证和单点登录的能力. 统一认证与身份管理系统主要完成的功能和提供的服务包括:

1) 用户身份生命周期管理服务. 提供一站式的管理接口,实现用户数字身份的全生命周期管理,包括创建、修改、删除等. 同时提供用户身份信息与认证凭证的在线自助服务,包括口令修改、证书下载、证书更新等. 对用户进行授权,即允许用户访问哪个或者哪些业务系统.

2) 单点登录服务. 通过一个统一的登录入口实现用户在业务系统的单点登录,支持用户名口令和数字证书等多种认证方式,通过安全票据、SAML[9]、OpenID[10]等技术实现各个业务系统的单点登录.

3) 用户查询与认证服务. 提供集中的用户身份信息存储和查询服务,提供 LDAP、AD、Web Services 等查询接口. 同时提供 LDAP 认证、AD 认证、Radius 认证等用户认证接口.

4) 用户信息同步服务. 与各个业务系统的用户数据库进行信息同步. 根据用户数据库的类型不同,包含数据库同步、LDAP 同步、AD 同步等功能.

5) 认证策略管理服务. 实现身份管理与单点登录等安全策略的统一管理和实施.

统一认证与身份管理系统功能和提供的服务如图 2 所示.

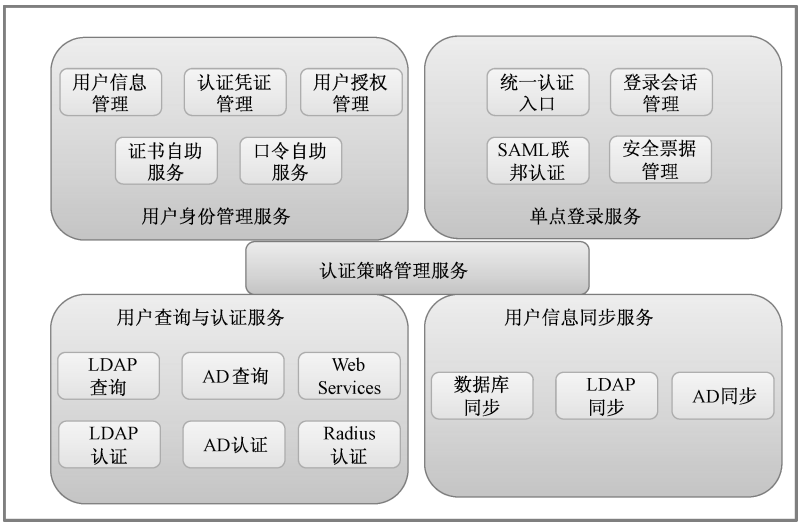

图 2　统一认证服务组成

Fig. 2　Component modules of the unified authentication and identity management service

2.4　系统组成架构

统一认证与身份管理系统由统一身份管理系统、统一认证与身份管理系统以及用户数据库 3 部分组成. 其中

1) 统一身份管理系统主要进行用户数字身份全生命周期的统一管理,由用户身份管理 Web 服务器、用户管理服务器、策略管理服务器和用户查询服务器等组成. 身份管理系统通过 Web 服务方式提供接口供管理员进行用户身份信息的管理. 其中 a) 用户身份管理 Web 服务器为用户管理员提供用户信息管理、用户认证凭证管理、授权管理的接口,同时提供统一安全策略管理的接口. 用户身份管理 Web 服务器还为用户提供口令修改、证书更新等自助服务的接口. b) 策略管理服务器主要负责管理和存储统一认证与身份管理系统的安全策略,并将安全策略下发到用户管理服务器、单点登录服务器等处执行. c) 用户管理服务器主要负责接收用户身份管理 Web 服务器录入的用户信息并存储到用户数据库中,同时还与业务系统的数据同步接口模块进行数据同步,包括从应用系统同步最新的用户数据,以及将最新的用户数据同步到各个业务系统中. 用户管理服务器还与 CA 系统进行交互,自动完成证书申请、撤销等操作. d) 用户查询服务器主要负责为各个业务系统提供基于 LDAP、AD、Web Services 的用户信息查询接口.

2) 统一认证与身份管理系统主要实现应用的单点登录功能,由统一认证网关、单点登录服务器、用户认证接口服务器组成. 其中 a) 统一认证网关主要进行用户身份信息的验证,支持用户名口令认证、基于 UKey 的证书认证等多种认证方式. b) 单点登录服务器主要进行单点登录安全票据的管理,以及登录会话的管理. c) 用户认证接口服务器主要为业务系统、网络设备或者用户操作系统提供用户认证接口,包括 LDAP 认证、AD 认证、Radius 认证等等.

3) 用户数据库存储用户的身份信息、认证凭证、授权信息等,它通过身份管理系统进行信息更新和维护,通过用户管理服务器与各业务系统进行数据同步,通过用户查询服务器向业务系统提供用户信息查询服务,通过统一认证与身份管理系统实现用户的认证和单点登录.

统一认证与身份管理系统通单点登录、数据同步、用户信息查询、用户认证等接口与业务系统进行交互.

系统组成架构如图 3 所示. 统一认证与身份管理系统由统一身份管理系统和统一认证与身份管理系统两部分组成,其中统一身份管理系统主要负责用户身份信息管理以及与其他业务系统进行用户信息的同步,主要软件模块包括用户身份管理界面,策略管理,用户管理,用户数据同步,用户信息查询等.

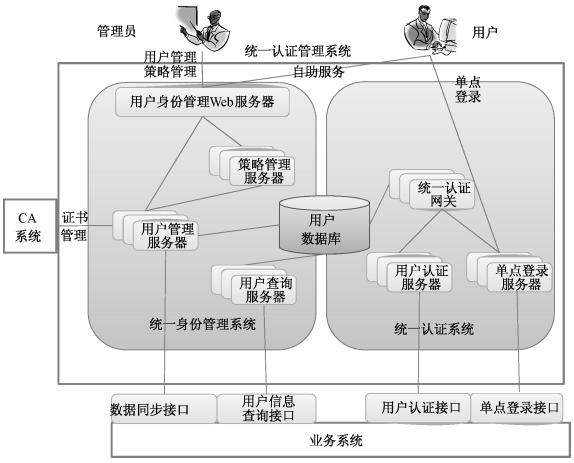

图 3 系统组成架构图

Fig. 3 Architecture of the unified authentication and identity management system

统一认证与身份管理系统主要负责用户认证与单点登录,主要软件模块包括统一认证网关,单点登录入口,单点登录管理,登录会话管理,用户认证等.

3 统一认证与身份管理关键技术

3.1 单点登录技术方案

统一认证与身份管理系统单点登录的工作原理如图 4 所示.

用户通过统一认证与身份管理系统的一个单点登录入口(基于 Web 的用户登录界面)进行登录,登录可以利用用户名/口令的方式进行,也可以使用基于 UKey 的数字证书的方式进行,登录成功以后,统一认证与身份管理系统为用户浏览器发放一个安全票据供用户访问业务系统时使

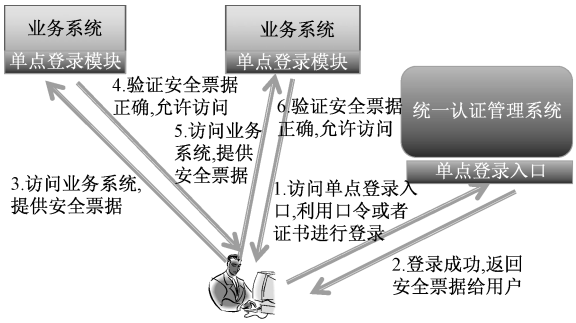

图 4 单点登录技术方案

Fig. 4 Technical solution of the single sign on

用,安全票据记录用户登录成功的信息,并由统一认证与身份管理系统进行数字签名,保证其不可伪造和篡改. 用户访问业务系统时,用户浏览器会自动将安全票据附加在请求中一并提交给业务系统,业务系统的单点登录模块如果未在用户的请求中发现安全票据则会将用户重定向到单点登录入口要求用户进行登录,如果发现了安全票据,则会对票据进行验证,验证通过以后允许用户访问业务系统. 当用户访问另外一个业务系统时,也采用上面的方式来验证用户身份.

由于采用单点登录模块取代原有业务系统的用户登录界面,用户只需要在统一认证与身份管理系统的单点登录入口登录一次并获得安全票据以后,就可以直接访问具备单点登录模块的各个业务系统,实现单点登录.

3.2 用户认证技术

为适应不同安全强度和应用场景的需求,统一认证与身份管理系统提供多种认证方式,如表 3 所示.

表 3 用户认证方式

Table 3 Methods of users' identification and authentication

认证方式	认证凭证	凭证申请和更新	应用场景	备注
UKey 证书	UKey 硬件介质,用户输入 UKey 的 PIN 码后认证成功	支持发放和用户自助下载证书,过期时用户可自助完成证书更新	适用所有应用场景(用户需携带 UKey)	UKey 集成主机安全检查工具,证书管理工具
用户名口令	用户名口令	管理员设置初始口令,用户自助修改口令	仅访问低安全级别的业务系统(不可访问 ARP 系统)	可根据安全策略设置口令强度、定期口令更新要求
手机一次一密	用户输入用户名和手机号后 4 位后,系统通过短信发放一次性可用的口令	用户通过手机可以申请并获取一次性口令	用户出差忘了携带 UKey 时使用	短信可能会存在一定的延迟,仅在别的方式不可用时作为应急方案

3.3 用户映射技术

统一认证与身份管理系统和业务系统各自拥有独立的一套用户和用户管理体系,为了实现单点登录,需要将统一认证与身份管理系统中的用

户与业务系统中的用户建立一个映射关系. 例如统一认证与身份管理系统中有一个用户账号是 zhangsan,而一个业务系统中有一个用户账号是 szhang,事实上这 2 个账号都是对应到 1 个特定用户,通过映射可以将 zhangsan 和 szhang 这 2 个系统中的账号关联起来,以实现单点登录.

统一认证与身份管理系统与业务系统的用户账号进行映射是实现单点登录的前提,这样用户在统一认证与身份管理系统登录以后,统一认证与身份管理系统可以通过安全票据将用户在业务系统中的用户账号提交给业务系统. 用户映射有如下 3 种方式:

1) 统一认证与身份管理系统与业务系统通过一个全局唯一的用户 ID 进行用户账号映射,统一认证与身份管理系统和业务系统的用户数据库中除了保存自己的用户账号以后,还保存一个全局唯一的用户 ID,这样通过用户 ID 可以实现统一认证与身份管理系统和业务系统的用户映射.

2) 统一认证与身份管理系统完成用户映射,统一认证与身份管理系统的用户数据库中除了保存用户在本系统的账号外,还保存用户在其他业务系统的账号,在单点登录的安全票据中,统一认证与身份管理系统直接放置用户在目标业务系统的用户账号.

3) 业务系统使用统一认证与身份管理系统的用户账号,业务系统可以通过 LDAP 等接口获得并使用统一认证与身份管理系统的用户账号,这样就不需要进行用户映射.

用户 ID 方式可以通过统一用户身份管理方式自动实现用户信息的映射和同步,但是需要对业务系统的管理模块进行改造. 第 2 种方式的优点是用户映射由统一认证与身份管理系统完成,业务系统的用户管理不需要进行改造,但是需要设计一种安全的机制实现统一认证与身份管理系统账号和业务系统账号之间的同步.

4　实现与部署

基于 SAML 协议,我们参照并修改 Shibboleth[11] 的部分实现方式,实现了上述方案的原型系统,统一认证与身份管理系统的服务器分别部署在 3 个区域中(见图 5),分别是:

1) 服务区:主要部署直接与用户和业务系统接口的服务器,包括用户身份管理 Web 服务器、单点登录服务器、用户查询服务器、用户认证接口服务器等.

2) 管理区:主要部署用户管理服务器、策略管理服务器和统一认证网关等.

3) 核心数据区:主要部署用户数据库.

统一认证与身份管理系统中的关键服务器和数据库采用双机热备的方式进行部署,保证系统

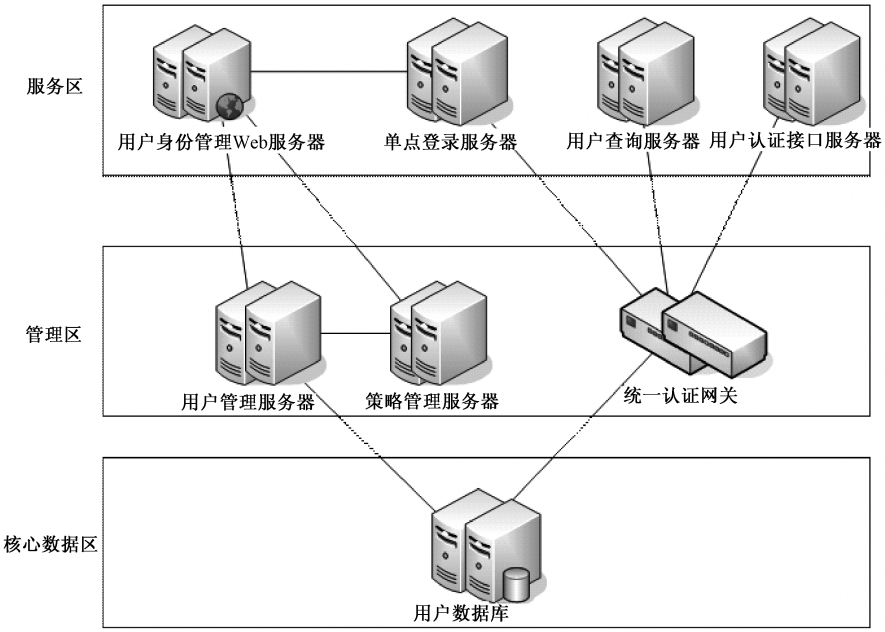

图 5　统一认证网络部署

Fig. 5　Network deployment of the unified authentication and identity management system

的正常运行,同时采用应用服务器虚拟化技术,将多个系统模块部署于同一台物理服务器,易于实现各个服务器系统的迁移. 实验表明,本原型系统能够支持上万用户的并发访问.

5 总结

本文针对云存储环境中多个应用之间数据访问的安全需求,提出一种统一认证和身份管理云服务方案,该方案采用单点登录,在满足不断递增的云应用对用户认证需求的同时,降低了用户的登录频率;通过统一的安全策略执行权限管理的同时,不需要向应用泄露额外的用户隐私信息;采用统一身份管理机制,满足组织机构在大量应用中对内部员工的统一管理需求;同时,该方案还支持通过少量的改造将已有应用迁移到云环境.

参考文献

[1] Brunette G, Mogull R. Security Guidance for critical areas of focus in Cloud Computing V2.1 [R/OL]. CSA (Cloud Security Alliance), USA. (2009-12)[2014-07-02]. https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.

[2] Amazon. Amazon simple storage service (Amazon S3)[EB/OL]. [2014-07-02]. http://aws.amazon.com/s3/.

[3] Chappell D. Introducing the Windows Azure Platform [R/OL]. (2009-12)[2014-07-02] http://www.davidchappell.com/writing/white_papers/Windows_Azure_Platform_v1.3—Chappell.pdf.

[4] Google. Google storage for developers: developer's guide[G/OL]. [2014-07-02]. https://cloud.google.com/storage/docs/concepts-techniques.

[5] Richardson L, Ruby S. RESTful Web Services 中文版[M]. 徐涵,李红军,胡伟,等译. 北京:电子工业出版社, 2008.

[6] W3C. W3C soap specifications[EB/OL]. [2014-07-02]. http://www.w3.org/TR/soap/.

[7] 王平建,荆继武,王琼霄,等. 云存储中的访问控制技术研究[J]. 信息网络安全,2011(9):41-43.

[8] Bellare M, Canetti R, Krawczyk H. Keying Hash functions for message authentication [C/OL]//Proceedings of the 16th Annual International Cryptology Conference (CRYPTO). 1996: 1-15.

[9] OASIS. Security assertion markup language (SAML) V2.0 Technical Overview [S/OL]. OASIS Standard. (2008-03)[2014-07-02]. https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.

[10] OpenID Authentication 2.0[EB/OL]. OpenID.Net. [2014-07-02]. https://openid.net/specs/openid-authentication-2_0.html.

[11] Shibboleth [EB/OL]. [2014-07-02]. http://www.shibboleth.net/.