浙江理工大学学报(自然科学版),第31卷,第1期,2014年1月
Journal of Zhejiang Sci-Tech University (Natural Sciences)
Vol. 31, No. 1, Jan. 2014

文章编号:1673-3851 (2014) 01-0075-04

# Windows Azure平台数据存储的访问控制研究

宁方华[1],牛建瑞[1],俞武嘉[2],郭玉明[3]

(1. 浙江理工大学先进制造技术研究所,杭州 310018; 2. 杭州电子科技大学自动化学院,杭州 310018;
3. 山东电工电气日立高压开关有限公司,济南 250101)

**摘　要**:访问控制是保证信息机密性和完整性的关键。针对微软的云平台——Windows Azure平台,着重研究其具有存储功能服务的访问控制技术,其中具有存储功能的服务包括Windows Azure的Storage Service和数据库SQL Database,从用户验证和授权两个过程对这两种存储服务的访问控制技术进行分析探讨。最后根据这两种服务的存储特点,以基于Windows Azure的门禁管理系统为例,给出系统在Windows Azure平台的安全存储的部署方案,保证系统的安全性和灵活性。

**关键词**:Windows Azure平台;访问控制技术;云计算

**中图分类号**:TP399　　**文献标志码**:A

## 0　引　言

目前,微软、谷歌、亚马逊和IBM等IT业巨头都建立了云计算平台,随着云计算及应用范围的不断扩大,信息安全问题已成为制约云平台快速发展和推广的重要因素之一。Windows Azure平台是微软于2008年发布的云计算平台,它也可以通过Internet为在其他地方运行的应用程序提供服务,可以直接运行应用程序,并保证性能不降低[1-3]。该平台提供的服务主要有Windows Azure、SQL Database和AppFabric,其中Windows Azure的Storage Service和SQL Database具有数据存储功能。目前为止,Windows Azure刚刚落户中国,实际应用还处于初级阶段,如何充分利用Windows Azure平台数据存储的安全控制技术,以保证系统开发的安全性和灵活性值得深入研究[4-5]。

访问控制作为一种重要的信息安全技术,是保证云平台的信息机密性和完整性的关键技术[6]。访问控制过程大致可以分为验证和授权两个过程。本文在明确区分验证和授权两个过程的基础上,着重研究Windows Azure平台数据存储功能服务的访问控制技术,旨在提供应用程序以最小权限运行的设计指导,提高系统的安全性和访问灵活性。

## 1　在Windows Azure Storage Service中的访问控制

### 1.1　Windows Azure Storage Service

Storage Service由Windows Azure提供,具有数据存储功能。它主要开放Blob、Table和Queue 3种存储方式,分别存储非结构化数据(如文档、图片和影像等)、结构化数据(订单信息或用户注册信息等)和用于应用程序不同模块之间异步通信机制,以此满足用户不同数据存储需求[7]。

Storage Service支持访问协议HTTP/HTTPS,使用单一的URL作为访问入口。服务接口使用REST接口和Windows Azure SDK类库,其中REST是一种针对网络应用的设计和开发方式,可以降低开发的复杂性,提高系统的可伸缩性;Windows Azure SDK类库是REST接口的封装,由微软专门为.NET平台开发人员提供,使.NET平台开发相较于PHP/

收稿日期:2013－04－22
基金项目:浙江省重点创新团队项目(2011R09015－13)
作者简介:宁方华,(1978－),女,山东泰安,博士,副教授,研究方向为现代物流与供应链管理、物联网技术、物流信息化。

Java/Perl/Ruby 等其他平台难度降低。

### 1.2 基于密钥的身份验证

Storage Service 采用访问密钥这种安全性较高的验证方式。Storage Service 端与客户端使用相同的访问密钥,并采用相同方式利用 HMAC-SHA256 加密算法对数据请求进行数字签名,最后 Storage Service 端通过判断生成的数字签名与客户端的是否相同达到验证目的。用户请求访问 Storage Service时验证过程如图 1 所示。

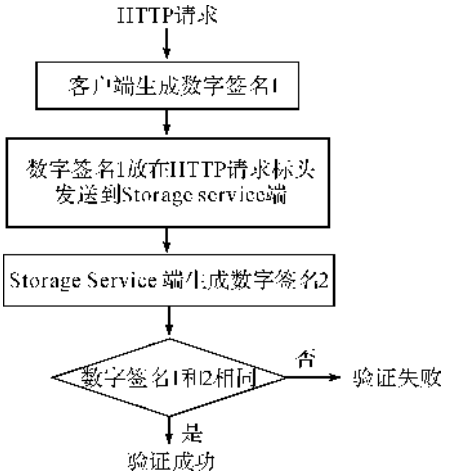


图 1 Storage Service 使用访问密钥进行身份验证的流程

### 1.3 授权方式

Storage Service 有两种访问角色,一种是拥有账户名称和密钥的所有者,另一种是匿名者,其中所有者可以通过访问密钥获得 Storage Service 的完全访问权。所以下面的权限设置针对匿名用户,内容包含增加、删除、修改和查询的操作权限。

Storage Service 中 Table 和 Queue 不允许匿名用户访问,Blob 的授权方式比较灵活。Blob 采用两层的方式组织存储,外层是 Blob 容器,里层是一组 Blob 对象。Blob 容器本身可以作为访问控制单元进行权限设置,也可以对其进一步设置访问控制策略(Shared Access Policy)实现对 Blob 对象的访问权限设置。通过设置 Shared Access Policy 的 Start Time、Expiry Time 和 Permissions(包括 Read、Write、Delete、List 和 None)生成共享访问签名(Shared Access Signatures URL)。使用 Shared Access Signatures URL 访问 Blob 对象可以授权匿名用户而不用公开密钥或者将 Blob 容器设置为允许匿名用户,从而实现匿名用户安全访问。

## 2 在 SQL Database 中的访问控制技术

### 2.1 SQL Database

Windows Azure 虽有 Storage Service 用于存储,但 Storage Service 并非关系型数据库,无 JOIN 等常用功能,并且其采用分布式海量数据存储法,在处理复杂应用时,无法用规范化机制过滤重复数据,大量数据在应用程序与 Storage Service 之间的不断传输和计算将花费大量时间。鉴于此,微软提供 SQL Database(旧称为 SQL Azure)开发和部署关系型数据库。SQL Database 的高扩展性和高可用性使用户可以轻松扩展解决方案和无需备份及容灾处理,并且使用通用的通信协议 TDS,支持 ADO.NET、ODBC、JDBC 和 SQL Server 客户端类库,使得用户可以利用 Transact-SQL 和 SQL Server 工具管理数据库,从而降低开发难度[8]。

### 2.2 防火墙+SQL 身份验证模式

SQL Database 采用防火墙+SQL 身份验证模式验证客户端,确保每个连接到 SQL Database 的请求都通过验证。其中防火墙验证客户端计算机的 IP 地址是否在防火墙指定的允许计算机连接范围以内,SQL 身份验证客户端用户的账户和密码与 sys.sql_logins(必须连接到 Master 数据库)中的清单是否匹配,只有两种验证都成功,SQL Database 才接受访问请求,验证过程如图 2 所示。

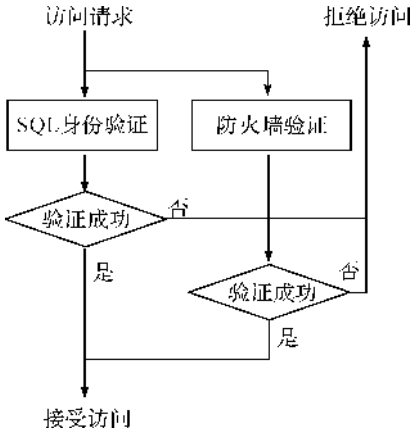


图 2 SQL Database 用户验证流程

### 2.3 基于角色的授权方式

SQL Database 在防火墙规则中设置允许访问的 IP 地址范围后,通过采用基于角色的方式授予用户访问权限,授权内容包括对数据库和登录名增加、删除、修改的操作权限。SQL Database 通过分配权限给角色,再将角色赋给用户完成对用户的授权,提供的安全角色有两个:loginmanager 和 dbmanager,分别授权用户对登录名和数据库的操作权限。在 SQL Database 服务申请验证配置后,用户会拥有一个 SQL Database 服务器、一个 master 数据库和一个 Server-lever Principal Login 登录名,Server-le-

ver Principal Login 登录名类似于 SQL Server 实例的服务器级别的 sa,拥有对数据库管理的权限,master 数据库负责跟踪创建数据库或其他登录名,对登录名或数据库的操作必须先连接到 master 数据库。

## 3　系统在 Windows Azure 平台的安全部署方案

由于门禁管理系统对信息存储和传输的安全要求较高,所以本文以基于云的门禁管理系统为例,设计在 Windows Azure 平台上系统的安全部署方案,通过充分利用 Windows Azure 平台提供的权限设置来有效提高系统安全性和灵活性。

在门禁管理系统中,数据主要包括用户信息、门禁机管理信息、刷卡记录、卡片信息、文件管理等。通过分析存储信息是否需要 JOIN 等复杂操作,决定使用 SQL Database 存储用户信息、门禁机管理信息、刷卡记录、卡片信息等,使用 Storage Service 中 Blob 存储文件管理(包括对门禁机版本文件、声音文件信息的管理)。下面讨论对它们的安全权限进行设置的问题。

### 3.1　SQL Database 设置

使用 SQL Database 最常采用的方式是使用本地 SQL Server 设计数据库后,再上传云端。本案例采用这种方式,首先使用本地 SQL Server2008 R2 设计出数据库 AccessManegement,然后配置数据库在云的端运行环境,包括创建 SQL 服务器、数据库和进行防火墙设置,设置防火墙如图 3 所示,最后将本地 SQL Server2008R2 上的数据库生成的脚本上传到 Windows Azure 平台,上传云端后数据库 AccessManegement 如图 4 所示。

SQL Database 采用基于角色授权方式,下面的代码创建一个登录名为 mylogin 和用户名为mylgUser的数据库用户,通过赋予用户角色,该用户具有创建数据库或其他登录名的权限(连接到 master 数据库)。


图 3　防火墙设置


图 4　云上数据库 AccessManegement

```
CREATE LOGIN mylogin WITH password='< mylogin password>';—创建登录名 mylogin
CREATE USER mylgUser FROM LOGIN mylogin;—创建用户名 loginUser
EXEC sp _ addrolemember 'dbmanager', 'mylgUser';—login1User 被赋予 dbmanager 角色
EXEC sp _ addrolemember 'loginmanager', 'mylgUser';—login1User 被赋予 loginmanager 角色
```

数据库连接字符串在数据库创建完后获得,用户使用连接字符串创建连接信息,在用户应用程序配置文件 Web. config 中的连接信息设置如下:

```
<connectionStrings>
<add name="localAccessManagementConnectionString" connectionString="Data Source=JANE-PC\SQLEXPRESS;Initial Catalog=AccessManagement;Integrated Security=True" providerName="System. Data. SqlClient"/>
<add name="Access ManagementConnectionString" connectionString="Server=tcp:rc5i1ch80k. database. windows. net,1433;Database=AccessManagement;User ID=njrfish@rc5i1ch80k;Password=HEZI2pingzi;Trusted _ Connection=False;Encrypt=True;Connection Timeout=30" providerName="System. Data. SqlClient" />
</connectionStrings>
```

其中,字符串“localAccessManagementConnectionString”用于访问本地数据库,字符串“Access ManagementConnectionString”用于访问上传到云端的数据库,应用程序使用 LINQ TO SQL 实体访问数据库时,可以根据需要在属性连接中设置相应字符串。

3.2 存储服务设置

本案例利用 Blob 存储作为文件存储器,文件管理界面如图 5 所示。使用 Blob 开发,首先需要用户申请 Storage Service 获得主密钥和辅助密钥两个访问密钥,这两个密钥功能相同,之所以有两个是出于安全和减少不必要宕机时间考虑的:通常情况下用户使用主密钥,主密钥泄露时可以在最短时间内使主密钥失效并启用辅助密钥,在此过程中,用户无需修改程序代码,只需更新服务配置文件,不会产生宕机时间。用户获得的两个访问密钥如图 6 所示。最


图 5 文件管理界面


图 6 访问密钥图

后使用获得的访问密钥创建存储服务的连接信息,通过连接信息访问存储服务,配置文件中设置片段如下:

```
<ConfigurationSettings>
.....
<Setting name="AccessFileDataSource.ConnectionString" value="DefaultEndpointsProtocol=https;AccountName=accesssmgstorage;AccountKey=umBvYmFqJJz……NdtrH2ydJ6uZryS8RlFUlrWlgmnz7a0d/LF2P2uQ==" />
</ConfigurationSettings>
```

对于匿名用户对文件管理的操作权限(增、删、读、改)的分配,可以通过共享访问签名实现。下面代码是使用共享访问控制对容器访问控制策略的设置,匿名用户只具有读取文件的权限,并且有效时间是 1 d:

```
BlobContainerPermissions blobPermission = new BlobContainerPermissions();
blobPermission.PublicAccess = BlobContainerPublicAccessType.Container;
blobPermission.SharedAccessPolicies.Add("AccessFileTimePolicy", new SharedAccessPolicy()
{Permissions=SharedAccessPermissions.List|SharedAccessPermissions.Read,
SharedAccessStartTime=DateTime.Now,
SharedAccessExpiryTime = DateTime.Now.AddDays(1) });
container.SetPermissions(blobPermission);
```

## 4 结 语

本文着重研究了 Windows Azure 平台中用于数据存储的 Storage Service 和 SQL Database 的访问控制技术,从访问控制技术的身份验证模式和授权方式两方面分析中可以看出,Windows Azure 平台针对不同服务提供不同的访问控制管理,并且验证、授权方式比较完善。不过,在访问灵活性和安全性方面尚仍存在不足,现在常见的网络攻击下其依然存在安全威胁。所以在利用 Windows Azure 云平台软件开发时,仍应以信息安全为第一考虑因素,设计应用程序在默认设置下以最小权限运行,选择适当的权限模式实现最佳解决方案。

**参考文献:**

[1] 张月雷. 云计算及 Windows Azure Platform 简介[J]. 黑龙江科技信息,2011(28):116-117.

[2] Costa P J P, Cruz A M R. Migration to Windows Azure: analysis and comparison[J]. Procedia Technology, 2012(5): 93-102.

[3] Hill Z, Li J, Mao M, et al. Early observations on the performance of Windows Azure [J]. Scientific Programming, 2011, 19(2/3): 121-132.

[4] 朱明中. 走进云计算 Windows Azure 实战手记[M]. 北京:中国水利水电出版社, 2011: 201-204.

[5] 徐子岩. 实战 Windows Azure:微软云计算平台技术详解[M]. 北京:电子工业出版社, 2011: 206-209.

[6] 王宇杰, 王 锋, 杨文宾. 计算机网络访问控制技术研究[J]. 现代计算机, 2010(7): 20-21.

[7] 方国伟, Bill Liu. 详解微软 Windows Azure 云计算平台[M]. 北京:电子工业出版社, 2011: 151-154.

[8] 涂兰敬. 细数选择云数据库 SQL Azure 的六大理由[J]. 网络与信息, 2012(6): 37.

(下转第 97 页)

# A Property of Trigonometric Series with Piecewise Bounded Variation Coefficients

*HE Ji-long*

(Institute of Mathematics, Zhejiang Sci-Tech University, Hangzhou 310018, China)

**Abstract**: When Fourier coefficient of sine series meets bounded variation condition, this paper generalizes the conditions in Leindler theorem to piecewise bounded variation sequence(PBVS), obtains the relational expression of optimal approximation and coefficient of sine series through research under $L_{2\pi}^{\beta}$ norm with piecewise discussion method in combination with the definition of optimal approximation, and proves the formula.

**Key words**: trigonometric series, PBVS(piecewise bounded variation sequence), Fourier coefficient, best approximation

(责任编辑: 马春晓)

(上接第 78 页)

# Study on Access Control Technology of Data Storage on Windows Azure Platform

*NING Fang-hua*[1], *NIU Jian-rui*[1], *YU Wu-jia*[2], *GUO Yu-ming*[3]

(1. Institute of Advanced Manufacturing Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China; 2. College of Automation, Hangzhou Electronic Science and Technology University, Hangzhou 310018, China; 3. SDEE Hitachi High-Voltage Switchgear Co Ltd, Jinan 250101, China)

**Abstract**: In allusion to Microsoft cloud platform-Windows Azure platform, this paper focuses on studying access control technology of its services with storage function which include Storage Service and SQL Database of Windows Azure; analyzes and discusses access control technology of both storage services from two processes-user authentication and authorization; finally takes access control system based on Windows Azure for example according to storage characteristics of both services, gives the deployment scheme of secure storage of the system on Windows Azure platform and ensures the security and flexibility of the system.

**Key words**: Windows Azure Platform; access control technology; cloud computing

(责任编辑: 张祖尧)