基于 SAMBA 和 CP-ABE 的异构系统访问控制方法

刘青芳,郭银章,胡　鹰
(太原科技大学 群智计算与云计算实验室,山西 太原 034000)

摘　要:针对企业私有云计算环境下原有的 Windows 操作系统所采用的 AD 单点登录不能直接访问云服务器的问题,提出一种基于 SAMBA 协议的异构系统 CP-ABE 加密访问控制方法。现有的异构系统单点登录依赖外部服务器完成身份认证,存在安全隐患且响应速度受网络环境影响,通过在 Linux 服务器上配置 SAMBA 本地服务器作为中介,利用 Winbind 组件和 Kerberos 组件实现 AD 账户到 SAMBA 服务器的映射和身份认证,避免了依赖第三方认证服务器存在的安全风险以及信息交互期间存在的网络性能隐患,同时 iSCSI 组件将云存储系统与 SAMBA 服务器相连,Quota 工具对不同用户和组设置磁盘配额,实现了对云存储空间的合理利用。最后,采用 CP-ABE 技术进行访问控制和文件加密确保数据的安全传输和隐私保护,最终实现 AD 账户单点登录云存储系统。实验表明,该方法在企业私有云环境下能够有效解决异构系统的加密访问控制问题,为混合云环境下的访问控制提供了一种有效的解决方案,为企业数据安全和管理提供了有力支持。

关键词:AD 单点登陆;异构系统;SAMBA;CP-ABE;混合云环境
中图分类号:TP309　　**文献标识码**:A　　**文章编号**:1673-629X(2024)11-0080-07
doi:10.20165/j.cnki.ISSN1673-629X.2024.0243

Access Control Method for Heterogeneous Systems Based on SAMBA and CP-ABE

LIU Qing-fang, GUO Yin-zhang, HU Ying
(Group Computing and Cloud Computing Laboratory, Taiyuan University of Science and Technology, Taiyuan 034000, China)

Abstract: The issue of the original Active Directory (AD) single sign-on used in the enterprise private cloud computing environment not being able to directly access cloud servers is addressed by proposing a cloud storage heterogeneous system CP-ABE encryption access control method based on the SAMBA protocol. Existing cross-platform single sign-on relies on external servers to complete identity authentication, which introduces security risks and is influenced by network environments in terms of response speed. By configuring the SAMBA local server as an intermediary on a Linux server, mapping AD accounts to the SAMBA server, and completing identity authentication using Winbind and Kerberos components, reliance on third-party authentication servers' security risks and network performance issues during information exchange are avoided. Additionally, the iSCSI component connects the cloud storage system with the SAMBA server, and disk quotas for different users and groups are set using the Quota tool, ensuring the rational utilization of cloud storage space. Finally, CP-ABE technology is employed for access control and file encryption to ensure secure data transmission and privacy protection, ultimately achieving AD account single sign-on to the cloud storage system. Experiments demonstrate that the proposed method effectively resolves the cross-platform encrypted access control problem in enterprise private cloud environments, providing an effective solution for access control in hybrid cloud environments and strong support for enterprise data security and management.

Key words: AD single sign-on; heterogeneous system; SAMBA; CP-ABE; hybrid cloud

收稿日期:2024-04-12　　**修回日期**:2024-08-15
基金项目:中央引导地方科技发展资金项目(YDZJSX1A044);国家大学生创新创业训练计划项目(202310109650);2023 年太原科技大学研究生教育创新项目(SY2023041)
作者简介:刘青芳(1995-),女,硕士研究生,CCF 会员(T9755G),研究方向为云计算与云安全;通信作者:郭银章(1968-),男,博士,教授,硕导,CCF 杰出会员(11082D),研究方向为群智计算与云计算、云制造与云安全;胡　鹰(1976-),男,硕士、副教授,硕导,研究方向为智能制造与智能装备设计、计算机控制技术与人工智能、物联网技术应用及智能机器人系统、多目标优化理论及应用等。

0　引　言

随着云计算技术[1]的发展,混合云环境已成为企业数据管理的主要方式之一。然而,企业信息管理系统均采用 Windows 环境下的 AD 单点登录[2]方案,而云计算服务器不支持 AD 域服务器[3]的直接接入,导致无法实现企业私有云环境下的异构系统访问控制,面临数据访问和安全管理挑战。同时数据安全是云环境中的关键问题,传统访问控制[4]模型如 DAC、MAC 和 RBAC[5]虽然发挥了重要作用,但在处理复杂的访问控制需求时表现不足[6]。

针对企业混合云异构系统的访问控制问题,目前国内外开展了相关研究。Vehniä V J 等人[7]提出将云服务器身份验证委托给基于云的 IAM 服务实现异构系统单点登录,提高了用户的便利性和工作效率,但过度依赖外部服务器增加系统风险。杨斌等人[8]利用 LDAP 技术实现异构系统的统一身份管理,但在频繁的身份验证和用户查询场景下易出现性能瓶颈。纪健全等人[9]利用 OpenID Connect 协议实现异构系统统一身份认证,但对网络连接依赖性较高,增加系统的可用性风险。陆志刚等人[10]利用 SAML 协议实现异构系统单点登录,但协议涉及多次交互,影响系统的响应速度和吞吐量。

综上所述,该文提出一种基于 SAMBA 和 CP-ABE 的云存储异构系统访问控制方法,解决了异构系统单点登录时存在的访问控制问题,该方法主要有以下贡献:

●将 Linux 端 SAMBA 文件管理器作为本地服务器实现身份认证,避免了依赖第三方认证服务器存在的安全风险以及信息交互期间存在的性能隐患。

●CP-ABE 策略实现了对共享数据的细粒度访问控制和加密,从而提高了数据共享过程中的访问效率和安全性。

1　相关技术

1.1　SAMBA

SAMBA 是一个开源的 SMB/CIFS 协议,它允许 Linux 系统与 Windows 系统之间进行文件共享。由于 Windows 系统和 Linux 系统的差异,两者无法直接沟通,因此需要两者都支持的协议进行交互,通过在本地 Linux 服务器上配置 SAMBA 服务,使其充当文件服务器向 Windows 客户端提供共享文件和打印服务。

Winbind[11]是 SAMBA 的一个重要组件,它允许将 Linux 服务器集成到 Windows 域环境中,并将 AD 活动目录中的用户和组信息映射到 Linux 系统上,通过 Winbind,Linux 系统可以与 Windows AD 域进行集成,提高了系统的安全性和管理效率。Winbind 工作流程如图 1 所示。

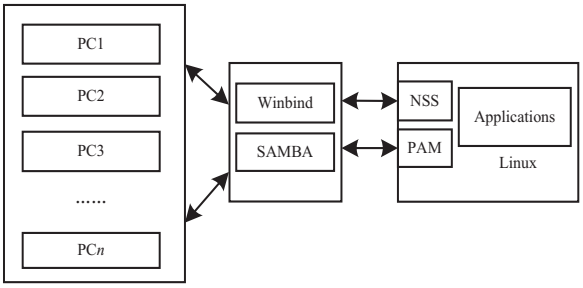

图 1　Winbind 工作流程

Winbind 工作流程主要包含以下步骤:①请求验证:当 Windows 用户尝试访问 Samba 共享资源时,Samba 服务器会收到该请求。Samba 服务器会将该请求发送给 Winbind,以便进行用户身份验证。②查询用户信息:Winbind 组件使用 SMB/CIFS 协议向 Windows 域控制器发送请求,以查询用户的身份验证信息和组成员关系。Windows 域控制器会响应 Winbind 的请求,提供用户的身份验证信息和组成员关系。③本地映射:Winbind 将查询到的用户信息映射到 Linux 系统上的本地用户和组。它会生成本地的用户标识和组标识,以便在 Linux 系统中进行用户身份验证和授权操作。映射后的用户和组信息可以通过 Linux 系统的标准用户和组管理工具进行查看和管理。④用户认证:当用户尝试访问 Samba 共享资源时,Samba 服务器会使用本地映射的用户信息进行用户身份验证。如果用户提供的凭据与本地映射的用户信息匹配,则用户被授权访问共享资源。

除了 Winbind, SAMBA 还结合了 Kerberos 认证[12]来增强系统的安全性。Kerberos 是一种用于网络身份验证的协议,它通过使用票据来验证用户的身份,并确保通信的安全性,它以对称密码体制为基础,提供了一种单点登录的方法。Kerberos 系统包含三个核心角色:认证服务器(KDC)、客户端(Client)和服务端(Server)。在这个系统中,客户端和服务端通过认证服务器相互验证身份。每个客户端和服务端都有自己的密码,这些密码只有它们自己和认证服务器知道。Kerberos 工作流程如图 2 所示。

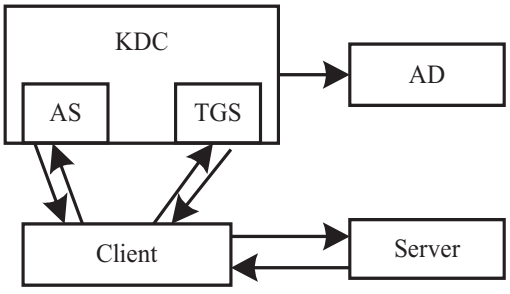

图 2　Kerberos 工作流程

Kerberos 工作流程主要包含以下步骤:①客户机

Client 向 KDC 发送用户信息,向 AS 请求 TGT 票据访问 Server。②KDC 收到了客户端发送的消息后,首先会根据在 Active Directory(AD)中存储的黑名单或白名单信息来判断客户端的可信度。如果客户端可信,则认证服务器(AS)会生成一个随机的 Session Key,并使用客户端的 NTLM 哈希对该 Session Key 进行加密,得到密文 A。然后,AS 使用 krbtgt 的 NTLM 哈希对 Session Key、客户端信息(Client Info)和客户端时间戳(timestamp)进行加密,生成 TGT(Ticket Granting Ticket)。最后,AS 将密文 A 和 TGT 一起返回给客户端。③Client 收到服务器返回的响应后,首先使用自己的 NTLM 哈希对密文 A 进行解密,得到 Session Key。然后,客户端使用 Session Key 对客户端信息和请求访问的服务标识符或名称等加密生成密文 B。接着,客户端将密文 B 和 TGT 一起发送给 KDC 的 TGS(Ticket Granting Server)。④TGS 收到客户端的请求后,首先使用 krbtgt 的 NTLM 哈希对 TGT 进行解密,从中获取 Session Key、时间戳和客户端信息。然后,TGS 使用解密后的 Session Key 对密文 B 进行解密,得到的时间戳和客户端信息以及客户端请求的服务信息生成 Ticket 发送给 Clint。⑤Client 将解密后的时间戳和客户端信息同 Ticket 一起发送给 server,请求服务。⑥Server 收到后用自己的 NTLM HASH 解密出 ticket,ticket 中包含 Server Session key 和 timestamp 和 Client Info,再利用 Server Session key 解密密文 Enc 得到和 timestamp 和 Client Info,两相对比一致则可以提供 Client 访问。

另外,quota 工具在 SAMBA 服务器上也发挥着重要作用。quota 工具用于配置磁盘使用额度,允许管理员限制用户或组在文件系统上的磁盘使用空间。通过设置配额,管理员可以控制用户或组的磁盘使用量,避免资源的滥用和不合理分配。这样可以保证系统的稳定性和性能,并确保资源的合理利用。

1.2 CP-ABE

基于策略的属性加密 CP-ABE[13-15]是一种公钥加密算法,适用于数据共享场景。它通过在密文中嵌入访问策略和在密钥中嵌入用户属性信息的方式,实现了一对多加密,即同一份密文可以被多个满足访问策略的私钥解密。相比传统的访问控制方法,如 RBAC、DAC 等[16]基于角色或身份的访问控制,CP-ABE 提供了更灵活和细粒度的访问控制。CP-ABE 主要涉及以下 4 个算法:

(1)初始化算法(Setup):生成主密钥(MK)和公开参数(PK)

(PK,MK) = Setup(S)

(2)加密算法(Encrypt):根据公开参数(PK)、数据明文(D)和访问结构(AS)生成数据密文(DC)。

DC = Encrypt(PK,D,AS)

(3)密钥生成算法(KeyGen):根据主密钥(MK)和一组属性(A)生成用户私钥(SK)。

SK = KeyGen(MK,A)

(4)解密算法(Decrypt):使用公开参数(PK)、数据密文(DC)和用户私钥(SK)解密数据密文并还原数据明文(D)。

D = Decrypt(PK,DC,SK)

在 CP-ABE 中,访问策略由属性构成,而用户的权限由其属性集合决定。文件被加密时,可以定义一组属性来表示访问策略,只有具有满足这些属性的用户才能解密和访问文件。这种基于属性的访问控制模型使得管理员可以根据需要定义复杂的访问策略,从而实现对文件的精细化控制。结合 CP-ABE 技术,可以实现对重要文件的加密保护。管理员可以根据文件的敏感程度和业务需求,定义相应的访问策略,并将其应用于文件加密过程中。这样,即使文件被不同权限的用户访问,也能确保文件的安全性和保密性。另外,CP-ABE 还具有一定的扩展性和适应性。它可以轻松地与其他安全技术和加密方法结合使用,如数字签名、密钥管理等,从而构建更完善的安全解决方案。此外,CP-ABE 还能够应对动态的访问控制需求,灵活地适应不同环境和应用场景的变化。

2 系统总体框架设计及实现策略

2.1 整体框架

该文搭建了一个混合云环境,其中 Linux 上配置了 SAMBA 服务器作为中介,利用 Winbind 组件实现了与 Active Directory(AD)活动目录的映射。同时,使用 Kerberos 组件实现对 AD 账户的认证,确保用户可以安全地访问系统资源。进一步地,将云存储系统通过 iSCSI 组件与 SAMBA 服务器相连,使得用户可以方便地访问远程云存储资源,而无需直接接入云服务提供商的管理界面。为了合理分配存储资源并确保资源的有效利用,使用 quota 工具对不同用户和组设置了磁盘配额,这有助于控制存储资源的使用情况,防止资源滥用。为了提高数据的安全性,采用了 CP-ABE(Ciphertext-Policy Attribute-Based Encryption)技术来设置访问控制和文件加密。通过 CP-ABE 技术,可以根据用户或组的属性设置访问策略,确保只有授权用户能够访问敏感数据,从而有效地保护数据的安全性和隐私。

通过搭建混合云环境并合理配置相关组件,可以实现 AD 账户单点登录到云存储系统,提高数据的安全性和管理效率,整体框架如图 3 所示。

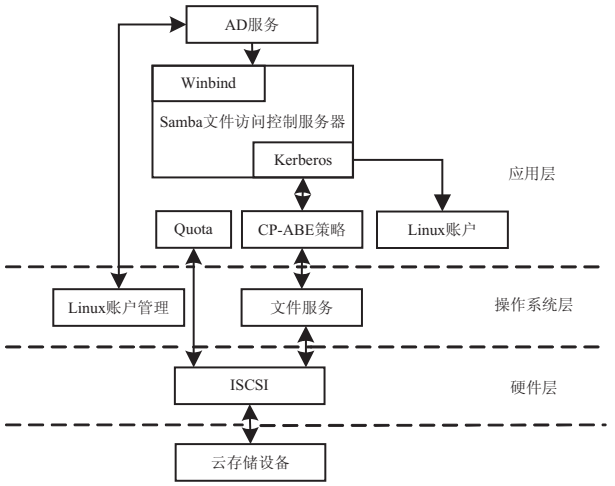

图 3　整体框架

整体框架主要包含以下部分:① AD(Active Directory)域服务器用来统一管理和存储组织内的用户身份信息、组信息以及其他网络资源。②SAMBA 服务器上的 Winbind 组件用来将 AD 活动目录映射到 Linux 系统,使得 Linux 系统可以使用 AD 中的用户和组信息,Kerberos 组件用于实现身份认证,确保用户在访问 Linux 系统时能够通过 AD 身份验证。CP-ABE(Ciphertext-Policy Attribute-Based Encryption)技术用来配置访问控制策略,以确保只有经过授权的用户可以访问特定的云存储资源。③Linux 系统上的 iSCSI 组件用于将云存储系统挂载到本地系统中,使得用户可以通过本地系统访问云存储资源。quota 工具用于为 AD 用户分配可用空间,确保用户使用云存储系统时不会超出配额限制。

最终,AD 账户用户只需在访问页面输入服务器网址,即可通过单点登录方式访问到云存储系统,实现了异构系统的身份认证和访问控制。

2.2　实现策略

(1)SAMBA 服务器配置及 Winbind 映射。

SAMBA 的主配置文件中,指定 Samba 服务器的安全模式,即使用 Active Directory 身份验证服务,将允许访问 Samba 服务器的主机 IP 地址范围定义为 AD 域内 IP 地址,将采用 Winbind 组件 Samba 用户映射到 Linux 系统用户,核心代码如下:

```
[global]
        workgroup = GOOD
        server string = Samba Server Version %v
        netbios name = smb3
        interfaces = lo ens33
        hosts allow = 192.168.40.0/24
        bind interfaces only = yes
        log level = 3
        syslog = 3
        log file = /var/log/samba/%m.log
        max log size = 50
        security = ADS
        realm = GOOD.COM
        username map = /etc/samba/smbusers
        ldap ssl = off
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        winbind separator = /
        idmap backend = tdb
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
```

(2)Kerberos 身份认证。

Kerberos 组件是一个用于实现网络身份认证的重要组件,它在配置文件中包含了多个部分,用于指定各种参数和选项,以确保系统能够正确进行认证和授权操作。在配置文件中,通常包含以下几个重要部分:[logging]:指定了日志文件的路径和级别,用于记录 Kerberos 组件的运行日志,帮助诊断和调试问题。[libdefaults]:指定了默认的参数和选项,包括默认领域、是否通过 DNS 查找领域和 KDC 的信息、票据有效期等。它可以确保系统在缺少特定配置时能够有一个合理的默认行为。[REALM]:定义了默认域的配置信息,包括 Kerberos 服务器(KDC)和管理员服务器的位置,以及默认的域名。这些信息对于 Kerberos 组件的正常运行至关重要。[domain_realm]:指定了域名到领域的映射关系,帮助 Kerberos 组件确定应该向哪个领域发送认证请求。[appdefaults]:包含了特定应用程序的配置选项,例如 PAM(Pluggable Authentication Modules)等。通过配置这些选项,可以确保 Kerberos 认证以 AD 域环境进行集成和交互。核心代码如下:

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
default_realm = GOOD.COM
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
forwardable = true
GOOD.COM = {
        kdc = DC2.good.com:88
        admin_server = DC2.good.com:749
```

```
        default_domain = good.com
    }
[domain_realm]
  .good.com = good.com
   good.com = good.com
[appdefaults]
   pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = tr
        krb4_convert = false
    }
```

(3)iSCSI 组件与 SAMBA 服务器挂载。

将远程云服务器上的存储空间通过网络连接挂载到 Linux 中,并通过 SAMBA 服务器将其共享给 Windows 或其他操作系统的用户,使其在本地计算机上表现为一个本地磁盘或文件系统,并且允许用户在本地计算机上对云服务器上的文件进行读写操作,无需额外的复杂操作,这种方式可以为云存储异构系统访问控制提供便利。

(4)CP-ABE 加密访问控制。

采用 libbswabe 中的 cpabe 库实现云服务器中文件的访问控制和加密,首先生成公钥文件 pub_key 和主密钥文件 master_key,再根据指定的属性生成私钥文件 kevin_priv_key,利用公钥对文件进行加密,最后进行解密,解密后的文件可以保存到指定目录中。核心代码如下:

```
(myenv)[root@linux ~]#cpabe-setup
(myenv)[root@linux ~]#cpabe-keygen -o kevin_priv_key pub_key master_key "finance"
(myenv)[root@linux ~]#cpabe-enc pub_key /home/GOOD/finance/finance 'finance'
```

3 实验分析

实验环境为一台 CentOS Linux release 7.9.2009 (Core)系统的服务器,内核版本为 3.10.0-1160.102.1.el7.x86_64,处理器为 12th Gen Intel(R) Core(TM) i5-1240P。在实验中,建立了一个包括 Windows Server 和 Linux 两个操作系统的环境。在 Windows Server 端,构建了一个 Active Directory(AD)域服务器,用于管理和验证用户身份。在 Linux 端,配置了 SAMBA 服务器,实现了文件共享功能,通过 Winbind 组件将 AD 域中的用户和组映射到 Linux 系统中,使用 kerberos 组件建立了认证机制,确保安全通信和身份验证。通过 iSCSI 组件,将云服务器上的数据挂载到 Linux 系统上,方便进行访问和管理,quota 工具对用户磁盘配额,最后,CP-ABE 基于 cpabe 库实现对文件的访问控制和加密,以确保数据的安全性和隐私保护。该文模拟公司人事系统进行实验,公司活动目录如表 1 所示。

表 1 活动目录

部门	AD 组名	AD 用户名
服务器部	-	dc2
网络共享部	joiners	smb1
		smb2
财务部	finance	pc1
		pc3
人力资源部	hr	pc2
生产部	production	pc4
法务部	legal	pc5
销售部	sales	pc6

3.1 系统测试

查看 AD 活动目录的映射情况,所有 AD 用户和组都会映射到 Linux 系统中,如图 4 所示。

```
(base) [root@linux ~]# wbinfo -u
administrator
guest
krbtgt
dc1
dc2
smb1
pc1
pc2
pc3
pc4
smb2
pc5
pc6
(base) [root@linux ~]# wbinfo -g
enterprise read-only domain controllers
domain admins
domain users
domain guests
domain computers
domain controllers
schema admins
enterprise admins
group policy creator owners
read-only domain controllers
cloneable domain controllers
protected users
dnsupdateproxy
joiners
finance
hr
legal
production
sales
```

图 4 AD 活动目录映射图

查看 CP-ABE 加密情况,加密标志是一个后缀为 cpabe 的文件显示在加密文件所在目录中,如图 5 所示。

```
(myenv) [root@linux ~]# cd /home/GOOD/
(myenv) [root@linux GOOD]# ls
administrator  ARIMA  decrypted_file.txt  legal       pc1  pc4  priv_key    public  smb2
aquota.group   dc1    finance             lost+found  pc2  pc5  production  sales
aquota.user    dc2    hr                  master_key  pc3  pc6  pub_key     smb1
(myenv) [root@linux GOOD]# cpabe-enc pub_key /home/GOOD/finance/finance 'finance'
(myenv) [root@linux GOOD]# ls finance/
finance  finance.cpabe  public-finance
```

图 5　CP-ABE 加密成功图

3.2　系统实现

3.2.1　单点登录功能展示

在 Windows 端输入 AD 用户名和密码访问云存储系统,如图 6 所示。

图 6　访问界面图

账户验证通过后云存储设备以磁盘形式显示,并且每个用户对磁盘空间的使用都有不同的容量限制,如果超出则无法创建文件,如图 7 所示。

图 7　用户磁盘限额图

3.2.2　访问控制与加密功能展示

对于云服务器内文件,满足访问控制策略即可自动解密并访问,否则无法访问加密文件。以登录用户 pc1 为例,双击 pc1 文件夹,用户 pc1 有权访问并解密的 pc1 文件夹,如图 8 所示。

返回,双击 pc3 文件夹,用户 pc1 无权限访问加密文件 pc3,如图 9 所示。

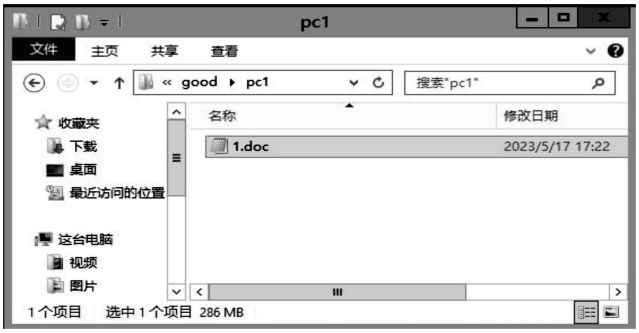

图 8　用户有权访问文件夹图

图 9　用户无权访问文件夹图

4 结束语

该文提出一种基于 SAMBA 和 CP-ABE 的云存储异构系统访问控制方法,解决了 AD 账户无法单点登录云服务器的问题。相较于现有方法,该方法通过在 Linux 上配置 SAMBA 本地服务器完成身份认证,系统响应速度不受第三方认证服务器影响,而且防止了信息被第三方泄露。同时结合 CP-ABE 技术对重要文件进行加密保护,进一步保证了云存储数据在共享过程中的安全性,在混合云环境中取得了良好的效果。实验结果表明,该方法有效解决了云服务器不支持 AD 账户单点登录的问题,提高了系统的安全性和灵活性。未来,将进一步优化系统性能,并探索将该方法应用于更广泛的实际工程场景中。

参考文献:

[1] 李 乔,郑 啸. 云计算研究现状综述[J]. 计算机科学,2011,38(4):32-37.

[2] 汤永利,李 英,赵宗渠,等. 格上可追溯的匿名单点登录方案[J]. 计算机研究与发展,2023,60(6):1417-1430.

[3] 张 锋,郭杰峰,高 原. 基于 AD 和 CA 的统一认证方案在医院的实现[J]. 中国卫生信息管理杂志,2019,16(2):214-217.

[4] FANG L,YIN L H,GUO Y C,et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers,2017,40(7):1680-1698.

[5] 李唯冠,赵逢禹. 带属性策略的 RBAC 权限访问控制模型[J]. 小型微型计算机系统,2013,34(2):328-331.

[6] 丁 滟,王 鹏,王 闯,等. 基于属性的操作系统动态强制访问控制机制[J]. 计算机工程与科学,2023,45(10):1770-1778.

[7] VEHNIÄ V J. Implementing azure active directory integration with an existing cloud service[D]. Vaasa:University of Vaasa,2020.

[8] 杨 斌. 智慧农垦统一身份认证平台设计与规划[J]. 数字技术与应用,2022,40(7):209-211.

[9] 纪健全,姚英英,常晓林. 基于 OpenID Connect 的工业互联网平台认证与授权方案[J]. 网络空间安全,2020,11(7):15-22.

[10] 陆志刚,王 杰,魏 峻. 基于 SAML 的真单点登录框架[J]. 计算机系统应用,2016,25(2):52-57.

[11] VAZQUEZ A,VAZQUEZ A. Practical LPIC-3 300:prepare for the highest level professional linux certification[M]. Berkeley:Apress,2019:381-394.

[12] 冯志华,张宇轩,卢文涛,等. 基于 PUF 的 Kerberos 认证协议[J]. 计算机工程与设计,2022,43(11):3045-3050.

[13] JEMEL M,SERHROUCHNI A. Decentralized access control mechanism with temporal dimension based on blockchain[C]//2017 IEEE 14th international conference on e-business engineering (ICEBE). Shanghai:IEEE,2017:177-182.

[14] 黄 穗,陈丽炜,范冰冰. 基于 CP-ABE 和区块链的数据安全共享方法[J]. 计算机系统应用,2019,28(11):79-86.

[15] 芦效峰,付淞兵. 属性基加密和区块链结合的可信数据访问控制方案[J]. 信息网络安全,2021,21(3):7-14.

[16] LIN L,XU J,YUAN J,et al. Compressive strength and elastic modulus of RBAC:an analysis of existing data and an artificial intelligence based prediction[J]. Case Studies in Construction Materials,2023,18:e02184.