文章编号:1671-4598(2019)08-0276-05 DOI:10.16526/j.cnki.11—4762/tp.2019.08.058 中图分类号:TP309 文献标识码:A

云计算中跨域安全认证的关键技术研究

梁 爽[1,2]
(1. 沈阳工学院 教学管理部，辽宁 抚顺 113122；
2. 沈阳工学院 辽宁省数控机床信息物理融合与智能制造重点实验室，辽宁 抚顺 113122)

摘要：针对云计算环境中的数据访问，不仅要确保合法用户能快速访问到数据资源，而且要保证非法用户的访问权限受限，合理解决信任域内部的威胁以解决云计算技术带来的数据安全等问题，提出了一种能有效实现数据跨域访问的CDSSM模型，通过设置代理者Agent，首先区分首次跨域安全身份认证和重复跨域安全认证，巧妙优化了数据跨域安全身份认证的流程，然后通过充分利用身份认证中消息加密的密钥，将数据分块加密存储，最后有效地解决了域内的安全威胁，保证了用户数据的安全性；最后，笔者实现了CDSSM模型，实验表明本方案中的密钥不可伪造，可有效避免重放攻击，重复跨域身份认证的效率在50%以上，100 MB以下文件的读写性能较好，大大提高了数据存储在云端的可靠性和安全认证的有效性。

关键词：云计算；安全；身份认证；数据存储；跨域

Research on Key Technologies of Cross—domain Secure Storage in Cloud Environment

Liang Shuang[1,2]
(1. Departemnt of Teaching Management, Shenyang Technology College, Fushun 113122, China;
2. Liaoning Provincial Key Laboratory of Information Machine Physics Fusion and Intelligent Manufacturing for CNC Machine Tools, Fushun 113122, China)

Abstract: For the data access in the cloud computing environment, it not only assure the legitimate users can access the data resources quickly, but also assure the access rights of the illegal users are limited, and the threats inside the trust domain are reasonably solved. The security issues have been solved brought by the cloud computing technology. CDSSM model that can effectively implement cross—domain data access is proposed. By setting up the agent, the first cross—domain security identity authentication and repeated cross—domain security authentication are distinguished first, and the cross—domain security identity authentication of data is skillfully optimized. And then the key of the message encryption in the identity authentication was utilized to encrypts and stores the data block. And finally the security threat in the domain was solved, the security of the user data was ensured. Finally, the CDSSM model has been implemented, and Experiments has shown the key in this scheme cannot be forged, replay attacks can be effectively avoided. The efficiency of repeating cross—domain identity authentication is more than 50%, and the read/write performance of files below 100 MB is better. It has improved the reliability of data storage and the effectiveness of security certification in the cloud.

Keywords: cloud computing; security; ID identification; data storage; cross domain

0 引言

云计算因其强大的计算能力和能为各类用户提供海量数据的存储能力而存在，其最大的魅力就是可以确保不同位置的用户可以访问任意服务器的资源[1]。一方面，不同信任域的用户需要互相访问其他信任域的资源，另一方面，来自同一信任域的内部威胁也造成了对相关数据的滥用[2-3]。因此，不仅要实现用户在不降低访问效率的前提下可以简单的跨域认证，而且要有效阻止数据的内部攻击[4]。

收稿日期:2019-01-16； **修回日期**:2019-02-27。
基金项目:国家自然科学基金资助项目(61603262)。
作者简介:梁 爽(1976-),女,辽宁锦州人,硕士,副教授,主要从事信息安全、大数据方向的研究。

1 相关工作

1.1 公钥基础设施

一个公钥基础设施基本系统的组成及结构如图1所示。

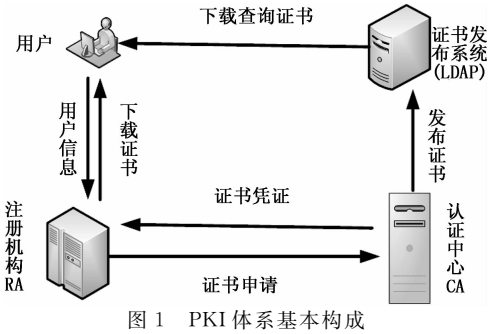

图1 PKI体系基本构成

一个简单的PKI系统包括认证中心（Certificate, CA Authority)、注册机构（register authority, RA）和证书发布系统。认证中心CA是公钥基础设施（Public Key Infrat-

ructure）信任的基础，他管理公钥的整个生命周期，包括证书的发放、规定证书的有效期和确定证书废除列表等[5]。注册机构 RA 是用户和 CA 之间的接口，他接受用户注册申请，审查用户资格，并决定是否同意 CA 为其签发证书[5]，但其并不为用户签发证书，证书签发的工作由 CA 来完成。证书发布系统主要通过目录服务或用户自己负责证书的发放，用户可以通过证书发布系统下载、查询其数字证书[6-7]。

本文中的 CA 中心还负责本信任域的 PKI 策略，授权代理服务器实现与其他信任域的认证中心的交叉认证。

1.2　跨域身份认证

随着云计算技术的不断成熟，云资源环境的不断优化，跨域身份认证的研究正逐渐成为专家学者研究的重点[8-9]。

目前，用户名＋口令的认证方式被大部分云计算平台采用，不过，这种方式安全度低，容易被监听和截取，而且用户往往会根据自己的习惯，多平台同账号＋密码的情况，用户身份信息非常容易泄露，给用户造成不可挽回的损失。

PKI 因其具有网络安全基础好，开放性强，身份认证保密性好，能保证身份的唯一性，能兼顾网络参与者各个主体的公共安全利益等优势，已经成为目前保障网络安全的最佳体系，并且广泛应用于电子商务、网上银行等需要较高安全级别的领域。现有的基于 PKI 的跨域身份认证主要存在扩展性差、灵活度低、互操作弱、证书验证繁杂等缺陷，若直接应用于云计算恐难胜任。

本文提出的跨域安全认证技术设置签名代理服务器，并优化认证流程，采用“密钥＋口令”的双因子认证形式，有效解决了现有的基于 PKI 的身份认证技术认证路径复杂、证书效率低等问题，可以实现用户和云服务提供商之间的双向身份认证，从而提高了跨域身份认证系统的认证过程的安全性；简化了信任路径复杂程度，减少了路径长度。

1.3　安全假设

本文的安全假设如下：本模型中的数据使用用户的可便携设备是可信的；存储服务器服务器是不可信的，且访问本存储服务器的用户数据可能会通过存储服务器被窃取；认证服务器和代理服务器是可信的，且认证中心和代理者之间的通信信道是安全的；数据传输信道有可能被攻击而泄漏数据。

2　跨域安全存储模型

2.1　框架设计

本文通过在云计算服务平台中设置签名代理服务器，将 PKI 技术与签名代理技术有效结合，提出了一种跨域安全存储模型（cross domain security storage model，CDSSM）。当有一个其他域用户想要访问本地域资源时，本地服务器与证书代理服务器联系，把异域的数字证书颁发给使用者，转换成本地可信任的临时新证书，用以确认用户身份是否合法，从而可以实现不同信任域间用户的互访。每个拥有合法数字证书的域间云用户和证书代理服务器，都可以实现域间云数据资源的访问，大大提高了验证效率。云数据资源在存储时可以采用私钥加密，待用户申请访问资源时，提供公钥解密，从而可以有效阻止域内用户攻击，提高云平台数据的安全性。为了更好的描述本模型设计，给出如下术语的定义。

定义 1　用户 User：利用任何可信的安全的便携式设备访问云服务资源，并能够与云服务资源提供者完成域内和跨域的身份认证[10]。便携式设备能确保安全且认证正确，可以通过数字证书的合法性来鉴别其身份是否真实，并能够利用证书获取对方的正确公钥[10]。

定义 2　云数据存储服务器 Server：为用户提供各类云存储服务，并能确保安全地进行证书、密钥等敏感数据的存储、加密和数字签名。

定义 3　认证中心 CA：负责其本信任域内数字证书的申请、审批、颁发、撤销、查询、管理等[10]。

定义 4　证书代理服务器 Agent：拥有域间数字签名的密钥，能够将一个信任域内的合法数字证书转换为转换为另一个信任域内的临时合法数字证书，建立域间信任关系，协助实现不同信任域间的用户的认证工作[10]。

跨域安全存储模型 CDSSM 模型的基本框架如图 2 所示。

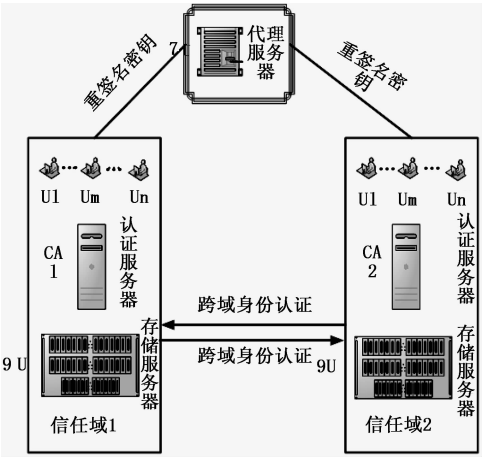

图 2　CDSSM 模型框架

为后续描述方便，本文以两个信任域一个中间代理服务器为例，分析其安全认证和存储访问过程。假设信任域 1 和信任域 2 分别为本模型的 2 个信任域，每个信任域中均存在用户集 $\{U_1, U_2, \cdots, U_n\}$，每个信任域中也存在多台存储服务器 $\{Server_1, Server2, \cdots, Servern\}$。$CA_1$ 是信任域 1 的认证中心，CA2 是信任域 2 的认证中心。下文描述的过程选择信任域 1 中的用户 U_1 和信任域 2 中的存储服务器 Server2 作为典型代表，以 U_1 访问 Server2 的跨域资源为例，说明如何通过双方持有的数字证书完成身份认证以及数据存取。

2.2 模型工作方式

本文提出的安全存储模型 CDSSM 在形式上可分为两个部分，即系统存储管理模块和系统安全认证管理模块。系统存储管理模块包括（$Server_1$，$Server_2$，…，$Server_n$），系统安全认证管理模块包括（CA1，CA2，……，Cam，A-gent），多用户集合为 $U=\{u_1, u_2, \cdots, u_p\}$，数据文件集合为 $F=\{f_1, f_2, \cdots, f_q\}$。CDSSM 的工作方式按照存储管理和安全认证管理的工作方式描述如下。

2.1.1 安全认证管理工作方式

1）CDSSM 认证的前期准备工作

用 ID1 表示信任域 1 中用户 U1 的真实身份标识，用 TID1 表示信任域 1 中用户 U1 的临时身份标识。用 ID2 表示信任域 2 中资源服务器的真实身份标识，用 TID2 表示信任域 2 中资源服务器的临时身份标识。用 CA1 表示信任域 1 中的认证中心，用 CA2 表示信任域 2 中的认证中心。IDA 表示代理者 Agent 的身份标识。

CDSSM 系统建立之初，代理者 Agent 需要根据指定的签名算法，生成认证中心 CA1 和 CA2 之间的重签名密钥。

2）证书的申请

用户 U1 向其所在的认证中心 CA 申请认证证书的过程如图 3 所示。

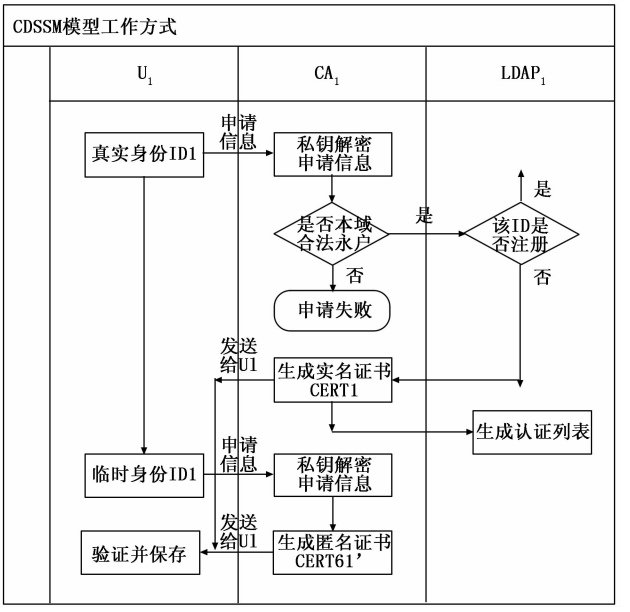

图 3 CDSSM 模型的证书申请

①用户 U1 利用真实身份 ID1 计算临时身份 TID1，向本信任域内认证中心 CA1 发送包含 CA1 根证书、时间戳和其公钥信息的证书申请信息给 CA1。

②CA1 用私钥解密 U1 发送的申请信息，首先根据 ID1 等相关信息验证 U1 是否为本信任域内的合法用户[10]，然后在 LDAP 中的认证列表中查询该 ID 是否注册，并通过临时身份验证其时间戳的有效性。如果上述验证过程未通过，CA1 返回用户 U1 申请失败的消息；否则验证通过，CA1 利用 ID1 等身份信息生成实名证书 Cert1，并同时返回给用户 U1 和发送到轻量目录访问协议（Lightweight Directory Access Protocol，LDAP）加入到认证列表中，CA1 利用包含时间戳信息的 TID1 生成匿名证书 Cert1’发送给 U1，为了保证该匿名证书有效性，可以设置该匿名证书 Cert1’有效期比较短。

③用户 U1 通过私钥解密收到的信息，验证 Cert1 和 Cert1’的合法性，若合法，则接受证书并存储在用户端，否则，拒绝接受该证书。

资源服务器 Server2 向所属的认证中心 CA 申请认证证书的过程与上述过程类似，可获得 CA2 签发的实名证书 Cert2 和匿名证书 Cert2’。

3）首次跨域认证

位于信任域 1 中的用户 U1 试图访问位于信任域 2 中的资源服务器 Server2 中文件 f_n，其首次访问身份认证过程如图 4 所示。

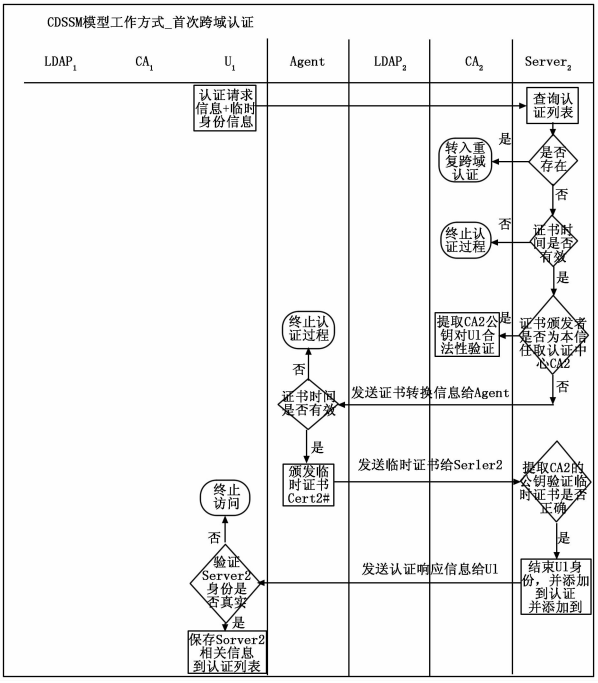

图 4 CDSSM 模型的首次跨域认证

①用户 U1 发送包含其临时身份、密码等信息的认证请求信息和身份证书 Cert1 经加密后发送给资源服务器 Server2。

②Server2 收到 U1 的认证请求后，首先在认证控制列表（certificate control list，CCL）中查询是否存在 TID1 的相关信息，如果存在，说明 U1 合法，直接进入步骤 4）后续跨域认证；若不存在，开始下列验证过程。

步骤一，检查证书 Cert1 的时间有效性，若失效，则终止认证过程；否则转入步骤二。

步骤二，检查证书的颁发者是否为本信任域的证书中心 CA2，如果是，说明用户和服务资源提供者属于同一信

任域，则直接提取 CA2 的公钥对证书 Cert1 进行合法验证；否则转入步骤三。

步骤三，发送证书转换信息给代理者 Agent。代理者 Agent 验证时间的有效性，用 CA1 的 PK 验证证书是否合法，不合法则终止转换过程；否则，用认证中心 CA1 与 CA2 间的重签名密钥将 CA1 颁发的证书 Cert1 转换为 CA2 签发的临时证书 Cert2＃。为了区分临时证书 Cert2＃是由 Agent 签发而非 CA2，可以通过设置 Cert2＃的有效期来实现，也可以在 Cert2＃中增加 Agent 的身份标识 IDA。代理者 Agent 不能独立生成新的合法证书，也不能对已有用户证书进行修改，只能转换已有的合法证书。代理者 Agent 发送证书转换响应信息给 Server2。

步骤四，Server2 提取 CA2 的公钥验证临时转换证书 Cert2＃中签名的正确性，若正确，Server2 接受用户 U1 的身份，完成对 U1 的匿名身份认证，并将 Cert1 添加到认证列表中保存，同时发送认证响应信息给 U1。

③用户 U1 根据收到的认证响应信息，验证 Server2 身份的真实性，以确认 Server2 是否是其想要访问的资源服务器；U1 完成身份认证后，也会将 Server2 的相关身份信息和证书保存到 U1 的认证列表中。

4）后续跨域认证

当用户与资源服务器通过首次认证后，后续的认证过程将会大大简化，其基本工作方式如图 5 所示。

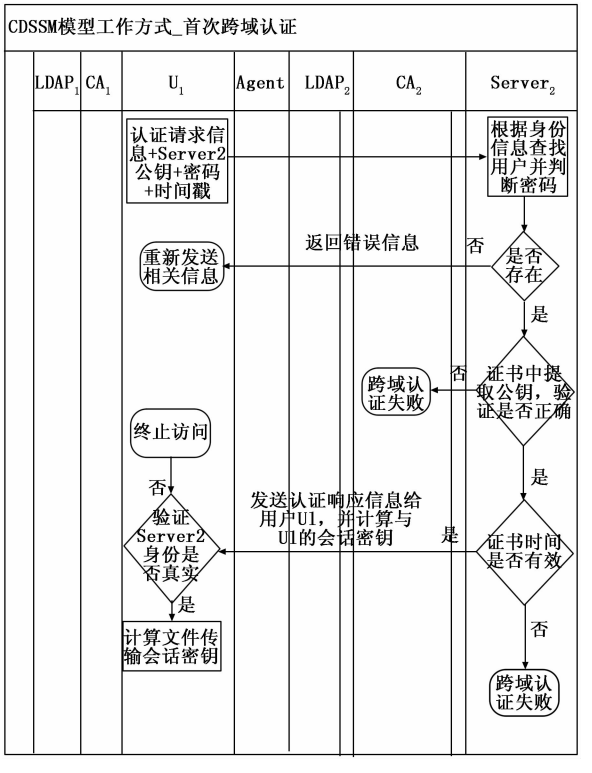

图 5　CDSSM 模型的后续跨域认证

①用户 U1 发送包含其身份信息、Server2 公钥、密码和时间戳等相关信息的认证请求信息给资源服务器 Server2。

②资源服务器 Server2 收到认证请求信息后，按照如下步骤进行身份认证。

步骤一，根据 TID1 在认证列表中查找该用户，并判断其密码是否正确，若不正确，则返回密码错误信息给用户 U1，否则，转入步骤二。

步骤二，从 U1 的证书 Cert1 中提取公钥，验证其身份的正确性，若验证不能通过，则跨域认证失败，否则，转入步骤三。

步骤三，验证存储的临时证书的有效性，若超出证书的有效时间，则认证失败，否则，认证通过。资源服务器 Server2 发送重复认证响应信息给用户 U1，并计算与用户 U1 的会话密钥。

③用户 U1 收到认证响应信息后，验证 Server2 身份的真实性，若验证通过，则 Server2 即为用户 U1 要访问的文件 fn 的资源存储服务器 Server2，同时计算文件传输过程中的会话密钥。

2.1.2　存储安全管理工作方式

通过上述方式完成用户 U1 的身份认证后，下面来介绍一下用户 U1 访问资源服务器 Server2 中文件 fn 的过程。CDSSM 模型的存储安全管理工作方式如图 6 所示。

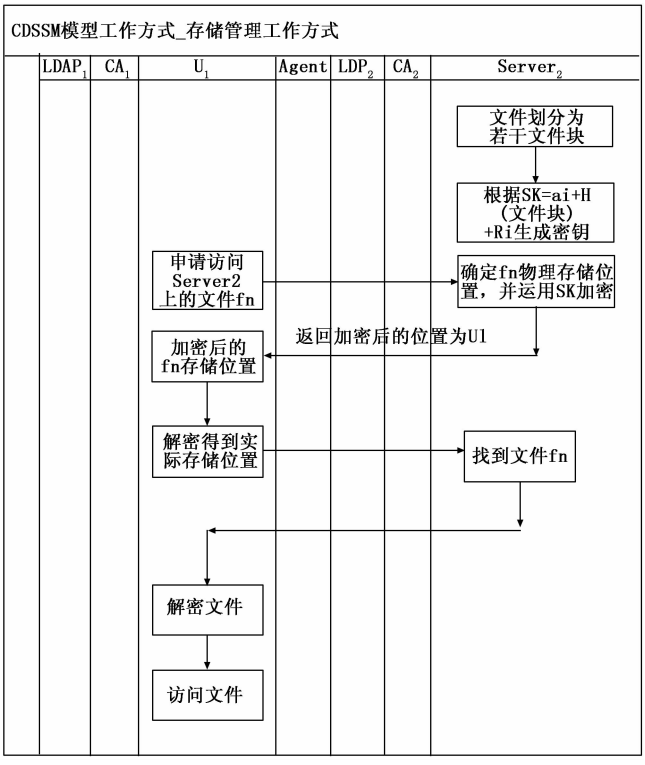

图 6　CDSSM 模型的存储管理工作方式

1）密钥更新与管理

本系统基于 PKI 技术，故密钥分为公钥和私钥。公钥是各认证中心发给相关信任域内的用户持有，凡用公钥加密的数据，均可用配套的私钥解密。在相关的密钥信息中包含时间戳，可以根据需要设置各密钥的有效期。

2）数据文件加密

对数据文件的加密可以采用收敛的加密方案[11]，即根据数据明文的某些属性生成密钥，同时对数据本身加密。可以采取如下的方案加密。首先，将数据文件分成合适的文件块，对每个文件块的加密密钥均结合明文和随机数生成。用 ai 标记该文件块是该文件的第 n 个文件块，H 是文件块的哈希函数值，Ri 为任意随机数，则密钥可表示为 SK＝ai ＋H（文件块）＋Ri。这样的密钥生成方式在保证数据保密性的同时可以校验数据的完整性，密钥会随着数据的变化而变化。

3）确定文件存放位置

合法用户 U1 查询数据文件 fn 的位置，Server2 确定 fn 的物理存储位置 Serveri，并运用 Server2 私钥对存储位置加密，将加密后的位置返回给用户 U1。

4）数据文件解密

用户接收到加密的存储位置后，用事先协商的会话密钥解密，从而得到有效的 fn 文件的存储位置。Server2 在指定存储位置取得事先加密的 fn 文件，同时发送给用户 U1。用户 U1 获得数据文件 fn 的加密数据块后，在本地进行解密计算，访问解密后的数据。

3 跨域安全存储的测试与评估

为证明 CDSSM 模型的有效性，笔者进行了系列实验，实验环境如下。存储服务器使用联想（Lenovo）IBM X3650 M5 机架服务器主机（OA/ERP 服务器）。存储服务器共 3 组，分别位于校园网的不同教学楼内，属于 PKI 的不同信任域。为方便实验，本实验方案中将 LDAP 服务器和认证中心 CA 服务器合二为一，该服务器的配置为：联想（Lenovo）IBM X3650 M5。认证代理服务器 Agent 的配置为：联想（Lenovo）IBM X3650 M5。客户端为华硕笔记本电脑。

3.1 安全性分析

由 PKI 的基础知识可知，CDSSM 模型的安全性主要在证书申请和跨域认证阶段。

3.1.1 证书申请阶段的安全性分析

给定 CA1 和 CA2 的私钥，使用文献［12］的安全通信协议为代理者 Agent 生成一个重签名密钥，由文献［12］可知，该密钥是正确的，且不可伪造。

3.1.2 跨域认证阶段的安全性分析

在跨域身份认证中，允许使用匿名身份信息进行身份验证。CDSSM 模型的验证过程中只有保证成果完成身份认证的用户才有可能进行匿名验证，而匿名证书的有效期很短，可以保证在后续跨域认证中临时身份的有效性。如果云资源服务器 Server2 收到的信息为虚假信息，Server2 会将相关信息发送给 CA1 验证其其证书 CERT1 的合法性，如果 CA1 证实该消息确实虚假，则 CA1 会将 CERT1’和 Cert1 同时加入证书撤销列表（Certificate Revoke List－CRL）中，反馈结果给资源服务器 Server2。上述分析说明，CDSSM 模型的匿名行为是可控的。

CDSSM 模型可以有效抵抗重放攻击，这是因为在身份认证和消息传递过程中，会话标识信息、随机数和时间戳等信息均有效的标识了认证与消息传递过程，如果攻击者替换认证消息中的身份标识，因为证书信息是事先保存的，故无法保证其身份信息和证书信息的完全匹配，所以无法完成认证，从而保证了本模型可以有效抵抗替换攻击。

3.2 安全性能分析与测试

从上述安全管理认证工作方式的过程可以看出，CDSSM 模型的安全性能损失主要出现在证书申请和跨域认证两个阶段。在证书申请阶段，CDSSM 模型为了安全送达用户的真实身份，对身份信息进行加密传送；为了保证 CERT 和 CERT′合法性，又对证书进行了两次签名；这一次加密和两次签名，可以充分发挥 PKI 技术的优势并有效保护用户的隐私，从而更适合于云计算的环境。在首次跨域认证阶段，Server2 与用户和 Agent 分别进行了两轮消息通信和证书转换，安全性能损耗较大，但首次跨域认证只发生一次，相比较后续跨域认证阶段节省的安全性能损耗是值得的。

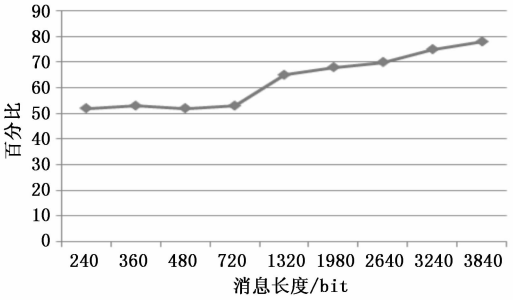

图 7 重复跨域身份认证效率与消息长度关系图

从图 7 可以看出，CDSSM 模型的重复跨域身份认证的效率均在 50％以上，当消息长度在 3 MB 左右时，认证效率接近 80％，效率很高，说明该模型用于跨域身份认证是可行的。

3.3 读写性能分析与测试

从存储管理工作方式的分析中可以看出，读写性能的损失主要集中在文件的加解密上。采用本文所述方式针对不同的文件大小所需花费的文件读写访问时间如图 8 所示。

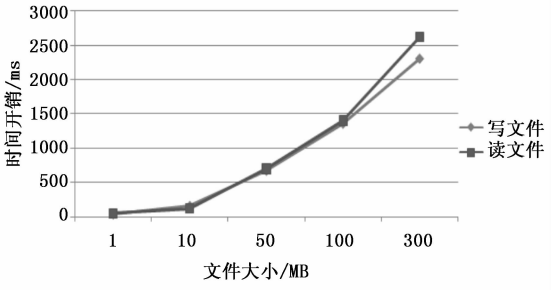

图 8 文件读写性能测试结果图

从图 8 可以看出，数据的读写性能主要跟文件的大小成正比，也就是说本文采用的数据加解密技术并未给数据

（下转第 290 页）