doi:10.3969/j.issn.1000-436x.2013.z1.003

分布式文件交互系统节点身份认证方案

何文才[1,2]，杜敏[1,2]，陈志伟[1,2]，刘培鹤[1]，韩妍妍[1]
(1. 北京电子科技学院 通信工程系，北京 100070；2. 西安电子科技大学 通信工程学院，陕西 西安 710071)

摘 要：基于分布式云存储系统利用椭圆曲线和散列函数等内容，提出了一种云环境下的双向身份认证方案，实现双向认证过程。新方案的优点在于产生对通信双方公正的会话密钥，同时设计了 2 种不同类型的认证：本地网内认证和跨网络认证。最后对该方案进行了安全性和性能分析，证明了本方案具有很强的安全性，能够保护用户的隐私性和抗抵赖性，且具有较低的计算量。该方案满足云存储在通信环境中的需求。

关键词：分布式文件系统；身份认证；云存储；双向认证
中图分类号：TP391 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0014-07

Scheme of node identify authentication in distributed file interaction system

HE Wen-cai[1,2], DU Min[1,2], CHEN Zhi-wei[1,2], LIU Pei-he[1] , HAN Yan-yan[1]
(1. Department of Telecommunications Engineering, Beijing Electronic Science & Technology Institute, Beijing 100070, China;
2. School of Telecommunications Engineering, Xidian University, Xi′an 710071, China)

Abstract: Under the mutual identity authentication, a scheme based on distributed cloud storage system was proposed, using symmetric encryption algorithm and hash function to realize bidirectional authentication process. Advantages of the novel project are to produce fair session key to both communications, and design the two different types of authentication: within the network and across a network authentication. Then the security of this scheme was analyzed. The scheme is more secure than the former ones and it can protect the privacy of users and non-repudiation, and has lower computational cost. Therefore, this scheme can meet the demand of cloud storage communication environments.

Key words: distributed file system; identify authentication; cloud storage; date interaction

1 引言

传统的分布式文件系统在存储容量和性能上存在瓶颈，云存储[1]可以提供一个巨大的存储空间，主要解决海量数据的存储问题，是一种超大规模的复杂分布式文件系统。在分布式文件系统数据交互的过程中，对节点进行身份认证是保证网络安全和管理的重要内容，是保证数据安全可靠传输的基础。

云存储是实现在线存储的一种新型存储模式，在安全云存储系统中，分布式文件交互系统是实现内部管理和对外服务的基础。大规模的数据访问时，充分利用网络中节点互相关联的特性，把用户安全认证管理和访问控制的责任分摊到多个节点上，这样就能大大降低单个节点的负担，同时也减少了通信节点间因身份认证而带来的巨大开销。

从存储系统的技术需求和发展来看，文件系统是构建云存储系统的重要部分，其优势在于可降低硬件存储设备、维护费用、灵活的应用模式以及高度自动处理过程[2,3]。无论是从安全性还是从费用支付的角度来看，用户与存储节点之间实现双向认证是必不可少的。目前针对云存储系统安全性的研究主要集中在存储安全性和传输安全性等方面，关于用户身

收稿日期：2013-07-03
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2007CB31120）；国家密码发展基金密码理论课题基金资助项目
Foundation Items: The National Basic Research Program of China (973 Program) (2007CB31120); The Cryptography Basic Development Fund of China on Cryptographic Theory

份认证的研究不是很多。身份认证是实现云服务平台安全体系的重要机制，是整个安全体系的基础，为云服务平台用户身份的真实性提供安全保证[4]。

面对云存储中复杂的应用环境，传统的基于用户名和口令的认证方式已经不能满足云存储环境中多种认证场景的安全需求。基于挑战与应答一次性口令的OTP(one-time password)认证中[5]，用户每次在向服务器发起认证的时候，所用的随机数和信息都是以明文形式传送，因此在传输过程中无法抵挡中间人的假冒攻击。OpenID[6]技术能够有效地解决上述问题，但是OpenID技术的标准认证协议中并没有认证云服务的身份，也没有对云服务请求的身份信息进行细粒度授权，会导致因身份的数据空间不同造成资源不可访问的现象[7]。基于安全确认标记语言(SAML)的单点登录方案与OpenID协议十分类似，可以灵活地设计自动发现机制[8]，但SAML只满足较少的互相信任的安全域内部署单点登录方案，很难构建一般用途的管理工具，具有一定的局限性。

针对现有方案的缺陷，为了解决分布式文件系统中用户和云服务器之间的双向认证问题，本文基于椭圆曲线离散对数问题提出了一种新的分布式交互系统中的节点身份认证模型，并建立了节点之间的双向认证关系。分析了方案的安全性，降低了通信转发过程中的复杂度。

2　分布式文件交互系统节点的身份认证模型设计

2.1　椭圆曲线加密算法

有限域 F_q 表示含有 q 个元素，且 q 为素数，$q>3$，取 $a,b\in F_q$，使得 $4a^3+27b^2\neq 0$。由参数 a,b 定义 F_q 上的椭圆曲线方程为：$y^2=x^3+ax+b(\mathrm{mod}\ p)$ 和曲线参数 $T=(q,a,b,G,n,h)$，其中，$qt\neq 1(\mathrm{mod}\ n)$，$1\leqslant t\leqslant 20$，$G$ 设为该椭圆曲线的基点；G 的阶为 n，n 为素数；h 为椭圆曲线上点个数 m 与阶 n 相除的整数部分，$h\leqslant 4$；$q\neq nh$。

椭圆曲线方程的一个无穷远点（记为 0）和所有正整数解 (x,y) 可以组成一个集合，记为 $E(F_q)$。设 $P\in E(F_q)$，若 P 周期很大，即 $P+P+\cdots+P=0$（共有 n 个 P 相加）成立的最小正整数 n 存在；若 n 不存在，则 P 为无限阶。事实上，在有限域上定义的椭圆曲线上所有点的阶 n 都存在，并且 $O\in E(F_q)$，一定存在一个正整数 m，满足 $Q=mp=P+P+\cdots+P$（共有 m 个 P 相加），可转换为 $m=\log_p Q$。

$E(F_q)$ 对点的“+”运算形成一个 Abel 群，相关它的离散对数问题是难解的，且 $Q=mp$（或 $m=\log_p Q$），其中，Q、P 为椭圆曲线在 $E(F_q)$ 上的点，m 为小于点 P 的阶。给定 m 和 P，可以计算出 Q；但给定 Q 和 P，求 m 是难解的，这是椭圆曲线加密算法的离散对数问题。

椭圆曲线加密算法的特点是不存在计算椭圆曲线有理点群的离散对数问题的指数算法，这就意味着在同等安全的前提下，椭圆曲线密码体制可以选择更小的参数，执行更快的运行速度，满足了云存储中节点间大量身份认证和密钥协商中的加解密需求。

2.2　分布式文件交互系统节点结构

作者把分布式云存储网络中的用户节点定义为 2 类：一类是用户交互数据在分布式存储的一个局域网内的节点，如服务器 A 下的用户，需要与节点 $A_1,\cdots,A_n$ 进行数据交互，此时 $A_1,\cdots,A_n$ 便称为内部节点。另一类是用户需要交互的数据在另一个服务器下的存储节点上，此类存储节点不能与用户直接通信，需要借助服务器的转发，例如，服务器 A 下的用户，需要与服务器 B 或 C 下的节点进行数据交互，此类存储节点称为外部节点。当与内部节点进行数据交互时，需要对其进行内部认证；当用户与外部节点进行数据交互时，需要对其进行外部认证。

本节首先阐述了如图 1 所示的云存储模型的密钥协商机制，再介绍内部认证和外部认证的详细步骤。

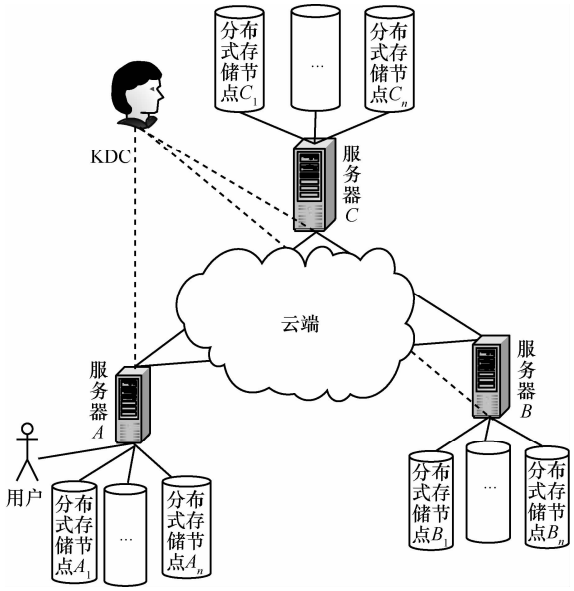

图 1　基于分布式的云存储系统模型

2.3 云存储身份认证系统初始化

在分布式的云存储系统中，作者首先建立了一个可信任的密钥分发中心 KDC(KDC, key distribution center)，用来产生并分发消息。KDC 在保证该椭圆曲线的离散对数问题是难解的情况下，选择有限域 F_q 上的一条安全椭圆曲线 $E(F_q)$。在 $E(F_q)$ 上选取一个基点 P，且保证 P 的阶数为一个大素数。KDC 产生一随机数 $s(s \in F_q)$ 作为其私钥，然后计算得到其公钥 $S_{\mathrm{KDC}} = sP$，其中，运算“·”为点乘。KDC 还负责为云存储系统中的节点和用户产生 ID 信息，且为每个存储节点和用户分发身份 $ID, ID \in \mathrm{GF}(q)$。

不失一般性，假设密钥分发中心 KDC 为了分发私钥给一个标识为 ID_{A_1} 的存储节点 A_1（A_1 为存储节点或需要进行数据请求的用户），KDC 首先计算关于存储节点 A_1 的签名参数：$R_{A_1} = r_{A_1} P$（随机选取 r_{A_1}）；$s_{A_1} = s \cdot h(ID_{A_1} \| R_{A_1}.x) + r_{A_1}$（其中，$h(\cdot)$为散列函数，$R_{A_1}.x$ 为椭圆曲线的上的点 R_{A_1} 在 x 轴的坐标值，$\|$为字符连接符）。其中，s_{A_1} 为云存储节点 A_1 的私钥，公钥为 $S_{A_1} = s_{A_1} P$。为了与其他节点或用户建立对等密钥（pairwise key），存储节点 A_1 需要存储参数（KDC 的公钥 S_{KDC}、自身的签名参数、R_{A_1}、s_{A_1}、身份标识 ID_{A_1}）。

通过上述系统初始化后，系统中的存储节点就建立了和用户对等的密钥。如果云存储系统中的用户 User 与存储节点 A_1 需要建立协商密钥，它们只需要交换对方的标识 ID 和签名参数即可。会话的另一方可以通过广播的方式来获得 ID 和签名参数。用户 User 和存储节点 A_1 可以通过下述协议分别来计算共享的对等密钥 K_{U,A_1}。

用户 User

广播：ID_U 和 R_U

计算：1) $S_{A_1} = h(ID_{A_1} \| R_{A_1}.x) \cdot S_{\mathrm{KDC}} + R_{A_1}$；

2) $K_{U,A_1} = s_U S_{A_1} = s_U s_{A_1} P$。

云存储节点 A_1

广播：ID_{A_1} 和 R_{A_1}

计算：1) $S_U = h(ID_U \| R_U.x) \cdot S_{\mathrm{KDC}} + R_U$；

2) $K_{U,A_1} = s_{A_1} S_U = s_{A_1} s_U P$。

本文采用的密钥协商机制不像其他密钥协商方式需要另外的授权中心 CA（certification authority）来帮助验证生成密钥的真伪，而是采取非显式的方式，所以，只有用密钥来进行加解密数据，或采用生成 MAC 校验码来辨别密钥的真伪[9]。这种方法大大简化了系统的结构，降低了计算和通信的复杂性。

3 身份认证协议实现方案

3.1 双向的本地网内身份认证协议

在云存储系统中，比较常见的数据交互模式是本地网络内的数据交互，这时用户和节点间不必进行太复杂的身份认证，因为复杂的身份认证协议在本地网络内会造成信息流的拥塞，同时也是得不偿失的。当某一云存储用户要与本地网络存储节点进行通信时，由于用户是新加入的节点，所以它只能在本地局域网内进行通信。为了在局域网内实现存储节点对用户节点的认证，用户 User 向 KDC 发送身份认证所必需信息的请求，包括身份标识、公私钥等。KDC 为新加入节点产生标识 $ID_{\mathrm{User}} \in \mathrm{GF}(q)$，并计算用户的签名参数：$R_{\mathrm{User}} = r_{\mathrm{User}} P$（$r_{\mathrm{User}}$ 是随机选取的），那么，用户的私钥为：$s_{\mathrm{User}} = s \cdot h(ID_{\mathrm{User}} \| R_{\mathrm{User}}.x) + r_{\mathrm{User}}$。$s_{\mathrm{User}}$ 即为标识为 ID_{User} 用户的私钥，其相应的公钥为 $S_{\mathrm{User}} = s_{\mathrm{User}} P$。

用 A_i 表示本地网络内部的一个存储节点，User 表示数据请求用户，本地认证过程如图 2 所示。

Step1 用户 User 首先生成一个绑定时间戳的随机数 $r_{\mathrm{User}} \| time$，计算 $MAC_{\mathrm{User}} = Encry(K_{\mathrm{User},i}, r_{\mathrm{User}} \| time)$，（例如用 3DES 算法加密）并向需要进行数据请求的本地云存储节点发送认证请求 Request 和 MAC_{User}，同时把验证需要的信息 ID_{User} 和 R_{User} 发送给需要进行通信的节点 A_i。

Step2 收到用户 User 的认证请求后，节点 A_i 也产生一个绑定时戳的随机数 $r_i \| time$，然后，存储节点 A_i 利用它和用户的对等密钥 K_{User,A_i} 加密随机数 $r_i \| time$，计算 $r' = Decrypt(K_{\mathrm{User},i}, MAC_{\mathrm{User}})$。

最后，数据存储节点 A_i 发送自己的相关信息 r' 以及校验码 MAC_i 给用户 User。

Step3 收到校验码 MAC_i，用户 User 验证 r' 和 $r_{\mathrm{User}} \| time$ 是否相等，若不相等则认证失败；若相等则用户对存储节点的身份认证成功，解密得到 $r = Decrypt(K_{\mathrm{User},i}, MAC_i)$，并发送 r 给存储节点 A_i。

Step4 存储节点 A_i 验证所收到的 r 是否和 $r_{\mathrm{User}} \| time$ 相等，相等则表示存储节点对用户的身份认证通过；否则，表明认证失败。

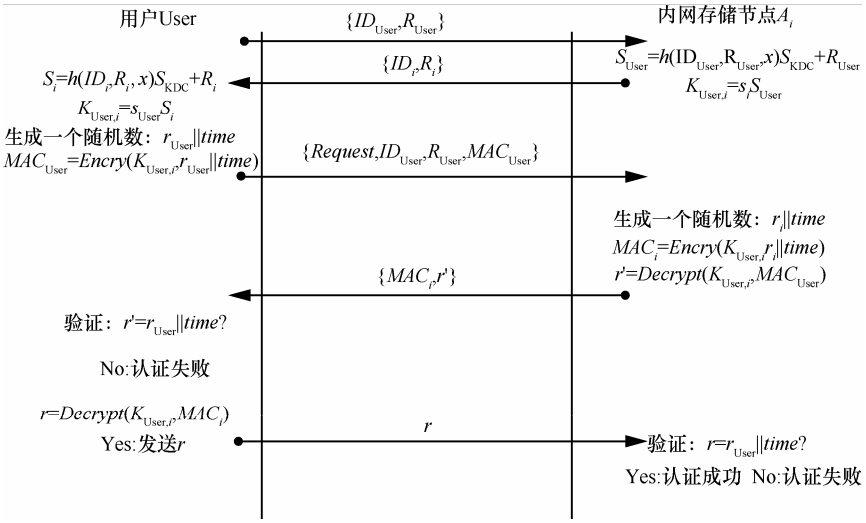

图 2　局域网用户与存储器节点之间的认证协议

当用户和存储节点之间成功验证后，云存储网络则为可信的，同时用户也是合法的。至此，达到用户和存储节点之间双向认证的目的。

3.2　双向的跨网络身份认证协议

如果 2 个不同局域网下的文件系统存储节点要进行通信，则网外的存储节点需要对要求数据请求的用户进行认证。在跨局域网认证时，用户不能直接和局域网外的数据存储节点进行通信，需要通过其他服务器多跳转发，数据才能到达远端节点。正是由于这种特殊的通信模式，跨局域网的身份认证不能直接套用局域网内的认证方式。在跨局域网络内，本方案对用户进行认证采用本地局域网内对节点签注的方式：即首先利用局域网内节点对用户进行认证，如果用户没有通过局域网内某一存储节点的认证，则本地服务器就会拒绝为该用户进行真签注，而对其进行伪签注，然后将伪签注值发送给用户。反之，则表示局域网内存储节点信任该用户，然后由局域网内的节点为用户产生一个真签注，并将真签注信息发送给用户。用户收集到局域网内的 k 个这样的签注后，发送给局域网外的节点，如果局域网外存储节点重建这 k 个签注，其中全部匹配正确，则表明跨局网认证通过，反之，则认证失败。由于可能存在一些恶意的数据请求用户，所以不能根据局域网内的某一个数据存储节点来进行判断，要把问题用户的通信范围限制在局域网内，这就是为什么需要 k 个这样的签注最终进行联合验签的原因。通过提高认证阈值 k（原始本地网内认证可以看作 k=1 的认证方式），保证了分布式文件系统跨网络认证的安全性。

跨局域网认证的具体过程可以描述如下。

用 $A_1,\cdots,A_s$ 来表示能和用户 U 直接通信的局域网内节点，ID_{Extranet} 为需要对用户进行认证的局域网外某一存储节点的标识。

Step1　用户向局域网内的节点广播跨网络身份认证请求 $ERequest(Extranet\ Request)$。然后，用户产生随机数 r_1，并绑定时间戳 $r_1 \| time$，将 $r_1 \| time$ 连同其他信息 ID_U 和 ID_{Extranet} 组成：$\{ID_{\text{User}},ID_{\text{Extranet}},r_1 \| time,ERequest\}$，将其广播给局域网内的节点。

Step2　收到用户跨网络身份认证请求 $ERequest$ 的一个局域网内节点（比如图 1 所示的节点 A_i），首先对用户按照上述的局域网内认证方案进行局域网内认证步骤，如果局域网内认证失败，则局域网内的节点认为这是一个不合法用户，并拒绝为该用户用自身与网外节点 ID_{Extranet} 的密钥进行真签注，而为其产生一个伪签注 $Trust_{\text{error}}$ 发送给用户。

如果此用户通过本地认证，则该局域网内的节点开始计算其自己和网外节点 ID_{Extranet} 的对等密钥 $Key_{i,\text{Extranet}}$，然后用此密钥对 $r_1 \| time$ 加密得到 $Trust_i$ 并发送给用户，称 $Trust_i$ 为本地节点 A_i 对该用户的一个签注，也是真签注。

Step3　当用户收集到系统设定的 k 个这样的签注后，对这些签注进行散列计算，得到的散列值连同产生这些签注的本地节点标识 $ID_1,\cdots,ID_k$ 一起发送给外网节点 ID_{Extranet}；其次，用户再生成一个随机数 r_2，并为自己进行签注，用于对外网存储节点的身份认证：$Trust_{\text{User}}=Encry(K_{\text{User,Extranet}},r_2 \| time)$，也将其发

送给外网节点 ID_{Extranet} 。

Step4 外网节点可以利用这些信息重建散列值 mac'，若 $mac' = mac$，则表示外网节点对用户的身份认证通过；若 $mac' \neq mac$，则此次外网节点对用户的身份认证失败。

Step5 外网节点恢复出用户自身的签注值 T 之后，返回给用户。然后，用户比较 T 与 $r_2 \| time$ 是否相等，若相等，此次身份认证成功；否则，认证失败。

为了形象地说明上述步骤，协议的交互过程可以描述如图 3 所示。

4 性能和安全性分析

4.1 安全性分析

基于椭圆曲线加密体制。本文方案提出了云存储环境中用户和存储节点之间的双向认证。在满足网络数据通信安全与隐秘的条件下，能够保证该方案的有效性和强安全性。

定理1 如果求解椭圆曲线离散对数困难问题成立，则跨网络身份认证协议满足不可区分性。

证明 在证明中，敌手能够正确地猜测*Test*查询中的$r_i \| time$事件为S_k。证明需要使用一系列的游戏，首先是从一个描述真实攻击的游戏开始，直至敌手的概率优势为0时，游戏结束。每个游戏描述一个不同的方面，游戏 G_0 是一个在随机预言机和理想密码模型中的真实协议。在游戏 G_1 中，通过维护列表 Λ_{mac} 、 Λ_{Trust_1} 、 Λ_{Trust_2} 、 Λ_{Trust_3} 、 $\Lambda_{Trust_\varepsilon}$ 、 Λ_{ε} 和 Λ_D 来模拟散列预言机 (mac) 和理想加解密预言机 $(\varepsilon, D, Trust_1, Trust_2, Trust_3, Trust_\varepsilon)$ 。另外，*Execute*、*Reveal*、*Send*、*Test*和*Corrupt*预言机在该游戏中按照真实攻击者进行模拟。在游戏 G_2 中，需要注意的是，在 $(\varepsilon, D, Trust_1, Trust_2, Trust_3, Trust_\varepsilon)$ 和 mac 中碰撞发生的概率，敌手在 G_2 游戏中的优势是，通过生日悖论来计算。在游戏 G_3 中，用随机数 $r_i \| time$ 、 $r_i \| time$ 来替换临时密钥 r_i ，即 $A(A_i)$ 的签名使用时间戳来区分每一次的 r_i 。敌手区分 mac 和 $r_i \| time$ 的概率优势小于 $\frac{q_{\text{send}}}{|D|} + negl()$ 。在游戏 G_4 中，用随机值 r_κ 代替产生的签注 $Trust_i$ 。假设协议是椭圆曲线离散对数问题是困难解的，那么敌手不能发现 G_4 和 G_3 之间的区别。在最后一个游戏 G_5 中，用到了散列函数进行总体的散列，并展示了计算最后认证参数和随机值的不可区分性。证毕。

用户隐私性分析。用户在获取云存储节点的认证过程中，绑定时间戳的随机数 $r_{\text{User}} \| time$ 是通过加密函数以密文的形式传输，根据信道传输的用户信息密文具有单向性，即使被截获也难以破解，从而保证了用户信息曲线的点乘，

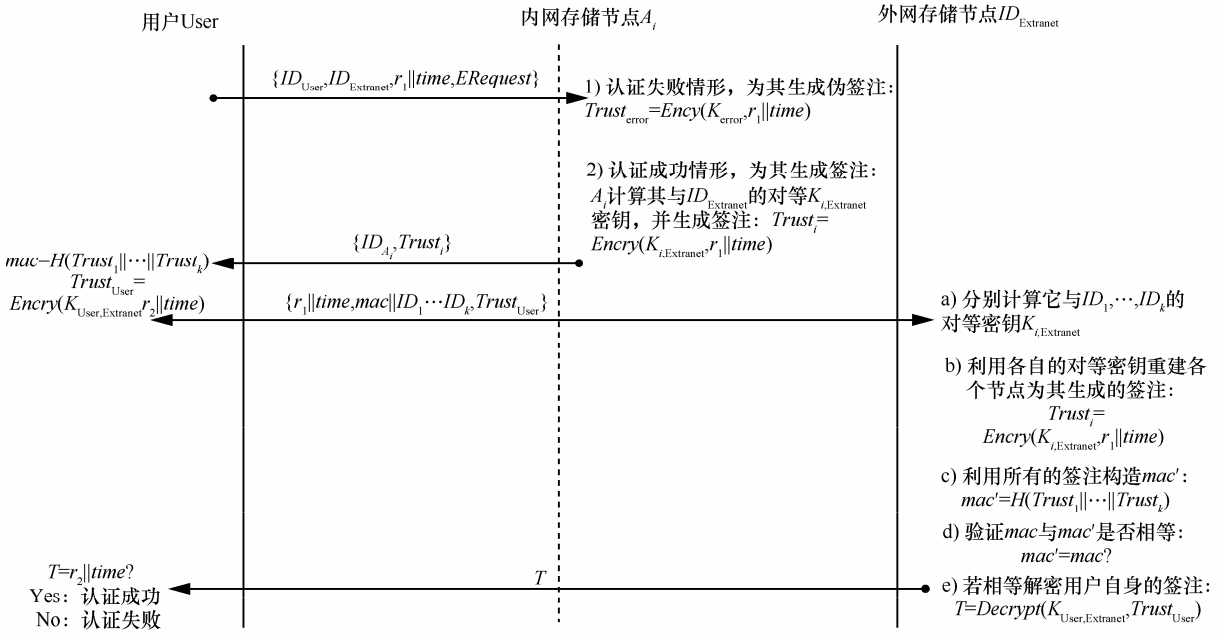

图 3 跨网络身份认证协议

以及一些对称加解密和散列函数，而且本方案利用自我验证密码系统，从而避免了复杂的证息数据隐私安全。

双向可认证性和安全性。本文协议是一种双向认证协议，被验证的双方都必须提供完整的有效验证信息。在 2 类认证方案中，使用已有的加密算法对消息进行加密。在加密算法是安全的前提下，任何恶意节点都很难解密密文。

在局域网内部，当用户发送密文给存储节点 $MAC_{\mathrm{User}} = Encry(K_{\mathrm{User},i}, r_{\mathrm{User}} \| time)$ 时，只有合法的存储节点能够解密得到 $r_{\mathrm{User}} \| time$ 并验证。因为恶意节点无法获得密钥信息，无法得到有用的用户信息。同理，也可验证存储节点对用户的认证过程。跨网络的双向认证是基于局域网内部的双向认证过程。一个恶意节点想要伪造出 $mac' = H(Trust_1 \| \cdots \| Trust_k)$ 中的k个签注是非常困难的，也就能保证mac与mac'是否相等的正确性。因此，本文方案的认证过程是安全的。

抗中间人攻击。网络之间发出会话时，只有用户和存储节点能计算出它们的会话密钥，由于发送的信息中含有随机数和时间戳等，任何人想伪造用户或存储节点进行通信都是不可能的。

抗重放攻击。User和存储节点每次会话时的相关参数和会话密钥都不一样，而且由于时戳的存在，即使入侵者截取了传输的数据信息并重放已经截获的信息，由于 $Encrypt(r \| time_1) \neq Encrypt(r \| time_2)$，所以有效地防止了重放攻击。所以，*User*和存储节点之间使用时戳也有力地抵抗了重放攻击。

防拒绝服务攻击。该模型需要首先进行*User*和存储节点之间的密钥协商才能进行认证服务，如果密钥的协商存在错误或者网络拥堵，造成密钥协商无法在限定的时间内完成，则认证进程不会开始。由上述分析可知，该协议能够有效地防范拒绝服务攻击。

4.2　协议性能分析

在表1中，作者分别给出了局域网内认证方案和Juang[10]的密钥协商方案，以及Xie[11]的密钥协商方案在计算量上的对比，从对比中可以看出在身份认证阶段Xie的协议耗用计算量为$8T_{\mathrm{m}}+5T_{\mathrm{h}}+9T_{\mathrm{e}}$，Juang的协议耗用计算量为$7T_{\mathrm{m}}+7T_{\mathrm{h}}+(nT_{\mathrm{h}})+(n+6)T_{\mathrm{e}}+2T_{\mathrm{i}}$，而本文方案的耗用计算量为$4T_{\mathrm{m}}+4T_{\mathrm{h}}+8T_{\mathrm{e}}+2T_{\mathrm{r}}$，显然本文提出的方案在局域网内的身份认证中优于Xie和Juang等的方案。

表 1　局域网双向认证方案的计算量和其他方案的计算量对比

方案	密钥协商/注册	身份认证	耗时总和
本文方案	$4T_{\mathrm{m}}$	$4T_{\mathrm{h}}+8T_{\mathrm{e}}+2T_{\mathrm{r}}$	$4T_{\mathrm{m}}+4T_{\mathrm{h}}+8T_{\mathrm{e}}+2T_{\mathrm{r}}$
Xie 的协议[10]	$5T_{\mathrm{m}}+4T_{\mathrm{h}}$	$8T_{\mathrm{m}}+5T_{\mathrm{h}}+9T_{\mathrm{e}}$	$13T_{\mathrm{m}}+9T_{\mathrm{h}}+9T_{\mathrm{e}}$
Juang 的协议[11]	$6T_{\mathrm{m}}+2T_{\mathrm{h}}$	$7T_{\mathrm{m}}+7T_{\mathrm{h}}+(nT_{\mathrm{h}})+(n+6)T_{\mathrm{e}}+2T_{\mathrm{i}}$	$13T_{\mathrm{m}}+(n+9)T_{\mathrm{h}}+(n+6)T_{\mathrm{e}}+2T_{\mathrm{i}}$

表 2　　跨网络身份认证方案的计算量

运算类型	运算次数 (内网节点)	运算次数 (外网节点)	运算次数 (用户)
T_{r}	1	1	1
T_{h}	1	2	n+1
T_{e}	2	n+1	n+1
T_{m}	2	2n	2n

设T_{r}是随机数生成的耗时，T_{m}是椭圆曲线上的点乘计算时间，T_{e}是对称加密/解密操作时间，T_{h}是散列操作时间，T_{i}是计算乘法逆元的时间，其他的计算量与这些相比，可以忽略。

跨网络身份认证所需要的计算量在表2中给出，总计算量为$(4n+2)T_{\mathrm{m}}+(n+4)T_{\mathrm{h}}+(n+4)T_{\mathrm{e}}+3T_{\mathrm{i}}$，相比RSA公钥密码体制，基于椭圆曲线密码体制具有更小的成本，更快的计算速度，更少的能量消耗。

5　结束语

保证应用服务中的数据空间资源只能被合法用户访问是身份认证的主要目的，也是实现安全可靠云存储网络的基础。该方案与已有方案相比，能确保节点身份的保密性，并给出了安全性分析。方案具有保护用户隐私性和双向可认证性，并且不需要更新用户的公钥等优点。为云存储网络中用户和存储节点之间的双向认证提供了一种较实用的解决方案。

参考文献：

[1] Cloud storage[EB/OL]. http://en.wikipedia.org/wiki/Cloud_srorage, 2012.

[2] ROHIT B, RITUPARNA C, NABENDU C, *et al*. A surveyon security issues in cloud computing[EB/OL]. http://arxiv.org/abs/1109.5388, 2012.

[3] 吴吉义, 傅建庆, 平玲娣等. 一种对等结构的云存储系统研究[J]. 电子学报, 2011, 39:1100-1107.
WU J Y, FU J Q, PING L D, *et al*. Study on the P2P cloud storage system[J]. Acta Electronica Sinica, 2011, 39:1100-1107.

[4] Towards trusted cloud computing[EB/OL]. http://www.usenix.org/events/hotcloud09/tech/full_papers/santos.pdf, 2009.

[5] 吴和生, 范训礼, 伍卫民等. 一种有效的一次性口令身份认证方案[J].

计算机应用, 2003, 23(5):45-47.
WU H S, FAN X L, WU W M, *et al*. An efficient one-time password authentication[J]. Journal of Computer Applications, 2003, 23(5):45-47.
[6] OpenID authentication 2.0-final[EB/OL]. http://openid.net/specs/openid-authentication-2_0.html.
[7] 江伟玉, 高能, 刘泽艺等. 一种云计算中的多重身份认证与授权方案[J]. 信息网络安全, 2012, (8):7-10.
JIANG W Y, GAO N, LIU Z Y, *et al*. A multi-identities authentication and authorization schema[J]. Netinfo Security, 2012, (8):7-10.
[8] OASIS standard SAML V2.0[EB/OL]. http://docs.oasis-open.org/secu-rity/saml/v2.0/.
[9] LI Z, GARCIA-LUNA-ACEVES J J. New non-interactive key agreement and progression (NIKAP) schemes and their applications to security in ad hoc network[A]. The 2005 International Workshop on Wireless and Sensor Networks Security(WSNS 2005)[C]. Washington DC, USA, 2005. 6.
[10] JUANG W S, CHIU J Y, CHANG H Y. A secure and efficient delegation-based authentication scheme in public clouds[A]. The 1st Cross-Straits Conference On Information Security[C]. Hangzhou, China, 2011. 96-102.
[11] 杜瑞忠，田俊峰，张焕国. 基于信任和个性偏好的云服务选择模型[J]. 浙江大学学报(工学版), 2013, (1):53-61.
DU R Z，TIAN J F，ZHANG H G. Cloud service selection model based on trust and personality preference[J]. Journal of Zhejiang University(Engineering Science), 2013, (1):53-61.

作者简介：

何文才（1956-），男，黑龙江鹤岗人，北京电子科技学院教授，主要研究方向为编码理论及其应用、信息安全及保密。

杜敏（1987-），女，陕西西安人，西安电子科技大学硕士生，主要研究方向为网络通信安全。

陈志伟（1989-），男，河南周口人，西安电子科技大学硕士生，主要研究方向为密码学与信息安全。

刘培鹤（1972-），男，黑龙江鹤岗人，北京电子科技学院教师，主要研究方向为信息安全。

韩妍妍（1982-），女，黑龙江哈尔滨人，北京电子科技学院助理研究员，主要研究方向为可视密码、密码学。

（上接第 13 页）

[14] GUO Z Z, LI M C, FAN X X. Attribute-based ring signcryption scheme[J]. Security and Communication Networks, 2013, 6(6):790-796.
[15] LI X X, QIAN H F, WENG J. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model[J]. Mathematical and Computer Modelling, 2013, 57(3-4):503-511.
[16] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11):612-613.

林志强（1988-），男，福建漳州人，武警工程大学硕士生，主要研究方向为密码学。

作者简介：

杨晓元（1959-），男，湖南湘潭人，武警工程大学教授，主要研究方向为信息安全与密码学。

韩益亮（1977-），男，甘肃会宁人，博士，武警工程大学副教授，主要研究方向为密码学。