# 混合云服务中的跨云际认证机制①

周艺华, 蒿金志, 赵 航

(北京工业大学 计算机学院, 北京 100124)

**摘 要**: 随着云计算的蓬勃发展, 越来越多的企业和个人将他们的存储和计算需求付诸于云端, 但由于安全问题得不到有效解决限制了企业跨云际数据访问的应用和发展. 提出了一种基于 Kerberos 的混合云服务中跨云际认证的机制, 在这种机制中, 云终端采取基于身份认证的方式直接和私有云进行认证,凭借企业私有云发放的票据访问企业存放在公有云中的数据. 该机制具有不需要管理和发放证书、密钥管理简单、易于存取控制等优点; 模拟实现了这种认证系统, 为跨云际访问数据的身份认证和访问控制奠定了安全基础.

**关键词**: 认证; Kerberos; 跨云际

## Authentication Mechanism of Crossing Clouds in Hybrid Cloud Services

ZHOU Yi-Hua, HAO Jin-Zhi, ZHAO Hang

(Computer Department, Beijing University of Technology, Beijing 100124, China)

**Abstract**: With the rapid development of cloud computing, more and more businesses and individuals put there storage and computing needs into clouds. But as people have no more effective solutions for the security problems, the use and development are limited when getting data across the clouds. In this paper, we present a Kerberos-based authentication mechanism of crossing the clouds in hybrid cloud services. In this mechanism the Cloudterminal get to the certification with the Private-clouds directly. Issued by the tickets of enterprise Private-clouds Cloudterminal can get the access to the data in the Public clouds in a way based on authentication. In this mechanism there's no need to manage and issue certificates and the key management is simple and easy to control. This paper achieved this certification system, laid the foundation for secure authentication and access controlling when getting data across clouds.

**Key words**: authentication; Kerberos; across clouds

云计算安全[1]问题是一个多层次并涉及到多研究领域的复杂问题. 混合云[2]环境下权限安全管理、跨云的资源数据访问[3]等方面存在着严重的安全挑战, 由此带来的身份认证、授权管理、传输控制等等问题更加严峻. 同时, 作为基础软硬件服务的提供者, 云计算的基础设施服务层为云计算的平台层和应用层提供了基本性的安全保障, 对其安全性的研究是整个云计算安全的基石. 云安全环境下大致分为两种认证, 单向认证: 包括密码口令、PIN 等. 它是依靠用户所知道的某些信息作为认证的一种方式, 该方式简单易用, 但是容易遭受口令猜测攻击和截获攻击; 用户所拥有的, 包括识别令牌, ID 卡等硬件设施, 容易损坏、丢失和被盗、携带不便, 且有硬件花费; 用户所特有的, 包括用户指纹、虹膜等生物识别方式; 但是该方式中的唯一认证标识不能改变, 限制了认证的灵活性. 双向认证: 比较熟知的认证技术有 PKI 体系结构[4], PKI 的基本要素依赖于数字证书, 如 SAP; 虽然 PKI 能够使得依赖端方便地验证其他人的证书, 但是在混合云环境下, 当面临超大规模的证书持有者和证书依赖方时, 建设满足大量用户访问的资料库系统, 为巨大的用户群提供证书撤销服务, 为所有的证书提供归档服务, 系统过于庞大, 将使得设计和实现的复杂程度迅速攀升, 并且由于证书有固定的生命周期, 当证书的生命周期比证书发布给资源的时间长时, 如果证书不能及

① 收稿时间:2014-07-27;收到修改稿时间:2014-09-02

时被撤销, 很容易受到攻击; 更有 IBC 认证技术[5], 实现了公钥绑定实体身份, 使得任何两个用户间能够安全地通信, 能够在不交换公钥的情况下直接验证对方的签名. 与 PKI 相比较 IBC 密钥管理难度较小, 使用较为方便, 但在大范围和开放式的环境中使用中也有较大难度.

因此, 本文通过对 Kerberos 认证系统[6,7]的分析, 提出了一种跨云际认证机制. 在该模型中, 云终端可以采取基于身份认证的方式直接和私有云进行认证, 凭借企业私有云发放的票据访问企业存放在公有云中的数据. 有利于企业对公有云中数据的存取控制, 不仅减轻了用户直接和外部云进行认证带来的云终端和云端比较大的负担, 而且大大方便了企业对用户访问外部云中数据的集中控制和实时改变存取策略.

## 1 混合云服务中的跨云认证方案

### 1.1 Kerberos 系统工作过程

Kerberos 实际上是一种基于票据(Ticket)的认证方式, 其工作过程如图 1.

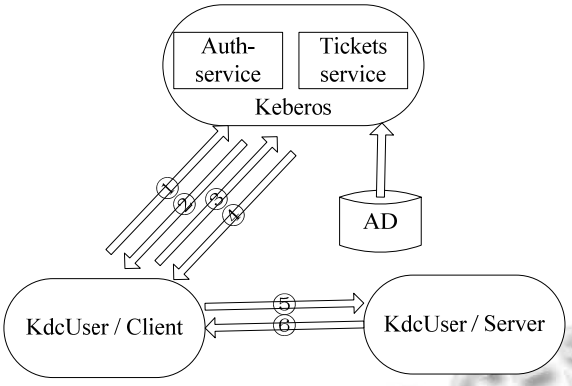


图 1 Kerberos 系统图

①中请求的信息格式为｛clientname, servername, Authenticator(密文)｝

②中返回的信息为｛Logon Session Key(由客户端派生的密钥加密)+TGT｛clientname+ Authenticator+ Logon Session Key｝(由 KDC 自己的密钥加密)｝

③中请求的信息格式为｛clientname+ servername+ Authenticator(由 Logon Session Key 加密+TGT)｝

④中返回给客户端的信息格式为｛｛clientname+ Authenticator+ Service Session Key｝(由 Logon Session Key 加密)+ST ｛clientname+Authenticator+Service Session Key｝( 由服务器密码派生的密钥加密)｝

⑤中请求的信息格式为｛ST ｛clientname+ Authenticator+ Service Session Key｝(客户端在④中缓存到的密文)+｛clientname+ Authenticator｝(利用客户端已经获取的 Service Session Key 加密)｝

⑥中返回的信息格式为｛clientname+ Authenticator｝(由服务端已经获取的 Service Session Key 加密)

### 1.2 跨云际访问数据工作模型

企业数据部分放在企业内的私有云中, 部分放在企业外的公有云 1 和公有云 2 中, 企业内的用户 Com-Client1 和企业外的用户 Out-Client 要访问企业在公有云中的数据. 图 2 中直接访问箭头代表 Com-Client1 和 Out-Client 通过直接和公有云认证的模型访问公有云中的数据, 间接访问箭头代表 Com-Client1 和 Out-Client 通过基于 Kerberos 的跨云际认证模型访问公有云中的数据. 我们以 Com-Client1 访问公有云 1 的数据为例来阐述本文的这种跨云际认证模型.

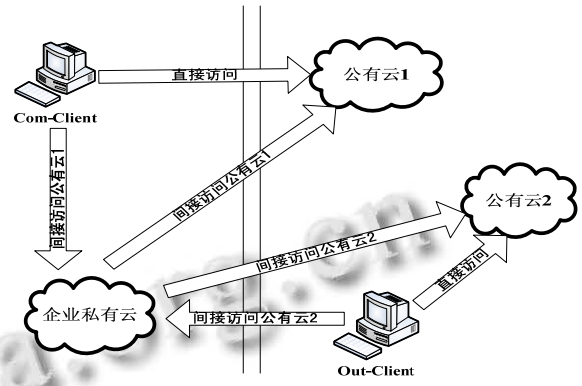


图 2 跨云际访问数据架构

### 1.3 基于身份的跨云际认证模型工作过程

(1)Com-Client1 向私有云端 INTA 发出请求, INTA 和 Com-Client1 进行身份认证对 Com-Client1 进行请求处理, 认证和请求通过, 转(2);否则结束;
Com-Client1:{IDClient , IDserver, Al, T1 } INTA 这里我们通过 Al 来确定 Kp, c

(2) INTA 用认证过程中取得的私有云和客户端的会话密钥 Kp, c 加密应答信息回复给 Com-Client1,
INTA:EKp, c[{Kc, c, T2, Lifetime, IDcloud, Ticket}]
Com-Client1Ticket= EKpb, c [{Kc, c , T2, Lifetime, IDcloud, IDClient1}]

实际上这里我们对 Ticket 信息加密了两次.

(3)Com-Client1 用客户端和私用云共有的的密钥解密应答信息, 获得与公有云 1 的会话密钥 Kc, c 用 Kc, c 加密票据等发送给公有云 1. Com-Client1:{Ticket, EKc, c [{ IDcloud, IDClient1, T3}] OUTTA 这里 Ticket 又加密了两次.

(4)公有云 1 收到 Com-Client1 的信息后, 用公有云与私有云的共享密钥 Kpb, c 解密 Ticket, 获得与 Com-Client1 的会话密钥 Kc, c 用 Kc, c 解密 EKc, c{ IDcloud, IDClient1, T3}]. 其后核对 Ticket 和 EKc, c [{ IDcloud, IDClient1, T3}]中的 IDcloud, IDClient1 信息是否符合, 符合则表明发信息的人确为 Client1, 信息的确为发给自己. 再检测 T3 是否在 Ticket 的有效期内, 如果所有核对均符合, 则转(5), 否则, 结束.

(5) 公有云 1 发送 EKc, c {IDcloud+T4} 给 Com-Client1, 表明自己的身份为 IDcloud 认证过程结束. 整个过程如图 3.

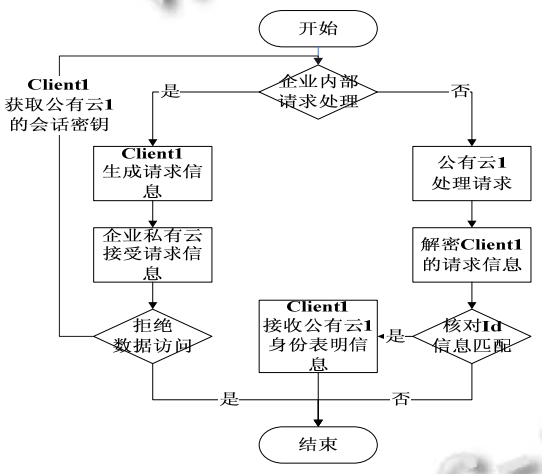


图 3　跨云际认证流程图

## 2　性能实验与分析

### 2.1 测试方案

云服务系统是一个庞大而综合的系统, 不是单个人能完成的. 所以本章设计并实现的云服务只是为了验证试验的可行性而搭建的模拟场景, 具备了云计算的一些基本特点, 如计算和存储的整合、计算向存储的迁移、文件的分布式存储、计算的并行化等. 云服务设备分为 : 私有云主服务器节点、私有云块服务器子节点和客户端, 公有云主服务器节点、公有云块服务器子节点. 其中本次试验中我们将私有云的主服务器节点用部署 windows 服务模拟, 公有云的主服务器节点用服务器端模拟, 整个系统主要有三部分组成客户端, windows 服务, 服务器端.

### 2.2 系统工作过程

(1) Com-Client1 向私有云端发送要访问的公有云端的 ID 信息, 同时向私有云端表明自己的身份, 私有云端对发送的请求信息进行请求处理. 测试方案中的会话加密算法用户可以自己设计实现, 测试方案中输入 0 表示我们采用的是 3Des 加密. 在测试过程中部署在私有云端的服务在某个端口一直处于监听的状态, Com-Client1 请求的示例信息如下: _Request=_Clientname+"#"+_Servername+"#"+T1+"#"+"0", T1 =DateTimeNow.ToString()+"#"+"5" 为时间戳这里我们定义为 5 分钟.

(2) 私有云端接收到_Request 信息查看有效期是否合法, 如果合法获取 Com-Client1 的_Clientname 以及要访问的目的服务器的_Servername, 判断用户名和服务器名是否合法, 然后根据请求信息中要求的会话加密算法(用户可以根据系统的安全需要来设计不同加密等级的算法)生成目的服务器和客户端的会话密钥_Sessionkey 以及会话秘钥向量_Sessioniv, 最后生成票据明文, 具体格式示例如下: _Ticket=_Clientname+"#"+_Servername+"#"+_Sessionkey+"#"+_Sessioniv+T2+"#"+"0", Ts2=DateTimeNow.ToString()+"#"+"5";将认证过程中取得的会话密钥加密应答信息(包括票据信息)回复给 Com-Client1, Com-Client1 收到应答信息之后对其解密, 获得与公有云的会话密钥 KC, C 处理结果如图 4.


图 4　Com-Client 认证成功图

(3) Com-Client1 获取 $K_{C, C}$ 之后加密票据等信息与公有云端发送请求, 公有云 1 收到 Com-Client1 的信息后, 用公有云与私有云端的共享密钥 $K_{p, c}$ 解密 Ticket, 获得与 Com-Client1 的会话密钥 $K_{C, C}$, 然后用 $K_{C, C}$ 解

密请求信息, 确认 Ticket 中 $ID_{cloud}$, $ID_{Client1}$, 同时向 Com-Client1 发送确认信息认证结束, 至此, Com-Client1 和公有云端都已方获取会话秘钥 $K_{C,C}$ 双方建立起来一个安全的通信通道如图 5.


图 5 公有云服务端认证成功图

## 3 结语

云服务是一种趋势, 而云服务中的的安全是制约其发展的重要因素. 本文提出的对于企业混合云中的跨云际访问数据提供了良好认证方案, 在该方案上模拟实现了认证过程, 对企业在混合云服务中的跨云际访问数据的应用实现起到了探索作用. 然而项目依然存在一些不足之处.

### 3.1 实验方案的系统分析

基于 Kerberos 的跨云际认证模型减轻了云终端的负担, 如果直接访问, 需要为每个访问公有云的用户维护一套数据, 本模型采用后, 只需要终端维护和企业私有云一套的认证数据即可; 同时降低了云终端的安全要求, 由于用户直接在企业网络环境下和私有云认证, 相对要求终端的安全性降低; 并且, 公有云避免了与每个用户进行认证, 而只需要和企业私有云进行认证即可, 降低了开销与花费. 带来以上优点的同时, 也带来了一些缺陷. 比如, 增加了企业私有云 1 系统的负担;增加了安全瓶颈, 即一旦企业私有云与公有云之间的共享密钥被攻破, 该认证系统便不能提供安全认证, 因此, 在真正的云服务环境中我们可以采用强共享密钥和定期更换共享密钥来保证安全, 同时对私有云中用户信息的存储的格式可以根据用户的数量级来采用存储的方式: 是按照数据表还是文件形式来提高访问效率并同时确保用户信息的安全.

我们对系统的通信性能进行分析. 因为每次通信都是信息的发送与接收, 数据量不会有明显差别, 所以这里我们以通信次数衡量通信的性能如下表 1 所示.

综合表 1 分析, 设公有云对平均每个用户的认证的花费为 1, 则直接访问带来的代价为 2*N, 而企业内部的认证服务我们可以忽略不计, 本实验中认证需要公有云服务 N+1 次, 云消费大约节省 50%.

表 1 通信性能

| 通信代价 | 直接访问 | 本实验方案 |
|---|---|---|
| 云终端<>私有云(单个用户 n=1) | 2 | 1 |
| 云终端<>私有云(单个用户 n=1) | 0 | 1 |
| 云终端<>私有云(单个用户 n=1) | 0 | 1 |
| …. | … | … |
| N 个用户 | 2*N | N |
| N 个用户 | 0 | N |
| N 个用户 | 0 | 1 |
| …. | … | … |

### 3.2 总结与展望

随着云计算的蓬勃发展, 越来越多的企业和个人将他们的存储和计算[8,9]云计算的安全问题不容忽视, 云计算安全相关的研究仍处于起步阶段, 许多问题仍待探索; 本文结合企业应用中的一种跨云际访问数据模型, 对 Kerberos 进行改进应用, 减轻了云终端的负担, 降低了云终端的安全要求, 对未来云计算应用[10,11]中的移动终端计算, 云存储, 物联网认证以及访问控制和电子商务的跨云际访问数据奠定了一定的基础.

## 参考文献

1 杨健,汪海航,等.云计算安全问题研究综述.小型微型计算机系统,2012,3.

2 沈建苗.2013—混合云之年. pcworld. com. cn/Article/ Show Article.asp ArticleID=15925

3 Nepal S, Friedrich C, Henry L, Chen SP. A secure storage service in the hybrid cloud. 2011 4th IEEE International Conference on Utility and Cloud Computing. 2011.

4 Faraj AST, Rasheed MA. Public-key cryptography enabled kerberos authentication. 2011 Developments in E-systems Engineering.

5 Liang Y, Zhao RC. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. Proc. of the 1st International Conference on Cloud Computing. Beijing, China. 2009.167.

6 Choi D, Jin SH, Yoon H. Trust management for user-centric

identity management on the internet. Consumer Electronics, IEEE International Symposium. IEEE Press. 2007.

7 Abdelmajid NT, Hossain MA, Mahmoud KSS. Improved Kerberos security protocol evaluation using modified BAN Logic. CIT 2010.

8 Slamanig D, Hanser C. On cloud storage and the cloud of clouds approach. 2012 International Conferece For Internet Technology and Secured Transactions. IEEE, 2012. 649–655.

9 Ramgovind S, Eloff MM, Smith E. The management of security in cloud computing. Proc. of IEEE Conference on Information Security for South Africa. South Africa. 2010.

10 Chang CW, Liu P, Wu JJ. Probability-based cloud storage providers selection algorithms with maximum availability. 2012 41st International Conference on Parallel Processing (ICPP). IEEE, 2012. 199–208.

11 Yao J, Chen S, Nepal S, Levy D, Zic. TrustStore: Making Amazon S3 trustworthy with services composition. Proc. of the CCGRID. 2010. 600–605.