

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 10 月 13 日 (13.10.2016)



(10) 国际公布号
WO 2016/161888 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
- (21) 国际申请号: PCT/CN2016/076879
- (22) 国际申请日: 2016 年 3 月 21 日 (21.03.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510161901.3 2015 年 4 月 7 日 (07.04.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼乔治城资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 方强 (FANG, Qiang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。朱红儒 (ZHU, Hongru) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。安勍 (AN, Qing) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969

号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。付颖芳 (FU, Yingfang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (CN)。

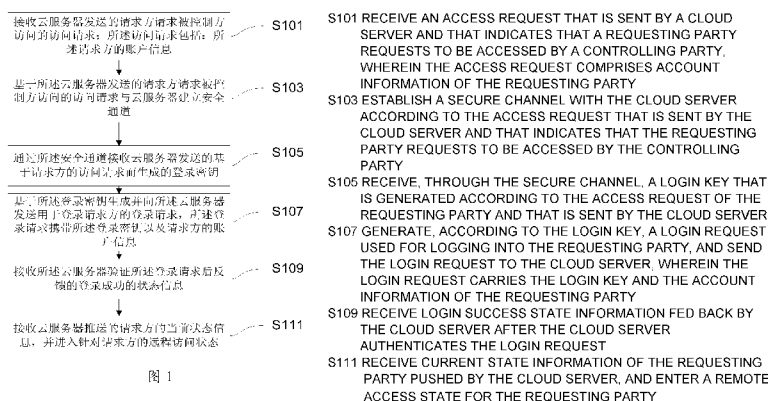
(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH,

[见续页]

(54) Title: METHOD, DEVICE AND SYSTEM FOR REMOTELY ACCESSING CLOUD APPLICATION

(54) 发明名称: 一种用于对云应用进行远程访问的方法、装置及系统



(57) Abstract: Disclosed are a method, device and system for remotely accessing a cloud application. The method comprises: receiving an access request that is sent by a cloud server and that indicates that a requesting party requests to be accessed by a controlling party; establishing a secure channel with the cloud server according to the access request that is sent by the cloud server and that indicates that the requesting party requests to be accessed by the controlling party; receiving, through the secure channel, a login key that is generated according to the access request of the requesting party and that is sent by the cloud server; generating, according to the login key, a login request used for logging into the requesting party, and sending the login request to the cloud server; receiving login success state information fed back by the cloud server after the cloud server authenticates the login request; and receiving current state information of the requesting party pushed by the cloud server, and entering a remote access state for the requesting party. By using the method, the problems of failing to implement remote access between different operating systems, and failing to implement a remote access request between terminals as well as the problem of traffic waste can be solved, and the risk of leaking a password during the remote access is also avoided.

(57) 摘要:

[见续页]



WO 2016/161888 A1



CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本申请公开了一种用于对云应用进行远程访问的方法、装置及系统。所述方法包括：接收云服务器发送的请求方请求被控制方访问的访问请求；基于云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道；通过安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥；基于登录密钥生成并向云服务器发送用于登录请求方的登录请求；接收云服务器验证登录请求后反馈的登录成功的状态信息；接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态。采用上述方法，能够解决不同操作系统间无法完成远程访问、终端与终端之间无法实现远程访问请求和浪费流量的问题，另外还避免了在远程访问期间密码泄露的风险。

一种用于对云应用进行远程访问的方法、装置及系统

技术领域

本申请涉及远程访问技术领域,具体涉及一种用于对云应用进行远程访问的方法、一种用于对云应用进行远程访问的装置、一种对云应用请求远程访问的方法、一种对云应用请求远程访问的装置、一种云服务器参与远程访问的方法、一种云服务器参与远程访问的装置以及一种用于对云应用进行远程访问的系统。

背景技术

随着智能终端的普及,越来越多的用户使用智能终端上的应用程序。不同的应用程序的操作方式都不同,经常会出现不会使用或应用程序的某个功能不会操作的情况,这时就需要向其他人询问使用方法,如果周围没有人或没有会使用该应用程序的人在,就只能通过电话或其他通信手段来询问该应用程序的使用方法,但是通过电话的描述往往很难理解其操作方法,这时就要使用远程访问来解决问题。

在现有技术下,常用的远程访问有以下几种:

1. 由微软提出的一种远程桌面 WEB 连接的方法。该方法是通过 ActiveX 控件提供与完整终端服务器客户端相同的功能。通过嵌入网页中的 ActiveX 控件可以实现终端服务器连接客户端服务器的功能,该技术基于 Windows RDP 协议,但是不基于 Windows 系统的终端无法使用该协议完成远程访问的请求。

2. MDM (Mobile Device Management) 技术可以实现对终端的管理功能,对于采用了云应用的移动终端来讲,通过 MDM 协议仅能够实现服务端对接入的各个移动设备的访问,无法实现各个移动终端之间的远程访问功能,尤其无法解决当某一客户端向另一客户端发起远程访问的应用场景,MDM 技术可以实现对纳入管理域的所有终端进行管理的功能,可以实现向终端推送服务器信息。但通过这种方式,仅能够实现将服务端状态同步至移动终端功能,无法实现终端与终端之间的远程访问请求。

3. RFB (Remote Frame Buffer) 协议,采用这种远程帧缓冲协议,可以实现将本地终端的屏幕信息发送至进行访问的终端。但是随着智能终端的普及,由

于远程访问的应用场景多为移动终端，若将本地终端的屏幕信息全部发送出去将会浪费宝贵的流量资源，并且网络速度将成为最大的限制。

由此可见，在现有的远程访问的技术下，远程访问在使用时存在诸多的限制与不足。另外，若用户将自己的应用程序的账号和密码都交给他人，让他人登录自己的应用程序帮助自己完成相应操作，虽然可以解决用户不会操作应用程序的某个功能或不会使用的问题，但是又增加了个人信息泄露的风险，和个人账户不安全的隐患。

发明内容

本申请提供一种用于对云应用进行远程访问的方法、一种用于对云应用进行远程访问的装置、一种对云应用请求远程访问的方法、一种对云应用请求远程访问的装置、一种云服务器参与远程访问的方法、一种云服务器参与远程访问的装置以及一种用于对云应用进行远程访问的系统，以解决上述技术问题。

本申请实施例提供了一种用于对云应用进行远程访问的方法，所述方法包括：

接收云服务器发送的请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；

基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道；

通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥；

基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求，所述登录请求携带所述登录密钥以及请求方的账户信息；

接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息；

接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态。

可选的，所述基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道问请求与云服务器建立安全通道，具体包括：

向所述云服务器发送建立安全通道的请求；所述建立安全通道的请求包括：

控制方的数字证书;

接收所述云服务器发送的建立安全通道的反馈信息;

若接收到的所述反馈信息为同意, 则与所述云服务器建立安全通道。

可选的, 在所述向所述云服务器发送建立安全通道的请求的步骤之前, 还包括:

向所述云服务器发送获取控制方的数字证书的请求; 其中, 所述数字证书用于与云服务器建立安全通道;

接收所述云服务器发送的控制方的数字证书。

可选的, 所述安全通道是 SSL 安全通道或 TLS 安全通道。

可选的, 在所述接收云服务器发送的请求方请求被控制方访问的访问请求的步骤之后, 还包括:

接收对所述访问请求的选择操作;

基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息。

可选的, 所述选择操作包括:

在所述控制方的屏幕显示区域内显示相应的选择窗口;

接收对所述选择窗口所展示的同意按钮或拒绝按钮的选取操作。

可选的, 在所述接收云服务器推送的请求方的当前状态信息, 并进入针对请求方的远程访问状态的步骤之后, 还包括:

接收对进入远程访问状态的请求方进行的操作;

向所述云服务器上传所述操作的结果。

可选的, 所述登录密钥包括: 请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

相应的, 本申请实施例还提供了一种用于对云应用进行远程访问的装置, 所述装置包括:

访问请求接收单元, 用于接收云服务器发送的请求方请求被控制方访问的访问请求; 所述访问请求包括: 所述请求方的账户信息;

安全通道建立单元, 用于基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道;

登录密钥接收单元,用于通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥;

登录请求发送单元,用于基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求,所述登录请求携带所述登录密钥以及请求方的账户信息;

登录接收单元,用于接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息;

远程访问状态建立单元,用于接收云服务器推送的请求方的当前状态信息,并进入针对请求方的远程访问状态。

可选的,所述安全通道建立单元,包括:

安全通道请求子单元,用于向所述云服务器发送建立安全通道的请求;所述建立安全通道的请求包括:控制方的数字证书;

反馈信息接收子单元,用于接收所述云服务器发送的建立安全通道的反馈信息;

安全通道建立子单元,用于判断所述反馈信息接收子单元的结果,若接收到的所述反馈信息为同意,则与所述云服务器建立安全通道。

可选的,所述用于对云应用进行远程访问的装置,还包括:

数字证书请求单元,用于在所述向所述云服务器发送建立安全通道的请求之前,向所述云服务器发送获取控制方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

数字证书接收单元,用于接收所述云服务器发送的控制方的数字证书。

可选的,所述安全通道建立单元具体用于建立SSL安全通道或TLS安全通道。

可选的,所述用于对云应用进行远程访问的装置,还包括:

选择操作接收单元,用于在所述接收云服务器发送的请求方请求被控制方访问的访问请求之后,接收对所述访问请求的选择操作;

反馈信息发送单元,用于基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息。

可选的,所述选择操作接收单元包括:

选择窗口显示单元,用于在所述控制方的屏幕显示区域内显示相应的选择窗

口；

选取操作接收单元，用于接收对所述选择窗口所展示的同意按钮或拒绝按钮的选取操作。

可选的，所述用于对云应用进行远程访问的装置，还包括：操作接收单元，用于在所述接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态之后，接收对进入远程访问状态请求方进行的操作；

操作结果上传单元，用于向所述云服务器上传所述操作的结果。

可选的，所述登录密钥接收单元，具体用于接收请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

此外，本申请实施例还提供了一种对云应用请求远程访问的方法，所述方法包括：

与云服务器建立安全通道；

通过所述安全通道向云服务器发送请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户信息；

向所述云服务器上传所述请求方的当前状态信息。

可选的，所述与云服务器建立安全通道，具体包括：

向所述云服务器发送建立安全通道的请求；所述建立安全通道的请求包括：请求方的数字证书；

接收所述云服务器发送的建立安全通道的反馈信息；

若接收到的所述反馈信息为同意，则与所述云服务器建立安全通道。

可选的，在所述向所述云服务器发送建立安全通道的请求的步骤之前，还包括：

向所述云服务器发送获取请求方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

接收所述云服务器发送的请求方的数字证书。

可选的，所述安全通道是 SSL 安全通道或 TLS 安全通道。

可选的，在所述与云服务器建立安全通道的步骤之后，还包括：

接收所述请求方的登录操作；

向所述云服务器发送用于登录请求方的登录请求，所述登录请求包括：所述

请求方的账户信息和登录密码;

接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息;

与所述云服务器建立连接。

可选的,在所述向所述云服务器上传所述请求方的当前状态信息的步骤之前,还包括:

接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;

若所述反馈信息为同意,则执行向所述云服务器上传所述请求方的当前状态信息的步骤。

可选的,在所述向所述云服务器上传所述请求方的当前状态信息的步骤中,还包括:停止所述请求方的本地计算。

可选的,所述停止所述请求方的本地计算,包括:禁止启动所述请求方;或者,暂停启动所述请求方。

可选的,所述当前状态信息,包括:所述请求方中未保存的信息以及当前运行状态。

可选的,在所述向所述云服务器上传所述请求方的当前状态信息的步骤之后,还包括:

接收所述云服务器发送的控制方对所述请求方的操作结果。

相应的,本申请实施例还提供了一种对云应用请求远程访问的装置,所述装置包括:

安全通道建立单元,用于与云服务器建立安全通道;

访问请求发送单元,用于通过所述安全通道向云服务器发送请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息以及控制方的账户信息;

状态信息上传单元,用于向所述云服务器上传所述请求方的当前状态信息。

可选的,所述安全通道建立单元,包括:

安全通道请求子单元,用于向所述云服务器发送建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

反馈信息接收子单元,用于接收所述云服务器发送的建立安全通道的反馈信

息;

安全通道建立子单元,用于判断所述反馈信息接收子单元的结果,若接收到的所述反馈信息为同意,则与所述云服务器建立安全通道。

可选的,所述对云应用请求远程访问的装置,还包括:

数字证书请求单元,用于在所述向所述云服务器发送建立安全通道的请求之前,向所述云服务器发送获取请求方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

数字证书接收单元,用于接收所述云服务器发送的请求方的数字证书。

可选的,所述安全通道建立单元具体用于建立SSL安全通道或TLS安全通道。

可选的,所述对云应用请求远程访问的装置,还包括:

登录操作接收单元,用于在所述与云服务器建立安全通道之前,接收所述请求方的登录操作;

登录验证请求发送单元,用于向所述云服务器发送用于登录请求方的登录请求,所述登录请求包括:所述请求方的账户信息和登录密码;

登录信息接收单元,用于接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息;

连接建立单元,用于与所述云服务器建立连接。

可选的,所述对云应用请求远程访问的装置,还包括:

反馈信息接收单元,用于在所述向所述云服务器上传所述请求方的当前状态信息之前,接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;

反馈信息判断单元,用于接收所述反馈信息接收单元的结果,若所述反馈信息为同意,则执行向所述云服务器上传所述请求方的当前状态信息的步骤。

可选的,所述状态信息上传单元,还包括:

本地计算停止子单元,用于在所述向所述云服务器上传所述请求方的当前状态信息中,停止所述请求方的本地计算。

可选的,所述本地计算停止子单元,具体用于禁止启动所述请求方;或者,暂停启动所述请求方。

可选的,所述状态信息上传单元,具体用于上传所述请求方中未保存的信息

以及当前运行状态。

可选的,所述对云应用请求远程访问的装置,还包括:

操作结果接收单元,用于在所述向所述云服务器上传所述请求方的当前状态信息之后,接收所述云服务器发送的控制方对所述请求方的操作结果。

此外,本申请实施例还提供了一种云服务器参与远程访问的方法,所述方法包括:

与请求方建立安全通道;

通过安全通道接收请求方发送的请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息以及控制方的账户信息;

向所述控制方发送请求方请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息;

基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道;

接收所述请求方上传的所述请求方的当前状态信息;

基于所述请求被控制方访问的访问请求生成登录密钥;

通过所述安全通道向所述控制方发送所述登录密钥;

接收所述控制方发送的用于登录请求方的登录请求,所述登录请求携带所述登录密钥以及请求方的账户信息;

验证所述登录密钥是否正确;

若正确,则向所述控制方发送登录成功的状态信息;

向所述控制方推送请求方的当前状态信息,建立所述控制方与所述请求方的远程访问状态。

可选的,所述与请求方建立安全通道,具体包括:

接收所述请求方发送的建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

判断所述请求方的数字证书是否正确;

若正确,则向所述请求方发送内容为同意的反馈信息。

可选的,在所述接收所述请求方发送的建立安全通道的请求的步骤之前,还包括:

接收所述请求方发送的获取请求方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

根据所述请求方的注册信息生成请求方的数字证书；

向所述请求方发送请求方的数字证书。

可选的，在所述与请求方建立安全通道的步骤之后，还包括：

接收所述请求方发送的用于登录请求方的登录请求，所述登录请求包括：所述请求方的账户信息和登录密码；

判断所述登录请求中所述请求方的账户信息和登录密码是否匹配和正确；

若正确，则向所述请求方发送登录成功的信息；

与所述请求方建立连接。

可选的，在所述向所述控制方发送请求方请求被控制方访问的访问请求的步骤之后，还包括：

接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息；

向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

可选的，在所述基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道，具体包括：

接收所述控制方发送的建立安全通道的请求；所述建立安全通道的请求包括：控制方的数字证书；

判断所述控制方的数字证书是否正确；

若正确，则向所述控制方发送内容为同意的反馈信息。

可选的，在所述接收所述控制方发送的建立安全通道的请求的步骤之前，还包括：

接收所述控制方发送的获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

根据所述控制方的注册信息生成控制方的数字证书；

向所述控制方发送控制方的数字证书。

可选的，所述登录密钥包括：

请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

可选的，在所述向所述控制方推送请求方的当前状态信息，建立所述控制方与所述请求方的远程访问状态的步骤之后，还包括：

接收所述控制方对请求方的操作结果；

向所述请求方发送所述操作结果。

相应的，本申请实施例还提供了一种云服务器参与远程访问的装置，所述装置包括：

安全通道建立单元，用于与请求方建立安全通道，并用于基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道；

访问请求接收单元，用于通过安全通道接收请求方发送的请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户信息；

访问请求发送单元，用于向所述控制方发送请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；

状态信息接收单元，用于接收所述请求方上传的所述请求方的当前状态信息；

登录密钥生成单元，用于基于所述请求被控制方访问的访问请求生成登录密钥；

登录密钥发送单元，用于通过所述安全通道向所述控制方发送所述登录密钥；

登录请求接收单元，用于接收所述控制方发送的用于登录请求方的登录请求，所述登录请求携带所述登录密钥以及请求方的账户信息；

登录密钥验证单元，用于验证所述登录密钥是否正确；

登录状态发送单元，用于接收所述登录密钥验证单元的验证结果，若正确则向所述控制方发送登录成功的状态信息；

远程访问建立单元，用于向所述控制方推送请求方的当前状态信息，建立所述控制方与所述请求方的远程访问状态。

可选的，所述安全通道建立单元，包括：

请求方安全通道建立子单元,用于接收所述请求方发送的建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

请求方数字证书判断子单元,用于判断所述请求方的数字证书是否正确;

请求方反馈信息发送子单元,用于接收请求方数字证书判断单元的判断结果,若正确,则向所述请求方发送内容为同意的反馈信息。

可选的,所述云服务器参与远程访问的装置,还包括:

请求方数字证书请求接收单元,用于在所述接收所述请求方发送的建立安全通道的请求之前,接收所述请求方发送的获取请求方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

请求方数字证书生成单元,用于根据所述请求方的注册信息生成请求方的数字证书;

请求方数字证书发送单元,用于向所述请求方发送请求方的数字证书。

可选的,所述云服务器参与远程访问的装置,还包括:

登录请求接收单元,用于在所述与请求方建立安全通道之后,接收所述请求方发送的用于登录请求方的登录请求,所述登录请求包括:所述请求方的账户信息和登录密码;

登录请求判断单元,用于判断所述登录请求中所述请求方的账户信息和登录密码是否匹配和正确;

登录信息发送单元,用于接收所述登录请求判断单元的判断结果,若正确,则向所述请求方发送登录成功的状态信息;

连接建立单元,用于与所述请求方建立连接。

可选的,所述云服务器参与远程访问的装置,还包括:

反馈信息接收单元,用于在所述向所述控制方发送请求方请求被控制方访问的访问请求之后,接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息;

反馈信息发送单元,用于向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

可选的,所述安全通道建立单元,还包括:

控制方安全通道建立子单元,用于接收所述控制方发送的建立安全通道的请

求；所述建立安全通道的请求包括：控制方的数字证书；

控制方数字证书判断子单元，用于判断所述控制方的数字证书是否正确；

控制方反馈信息发送子单元，用于接收控制方数字证书判断单元的判断结果，若正确，则向所述控制方发送内容为同意的反馈信息。

可选的，所述云服务器参与远程访问的装置，还包括：

控制方数字证书请求接收单元，用于在所述接收所述控制方发送的建立安全通道的请求之前，接收所述控制方发送的获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

控制方数字证书生成单元，用于根据所述控制方的注册信息生成控制方的数字证书；

控制方数字证书发送单元，用于向所述控制方发送控制方的数字证书。

可选的，所述登录密钥生成单元生成的所述登录密钥包括：请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

可选的，所述云服务器参与远程访问的装置，还包括：操作结果接收单元，用于在所述向所述控制方推送请求方的当前状态信息，建立所述控制方与所述请求方的远程访问状态之后，接收所述控制方对请求方的操作结果；

操作结果发送单元，用于向所述请求方发送所述操作结果。

此外，本申请实施例还提供了一种用于对云应用进行远程访问的系统，所述系统包括：

根据上述任一项所述的用于对云应用进行远程访问的装置、根据上述任一项所述的对云应用请求远程访问的装置以及根据上述任一项所述的云服务器参与远程访问的装置。

与现有技术相比，本申请具有以下优点：

本申请提供的一种用于对云应用进行远程访问的方法、装置及系统，通过接收云服务器发送的请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道；通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥；基于所述登录密钥生成并向所述云服

务器发送用于登录请求方的登录请求，所述登录请求携带所述登录密钥以及请求方的账户信息；接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息；接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态。所述技术方案解决了不同操作系统间无法使用 RDP 协议完成远程访问、终端与终端之间无法实现远程访问请求和浪费流量的问题，另外本申请的技术方案在远程访问期间还避免了密码泄露的风险。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

图 1 示出了根据本申请的实施例提供的用于对云应用进行远程访问的方法的流程图；

图 2 示出了根据本申请的实施例提供的用于对云应用进行远程访问的装置的示意图；

图 3 示出了根据本申请的实施例提供的对云应用请求远程访问的方法的流程图；

图 4 示出了根据本申请的实施例提供的对云应用请求远程访问的装置的示意图；

图 5 示出了根据本申请的实施例提供的云服务器参与远程访问的方法的流程图；

图 6 示出了根据本申请的实施例提供的云服务器参与远程访问的装置的示意图；

图 7 示出了根据本申请的实施例提供的用于对云应用进行远程访问的系统的示意图。

具体实施方式

为了能够更清楚地理解本申请的上述目的、特征和优点，下面结合附图和具体实施方式对本申请进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是，本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此，本申请不受下面公开的具体实施的限制。

本申请的实施例提供了一种用于对云应用进行远程访问的方法、一种用于对云应用进行远程访问的装置、一种对云应用请求远程访问的方法、一种对云应用请求远程访问的装置、一种云服务器参与远程访问的方法、一种云服务器参与远程访问的装置以及一种用于对云应用进行远程访问的系统。在下面的实施例中逐一进行详细说明。

目前，不同操作系统的终端之间无法使用 RDP 协议完成远程访问；若采用 RFB (Remote Frame Buffer) 远程帧缓冲协议，虽然可以实现将本地终端的屏幕信息发送至进行访问的终端，若将本地终端的屏幕信息全部发送出去将会浪费流量资源，并且网络速度将成为最大的限制；若使用 MDM (Mobile Device Management) 技术，仅能够实现服务端对接入的各个移动设备的访问，无法实现各个移动终端之间的远程访问功能。针对上述问题，本申请实施例的技术方案基于云应用环境下，通过对控制终端云应用进行授权，控制终端使用云服务器提供的临时登录密钥登录被控制终端云应用的方法，从而实现了不同操作系统的终端之间进行远程访问的功能，节约流量并且在远程访问期间还避免了密码泄露的风险。

云应用的工作原理是把传统软件本地安装、本地运算的使用方式变为即取即用的服务，通过互联网或局域网连接并操控远程服务器集群，完成业务逻辑或运算任务的一种新型应用。云应用的主要载体为互联网技术，以瘦客户端 (Thin Client) 或智能客户端 (Smart Client) 的展现形式，其界面实质上是 HTML5, Javascript, 或 Flash 等技术的集成。

本申请的技术方案虽然是针对云应用环境下终端之间进行远程访问而提出的，但是，其应用领域并不局限于云应用，在现有的应用程序中，只要是服务端可以生成用于临时登录的登录密钥，并且应用程序中的数据都在服务器中存储或备份，都可以采用本申请提供的方法，并获得相应的有益效果。

在详细描述本实施例的具体步骤之前，先对本技术方案涉及的控制终端云应用和被控制终端云应用作简要说明。

本申请的技术方案是针对云应用环境下，终端之间进行远程访问的方法，即：控制终端云应用远程访问被控制终端云应用。其中，被控制终端云应用是发送远程访问请求的一方，在下文实施例的描述中对被控制终端云应用称为请求方；控制终端云应用是接收远程访问请求的一方，在下文实施例的描述中对控制终端云应用称为控制方。需要说明的是，云应用在不同的应用场景之下，即可作为控制方，也可以作为请求方，下面对本实施例作详细说明。

本申请的实施例提供了一种用于对云应用进行远程访问的方法。所述对云应用进行远程访问的方法实施例如下：

请参考图 1，其示出了根据本申请的实施例提供的用于对云应用进行远程访问的方法的流程图。

一般性的，本实施例所述对云应用进行远程访问的方法由控制方完成，所述控制方接收云服务器分配的临时登录密钥，使用所述登录密钥登录请求方。

所述对云应用进行远程访问的方法包括：

步骤 S101，接收云服务器发送的请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息。

本实施例中，控制方在接收到所述云服务器发送的请求方请求被控制方访问的访问请求之后，在终端的屏幕显示区域内弹出所述访问请求的信息，在所述访问请求信息中显示请求方的账户信息。

在控制方接收到所述云服务器发送的请求方请求被控制方访问的访问请求并确认请求方的账户信息之后，控制方还需对所述访问请求进行选择，控制方可以接受所述访问请求，也可以拒绝所述访问请求，具体步骤 S101-1 至 S101-2 如下：

步骤 S101-1，接收对所述访问请求的选择操作；

步骤 S101-2，基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息。

具体说，若所述控制方接收到的用户对所述访问请求的选择操作为同意，则基于所述选择操作向所述云服务器发送针对请求方请求被控制方访问的访问请求而生成的内容为同意的反馈信息；同样的道理，若所述控制方接收到的用户

对所述访问请求的选择操作为拒绝,则基于所述选择操作向所述云服务器发送针对请求方请求被控制方访问的访问请求而生成的内容为拒绝的反馈信息。

为了使用户在选择时更加便捷,本实施例的技术方案提供了一种接收对所述访问请求的选择操作的优选实施方式,具体包括步骤 S101-1-1 至 S101-1-2。

在优选方式下,所述接收对所述访问请求的选择操作,包括:

步骤 S101-1-1,在所述控制方的屏幕显示区域内显示相应的选择窗口;

步骤 S101-1-2,接收对所述选择窗口所展示的同意按钮或拒绝按钮的选取操作。

具体的,所述控制方在终端的屏幕显示区域内弹出所述访问请求的信息之后,在屏幕显示区域内显示相应的选择窗口,所述选择窗口内包含接收用户选取操作的选择控件。

所述选择控件可以包括多种形式,例如下拉列表或者按钮等形式,为了向用户提供更为友好的图形界面,本实施例提供了一种优选实施方式:采用按钮选择控件,即:在终端的屏幕显示区域内弹出所述访问请求的信息后,可以在控制方终端的屏幕显示区域内中展示具有同意按钮和拒绝按钮的选择控件。在采用按钮选择控件时,本步骤中接收到的就是用户对同意按钮或拒绝按钮的触控操作,例如:单击或者长按操作。

上面描述了采用按钮选择控件的优选实施方式。在其他实施方式中,还可以采用显示文本输入框的方式。具体说,可以在控制方终端的屏幕显示区域内弹出所述访问请求的信息后,在屏幕显示区域中显示文本输入框,同时在显示屏幕上显示虚拟键盘,并接收用户对虚拟键盘的触控操作,采用这种方式同样可以实现本技术方案,后续不再赘述。

步骤 S103,基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道。

本实施例中,在执行步骤 S101 控制方接收云服务器发送的请求方请求被控制方访问的访问请求后,为了保护与云服务器之间进行数据交换和信息验证的安全,需要与所述云服务器之间建立安全通道,所述基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道,具体包括步骤 S103-1 至 S103-3 如下:

步骤 S103-1,向所述云服务器发送建立安全通道的请求;所述建立安全通

道的请求包括：控制方的数字证书；

步骤 S103-2，接收所述云服务器发送的建立安全通道的反馈信息；

步骤 S103-3，若接收到的所述反馈信息为同意，则与所述云服务器建立安全通道。

需要说明的是，所述建立安全通道的请求中包含云服务器向控制方颁发的用于建立安全通道的数字证书，所以在向所述云服务器发送建立安全通道的请求的步骤之前，控制方需要先从云服务器获取所述数字证书，具体包括步骤 S103-01 至 S103-02 如下：

步骤 S103-01，向所述云服务器发送获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

步骤 S103-02，接收所述云服务器发送的控制方的数字证书。

需要说明的是，本实施例中，控制方与云服务器之间建立的安全通道为 SSL 安全通道，所以用于与云服务器建立安全通道的数字证书为 SSL 证书。

SSL 证书遵守 SSL 协议，在验证服务器身份后颁发，具有服务器身份验证和数据传输加密功能，是一种允许 web 浏览器和 web 服务器通过一个安全的连接进行交流的技术。这意味着将被发送的数据在一端被翻译成密码，传送出去，然后在另一端解开密码，再进行处理。这是一个双向的过程，也就是浏览器和服务器都需要在发送数据之前对它们进行加密。该安全协议主要用来提供对用户和服务器的认证；对传送的数据进行加密和隐藏；确保数据在传送中不被改变，即数据的完整性。

上面描述了采用 SSL 安全通道的实施方式，在其他实施方式中，控制方与云服务器之间还可以建立 TLS 安全通道。具体说，TLS 安全通道用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议和 TLS 握手协议，采用这种方式同样可以实现本技术方案，后续不再赘述。

步骤 S105，通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥。

本实施例中，所述登录密钥包括：请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

在具体实施时，控制方通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的 token，该 token 由请求方的账户信息、控制方的账户信息、

token 生成时的时间戳以及 token 生成时产生的一组随机数组成, 即: token=f (请求方的账户信息, 控制方的账户信息, timestamp, random)。

需要说明的是, 所述登录密钥生成时产生的验证码是指: 所述登录密钥在生成时产生的一组随机数, 所述验证码还可以是其他种形式的, 包括在现有技术下的任何可行的方式, 也不排除随着技术进步使用其它新出现的方式, 在此不作限定。例如: Gif 动画验证码。

步骤 S107, 基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求, 所述登录请求携带所述登录密钥以及请求方的账户信息。

本实施例中, 控制方从所述云服务器发送的登录密钥中获取请求方的账户信息, 将所述请求方的账户信息和从所述云服务器接收的登录密钥放入所述用于登录请求方的登录请求中, 并向所述云服务器发送该登录请求。需要说明的是, 所述请求方的账户信息是指: 请求方的账户名称, 即请求方的用户名。

通常在终端登录应用程序时, 都是使用用户名和用户设置的登录密码进行登录, 本实施例采用本申请提供的技术方案, 在控制方登录请求方时使用云应用的用户名和云服务器提供的登录密钥进行登录应用程序, 实现了对请求方账户信息的保护。

考虑到用户采用本技术方案提供的使用登录密钥对云应用进行远程访问的方式, 通常情况下, 可能是因为一些突发情况产生的临时需求, 而不是长期的需求, 因此在本步骤中登录请求包含的登录密钥可以为仅使用一次的临时登录密钥 (也称一次性登录密钥), 也就是说, 在控制方使用接收到的所述登录密钥进行登录请求方一次之后, 该登录密钥就将失效。

步骤 S109, 接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息。

本实施例中, 控制方接收到所述云服务器验证所述登录请求后反馈的登录成功的状态信息之后, 控制方登录至请求方, 与云服务器建立连接。

步骤 S111, 接收云服务器推送的请求方的当前状态信息, 并进入针对请求方的远程访问状态。

本实施例中, 在执行步骤 S109 控制方接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息, 控制方登录至请求方, 与云服务器建立连接之后, 接收云服务器推送的请求方的当前状态信息, 所述请求方的当前状态信息

包括：所述请求方在发送请求被控制方访问的访问请求后，在本地未保存的信息和本地当前的运行状态以及云服务器上存储的请求方的信息。

所述控制方在接收到云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态后，所述控制方就可以对所述请求方进行操作，所述控制方对请求方的操作可以是对请求方在云服务器上存储的信息进行增加、修改、删除或查询，针对不同的云应用可能还包括相应云应用中的特有的操作，具体而言，控制方可以对进入远程访问状态的请求方进行该请求方中包括的所有功能进行操作，具体包括步骤 S113 至 S114 如下：

步骤 S113，接收对进入远程访问状态的请求方进行的操作；

步骤 S114，向所述云服务器上传所述操作的结果。

在上述的实施例中，提供了一种对云应用进行远程访问的方法，与上述对云应用进行远程访问的方法相对应的，本申请还提供了对云应用进行远程访问的装置。由于装置的实施例基本相似于方法的实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。所述对云应用进行远程访问的装置实施例如下：

请参考图 2，其示出了根据本申请的实施例提供的用于对云应用进行远程访问的装置的示意图。

所述对云应用进行远程访问的装置，包括：

访问请求接收单元 201，用于接收云服务器发送的请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；

安全通道建立单元 202，用于基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道；

登录密钥接收单元 203，用于通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥；

登录请求发送单元 204，用于基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求，所述登录请求携带所述登录密钥以及请求方的账户信息；

登录接收单元 205，用于接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息；

远程访问状态建立单元 206，用于接收云服务器推送的请求方的当前状态信

息，并进入针对请求方的远程访问状态。

可选的，所述安全通道建立单元 202，包括：

安全通道请求子单元，用于向所述云服务器发送建立安全通道的请求；所述建立安全通道的请求包括：控制方的数字证书；

反馈信息接收子单元，用于接收所述云服务器发送的建立安全通道的反馈信息；

安全通道建立子单元，用于判断所述反馈信息接收子单元的结果，若接收到的所述反馈信息为同意，则与所述云服务器建立安全通道。

可选的，所述用于对云应用进行远程访问的装置，还包括：

数字证书请求单元，用于在所述向所述云服务器发送建立安全通道的请求之前，向所述云服务器发送获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

数字证书接收单元，用于接收所述云服务器发送的控制方的数字证书。

可选的，所述安全通道建立单元 202 具体用于建立 SSL 安全通道或 TLS 安全通道。

可选的，所述用于对云应用进行远程访问的装置，还包括：

选择操作接收单元，用于在所述接收云服务器发送的请求方请求被控制方访问的访问请求之后，接收对所述访问请求的选择操作；

反馈信息发送单元，用于基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息。

可选的，所述选择操作接收单元包括：

选择窗口显示单元，用于在所述控制方的屏幕显示区域内显示相应的选择窗口；

选取操作接收单元，用于接收对所述选择窗口所展示的同意按钮或拒绝按钮的选取操作。

可选的，所述用于对云应用进行远程访问的装置，还包括：

操作接收单元，用于在所述接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态之后，接收对进入远程访问状态请求方进行的操作；

操作结果上传单元,用于向所述云服务器上传所述操作的结果。

可选的,所述登录密钥接收单元,具体用于接收请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

在上述的实施例中,提供了一种用于对云应用进行远程访问的方法以及一种用于对云应用进行远程访问的装置,此外,本申请还提供了一种对云应用请求远程访问的方法;所述对云应用请求远程访问的方法实施例如下:

请参考图 3,其示出了根据本申请的实施例提供的对云应用请求远程访问的方法的流程图。

所述对云应用请求远程访问的方法包括:

步骤 S301,与云服务器建立安全通道。

本实施例中,为了保护与云服务器之间进行数据交换和信息验证的安全,请求方需要与所述云服务器之间建立安全通道,所述与云服务器建立安全通道,具体包括步骤 S301-1 至 S301-3 如下:

步骤 S301-1,向所述云服务器发送建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

步骤 S301-2,接收所述云服务器发送的建立安全通道的反馈信息;

步骤 S301-3,若接收到的所述反馈信息为同意,则与所述云服务器建立安全通道。

需要说明的是,所述建立安全通道的请求中包含云服务器向请求方颁发的用于建立安全通道的数字证书,所以在向所述云服务器发送建立安全通道的请求的步骤之前,请求方需要先从云服务器获取所述数字证书,具体包括步骤 S301-01 至 S301-02 如下:

步骤 S301-01,向所述云服务器发送获取请求方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

步骤 S301-02,接收所述云服务器发送的请求方的数字证书。

需要说明的是,本实施例中,请求方与云服务器之间建立的安全通道为 SSL 安全通道,所以用于与云服务器建立安全通道的数字证书为 SSL 证书。

上面描述了请求方采用与云服务器建立 SSL 安全通道的实施方式,在其他实施方式中,请求方与云服务器之间还可以建立 TLS 安全通道。具体说, TLS 安全

通道用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议和 TLS 握手协议，采用这种方式同样可以实现本技术方案，后续不再赘述。

所述请求方在与云服务器之间建立安全通道之后，就可以保护与云服务器之间进行数据交换和信息验证的安全，基于所述安全通道，请求方可以向云服务器发送进行登录的请求，该登录请求包括所述请求方的账户信息和登录密码，所述请求方进行登录的步骤具体包括如下步骤 S302-1 至 S302-4：

步骤 S302-1，接收所述请求方的登录操作。

具体的，请求方接收用户对所述请求方的登录操作，例如：用户在请求方登录界面上输入请求方的账户信息和登录密码，并点击登录按钮。

步骤 S302-2，向所述云服务器发送用于登录请求方的登录请求，所述登录请求包括：所述请求方的账户信息和登录密码。

本实施例中，将所述请求方的账户信息和登录密码放入用于登录请求方的登录请求中，并向所述云服务器发送所述登录请求。

步骤 S302-3，接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息。

步骤 S302-4，与所述云服务器建立连接。

根据上述步骤 S302-3 接收到所述云服务器验证所述登录请求后反馈的登录成功的状态信息之后，基于所述登录成功的状态信息当中的请求方账户信息，请求方成功登录与云服务器建立连接。

步骤 S303，通过所述安全通道向云服务器发送请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户信息。

本实施例中，所述通过所述安全通道向云服务器发送请求被控制方访问的访问请求可以采用如下方式实现：用户在请求方的访问请求界面中输入的控制方的账户信息，所述请求方获取用户输入的所述控制方的账户信息，并将所述请求方的账户信息和获取的控制方的账户信息放入请求被控制方访问的访问请求中，并通过所述安全通道向云服务器发送请求被控制方访问的访问请求。例如：用户在请求方中点击访问请求按钮，在弹出的窗口中输入控制方的账户信息，或/和用户在访问请求按钮后，显示下拉列表，列表中包含请求方中保存的通讯录名单，用户在所述下拉列表中的通讯录名单里选择控制方。

步骤 S305, 向所述云服务器上传所述请求方的当前状态信息。

在本实施例中, 在执行步骤 S303 之后, 由于控制方可以接受请求方发送的所述访问请求, 也可以拒绝请求方发送的所述访问请求, 所以在执行步骤 S305 之前, 还需要接收控制方对请求方通过所述安全通道向云服务器发送请求被控制方访问的访问请求的反馈信息, 具体包括步骤 S304-1 至 S304-2 如下:

步骤 S304-1, 接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;

需要说明的是, 若所述控制方接受请求方发送的所述访问请求, 则控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息为同意; 同样的道理, 若所述控制方拒绝请求方发送的所述访问请求, 则控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息为拒绝。

步骤 S304-2, 若所述反馈信息为同意, 则执行向所述云服务器上传所述请求方的当前状态信息的步骤。

请求方接收到所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息后, 对所述反馈信息进行判断, 若所述反馈信息为同意, 则执行步骤 S305。

在本实施例中, 请求方在通过所述安全通道向云服务器发送请求被控制方访问的访问请求之后和接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息之前, 通常用户还在对请求方进行操作, 所以在控制方接受了请求方的访问请求时, 用户对所述请求方进行的操作可能还未保存, 控制方接收到云服务器推送的云服务器上存储的请求方的信息时, 数据信息就不完整, 所以请求方在接收到反馈信息之后, 需要向所述云服务器上传所述请求方的当前状态信息。所述请求方的当前状态信息, 包括: 所述请求方中未保存的信息以及当前运行状态。

在请求方向所述云服务器上传所述请求方的当前状态信息的步骤之后, 控制方已经进入针对请求方的远程访问状态, 若用户继续对请求方进行操作, 控制方在远程访问状态操作时, 数据信息可能会发生冲突, 为了防止用户对请求方继续进行操作, 本实施例的技术方案提供了一种优选实施方式。

在优选方式下, 在所述向所述云服务器上传所述请求方的当前状态信息的同时, 还需停止所述请求方的本地计算。所述停止所述请求方的本地计算, 包

括：禁止启动所述请求方；或者，暂停启动所述请求方。

在本实施例中，在执行步骤 S305 之后，还需要接收控制方进行远程访问之后，对请求方进行操作的结果，具体包括步骤 S306 如下：

步骤 S306，接收所述云服务器发送的控制方对所述请求方的操作结果。

所述接收所述云服务器发送的控制方对所述请求方的操作结果可以采用如下方式实现：所述请求方接收所述云服务器发送的控制方对所述请求方的操作结果，该操作结果显示控制方对请求方的数据信息的修改内容。

在上述的实施例中，提供了一种对云应用请求远程访问的方法，与上述对云应用请求远程访问的方法相对应的，本申请还提供了对云应用请求远程访问的装置。由于装置的实施例基本相似于方法的实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。所述对云应用请求远程访问的装置实施例如下：

请参考图 4，其示出了根据本申请的实施例提供的对云应用请求远程访问的装置的示意图。

所述对云应用请求远程访问的装置，包括：

安全通道建立单元 401，用于与云服务器建立安全通道；

访问请求发送单元 402，用于通过所述安全通道向云服务器发送请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户信息；

状态信息上传单元 403，用于向所述云服务器上传所述请求方的当前状态信息。

可选的，所述安全通道建立单元 401，包括：

安全通道请求子单元，用于向所述云服务器发送建立安全通道的请求；所述建立安全通道的请求包括：请求方的数字证书；

反馈信息接收子单元，用于接收所述云服务器发送的建立安全通道的反馈信息；

安全通道建立子单元，用于判断所述反馈信息接收子单元的结果，若接收到的所述反馈信息为同意，则与所述云服务器建立安全通道。

可选的，所述对云应用请求远程访问的装置，还包括：

数字证书请求单元,用于在所述向所述云服务器发送建立安全通道的请求之前,向所述云服务器发送获取请求方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

数字证书接收单元,用于接收所述云服务器发送的请求方的数字证书。

可选的,所述安全通道建立单元 401 具体用于建立 SSL 安全通道或 TLS 安全通道。

可选的,所述对云应用请求远程访问的装置,还包括:

登录操作接收单元,用于在所述与云服务器建立安全通道之前,接收所述请求方的登录操作;

登录验证请求发送单元,用于向所述云服务器发送用于登录请求方的登录请求,所述登录请求包括:所述请求方的账户信息和登录密码;

登录信息接收单元,用于接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息;

连接建立单元,用于与所述云服务器建立连接。

可选的,所述对云应用请求远程访问的装置,还包括:

反馈信息接收单元,用于在所述向所述云服务器上传所述请求方的当前状态信息之前,接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;

反馈信息判断单元,用于接收所述反馈信息接收单元的结果,若所述反馈信息为同意,则执行向所述云服务器上传所述请求方的当前状态信息的步骤。

可选的,所述状态信息上传单元 403,还包括:

本地计算停止子单元,用于在所述向所述云服务器上传所述请求方的当前状态信息中,停止所述请求方的本地计算。

可选的,所述本地计算停止子单元,具体用于禁止启动所述请求方;或者,暂停启动所述请求方。

可选的,所述状态信息上传单元 403,具体用于上传所述请求方中未保存的信息以及当前运行状态。

可选的,所述对云应用请求远程访问的装置,还包括:

操作结果接收单元,用于在所述向所述云服务器上传所述请求方的当前状态

信息之后，接收所述云服务器发送的控制方对所述请求方的操作结果。

在上述的实施例中，提供了一种进行信息推送的方法、一种进行信息推送的装置、一种对云应用请求远程访问的方法以及一种对云应用请求远程访问的装置，此外，本申请还提供了一种云服务器参与远程访问的方法；所述云服务器参与远程访问的方法实施例如下：

请参考图 5，示出了根据本申请的实施例提供的云服务器参与远程访问的方法的流程图。

所述云服务器参与远程访问的方法包括：

步骤 S501，与请求方建立安全通道。

本实施例中，为了保护与所述请求方之间进行数据交换和信息验证的安全，所述云服务器需要与请求方之间建立安全通道，所述与请求方建立安全通道，具体包括步骤 S501-1 至 S501-3 如下：

步骤 S501-1，接收所述请求方发送的建立安全通道的请求；所述建立安全通道的请求包括：请求方的数字证书；

步骤 S501-2，判断所述请求方的数字证书是否正确；

步骤 S501-3，若正确，则向所述请求方发送内容为同意的反馈信息。

需要说明的是，所述云服务器从所述请求方发送的建立安全通道的请求中获取请求方的数字证书，将所述数字证书与云服务器中存储的该请求方的数字证书进行比对，若正确，则向所述请求方发送内容为同意的反馈信息；若不正确，则向所述请求方发送内容为拒绝的反馈信息。

此外，所述云服务器接收到的所述的建立安全通道的请求中包含云服务器向请求方颁发的用于建立安全通道的数字证书，所以在接收所述请求方发送建立安全通道的请求的步骤之前，云服务器需要先向所述请求方颁发所述数字证书，具体包括步骤 S501-01 至 S501-03 如下：

步骤 S501-01，接收所述请求方发送的获取请求方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

步骤 S501-02，根据所述请求方的注册信息生成请求方的数字证书；

步骤 S501-03，向所述请求方发送请求方的数字证书。

需要说明的是，本实施例中，云服务器与请求方之间建立的安全通道为 SSL

安全通道，所以用于与云服务器建立安全通道的数字证书为 SSL 证书。

上面描述了云服务器接受与请求方 SSL 安全通道的实施方式，在其他实施方式中，云服务器与请求方之间还可以建立 TLS 安全通道。具体说，TLS 安全通道用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议和 TLS 握手协议，采用这种方式同样可以实现本技术方案，后续不再赘述。

所述云服务器与请求方之间建立安全通道之后，就可以保护与请求方之间进行数据交换和信息验证的安全，基于所述安全通道，云服务器可以接收请求方发送的登录请求，所述云服务器接受并验证请求方进行登录的步骤具体包括如下步骤 S502-1 至 S502-4：

步骤 S502-1，接收所述请求方发送的用于登录请求方的登录请求，所述登录请求包括：所述请求方的账户信息和登录密码。

具体的，所述云服务器从所述登录请求中获取所述请求方的账户信息和登录密码。

步骤 S502-2，判断所述登录请求中所述请求方的账户信息和登录密码是否匹配和正确。

查询在云服务器保存的所述请求方的账户信息和登录密码，并判断与步骤 S502-1 中获取的所述请求方的账户信息和登录密码是否匹配和正确。

步骤 S502-3，若正确，则向所述请求方发送登录成功的状态信息。

步骤 S502-4，与所述请求方建立连接。

根据上述步骤 S502-3 向所述请求方发送登录成功的状态信息之后，基于所述送登录成功的状态信息当中的请求方账户信息，与所述请求方建立连接。

步骤 S503，通过安全通道接收请求方发送的请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户信息。

本实施例中，所述云服务器通过安全通道接收请求方发送的请求被控制方访问的访问请求，并从所述访问请求中获取所述请求方的账户信息以及控制方的账户信息。

步骤 S505，向所述控制方发送请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息。

本实施例中，所述云服务器基于步骤 S503 中获取的控制方的账户信息，在云服务器中查找所述控制方，若查找到所述控制方，则向所述控制方发送请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息。

在向所述控制方发送请求方请求被控制方访问的访问请求之后，由于控制方可以接受请求方发送的所述访问请求，也可以拒绝请求方发送的所述访问请求，所述云服务器还需接收所述控制方对所述访问请求的反馈信息，具体包括步骤 S505-1 至 S505-2 如下：

步骤 S505-1，接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息；

步骤 S505-2，向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

需要说明的是，在所述云服务器接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息之后，由于所述请求方不知道所述控制方是否接受所述请求方请求被控制方访问的访问请求，则还需向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

步骤 S507，基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道。

本实施例中，为了保护与所述控制方之间进行数据交换和信息验证的安全，所述云服务器需要与控制方之间建立安全通道，所述与控制方建立安全通道，具体包括步骤 S507-1 至 S507-3 如下：

步骤 S507-1，接收所述控制方发送的建立安全通道的请求；所述建立安全通道的请求包括：控制方的数字证书；

步骤 S507-2，判断所述控制方的数字证书是否正确；

步骤 S507-3，若正确，则向所述控制方发送内容为同意的反馈信息

需要说明的是，所述云服务器从所述控制方发送的建立安全通道的请求中获取控制方的数字证书，将所述数字证书与云服务器中存储的该控制方的数字证书进行比对，若正确，则向所述控制方发送内容为同意的反馈信息；若不正确，则向所述控制方发送内容为拒绝的反馈信息。

此外，所述云服务器接收到的所述的建立安全通道的请求中包含云服务器向控制方颁发的用于建立安全通道的数字证书，所以在接收所述控制方发送建立

安全通道的请求的步骤之前，云服务器需要先向所述控制方颁发所述数字证书，具体包括步骤 S507-01 至 S507-03 如下：

步骤 S507-01，接收所述控制方发送的获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

步骤 S507-02，根据所述控制方的注册信息生成控制方的数字证书；

步骤 S507-03，向所述控制方发送控制方的数字证书。

需要说明的是，本实施例中，云服务器与控制方之间建立的安全通道为 SSL 安全通道，所以用于与云服务器建立安全通道的数字证书为 SSL 证书。

上面描述了云服务器接受与控制方 SSL 安全通道的实施方式，在其他实施方式中，云服务器与控制方之间还可以建立 TLS 安全通道。具体说，TLS 安全通道用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议和 TLS 握手协议，采用这种方式同样可以实现本技术方案，后续不再赘述。

步骤 S509，接收所述请求方上传的所述请求方的当前状态信息。

本实施例中，云服务器接收所述请求方上传的所述请求方的当前状态信息，并将所述请求方的当前状态信息保存在云服务器中。所述请求方的当前状态信息，包括：所述请求方中未保存的信息以及当前运行状态。

步骤 S511，基于所述请求被控制方访问的访问请求生成登录密钥。

本实施例中，所述基于所述请求被控制方访问的访问请求生成登录密钥，可以采用如下步骤实现：

步骤 S511-1，所述云服务器基于所述请求被控制方访问的访问请求生成登录密钥云服务器基于从所述访问请求中获取所述请求方的账户信息以及控制方的账户信息生成登录密钥；

步骤 S511-2，生成验证码并获取生成所述登录密钥时的时间戳；

步骤 S511-3，将所述时间戳和验证码放入所述登录密钥中。

可以理解的，所述登录密钥包括：请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

需要说明的是，所述生成验证码是指：所述登录密钥在生成时产生的一组随机数，所述验证码是为了提高所述登录密钥的安全性而生成的。所述验证码还

可以是其他种形式的, 包括在现有技术下的任何可行的方式, 也不排除随着技术进步使用其它新出现的方式, 在此不作限定。例如: Gif 动画验证码。

需要说明的是, 在本步骤 S511 中生成的登录密钥为仅使用一次的临时登录密钥(也称一次性登录密钥), 也就是说, 在控制方使用接收到的所述登录密钥进行登录请求方一次之后, 该登录密钥就将失效。

在具体实施时, 所述云服务器基于所述请求被控制方访问的访问请求生成登录密钥云服务器基于从所述访问请求中获取所述请求方的账户信息以及控制方的账户信息生成一个 token, 并生成验证码和获取生成所述 token 时的时间戳, 将所述时间戳和验证码放入所述 token 中, 该 token 由请求方的账户信息、控制方的账户信息、token 生成时的时间戳以及 token 生成时产生的一组随机数组组成, 即: $\text{token} = f(\text{请求方的账户信息}, \text{控制方的账户信息}, \text{timestamp}, \text{random})$ 。

步骤 S513, 通过所述安全通道向所述控制方发送所述登录密钥。

本实施例中, 所述云服务器将步骤 S511 中生成的所述登录密钥, 通过所述安全通道向所述控制方发送所述登录密钥。所述登录密钥包括: 请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

步骤 S515, 接收所述控制方发送的用于登录请求方的登录请求, 所述登录请求携带所述登录密钥以及请求方的账户信息。

本实施例中, 云服务器接收所述控制方发送的用于登录请求方的登录请求, 并从所述登录请求中获取所述登录密钥以及请求方的账户信息。需要说明的是, 所述请求方的账户信息是指: 请求方的账户名称, 即请求方的用户名。

步骤 S517, 验证所述登录密钥是否正确。

所述验证所述登录密钥是否正确可以采用如下方式实现:

根据步骤 S515 中获取的所述请求方的账户名称查询云服务器中该请求方的账户名称的登录密钥;

判断步骤 S515 中获取的登录密钥与云服务器中查询出的登录密钥是否正确;

若正确, 则进入步骤 S519。

步骤 S519, 若正确, 则向所述控制方发送登录成功的信息。

本实施例中，接收步骤 S517 中的判断结果，向所述控制方发送登录成功的状态信息，与控制方建立连接。

步骤 S521，向所述控制方推送请求方的当前状态信息，建立所述控制方与所述请求方的远程访问状态。

本实施例中，查询云服务器中请求方的当前状态信息，将所述请求方的当前状态信息推送给所述控制方。所述请求方的当前状态信息包括：所述请求方在发送请求被控制方访问的访问请求后，在本地未保存的信息和本地当前的运行状态以及云服务器上存储的请求方的信息。

在建立所述控制方与所述请求方的远程访问状态之后，还需接收控制方对请求方的操作结果，在控制方结束对请求方的远程访问状态之后，将所述操作结果发送给所述请求方，具体包括步骤 S522 至 S523 如下：

步骤 S522，接收所述控制方对请求方的操作结果；

步骤 S523，向所述请求方发送所述操作结果。

在上述的实施例中，提供了一种云服务器参与远程访问的方法，与上述云服务器参与远程访问的方法相对应的，本申请还提供了云服务器参与远程访问的装置。由于装置的实施例基本相似于方法的实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。所述云服务器参与远程访问的实施例如下：

请参考图 6，其示出了根据本申请的实施例提供的云服务器参与远程访问的装置的示意图。

所述云服务器参与远程访问的装置，包括：

安全通道建立单元 601，用于与请求方建立安全通道，并用于基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道；

访问请求接收单元 602，用于通过安全通道接收请求方发送的请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户信息；

访问请求发送单元 603，用于向所述控制方发送请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；

状态信息接收单元 604，用于接收所述请求方上传的所述请求方的当前状态信息；

登录密钥生成单元 605, 用于基于所述请求被控制方访问的访问请求生成登录密钥;

登录密钥发送单元 606, 用于通过所述安全通道向所述控制方发送所述登录密钥;

登录请求接收单元 607, 用于接收所述控制方发送的用于登录请求方的登录请求, 所述登录请求携带所述登录密钥以及请求方的账户信息;

登录密钥验证单元 608, 用于验证所述登录密钥是否正确;

登录状态发送单元 609, 用于接收所述登录密钥验证单元的验证结果, 若正确则向所述控制方发送登录成功的状态信息;

远程访问建立单元 610, 用于向所述控制方推送请求方的当前状态信息, 建立所述控制方与所述请求方的远程访问状态。

可选的, 所述安全通道建立单元 601, 包括:

请求方安全通道建立子单元, 用于接收所述请求方发送的建立安全通道的请求; 所述建立安全通道的请求包括: 请求方的数字证书;

请求方数字证书判断子单元, 用于判断所述请求方的数字证书是否正确;

请求方反馈信息发送子单元, 用于接收请求方数字证书判断单元的判断结果, 若正确, 则向所述请求方发送内容为同意的反馈信息。

可选的, 所述云服务器参与远程访问的装置, 还包括:

请求方数字证书请求接收单元, 用于在所述接收所述请求方发送的建立安全通道的请求之前, 接收所述请求方发送的获取请求方的数字证书的请求; 其中, 所述数字证书用于与云服务器建立安全通道;

请求方数字证书生成单元, 用于根据所述请求方的注册信息生成请求方的数字证书;

请求方数字证书发送单元, 用于向所述请求方发送请求方的数字证书。

可选的, 所述云服务器参与远程访问的装置, 还包括:

登录请求接收单元, 用于在所述与请求方建立安全通道之后, 接收所述请求方发送的用于登录请求方的登录请求, 所述登录请求包括: 所述请求方的账户信息和登录密码;

登录请求判断单元, 用于判断所述登录请求中所述请求方的账户信息和登录

密码是否匹配和正确;

登录信息发送单元,用于接收所述登录请求判断单元的判断结果,若正确,则向所述请求方发送登录成功的状态信息;

连接建立单元,用于与所述请求方建立连接。

可选的,所述云服务器参与远程访问的装置,还包括:

反馈信息接收单元,用于在所述向所述控制方发送请求方请求被控制方访问的访问请求之后,接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息;

反馈信息发送单元,用于向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

可选的,所述安全通道建立单元 601,还包括:

控制方安全通道建立子单元,用于接收所述控制方发送的建立安全通道的请求;所述建立安全通道的请求包括:控制方的数字证书;

控制方数字证书判断子单元,用于判断所述控制方的数字证书是否正确;

控制方反馈信息发送子单元,用于接收控制方数字证书判断单元的判断结果,若正确,则向所述控制方发送内容为同意的反馈信息。

可选的,所述云服务器参与远程访问的装置,还包括:

控制方数字证书请求接收单元,用于在所述接收所述控制方发送的建立安全通道的请求之前,接收所述控制方发送的获取控制方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

控制方数字证书生成单元,用于根据所述控制方的注册信息生成控制方的数字证书;

控制方数字证书发送单元,用于向所述控制方发送控制方的数字证书。

可选的,所述登录密钥生成单元 605 生成的所述登录密钥包括:请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

可选的,所述云服务器参与远程访问的装置,还包括:

操作结果接收单元,用于在所述向所述控制方推送请求方的当前状态信息,建立所述控制方与所述请求方的远程访问状态之后,接收所述控制方对请求方

的操作结果；

操作结果发送单元，用于向所述请求方发送所述操作结果。

在上述的实施例中，提供了一种进行信息推送的方法、一种进行信息推送的装置、一种对云应用请求远程访问的方法、一种对云应用请求远程访问的装置、一种云服务器参与远程访问的方法以及一种云服务器参与远程访问的装置，此外，本申请还提供了一种用于对云应用进行远程访问的系统；所述用于对云应用进行远程访问的系统实施例如下：

请参考图 7，示出了根据本申请的实施例提供的用于对云应用进行远程访问的系统的流程图。

所述用于对云应用进行远程访问的系统包括：对云应用请求远程访问的装置 701、用于对云应用进行远程访问的装置 702 以及云服务器参与远程访问的装置 703；

其中，所述对云应用请求远程访问的装置 701，用于与云服务器建立安全通道，通过所述安全通道向云服务器发送请求被控制方访问的访问请求，并上传请求方的当前状态信息；

所述对云应用请求远程访问的装置 702，用于接收云服务器发送的请求方请求被控制方访问的访问请求，并与云服务器建立安全通道，基于所述安全通道接收云服务器发送的登录密钥，并使用所述登录密钥访问所述请求方；

所述云服务器参与远程访问的装置 703，用于与请求方和控制方建立安全通道，并根据所述安全通道接收并发送请求方发送的请求被控制方访问的访问请求，并根据所述访问请求生成登录密钥后将所述登录密钥发送给控制方，并具有存储所述请求方与控制方的用户账户数据库。

下面对所述用于对云应用进行远程访问的系统进行远程访问的流程作简要说明。其中，对云应用请求远程访问的装置 701，简称为请求方，对云应用请求远程访问的装置 702，简称为控制方，云服务器参与远程访问的装置 703，简称为云服务器。

- 1) 控制方向云服务器发送获取请求方的数字证书的请求；
- 2) 云服务器接收控制方的数字证书的请求，并向控制方发送所述数字证书；
- 3) 控制方接收所述数字证书；
- 4) 请求方向云服务器发送获取请求方的数字证书的请求；

- 5) 云服务器接收请求方的数字证书的请求,并向请求方发送所述数字证书;
- 6) 请求方接收所述数字证书;
- 7) 请求方利用所述数字证书向所述云服务器发送建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;
- 8) 云服务器接收建立安全通道的请求,并判断所述建立安全通道的请求中的数字证书是否正确,若正确,则与所述请求方建立安全通道;
- 9) 请求方基于所述安全通道向所述云服务器发送用于登录请求方的登录请求,所述登录请求包括:所述请求方的账户信息和登录密码;
- 10) 云服务器接收所述用于登录请求方的登录请求,并验证所述请求方的账户信息和登录密码是否正确,若正确,则向所述请求方反馈登录成功的信息;
- 11) 请求方通过所述安全通道向云服务器发送请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息以及控制方的账户信息;
- 12) 云服务器通过所述请求被控制方访问的访问请求查询控制方,并向所述控制方发送请求方请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息;
- 13) 控制方接收所述请求被控制方访问的访问请求;
- 14) 控制方利用所述数字证书向所述云服务器发送建立安全通道的请求;所述建立安全通道的请求包括:控制方的数字证书;
- 15) 云服务器接收建立安全通道的请求,并判断所述建立安全通道的请求中的数字证书是否正确,若正确,则与所述请求方建立安全通道;
- 16) 控制方对所述访问请求进行选择操作,并基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息;
- 17) 云服务器接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息;并向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;
- 18) 请求方接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;
- 19) 请求方向所述云服务器上传所述请求方的当前状态信息;

- 20) 云服务器接收所述请求方上传的所述请求方的当前状态信息;
- 21) 云服务器基于所述请求被控制方访问的访问请求生成登录密钥;
- 22) 云服务器通过所述安全通道向所述控制方发送所述登录密钥;
- 23) 控制方通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥;
- 24) 控制方基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求, 所述登录请求携带所述登录密钥以及请求方的账户信息;
- 25) 云服务器接收所述控制方发送的用于登录请求方的登录请求, 所述登录请求携带所述登录密钥以及请求方的账户信息;
- 26) 云服务器验证所述登录密钥是否正确;
- 27) 若正确, 云服务器则向所述控制方发送登录成功的状态信息;
- 28) 控制方接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息;
- 29) 服务器端向所述控制方推送请求方的当前状态信息, 建立所述控制方与所述请求方的远程访问状态;
- 30) 控制方接收云服务器推送的请求方的当前状态信息, 并进入针对请求方的远程访问状态;
- 31) 控制方接收对进入远程访问状态的请求方进行的操作, 并向所述云服务器上传所述操作的结果;
- 32) 云服务器接收所述控制方对请求方的操作结果, 并向所述请求方发送所述操作结果;
- 33) 请求方接收所述云服务器发送的控制方对所述请求方的操作结果。

需要说明的是, 上述示出的是本系统的一种优选实施方式, 在其他实施方式中可以采用不同的交互方式, 例如, 可以不执行其中 1) 至 6) 的获取数字证书环节、16) 至 18) 的控制方对访问请求的选择反馈环节以及 31) 至 33) 对请求方进行远程操作的环节。只要在 7) 至 8) 和 14) 至 15) 建立安全通道环节、11) 至 13) 发送访问请求环节、19) 至 20) 上传状态信息环节以及 21) 至 30) 控制方登录请求方环节, 完成控制方远程访问请求方, 就不偏离本申请的核心, 都在本申请的保护范围之内。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存 (flash RAM)。内存是计算机可读介质的示例。

1、计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

2、本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质 (包括但不限于磁盘存储器、CD-ROM、光学存储器等) 上实施的计算机程序产品的形式。

本申请虽然以较佳实施例公开如上，但其并不是用来限定本申请，任何本领域技术人员在不脱离本申请的精神和范围内，都可以做出可能的变动和修改，因此本申请的保护范围应当以本申请权利要求所界定的范围为准。

权利要求书

1、一种用于对云应用进行远程访问的方法，其特征在于，包括：

接收云服务器发送的请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；

基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道；

通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥；

基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求，所述登录请求携带所述登录密钥以及请求方的账户信息；

接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息；

接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态。

2、根据权利要求 1 所述的用于对云应用进行远程访问的方法，其特征在于，所述基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道问请求与云服务器建立安全通道，具体包括：

向所述云服务器发送建立安全通道的请求；所述建立安全通道的请求包括：控制方的数字证书；

接收所述云服务器发送的建立安全通道的反馈信息；

若接收到的所述反馈信息为同意，则与所述云服务器建立安全通道。

3、根据权利要求 2 所述的用于对云应用进行远程访问的方法，其特征在于，在所述向所述云服务器发送建立安全通道的请求的步骤之前，还包括：

向所述云服务器发送获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

接收所述云服务器发送的控制方的数字证书。

4、根据权利要求 1 至 3 任一所述的用于对云应用进行远程访问的方法，其特征在于，所述安全通道是 SSL 安全通道或 TLS 安全通道。

5、根据权利要求 1 所述的用于对云应用进行远程访问的方法，其特征在于，

在所述接收云服务器发送的请求方请求被控制方访问的访问请求的步骤之后，还包括：

接收对所述访问请求的选择操作；

基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息。

6、根据权利要求 5 所述的用于对云应用进行远程访问的方法，其特征在于，所述选择操作包括：

在所述控制方的屏幕显示区域内显示相应的选择窗口；

接收对所述选择窗口所展示的同意按钮或拒绝按钮的选取操作。

7、根据权利要求 1 所述的用于对云应用进行远程访问的方法，其特征在于，在所述接收云服务器推送的请求方的当前状态信息，并进入针对请求方的远程访问状态的步骤之后，还包括：

接收对进入远程访问状态请求方进行的操作；

向所述云服务器上传所述操作的结果。

8、根据权利要求 1 所述的用于对云应用进行远程访问的方法，其特征在于，所述登录密钥包括：请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

9、一种用于对云应用进行远程访问的装置，其特征在于，包括：

访问请求接收单元，用于接收云服务器发送的请求方请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息；

安全通道建立单元，用于基于所述云服务器发送的请求方请求被控制方访问的访问请求与云服务器建立安全通道；

登录密钥接收单元，用于通过所述安全通道接收云服务器发送的基于请求方的访问请求而生成的登录密钥；

登录请求发送单元，用于基于所述登录密钥生成并向所述云服务器发送用于登录请求方的登录请求，所述登录请求携带所述登录密钥以及请求方的账户信息；

登录接收单元，用于接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息；

远程访问状态建立单元, 用于接收云服务器推送的请求方的当前状态信息, 并进入针对请求方的远程访问状态。

10、根据权利要求 9 所述的用于对云应用进行远程访问的装置, 其特征在于, 所述安全通道建立单元, 包括:

安全通道请求子单元, 用于向所述云服务器发送建立安全通道的请求; 所述建立安全通道的请求包括: 控制方的数字证书;

反馈信息接收子单元, 用于接收所述云服务器发送的建立安全通道的反馈信息;

安全通道建立子单元, 用于判断所述反馈信息接收子单元的结果, 若接收到的所述反馈信息为同意, 则与所述云服务器建立安全通道。

11、根据权利要求 10 所述的用于对云应用进行远程访问的装置, 其特征在于, 还包括:

数字证书请求单元, 用于在所述向所述云服务器发送建立安全通道的请求之前, 向所述云服务器发送获取控制方的数字证书的请求; 其中, 所述数字证书用于与云服务器建立安全通道;

数字证书接收单元, 用于接收所述云服务器发送的控制方的数字证书。

12、根据权利要求 9 - 11 任一所述的用于对云应用进行远程访问的装置, 其特征在于, 所述安全通道建立单元具体用于建立 SSL 安全通道或 TLS 安全通道。

13、根据权利要求 9 所述的用于对云应用进行远程访问的装置, 其特征在于, 还包括:

选择操作接收单元, 用于在所述接收云服务器发送的请求方请求被控制方访问的访问请求之后, 接收对所述访问请求的选择操作;

反馈信息发送单元, 用于基于所述选择操作的结果向云服务器发送针对请求方请求被控制方访问的访问请求而生成的反馈信息。

14、根据权利要求 13 所述的用于对云应用进行远程访问的装置, 其特征在于, 所述选择操作接收单元包括:

选择窗口显示单元, 用于在所述控制方的屏幕显示区域内显示相应的选择窗口;

选取操作接收单元,用于接收对所述选择窗口所展示的同意按钮或拒绝按钮的选取操作。

15、根据权利要求 9 所述的用于对云应用进行远程访问的装置,其特征在于,还包括:

操作接收单元,用于在所述接收云服务器推送的请求方的当前状态信息,并进入针对请求方的远程访问状态之后,接收对进入远程访问状态请求方进行的操作;

操作结果上传单元,用于向所述云服务器上传所述操作的结果。

16、根据权利要求 9 所述的用于对云应用进行远程访问的装置,其特征在于,所述登录密钥接收单元,具体用于接收请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

17、一种对云应用请求远程访问的方法,其特征在于,包括:

与云服务器建立安全通道;

通过所述安全通道向云服务器发送请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息以及控制方的账户信息;

向所述云服务器上传所述请求方的当前状态信息。

18、根据权利要求 17 所述的对云应用请求远程访问的方法,其特征在于,所述与云服务器建立安全通道,具体包括:

向所述云服务器发送建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

接收所述云服务器发送的建立安全通道的反馈信息;

若接收到的所述反馈信息为同意,则与所述云服务器建立安全通道。

19、根据权利要求 18 所述的对云应用请求远程访问的方法,其特征在于,在所述向所述云服务器发送建立安全通道的请求的步骤之前,还包括:

向所述云服务器发送获取请求方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

接收所述云服务器发送的请求方的数字证书。

20、根据权利要求 17 至 19 任一所述的对云应用请求远程访问的方法,其特征在于,所述安全通道是 SSL 安全通道或 TLS 安全通道。

21、根据权利要求 17 所述的对云应用请求远程访问的方法，其特征在于，在所述与云服务器建立安全通道的步骤之后，还包括：

接收所述请求方的登录操作；

向所述云服务器发送用于登录请求方的登录请求，所述登录请求包括：所述请求方的账户信息和登录密码；

接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息；

与所述云服务器建立连接。

22、根据权利要求 17 所述的对云应用请求远程访问的方法，其特征在于，在所述向所述云服务器上传所述请求方的当前状态信息的步骤之前，还包括：

接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息；

若所述反馈信息为同意，则执行向所述云服务器上传所述请求方的当前状态信息的步骤。

23、根据权利要求 17 所述的对云应用请求远程访问的方法，其特征在于，在所述向所述云服务器上传所述请求方的当前状态信息的步骤中，还包括：停止所述请求方的本地计算。

24、根据权利要求 23 所述的对云应用请求远程访问的方法，其特征在于，所述停止所述请求方的本地计算，包括：禁止启动所述请求方；或者，暂停启动所述请求方。

25、根据权利要求 17 或 22 或 23 任一所述的对云应用请求远程访问的方法，其特征在于，所述当前状态信息，包括：所述请求方中未保存的信息以及当前运行状态。

26、根据权利要求 17 所述的对云应用请求远程访问的方法，其特征在于，在所述向所述云服务器上传所述请求方的当前状态信息的步骤之后，还包括：

接收所述云服务器发送的控制方对所述请求方的操作结果。

27、一种对云应用请求远程访问的装置，其特征在于，包括：

安全通道建立单元，用于与云服务器建立安全通道；

访问请求发送单元，用于通过所述安全通道向云服务器发送请求被控制方访问的访问请求；所述访问请求包括：所述请求方的账户信息以及控制方的账户

信息;

状态信息上传单元, 用于向所述云服务器上传所述请求方的当前状态信息。

28、根据权利要求 27 所述的对云应用请求远程访问的装置, 其特征在于, 所述安全通道建立单元, 包括:

安全通道请求子单元, 用于向所述云服务器发送建立安全通道的请求; 所述建立安全通道的请求包括: 请求方的数字证书;

反馈信息接收子单元, 用于接收所述云服务器发送的建立安全通道的反馈信息;

安全通道建立子单元, 用于判断所述反馈信息接收子单元的结果, 若接收到的所述反馈信息为同意, 则与所述云服务器建立安全通道。

29、根据权利要求 28 所述的对云应用请求远程访问的装置, 其特征在于, 还包括:

数字证书请求单元, 用于在所述向所述云服务器发送建立安全通道的请求之前, 向所述云服务器发送获取请求方的数字证书的请求; 其中, 所述数字证书用于与云服务器建立安全通道;

数字证书接收单元, 用于接收所述云服务器发送的请求方的数字证书。

30、根据权利要求 27 至 29 任一所述的对云应用请求远程访问的装置, 其特征在于, 所述安全通道建立单元具体用于建立 SSL 安全通道或 TLS 安全通道。

31、根据权利要求 27 所述的对云应用请求远程访问的装置, 其特征在于, 还包括:

登录操作接收单元, 用于在所述与云服务器建立安全通道之前, 接收所述请求方的登录操作;

登录验证请求发送单元, 用于向所述云服务器发送用于登录请求方的登录请求, 所述登录请求包括: 所述请求方的账户信息和登录密码;

登录信息接收单元, 用于接收所述云服务器验证所述登录请求后反馈的登录成功的状态信息;

连接建立单元, 用于与所述云服务器建立连接。

32、根据权利要求 27 所述的对云应用请求远程访问的装置, 其特征在于, 还包括:

反馈信息接收单元,用于在所述向所述云服务器上传所述请求方的当前状态信息之前,接收所述云服务器发送的控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息;

反馈信息判断单元,用于接收所述反馈信息接收单元的结果,若所述反馈信息为同意,则执行向所述云服务器上传所述请求方的当前状态信息的步骤。

33、根据权利要求 27 所述的对云应用请求远程访问的装置,其特征在于,所述状态信息上传单元,还包括:

本地计算停止子单元,用于在所述向所述云服务器上传所述请求方的当前状态信息中,停止所述请求方的本地计算。

34、根据权利要求 33 所述的对云应用请求远程访问的装置,其特征在于,所述本地计算停止子单元,具体用于禁止启动所述请求方;或者,暂停启动所述请求方。

35、根据权利要求 27 或 32 或 33 任一所述的对云应用请求远程访问的装置,其特征在于,所述状态信息上传单元,具体用于上传所述请求方中未保存的信息以及当前运行状态。

36、根据权利要求 27 所述的对云应用请求远程访问的装置,其特征在于,还包括:

操作结果接收单元,用于在所述向所述云服务器上传所述请求方的当前状态信息之后,接收所述云服务器发送的控制方对所述请求方的操作结果。

37、一种云服务器参与远程访问的方法,其特征在于,包括:

与请求方建立安全通道;

通过安全通道接收请求方发送的请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息以及控制方的账户信息;

向所述控制方发送请求方请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息;

基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道;

接收所述请求方上传的所述请求方的当前状态信息;

基于所述请求被控制方访问的访问请求生成登录密钥;

通过所述安全通道向所述控制方发送所述登录密钥;

接收所述控制方发送的用于登录请求方的登录请求,所述登录请求携带所述登录密钥以及请求方的账户信息;

验证所述登录密钥是否正确;

若正确,则向所述控制方发送登录成功的状态信息;

向所述控制方推送请求方的当前状态信息,建立所述控制方与所述请求方的远程访问状态。

38、根据权利要求 37 所述的云服务器参与远程访问的方法,其特征在于,所述与请求方建立安全通道,具体包括:

接收所述请求方发送的建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

判断所述请求方的数字证书是否正确;

若正确,则向所述请求方发送内容为同意的反馈信息。

39、根据权利要求 38 所述的云服务器参与远程访问的方法,其特征在于,在所述接收所述请求方发送的建立安全通道的请求的步骤之前,还包括:

接收所述请求方发送的获取请求方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

根据所述请求方的注册信息生成请求方的数字证书;

向所述请求方发送请求方的数字证书。

40、根据权利要求 39 所述的云服务器参与远程访问的方法,其特征在于,在所述与请求方建立安全通道的步骤之后,还包括:

接收所述请求方发送的用于登录请求方的登录请求,所述登录请求包括:所述请求方的账户信息和登录密码;

判断所述登录请求中所述请求方的账户信息和登录密码是否匹配和正确;

若正确,则向所述请求方发送登录成功的状态信息;

与所述请求方建立连接。

41、根据权利要求 37 所述的云服务器参与远程访问的方法,其特征在于,在所述向所述控制方发送请求方请求被控制方访问的访问请求的步骤之后,还包括:

接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息；

向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

42、根据权利要求 37 所述的云服务器参与远程访问的方法，其特征在于，在所述基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道，具体包括：

接收所述控制方发送的建立安全通道的请求；所述建立安全通道的请求包括：控制方的数字证书；

判断所述控制方的数字证书是否正确；

若正确，则向所述控制方发送内容为同意的反馈信息。

43、根据权利要求 42 所述的云服务器参与远程访问的方法，其特征在于，在所述接收所述控制方发送的建立安全通道的请求的步骤之前，还包括：

接收所述控制方发送的获取控制方的数字证书的请求；其中，所述数字证书用于与云服务器建立安全通道；

根据所述控制方的注册信息生成控制方的数字证书；

向所述控制方发送控制方的数字证书。

44、根据权利要求 37 所述的云服务器参与远程访问的方法，其特征在于，所述登录密钥包括：

请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

45、根据权利要求 37 所述的云服务器参与远程访问的方法，其特征在于，在所述向所述控制方推送请求方的当前状态信息，建立所述控制方与所述请求方的远程访问状态的步骤之后，还包括：

接收所述控制方对请求方的操作结果；

向所述请求方发送所述操作结果。

46、一种云服务器参与远程访问的装置，其特征在于，包括：

安全通道建立单元，用于与请求方建立安全通道，并用于基于所述请求方发送的请求方请求被控制方访问的访问请求与控制方建立安全通道；

访问请求接收单元,用于通过安全通道接收请求方发送的请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息以及控制方的账户信息;

访问请求发送单元,用于向所述控制方发送请求方请求被控制方访问的访问请求;所述访问请求包括:所述请求方的账户信息;

状态信息接收单元,用于接收所述请求方上传的所述请求方的当前状态信息;

登录密钥生成单元,用于基于所述请求被控制方访问的访问请求生成登录密钥;

登录密钥发送单元,用于通过所述安全通道向所述控制方发送所述登录密钥;

登录请求接收单元,用于接收所述控制方发送的用于登录请求方的登录请求,所述登录请求携带所述登录密钥以及请求方的账户信息;

登录密钥验证单元,用于验证所述登录密钥是否正确;

登录状态发送单元,用于接收所述登录密钥验证单元的验证结果,若正确则向所述控制方发送登录成功的状态信息;

远程访问建立单元,用于向所述控制方推送请求方的当前状态信息,建立所述控制方与所述请求方的远程访问状态。

47、根据权利要求 46 所述的云服务器参与远程访问的装置,其特征在于,所述安全通道建立单元,包括:

请求方安全通道建立子单元,用于接收所述请求方发送的建立安全通道的请求;所述建立安全通道的请求包括:请求方的数字证书;

请求方数字证书判断子单元,用于判断所述请求方的数字证书是否正确;

请求方反馈信息发送子单元,用于接收请求方数字证书判断单元的判断结果,若正确,则向所述请求方发送内容为同意的反馈信息。

48、根据权利要求 47 所述的云服务器参与远程访问的装置,其特征在于,还包括:

请求方数字证书请求接收单元,用于在所述接收所述请求方发送的建立安全通道的请求之前,接收所述请求方发送的获取请求方的数字证书的请求;其中,

所述数字证书用于与云服务器建立安全通道;

请求方数字证书生成单元,用于根据所述请求方的注册信息生成请求方的数字证书;

请求方数字证书发送单元,用于向所述请求方发送请求方的数字证书。

49、根据权利要求 48 所述的云服务器参与远程访问的装置,其特征在于,还包括:

登录请求接收单元,用于在所述与请求方建立安全通道之后,接收所述请求方发送的用于登录请求方的登录请求,所述登录请求包括:所述请求方的账户信息和登录密码;

登录请求判断单元,用于判断所述登录请求中所述请求方的账户信息和登录密码是否匹配和正确;

登录信息发送单元,用于接收所述登录请求判断单元的判断结果,若正确,则向所述请求方发送登录成功的状态信息;

连接建立单元,用于与所述请求方建立连接。

50、根据权利要求 46 所述的云服务器参与远程访问的装置,其特征在于,还包括:

反馈信息接收单元,用于在所述向所述控制方发送请求方请求被控制方访问的访问请求之后,接收所述控制方发送的基于所述请求方请求被控制方访问的访问请求而生成的反馈信息;

反馈信息发送单元,用于向所述请求方发送控制方基于请求方请求被控制方访问的访问请求而生成的反馈信息。

51、根据权利要求 46 所述的云服务器参与远程访问的装置,其特征在于,所述安全通道建立单元,还包括:

控制方安全通道建立子单元,用于接收所述控制方发送的建立安全通道的请求;所述建立安全通道的请求包括:控制方的数字证书;

控制方数字证书判断子单元,用于判断所述控制方的数字证书是否正确;

控制方反馈信息发送子单元,用于接收控制方数字证书判断单元的判断结果,若正确,则向所述控制方发送内容为同意的反馈信息。

52、根据权利要求 51 所述的云服务器参与远程访问的装置,其特征在于,

还包括:

控制方数字证书请求接收单元,用于在所述接收所述控制方发送的建立安全通道的请求之前,接收所述控制方发送的获取控制方的数字证书的请求;其中,所述数字证书用于与云服务器建立安全通道;

控制方数字证书生成单元,用于根据所述控制方的注册信息生成控制方的数字证书;

控制方数字证书发送单元,用于向所述控制方发送控制方的数字证书。

53、根据权利要求 46 所述的云服务器参与远程访问的装置,其特征在于,所述登录密钥生成单元生成的所述登录密钥包括:请求方的账户信息、控制方的账户信息、登录密钥生成时的时间戳以及登录密钥生成时产生的验证码。

54、根据权利要求 46 所述的云服务器参与远程访问的装置,其特征在于,还包括:

操作结果接收单元,用于在所述向所述控制方推送请求方的当前状态信息,建立所述控制方与所述请求方的远程访问状态之后,接收所述控制方对请求方的操作结果;

操作结果发送单元,用于向所述请求方发送所述操作结果。

55、一种用于对云应用进行远程访问的系统,其特征在于,包括:根据上述权利要求 9 至 16 中任一项所述的用于对云应用进行远程访问的装置、根据上述权利要求 27 至 36 中任一项所述的对云应用请求远程访问的装置以及根据上述权利要求 46 至 54 中任一项所述的云服务器参与远程访问的装置。



图 1

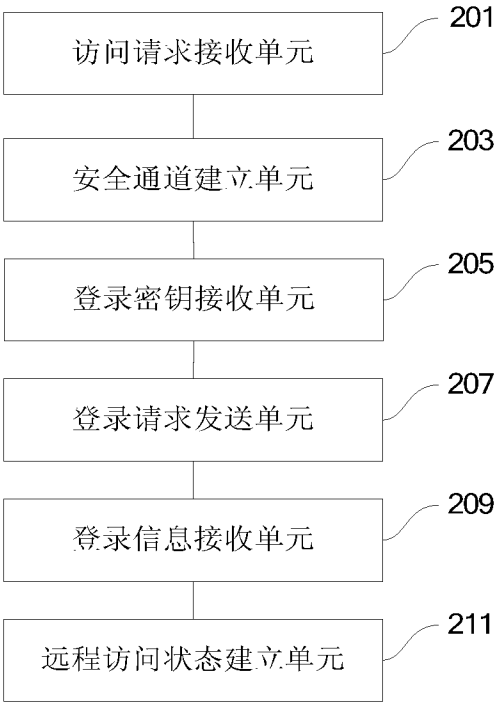


图 2

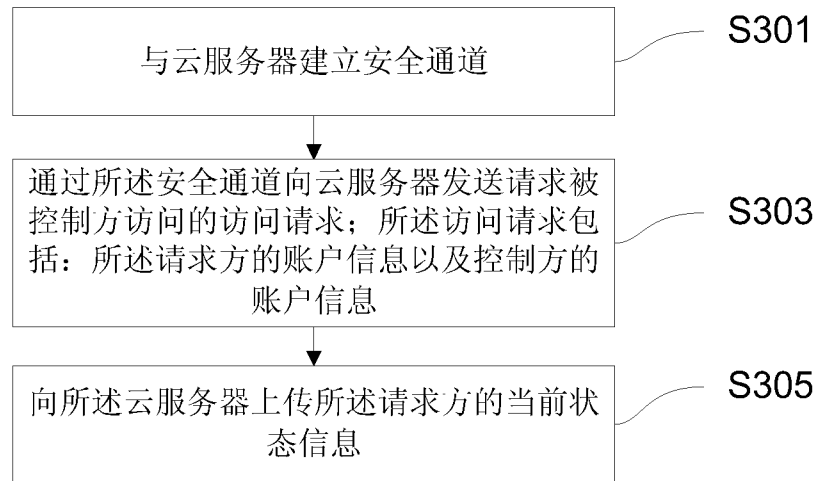


图 3

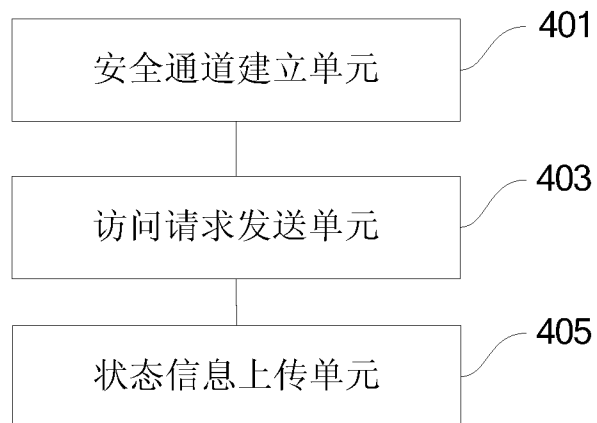


图 4



图 5



图 6

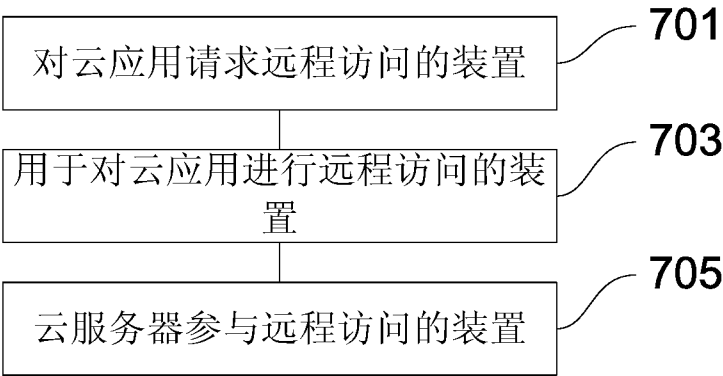


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/076879

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 29/08 (2006.01) i
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: app, cloud, application, server, remote, help, takeover, request+, control+, login, password?, generat+, security, temporal, leak

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1764116 A (IBM) 26 April 2006 (26.04.2006) description, page 4, line 1 to page 5, line 14, page 7, lines 7-10, page 8, lines 22-27, and figure 2	17-36
Y	CN 1764116 A (IBM) 26 April 2006 (26.04.2006) description, page 4, line 1 to page 5, line 14, page 7, lines 7-10, page 8, lines 22-27, and figure 2	1-16, 37-55
Y	CN 1592191 A (IBM) 09 March 2005 (09.03.2005) description, page 8, line 10 to page 9, line 11	1-16, 37-55
A	CN 102857361 A (YANG, Yuanjie) 02 January 2013 (02.01.2013) the whole document	1-55
A	CN 102196003 A (CHINA DIGITAL VIDEO (BEIJING) CO., LTD.) 21 September 2011 (21.09.2011) the whole document	1-55
A	US 2012166970 A1 (AMADEUS S. A. S.) 28 June 2012 (28.06.2012) the whole document	1-55

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search 19 May 2016	Date of mailing of the international search report 16 June 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Wenjuan Telephone No. (86-10) 62413337

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/076879

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1764116 A	26 April 2006	None	
CN 1592191 A	09 March 2005	TW 200533138 A	01 October 2005
		US 2005044378 A1	24 February 2005
		JP 2005063439 A	10 March 2005
CN 102857361 A	02 January 2013	None	
CN 102196003 A	21 September 2011	None	
US 2012166970 A1	28 June 2012	AU 2011351386 A1	02 May 2013
		EP 2472452 A1	04 July 2012
		KR 20140016259 A	07 February 2014
		CA 2821373 A1	05 July 2012
		WO 2012089750 A1	05 July 2012
		SG 191387 A1	30 August 2013
		JP 2014506359 A	13 March 2014
		CN 103282922 A	04 September 2013
		ZA 201304525 A	26 March 2014

国际检索报告

国际申请号

PCT/CN2016/076879

A. 主题的分类

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI, EPODOC, CNPAT, CNKI: 云服务器, 应用, app, 软件, 远程, 访问, 帮助, 求助, 协助, 接管, 请求, 控制, 登陆, 登录, 密码, 口令, 泄露, 安全, 生成, 产生, 暂时, 临时, cloud, application, server, remote, help, takeover, request+, control+, login, password?, generat+, security

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 1764116 A (国际商业机器公司) 2006年 4月 26日 (2006 - 04 - 26) 说明书第4页第1行-第5页第14行, 第7页第7-10行, 第8页第22-27行, 图2	17-36
Y	CN 1764116 A (国际商业机器公司) 2006年 4月 26日 (2006 - 04 - 26) 说明书第4页第1行-第5页第14行, 第7页第7-10行, 第8页第22-27行, 图2	1-16, 37-55
Y	CN 1592191 A (国际商业机器公司) 2005年 3月 9日 (2005 - 03 - 09) 说明书第8页第10行-第9页第11行	1-16, 37-55
A	CN 102857361 A (杨源杰) 2013年 1月 2日 (2013 - 01 - 02) 全文	1-55
A	CN 102196003 A (新奥特北京视频技术有限公司) 2011年 9月 21日 (2011 - 09 - 21) 全文	1-55
A	US 2012166970 A1 (AMADEUS S.A.S.) 2012年 6月 28日 (2012 - 06 - 28) 全文	1-55

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 5月 19日

国际检索报告邮寄日期

2016年 6月 16日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

李文娟

传真号 (86-10)62019451

电话号码 (86-10)62413337

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/076879

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	1764116	A	2006年 4月 26日	无			
CN	1592191	A	2005年 3月 9日	TW	200533138	A	2005年 10月 1日
				US	2005044378	A1	2005年 2月 24日
				JP	2005063439	A	2005年 3月 10日
CN	102857361	A	2013年 1月 2日	无			
CN	102196003	A	2011年 9月 21日	无			
US	2012166970	A1	2012年 6月 28日	AU	2011351386	A1	2013年 5月 2日
				EP	2472452	A1	2012年 7月 4日
				KR	20140016259	A	2014年 2月 7日
				CA	2821373	A1	2012年 7月 5日
				WO	2012089750	A1	2012年 7月 5日
				SG	191387	A1	2013年 8月 30日
				JP	2014506359	A	2014年 3月 13日
				CN	103282922	A	2013年 9月 4日
				ZA	201304525	A	2014年 3月 26日

表 PCT/ISA/210 (同族专利附件) (2009年7月)