(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114760138 B
(45)授权公告日 2024.02.13

(21)申请号 202210415537.9
(22)申请日 2022.04.20
(65)同一申请的已公布的文献号
申请公布号 CN 114760138 A
(43)申请公布日 2022.07.15
(73)专利权人 深圳市昊洋智能有限公司
地址 518101 广东省深圳市新安街道兴东社区67区高新奇厂房5层F02
(72)发明人 王小飞 鄢巍
(74)专利代理机构 深圳市沃德知识产权代理事务所(普通合伙) 44347
专利代理师 高杰 于志光
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04N 7/15(2006.01)

(56)对比文件
CN 101069402 A,2007.11.07
CN 103415008 A,2013.11.27
CN 105391734 A,2016.03.09
CN 110011950 A,2019.07.12
CN 112822675 A,2021.05.18
US 10826895 B1,2020.11.03
CN 109802941 A,2019.05.24
CN 102164079 A,2011.08.24
CN 103139146 A,2013.06.05
CN 109714176 A,2019.05.03
CN 111065097 A,2020.04.24
CN 109302425 A,2019.02.01
US 2017346851 A1,2017.11.30
娄悦.基于强认证技术的VoIP系统的研究与实现.中国知网硕士电子期刊.2007,(第2007年第06期),全文. (续)

审查员 冯晓晓

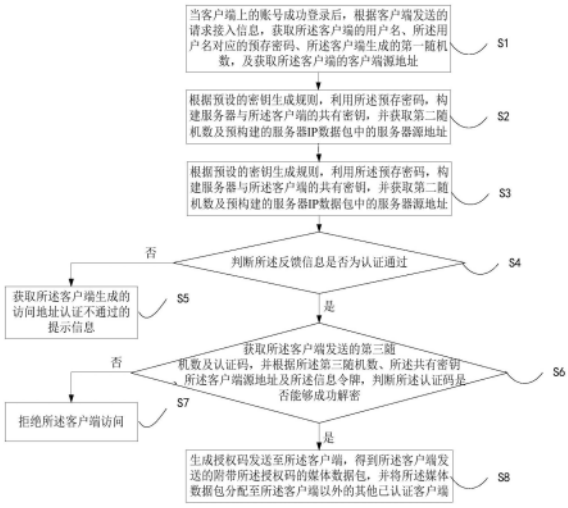
权利要求书3页 说明书10页 附图3页

(54)发明名称

基于云架构下的视频会议系统安全方法及装置

(57)摘要

本发明涉及云传输技术领域,提出一种基于云架构下的视频会议系统安全方法,包括:获取客户端的用户名、预存密码、第一随机数、客户端源地址;根据密钥生成规则,利用预存密码,构建共有密钥;对用户名、共有密钥、第一随机数、预构建的第二随机数及服务器源地址进行摘要认证,得到信息令牌,将信息令牌及第二随机数发送至客户端中,得到客户端的反馈信息,当反馈信息为认证无误时,获取客户端发送的第三随机数及认证码,并根据第三随机数、共有密钥、客户端源地址及信息令牌,判断认证码是否能够成功解密,当解密成果时,发送授权码至客户端,将所述客户端的媒体数据包分配至各个其他已认证客户端。本发明可以提高视频会议的安全性及互通效率。



CN 114760138 B

[转续页]

[接上页]

(56)对比文件

J. Wu, G. Ren and X. Li.Source Address Validation: Architecture and Protocol Design.2007 IEEE International Conference on Network Protocols.2007,全文.

刘鞭箭,陈相宁,李明久,赵宁.视频会议系统的安全分析与措施.武汉理工大学学报(信息与管理工程版).2005,(第03期),全文.

1.一种基于云架构下的视频会议系统安全方法,其特征在于,所述方法包括:

当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

当所述反馈信息为服务器源地址认证无误时,获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密,其中,所述认证码涉及所述用户名、共有秘钥、第二随机数、第三随机数和客户端源地址;

当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

2.如权利要求1所述的基于云架构下的视频会议系统安全方法,其特征在于,所述根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密,包括:

利用MD5算法,根据所述第三随机数、所述共有密钥及所述信息令牌,对所述认证码进行对称解密操作,得到解密源地址;

判断所述解密源地址是否与所述客户端源地址对应;

当所述解密源地址与所述客户端源地址对应,判定所述认证码成功解密;

当所述解密源地址未与所述客户端源地址对应,判定所述认证码未成功解密。

3.如权利要求1所述的基于云架构下的视频会议系统安全方法,其特征在于,所述根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,包括:

从预构建的种子数据库中查询所述预存密码对应的种子数据;

调取所述服务器的时间戳数据,并根据预设加密类别,对所述时间戳数据及所述种子数据进行的加密计算,得到共有密钥。

4.如权利要求1所述的基于云架构下的视频会议系统安全方法,其特征在于,所述将所述媒体数据包分配至所述客户端以外的其他已认证客户端,包括:

利用所述服务器中的网守,将所述媒体数据包进行编码,得到数据流;

获取所述媒体数据包中的设备信息及SIP信令;

利用所述服务器中的会议控制中心收集所述数据流,并根据所述会议控制中心中各个客户端的设备信息及SIP信令关系,将所述数据流分配至所述客户端以外的已认证客户端。

5.如权利要求1所述的基于云架构下的视频会议系统安全方法,其特征在于,所述客户端上的账号成功登录之前,所述方法还包括:

当检测到所述客户端访问所述服务器时,对所述客户端进行网关重定向至预设登录界面;

获取用户输入的账号及密码,并对所述账号及所述密码进行注册查询,得到是否成功登录的提示信息。

6.如权利要求1所述的基于云架构下的视频会议系统安全方法,其特征在于,所述获取所述客户端的客户端源地址之前,所述方法还包括:

利用预设的源地址认证服务,判断所述客户端与所述客户端源地址是否对应;

当所述客户端与所述客户端源地址不对应,拒绝所述客户端访问所述服务器;

当所述客户端与所述客户端源地址对应,则获取所述客户端的客户端源地址。

7.一种基于云架构下的视频会议系统安全装置,其特征在于,所述装置包括:

客户端数据获取模块,用于当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

共有密钥生成模块,用于根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

初级认证模块,用于对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

二级认证模块,用于当所述反馈信息为服务器源地址认证无误时,获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密,其中,所述认证码涉及所述用户名、共有秘钥、第二随机数、第三随机数和客户端源地址;

媒体数据传输模块,用于当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

8.如权利要求7所述的基于云架构下的视频会议系统安全装置,其特征在于,所述根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密,包括:

利用MD5算法,根据所述第三随机数、所述共有密钥及所述信息令牌,对所述认证码进行对称解密操作,得到解密源地址;

判断所述解密源地址是否与所述客户端源地址对应;

当所述解密源地址与所述客户端源地址对应,判定所述认证码成功解密;

当所述解密源地址未与所述客户端源地址对应,判定所述认证码未成功解密。

9.一种电子设备,其特征在于,所述电子设备包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的计算机程序,所述计算机程序被所述至少一个处理器执行,以使所述至少一个处理器能够执行如权利要求1至6中任意一项所述的基于云架构下的视频会议系统安全方法。

10.一种计算机可读存储介质,存储有计算机程序,其特征在于,所述计算机程序被处

理器执行时实现如权利要求1至6中任意一项所述的基于云架构下的视频会议系统安全方法。

基于云架构下的视频会议系统安全方法及装置

技术领域

[0001] 本发明涉及云传输技术领域,特别涉及一种基于云架构下的视频会议系统安全方法、装置。

背景技术

[0002] 随着网络技术的进步,视频会议逐渐兴起,目前受限于传统的基于E1专线的视频会议的专网成本问题,无法满足人们对多地多用户、随时开始会议的需求,视频会议逐渐转变为基于IP的云端视频会议方法。

[0003] 然而,随着时间的发展,基于IP的云端视频会议方法直接接入云架构的互联网中,暴露的网络安全问题日益严重,目前的会话注册方法主要是所述服务器单侧认证客户端的方法,当服务器认证客户端的信令通过时,则将所述客户端接入视频会议。基于这种情况,非法网络用户会通过伪造源地址的方式充当客户端与服务器的中间人,获取各个信令信息,当服务器认证客户端后,中间人会取代所述客户端,进而潜伏至视频会议中,从而造成网络破坏、泄露及监听的风险,因此,目前需要一种更加有效的安全有效的注册会话的方法,使得会议数据更加安全。

发明内容

[0004] 本发明实施方式的目的在于提供一种基于云架构下的视频会议系统安全方法、装置,其目的在于通过增强信令的可靠性,提高云架构下视频会议的安全性。

[0005] 为解决上述技术问题,本发明的实施方式提供了一种基于云架构下的视频会议系统安全方法,所述方法包括:

[0006] 当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

[0007] 根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

[0008] 对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

[0009] 当所述反馈信息为服务器源地址认证无误时,获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密;

[0010] 当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

[0011] 可选的,所述根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息

令牌,判断所述认证码是否能够成功解密,包括:

[0012] 利用MD5算法,根据所述第三随机数、所述共有密钥及所述信息令牌,对所述认证码进行对称解密操作,得到解密源地址;

[0013] 判断所述解密源地址是否与所述客户端源地址对应;

[0014] 当所述解密源地址与所述客户端源地址对应,判定所述认证码成功解密;

[0015] 当所述解密源地址未与所述客户端源地址对应,判定所述认证码未成功解密。

[0016] 可选的,所述根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,包括:

[0017] 从预构建的种子数据库中查询所述预存密码对应的种子数据;

[0018] 调取所述服务器的时间戳数据,并根据预设加密类别,对所述时间戳数据及所述种子数据进行的加密计算,得到共有密钥。

[0019] 可选的,所述将所述媒体数据包分配至所述客户端以外的其他已认证客户端,包括:

[0020] 利用所述服务器中的网守,将所述媒体数据包进行编码,得到数据流;

[0021] 获取所述媒体数据包中的设备信息及SIP信令;

[0022] 利用所述服务器中的会议控制中心收集所述数据流,并根据所述会议控制中心中各个客户端的设备信息及SIP信令关系,将所述数据流分配至所述客户端以外的已认证客户端。

[0023] 可选的,所述当客户端上的账号成功登录后之前,所述方法还包括:

[0024] 当检测到所述客户端访问所述服务器时,对所述客户端进行网关重定向至预设登录界面;

[0025] 获取用户输入的账号及密码,并对所述账号及所述密码进行注册查询,得到是否成功登录的提示信息。

[0026] 可选的,所述获取所述客户端的客户端源地址之前,所述方法还包括:

[0027] 利用预设的源地址认证服务,判断所述客户端与所述客户端源地址是否对应;

[0028] 当所述客户端与所述客户端源地址不对应,拒绝所述客户端访问所述服务器;

[0029] 当所述客户端与所述客户端源地址对应,则获取所述客户端的客户端源地址。

[0030] 为了解决上述问题,本发明还提供一种基于人脸识别的多模态语音交互方法装置,所述装置包括:

[0031] 客户端数据获取模块,用于当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

[0032] 共有密钥生成模块,用于根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

[0033] 初级认证模块,用于对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

[0034] 二级认证模块,用于当所述反馈信息为服务器源地址认证无误时,获取所述客户

端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密;

[0035] 媒体数据传输模块,用于当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

[0036] 为了解决上述问题,本发明还提供一种电子设备,所述电子设备包括:

[0037] 至少一个处理器;以及,

[0038] 与所述至少一个处理器通信连接的存储器;其中,

[0039] 所述存储器存储有可被所述至少一个处理器执行的计算机程序,所述计算机程序被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述所述的基于云架构下的视频会议系统安全方法。

[0040] 为了解决上述问题,本发明还提供一种计算机可读存储介质,所述计算机可读存储介质中存储有至少一个计算机程序,所述至少一个计算机程序被电子设备中的处理器执行以实现上述所述的基于云架构下的视频会议系统安全方法。

[0041] 本发明实施例中,当检测到客户端发送请求接入信息时,获取客户端的用户名及客户端源地址,并根据所述用户名查询所述用户名对应的预存密码,并根据所述预存密码制定共有密钥,其中,所述服务器及客户端中预先存有所述共有密码的生成方式,有利于通过共有密钥对认证的过程进行加密,此外,本发明实施例将所述客户端源地址导入传统信令认证过程中实现信令增强,其中,信令增强是指客户端先验证服务器的服务器源地址,然后服务器再认证客户端的认证码,通过两次认证,避免了中间人伪造源地址潜伏至客户端及服务器之间的情况,增加了视频会议的安全性。因此,本发明实施例中所述的基于云架构下的视频会议系统安全方法、装置,能提高云架构下视频会议的安全性。

附图说明

[0042] 图1为本发明一实施例提供的基于云架构下的视频会议系统安全的流程示意图;

[0043] 图2为本发明一实施例提供的基于云架构下的视频会议系统安全的其中一个步骤的详细流程示意图;

[0044] 图3为本发明一实施例提供的基于云架构下的视频会议系统安全设备间合作运行的流程示意图;

[0045] 图4为本发明一实施例提供的基于云架构下的视频会议系统安全装置的模块示意图;

[0046] 图5为本发明一实施例提供的基于云架构下的视频会议系统安全方法的电子设备的结构示意图。

[0047] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

具体实施方式

[0048] 应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0049] 本发明提供一种基于云架构下的视频会议系统安全的方法,应用于基于国际标准H.323下的SIPPING框架下的注册会话过程。其中,所述SIPPING框架为目前常见的云架构的

视频会议的管理框架,此处不加以赘述。参照图1所示,为本发明一实施例提供的基于云架构下的视频会议系统安全的流程示意图。该方法可以由一个装置执行,该装置可以由软件和/或硬件实现。

[0050] 在本实施例中,所述基于云架构下的视频会议系统安全方法包括:

[0051] S1、当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址。

[0052] 当客户端上的账号登录成功后,可以根据已登录的账号,将所述客户端与所述服务器构建有效链接,并根据所述有效链接,获取所述客户端中的部分数据,例如,客户端发送的视频会议的请求接入信息等。

[0053] 当所述服务器检测到所述请求接入信息时,可以解析所述请求接入信息,从而获取客户端中已登录状态的用户名,并获取所述客户端中随机生成的第一随机数。然后,再根据所述服务器中预构建的用户信息管理数据库,查询所述用户名对应的预存密码。其中,所述用户信息管理数据库是用于存储用户注册账号时的账号信息数据的数据库。

[0054] 进一步的,本发明实施例中为增强注册会话过程中的信令信息,还需获取所述客户端的客户端源地址,但为增强所述客户端源地址及所述客户端的一致性,本发明实施例中,所述客户端的客户端源地址之前,所述方法还包括:

[0055] 利用预设的源地址认证服务,判断所述客户端与所述客户端源地址是否对应;

[0056] 当所述客户端与所述客户端源地址不对应,拒绝所述客户端访问所述服务器;

[0057] 当所述客户端与所述客户端源地址对应,则获取所述客户端的客户端源地址。

[0058] 具体的,所述源地址认证服务(Source Address Validation Architecture,简称SAVA)是一种分层的体系结构,分别为接入网络的、自治域(Autonomous System,AS)内的、跨AS的源地址验证三个方面,使得保证所述客户端源地址是与所述客户端准确对应的。

[0059] 本发明实施例中,所述客户端源地址用于对传统信令认证的增强,因此要求所述客户端源地址必须准确,当所述客户端与所述客户端源地址不对应,拒绝所述客户端访问所述服务器,当所述客户端与所述客户端源地址对应,则获取所述客户端的客户端源地址。

[0060] 此外,本发明实施例中,所述客户端上的账号成功登录之前,所述方法还包括:

[0061] 当检测到所述客户端访问所述服务器时,对所述客户端进行网关重定向至预设登录界面;

[0062] 获取用户输入的账号及密码,并对所述账号及所述密码进行注册查询,得到是否成功登录的提示信息。

[0063] 具体的,本发明实施例中,所述服务器检测到客户端访问时,发送一个阈值信息给所述客户端,使得所述客户端的前端界面重定向至一个登录账号密码的界面,从而获取用户输入的账号密码。然后,将获取到的账号密码与所述用户信息管理数据库中进行核验,当核验通过后,则可以请求视频会议接入,反之,则拒绝所述客户端访问,并向所述客户端发送未成功登录的提示信息。

[0064] S2、根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址。

[0065] 详细的,参考图2所示,本发明实施例中,所述根据预设的密钥生成规则,利用所述

预存密码,构建服务器与所述客户端的共有密钥,包括:

[0066] S21、从预构建的种子数据库中查询所述预存密码对应的种子数据;

[0067] S22、调取所述服务器的时间戳数据,并根据预设加密类别,对所述时间戳数据及所述种子数据进行的加密计算,得到共有密钥。

[0068] 其中,所述种子数据可以为一组初始数据,某些应用程序(或模块),可能需要有所述种子数据才能够正常启动和运行,例如,管理员用户和角色必须在一开始就已经构建,否则就无法创建新用户和角色。

[0069] 本发明实施例中,本发明实施例通过查询所述预存密码对应的种子数据,再从服务器系统中获取系统的时间戳数据,通过任意的一种加密方式,如乘积、相加等方式,将所述种子数据与所述时间戳数据进行加密处理,即可获得共有密钥,其中,此前用户在进行账号注册时,即可分配一个可用而不可视的种子数据,并且客户端与所述服务器默认共用一套加密方式,使得客户端与所述服务器不需要发送密钥信息,即可使用同一个密钥,增加数据传输的安全性。

[0070] 进一步的,本发明实施例在所述服务器中随机生成一个第二随机数,并从服务器中的服务器IP数据包中调取服务器源地址,用于后续的信令验证过程。

[0071] S3、对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息。

[0072] 本发明实施例中,将所述用户名UN(Username),将所述共有密钥SK(Shared key)、第一随机数RN1(Random Number 1)、第二随机数RN2、服务器源地址IPS(IPServer)进行基于MD5的摘要认证计算,得到信息令牌IT(Information Token):

[0073] IT=UN|SK|RN1|RN1|RN2|IPS

[0074] 其中,“|”符号用于隔开组成所述信息信令的各种参数,所述MD5的摘要认证方法为一种对称加密算法,客户端可根据所述SK等信息对所述IT进行解密得到所述IPS,其中,所述MD5的摘要认证方法是一种被广泛使用的密码散列函数,可以产生出一个128位(16字节)的散列值(Hash Value,HV),用于确保信息传输完整一致,具体加密过程不加以赘述。

[0075] 当得到所述IT后,本发明实施例,将所述IT、RN2包装为非授权应答信息发送至所述客户端,客户端可以通过对称解密得到所述服务器源地址,通过第三方认证服务,判断所述服务器源地址是否合格,进而得到客户端的反馈信息(包括,通过及未通过)。

[0076] 进一步的,S4、判断所述反馈信息是否为认证通过;

[0077] 当所述反馈信息为服务器源地址认证不通过时,S5、获取所述客户端生成的访问地址认证不通过的提示信息。

[0078] 当所述反馈信息为服务器源地址认证无误时,S6、获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密。

[0079] 本发明实施例中,客户端随机产生的第三随机数为RN3,所述认证码AC(Authentication Code)为涉及(UN|SK|RN2|RN3|IPA),其中,所述IPA为客户端的客户端源地址IPagent。

[0080] 详细的,参考图3所示,本发明实施例中,所述根据所述第三随机数、所述共有密

钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密,包括:

[0081] S61、利用MD5算法,根据所述第三随机数、所述共有密钥及所述信息令牌,对所述认证码进行对称解密操作,得到解密源地址;

[0082] S62、判断所述解密源地址是否与所述客户端源地址对应;

[0083] 当所述解密源地址与所述客户端源地址对应,S63、判定所述认证码成功解密;

[0084] 当所述解密源地址未与所述客户端源地址对应,S64、判定所述认证码未成功解密。

[0085] 参考上述步骤S3中的内容,本发明实施例在所述服务器与所述客户端中均进行一次添加了源地址信息的预设的注册协议中制定的认证方法,其中,所述注册协议与国家或行业规则中制定的规则相关,而具体得加解密认证过程此处不加以赘述。

[0086] 当所述认证码未成功解密时,S7、拒绝所述客户端访问;

[0087] 当所述认证码成功解密时,S8、生成授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

[0088] 其中,所述授权码是指允许客户传输媒体数据的令牌,本发明实施例的服务器,根据所述SIPPING架构中注册协议的授权生成方法,得到授权码,并将所述授权码发送给客户端。

[0089] 详细的,本发明实施例中,所述将所述媒体数据包分配至所述客户端以外的其他已认证客户端,包括:

[0090] 利用所述服务器中的网守,将所述媒体数据包进行编码,得到数据流;

[0091] 获取所述媒体数据包中的设备信息及SIP信令;

[0092] 利用所述服务器中的会议控制中心收集所述数据流,并根据所述会议控制中心中各个客户端的设备信息及SIP信令关系,将所述数据流分配至所述客户端以外的已认证客户端。

[0093] 其中,所述SIP(Session initialization Protocol)信令关系中包括各个客户端的通话进程、授权码的信息及用户信息等,用于对视频会议的参与方进行管理。

[0094] 其中,所述网守可以给所述国际标准H.323协议下各个的端点,提供地址翻译和PBN接入控制服务,还可以提供带宽管理和网关定位等服务,本发明实施例利用所述网守将所述媒体数据包进行编码处理,转化为数据流,并将所述数据流从本地的客户端上传至云端,其中,所述媒体数据包中还存有各个客户端的设备信息及每个客户端的SIP信令关系,本发明实施例利用所述SIPPING框架下的会议控制中心Focus,根据所述设备信息及所述SIP信令关系,将所述数据流分配至所述客户端以外的已认证客户端。

[0095] 本发明实施例中,当检测到客户端发送请求接入信息时,获取客户端的用户名及客户端源地址,并根据所述用户名查询所述用户名对应的预存密码,并根据所述预存密码制定共有密钥,其中,所述服务器及客户端中预先存有所述共有密码的生成方式,有利于对认证过程进行加密,此外,本发明实施例将所述客户端源地址导入传统信令认证过程中实现信令增强,其中,信令增强是指客户端先验证服务器的服务器源地址,然后服务器再认证客户端的认证码,通过两次认证,避免了中间人伪造源地址潜伏至客户端及服务器之间的情况,增加了视频会议的安全性。因此,本发明实施例中所述的基于云架构下的视频会议系

统安全方法,能提高云架构下视频会议的安全性。

[0096] 如图4所示,是本发明基于云架构下的视频会议系统安全装置的模块示意图。

[0097] 本发明所述基于云架构下的视频会议系统安全装置100可以安装于电子设备中。根据实现的功能,所述基于云架构下的视频会议系统安全装置100可以包括客户端数据获取模块101、共有密钥生成模块102、初级认证模块103、二级认证模块104及媒体数据传输模块105。本发所述模块也可以称之为单元,是指一种能够被电子设备处理器所执行,并且能够完成固定功能的一系列计算机程序段,其存储在电子设备的存储器中。

[0098] 在本实施例中,关于各模块/单元的功能如下:

[0099] 所述客户端数据获取模块101,用于当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

[0100] 所述共有密钥生成模块102,用于根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

[0101] 所述初级认证模块103,用于对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

[0102] 所述二级认证模块104,用于当所述反馈信息为服务器源地址认证无误时,获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密;

[0103] 所述媒体数据传输模块105,用于当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

[0104] 详细地,本申请实施例中所述基于云架构下的视频会议系统安全装置100中所述的各模块在使用时采用与上述图1至图3中所述的基于云架构下的视频会议系统安全方法一样的技术手段,并能够产生相同的技术效果,这里不再赘述。

[0105] 如图5所示,是本发明实现基于云架构下的视频会议系统安全方法的电子设备的结构示意图。

[0106] 所述电子设备1可以包括处理器10、存储器11和总线,还可以包括存储在所述存储器11中并可在所述处理器10上运行的计算机程序,如基于云架构下的视频会议系统安全程序12。

[0107] 其中,所述存储器11至少包括一种类型的可读存储介质,所述可读存储介质包括闪存、移动硬盘、多媒体卡、卡型存储器(例如:SD或DX存储器等)、磁性存储器、磁盘、光盘等。所述存储器11在一些实施例中可以是电子设备1的内部存储单元,例如该电子设备1的移动硬盘。所述存储器11在另一些实施例中也可以是电子设备1的外部存储设备,例如电子设备1上配备的插接式移动硬盘、智能存储卡(Smart Media Card,SMC)、安全数字(Secure Digital,SD)卡、闪存卡(Flash Card)等。进一步地,所述存储器11还可以既包括电子设备1的内部存储单元也包括外部存储设备。所述存储器11不仅可以用于存储安装于电子设备1的应用软件及各类数据,例如基于云架构下的视频会议系统安全程序12的代码等,还可以

用于暂时地存储已经输出或者将要输出的数据。

[0108] 所述处理器10在一些实施例中可以由集成电路组成,例如可以由单个封装的集成电路所组成,也可以是由多个相同功能或不同功能封装的集成电路所组成,包括一个或者多个中央处理器(Central Processing unit,CPU)、微处理器、数字处理芯片、图形处理器及各种控制芯片的组合等。所述处理器10是所述电子设备的控制核心(Control Unit),利用各种接口和线路连接整个电子设备的各个部件,通过运行或执行存储在所述存储器11内的程序或者模块(例如执行基于云架构下的视频会议系统安全程序等),以及调用存储在所述存储器11内的数据,以执行电子设备1的各种功能和处理数据。

[0109] 所述总线可以是外设部件互连标准(peripheral component interconnect,简称PCI)总线或扩展工业标准结构(extended industry standard architecture,简称EISA)总线等。该总线可以分为地址总线、数据总线、控制总线等。所述总线被设置为实现所述存储器11以及至少一个处理器10等之间的连接通信。

[0110] 图5仅示出了具有部件的电子设备,本领域技术人员可以理解的是,图5示出的结构并不构成对所述电子设备1的限定,可以包括比图示更少或者更多的部件,或者组合某些部件,或者不同的部件布置。

[0111] 例如,尽管未示出,所述电子设备1还可以包括给各个部件供电的电源(比如电池),优选地,电源可以通过电源管理装置与所述至少一个处理器10逻辑相连,从而通过电源管理装置实现充电管理、放电管理、以及功耗管理等功能。电源还可以包括一个或一个以上的直流或交流电源、再充电装置、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。所述电子设备1还可以包括多种传感器、蓝牙模块、Wi-Fi模块等,在此不再赘述。

[0112] 进一步地,所述电子设备1还可以包括网络接口,可选地,所述网络接口可以包括有线接口和/或无线接口(如WI-FI接口、蓝牙接口等),通常用于在该电子设备1与其他电子设备之间建立通信连接。

[0113] 可选地,该电子设备1还可以包括用户接口,用户接口可以是显示器(Display)、输入单元(比如键盘(Keyboard)),可选地,用户接口还可以是标准的有线接口、无线接口。可选地,在一些实施例中,显示器可以是LED显示器、液晶显示器、触控式液晶显示器以及OLED(Organic Light-Emitting Diode,有机发光二极管)触摸器等。其中,显示器也可以适当的称为显示屏或显示单元,用于显示在电子设备1中处理的信息以及用于显示可视化的用户界面。

[0114] 应该了解,所述实施例仅为说明之用,在专利申请范围上并不受此结构的限制。

[0115] 所述电子设备1中的所述存储器11存储的基于云架构下的视频会议系统安全程序12是多个指令的组合,在所述处理器10中运行时,可以实现:

[0116] 当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

[0117] 根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

[0118] 对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源

地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

[0119] 当所述反馈信息为服务器源地址认证无误时,获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密;

[0120] 当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

[0121] 进一步地,所述电子设备1集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。所述计算机可读介质可以包括:能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM,Read-Only Memory)。

[0122] 进一步地,所述计算机可用存储介质可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序等;存储数据区可存储根据区块链节点的使用所创建的数据等。

[0123] 本发明还提供一种计算机可读存储介质,所述可读存储介质存储有计算机程序,所述计算机程序在被电子设备的处理器所执行时,可以实现:

[0124] 当客户端上的账号成功登录后,根据客户端发送的请求接入信息,获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数,及获取所述客户端的客户端源地址;

[0125] 根据预设的密钥生成规则,利用所述预存密码,构建服务器与所述客户端的共有密钥,并获取第二随机数及预构建的服务器IP数据包中的服务器源地址;

[0126] 对所述用户名、所述共有密钥、所述第一随机数、所述第二随机数及所述服务器源地址进行摘要认证计算,得到信息令牌,并将所述信息令牌及所述第二随机数发送至所述客户端中,得到所述客户端的反馈信息;

[0127] 当所述反馈信息为服务器源地址认证无误时,获取所述客户端发送的第三随机数及认证码,并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌,判断所述认证码是否能够成功解密;

[0128] 当所述认证码成功解密时,根据所述认证码生成授权码,并将所述授权码发送至所述客户端,得到所述客户端发送的附带所述授权码的媒体数据包,并将所述媒体数据包分配至所述客户端以外的其他已认证客户端。

[0129] 在本发明所提供的几个实施例中,应该理解到,所揭露的设备,装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述模块的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式。

[0130] 所述作为分离部件说明的模块可以是或者也可以不是物理上分开的,作为模块显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

[0131] 另外,在本发明各个实施例中的各功能模块可以集成在一个处理单元中,也可以

是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能模块的形式实现。

[0132] 对于本领域技术人员而言,显然本发明不限于上述示范性实施例的细节,而且在不背离本发明的精神或基本特征的情况下,能够以其他的具体形式实现本发明。

[0133] 因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本发明的范围由所附权利要求而不是上述说明限定,因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本发明内。不应将权利要求中的任何附关联图表记视为限制所涉及的权利要求。

[0134] 本发明所指区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain),本质上是一个去中心化的数据库,是一串使用密码学方法相关联产生的数据块,每一个数据块中包含了一批次网络交易的信息,用于验证其信息的有效性(防伪)和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层等。

[0135] 此外,显然“包括”一词不排除其他单元或步骤,单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第二等词语用来表示名称,而并不表示任何特定的顺序。

[0136] 最后应说明的是,以上实施例仅用以说明本发明的技术方案而非限制,尽管参照较佳实施例对本发明进行了详细说明,本领域的普通技术人员应当理解,可以对本发明的技术方案进行修改或等同替换,而不脱离本发明技术方案的精神和范围。

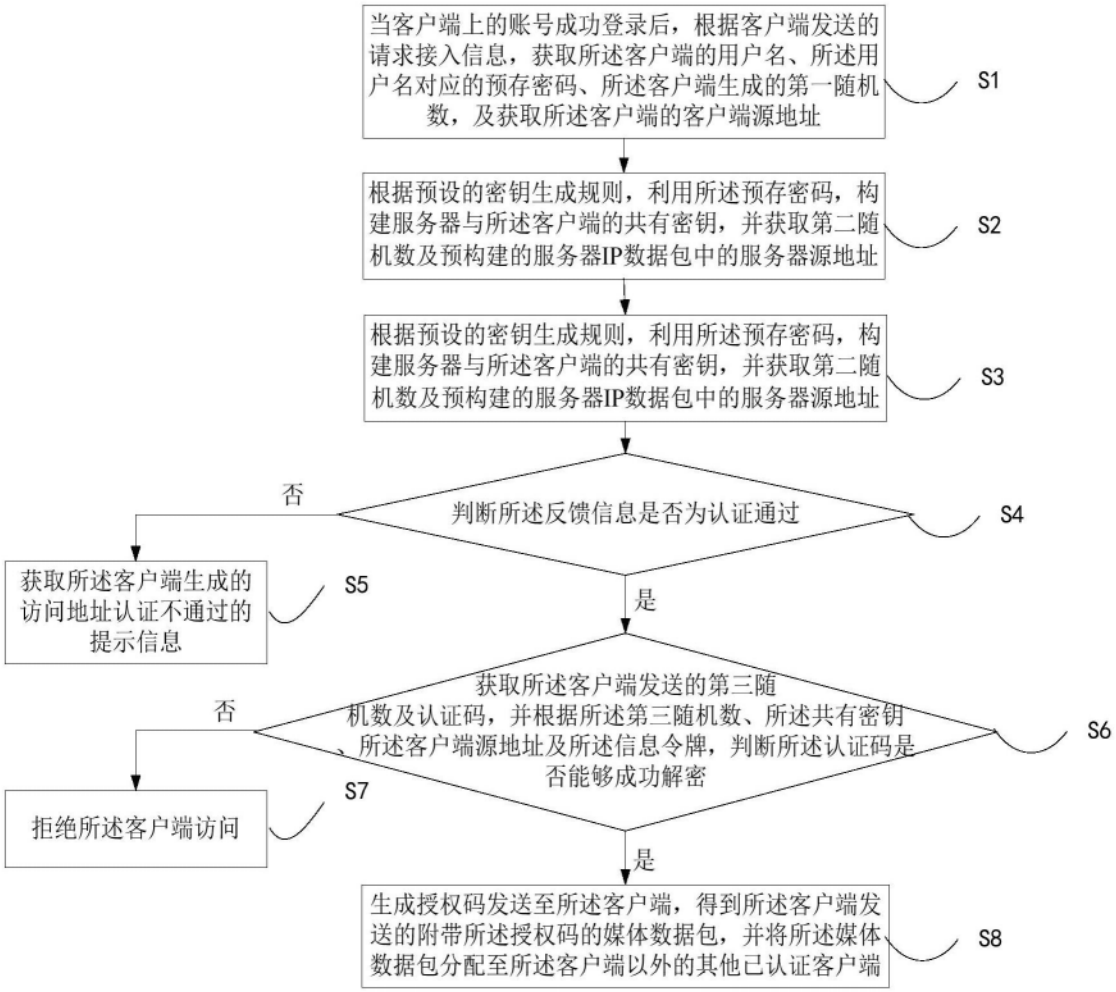

当客户端上的账号成功登录后，根据客户端发送的请求接入信息，获取所述客户端的用户名、所述用户名对应的预存密码、所述客户端生成的第一随机数，及获取所述客户端的客户端源地址
S1
根据预设的密钥生成规则，利用所述预存密码，构建服务器与所述客户端的共有密钥，并获取第二随机数及预构建的服务器IP数据包中的服务器源地址
S2
根据预设的密钥生成规则，利用所述预存密码，构建服务器与所述客户端的共有密钥，并获取第二随机数及预构建的服务器IP数据包中的服务器源地址
S3
判断所述反馈信息是否为认证通过
S4
否
是
获取所述客户端生成的访问地址认证不通过的提示信息
S5
获取所述客户端发送的第三随机数及认证码，并根据所述第三随机数、所述共有密钥、所述客户端源地址及所述信息令牌，判断所述认证码是否能够成功解密
S6
否
是
拒绝所述客户端访问
S7
生成授权码发送至所述客户端，得到所述客户端发送的附带所述授权码的媒体数据包，并将所述媒体数据包分配至所述客户端以外的其他已认证客户端
S8

图1

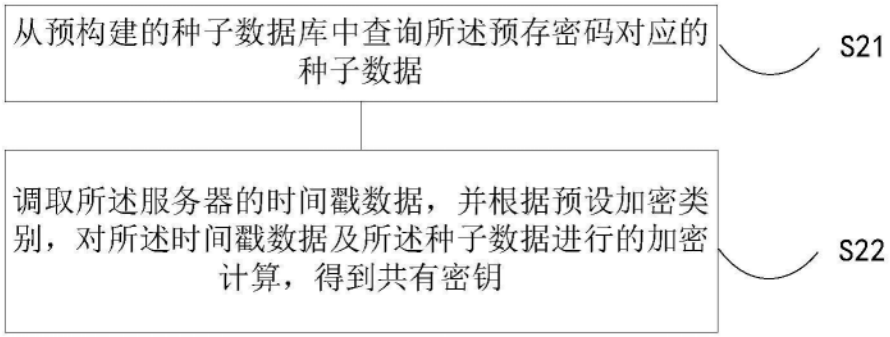

从预构建的种子数据库中查询所述预存密码对应的种子数据
S21
调取所述服务器的时间戳数据，并根据预设加密类别，对所述时间戳数据及所述种子数据进行的加密计算，得到共有密钥
S22

图2

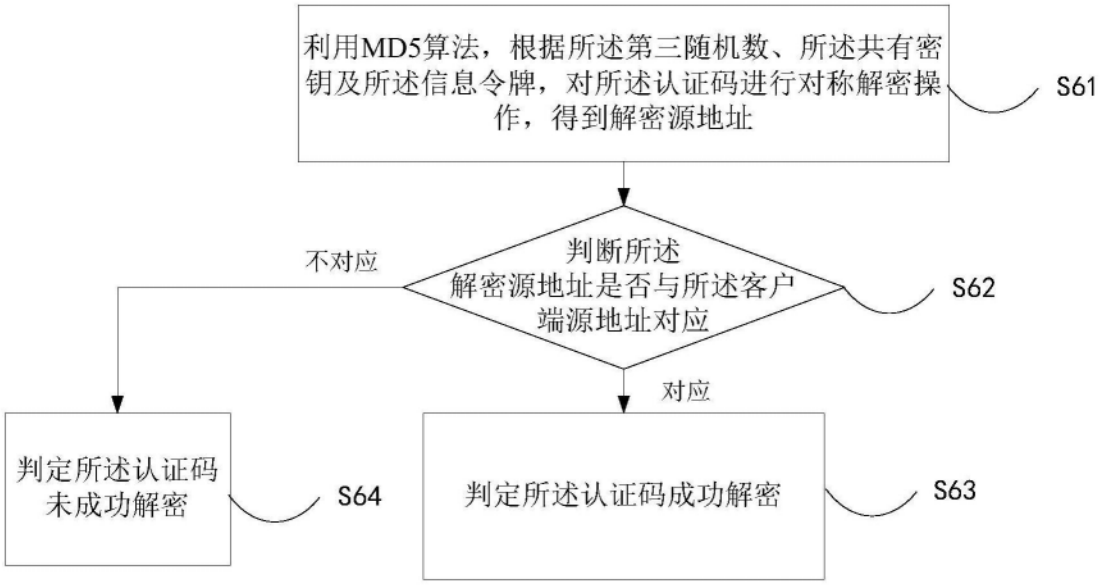

利用MD5算法，根据所述第三随机数、所述共有密钥及所述信息令牌，对所述认证码进行对称解密操作，得到解密源地址
S61
判断所述解密源地址是否与所述客户端源地址对应
S62
不对应
对应
判定所述认证码未成功解密
S64
判定所述认证码成功解密
S63

图3

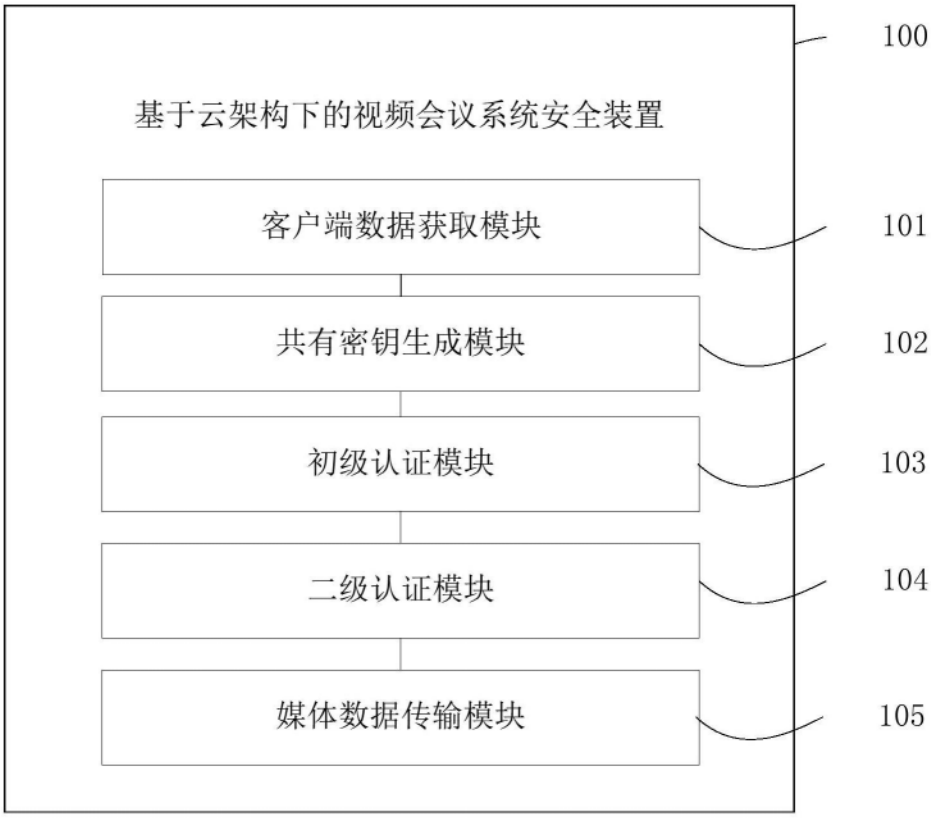

100
基于云架构下的视频会议系统安全装置
客户端数据获取模块
101
共有密钥生成模块
102
初级认证模块
103
二级认证模块
104
媒体数据传输模块
105

图4

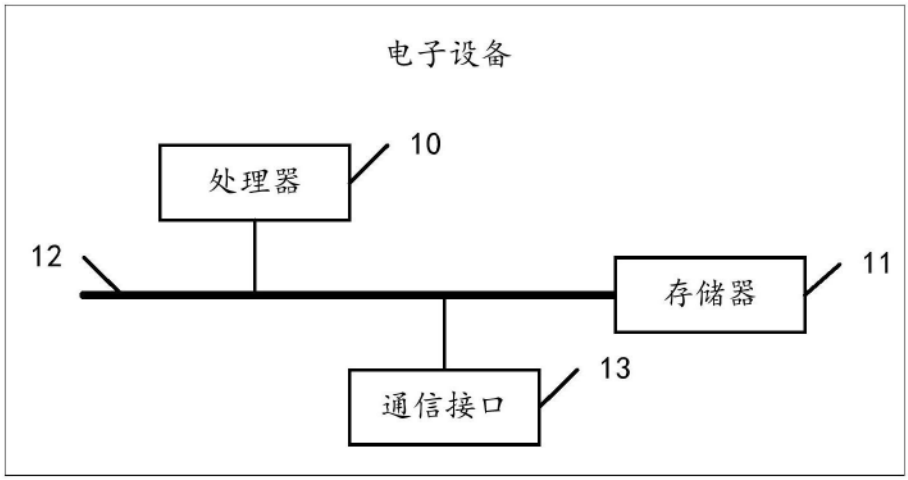


图5