(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114944959 B
(45)授权公告日 2024.07.02

(21)申请号 202210707282.3
(22)申请日 2018.04.04
(65)同一申请的已公布的文献号
申请公布号 CN 114944959 A
(43)申请公布日 2022.08.26
(30)优先权数据
17164869.4 2017.04.04 EP
(62)分案原申请数据
201880023503.7 2018.04.04
(73)专利权人 纳格拉影像有限公司
地址 瑞士舍索-苏尔-洛桑
(72)发明人 米歇尔·安格尔 阿尔夫·勒托罗 安东尼·切莱蒂
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 刘玉洁
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04N 7/18(2006.01)
H04N 21/2347(2011.01)
H04N 21/266(2011.01)
H04N 21/4627(2011.01)
G06F 21/10(2013.01)
G06F 21/00(2013.01)
(56)对比文件
US 2015235011 A1,2015.08.20
US 7508941 B1,2009.03.24
审查员 付苗

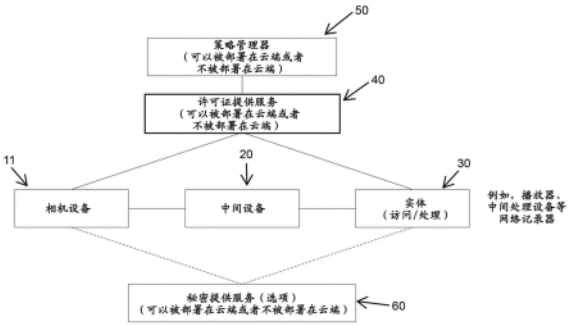
权利要求书2页 说明书6页 附图4页

(54)发明名称

监视媒体的保护

(57)摘要

媒体设备从服务提供商接收域密钥。所述媒体设备还使用媒体密钥对媒体进行加密,并使用所述域密钥对所述媒体密钥进行加密,以形成加密的媒体令牌:将受保护的媒体密钥封装在加密的媒体令牌中。然后,所述服务提供商可以接收加密的媒体令牌和与接收实体有关的一个或多个接收实体标识符,并确定所述接收实体是否有权访问来自所述媒体设备的媒体。如果所述接收实体有权访问来自所述媒体设备的媒体,则所述服务提供商使用所述域密钥来解密加密媒体令牌以获得所述媒体密钥并将所述媒体密钥提供给所述接收实体。这样,认证的接收实体可以获得解密所述媒体所必需的所述媒体密钥。此外,不需要任何中间实体具有类似的访问,因此在媒体从媒体设备到接收实体的整个传输过程中,由所述媒体密钥提供的加密是就位的。



CN 114944959 B

1.一种用于在网络中保护媒体内容的媒体设备,所述媒体设备包括:

密钥接收元件,用于从服务提供商接收域密钥;以及

加密元件,用于用媒体密钥对由所述媒体设备生成的媒体进行加密,并且用所述域密钥对所述媒体密钥进行加密,以形成加密的媒体令牌;

发送元件,用于将加密的媒体发送到接收实体;

其中,所述媒体包括数据分组,每个数据分组在从所述媒体设备传输之前使用所述媒体密钥来加密,如果所述媒体密钥被变更,在预定数目的数据分组之后,使用变更后的媒体密钥对相同媒体流的后续数据分组进行加密。

2.根据权利要求1所述的媒体设备,还包括:

在所述媒体设备处生成所述媒体密钥。

3.根据权利要求1或2所述的媒体设备,其中,所述域密钥与定义所述网络内的一个或多个媒体设备的域相关联。

4.根据权利要求1所述的媒体设备,其中,所述媒体设备用于以使用一个或多个媒体设备标识符加密的形式接收所述域密钥。

5.根据权利要求1所述的媒体设备,其中,所述加密的媒体令牌包括与所述域密钥相关联的元数据。

6.根据权利要求1所述的媒体设备,其中,所述媒体设备用于向接收实体发送所述加密的媒体令牌。

7.根据权利要求1所述的媒体设备,其中,所述媒体密钥周期性地进行变更,并且一旦所述媒体密钥被变更,在预定数目的数据分组之后,使用变更后的媒体密钥对相同媒体流的后续数据分组进行加密。

8.根据权利要求1所述的媒体设备,其中,所述域密钥周期性地进行变更。

9.根据权利要求1所述的媒体设备,其中,所述媒体包括音频和/或视觉内容。

10.根据权利要求1所述的媒体设备,还包括相机。

11.一种在网络中保护媒体内容的服务提供商,所述服务提供商包括:

密钥发送元件,用于发送域密钥到媒体设备;

媒体接收元件,用于接收加密的媒体令牌;

实体标识符接收元件,用于接收与接收实体相关的一个或多个接收实体标识符;

确定元件,用于确定所述接收实体是否有权访问来自所述媒体设备的媒体;以及

解密元件,用于使用域密钥选择性地解密所述加密的媒体令牌,以获得媒体密钥,并向所述接收实体提供所述媒体密钥;其中

仅当所述接收实体有权访问来自所述媒体设备的媒体时,才解密所述加密的媒体令牌。

12.根据权利要求11所述的服务提供商,其中,所述服务提供商用于认证所述接收实体,认证所述接收实体包括确认所述接收实体被授权访问来自在与所述域密钥相关联的所述域内的媒体设备的媒体。

13.根据权利要求11所述的服务提供商,所述服务提供商用于接收来自所述接收实体的所述加密的媒体令牌。

14.根据权利要求11所述的服务提供商,所述服务提供商还用于以使用一个或多个接

收设备标识符加密的形式来接收所述加密的媒体令牌。

15.根据权利要求11所述的服务提供商,所述服务提供商还用于以使用一个或多个接收设备标识符加密的形式向所述接收实体提供所述媒体密钥。

监视媒体的保护

[0001] 本申请是申请日为2018年4月4日、申请号为201880023503.7、发明名称为“监视媒体的保护”的发明专利申请的分案申请。

技术领域

[0002] 本公开涉及由诸如监视设备之类的媒体设备生成的媒体的保护。具体地,但不排他地,本公开涉及确保由监视相机生成的媒体的机密性。

背景技术

[0003] 许多视频监视系统在系统的元件之间传输期间保护所生成的监视媒体内容。例如,在相机生成用于在远程设备处观看的媒体流的情况下,在诸如相机、远程设备和通过其传输媒体流的任何中间设备之间的系统的元件之间的媒体流的传输中强制媒体的机密性。

[0004] 结果,在系统元件之间的安全通信阶段之外,通常不存在保护实施,并且媒体内容实际上是不受保护的、易受攻击的并且可以被公开。具有适当策略管理的访问控制并不总是或较弱地在系统的一个或多个元件上实现,这意味着:在没有有效访问控制或监测的元件中,可以在没有授权的情况下访问未受保护的媒体内容;当在任何元件处的访问控制或监测被黑客攻击或以其他方式绕过时,媒体内容是不受保护的和易受攻击的。

附图说明

[0005] 图1是用于实现优选实施方式的系统的示意图;

[0006] 图2是图1的示意图,其中附加信息表示每个实体处的处理步骤;

[0007] 图3是示出优选实施方式的过程的流程图;以及

[0008] 图4示出了用于实现优选实施方式的硬件基础设施。

具体实施方式

[0009] 概括地说,根据本公开的方法包括利用媒体密钥来保护由媒体设备生成的媒体,以及利用域密钥来保护所述媒体密钥以形成加密的媒体令牌。当接收实体希望访问媒体时,可信服务提供商可以对该接收实体进行认证并解密加密的媒体令牌以获取所述媒体密钥以供所述接收实体使用来解密所述媒体。以这种方式,所述媒体可以由生成它的所述媒体设备保护,而无需随后进行解密,直到所述媒体出现在授权的接收实体处。中间实体不需要能够访问解密的媒体。本公开还提供了一种被配置为执行该方法的计算机可读介质和系统。

[0010] 在本公开的一些方面中,提供了一种用于在网络中保护媒体内容的方法,包括以下步骤:媒体设备从服务提供商接收域密钥。所述媒体设备还使用媒体密钥对媒体进行加密,并使用所述域密钥对所述媒体密钥进行加密,以形成加密的媒体令牌:将受保护的媒体密钥封装在加密的媒体令牌中。然后,所述服务提供商可以接收加密的媒体令牌和与接收实体有关的一个或多个接收实体标识符,并确定所述接收实体是否有权访问来自所述媒体

设备的媒体。如果所述接收实体有权访问来自所述媒体设备的媒体，则所述服务提供商使用所述域密钥来解密加密媒体令牌以获得所述媒体密钥并将所述媒体密钥提供给所述接收实体。这样，认证的接收实体可以获得解密所述媒体所必需的所述媒体密钥。此外，不需要任何中间实体具有类似的访问，因此在媒体从媒体设备到接收实体的整个传输过程中，由所述媒体密钥提供的加密是就位的。

[0011] 在一些实施方式中，在所述媒体设备处生成所述媒体密钥。或者，所述媒体设备可从外部源(例如，所述服务提供商)接收所述媒体密钥。所述媒体密钥可以是例如随机生成的。

[0012] 可选地，所述域密钥与定义网络内的一个或多个媒体设备的域相关联。因此，所述域密钥可以对超过一个的媒体设备是公共的。给定媒体设备可以随时间被添加到域或从域移除，从而允许通过认证接收实体的过程来控制对来自该媒体设备的媒体的访问。接收实体可以在确定所述接收实体是否有权访问来自与所述域密钥相关联的所述域内的媒体设备的媒体的步骤之前被认证。

[0013] 所述媒体设备可以以使用一个或多个媒体设备标识符加密的形式从所述服务提供商接收所述域密钥。以此方式，所述服务提供商可以确保所述域密钥到所述媒体设备的传输的安全性。

[0014] 加密的媒体令牌可以包括与所述域密钥相关联的元数据。在这种情况下，受保护的媒体密钥被封装在具有元数据的加密媒体令牌中。例如，该元数据可以标识与所述域密钥相关联的所述域，或者可以以某种其他方式允许标识所述域密钥。这可以帮助所述服务提供商定位要用于对加密的媒体令牌进行解密的所述域密钥。

[0015] 在一些实施方式中，所述媒体设备向所述接收实体发送加密的媒体令牌，并且所述服务提供商从所述接收实体接收加密的媒体令牌。例如，加密的媒体令牌可以与所述媒体本身一起被发送到所述接收实体。在其他示例中，可以在带外通信中(例如，以与媒体分开的方式)向所述接收实体发送加密的媒体令牌。加密的媒体令牌可以直接从所述媒体设备发送到所述接收实体，或者可以经由一个或多个中间实体发送。

[0016] 所述服务提供商可以以使用一个或多个接收设备标识符加密的形式接收加密的媒体令牌。另选地或附加地，所述服务提供商可以以使用一个或多个接收设备标识符加密的形式向所述接收实体提供所述媒体密钥。该方法可以帮助保护所述接收实体和所述服务提供商之间的通信。

[0017] 媒体密钥和域密钥中的一个或双方可以周期性地改变。以这种方式，可以提高安全性。改变所述媒体密钥或所述域密钥可导致加密媒体令牌的再生。例如，所述媒体流可以包括数据分组，并且每个数据分组可以在从所述媒体设备传输之前使用所述媒体密钥来加密。如果所述媒体密钥被改变，例如，在预定长度时间之后或在预定数目的分组之后，则使用更新的媒体密钥对相同媒体流的后续分组进行加密。

[0018] 媒体可以包括音频和/或视觉内容。所述视觉内容可以包括视频或一个或多个静止图像。所述媒体还可以包括元数据。这样的元数据可以包括例如被设计为警告用户的警报指示。所述媒体可以是流媒体。所述媒体可以由所述媒体设备实时生成。所述媒体设备可以包括相机。例如，所述媒体设备可以是诸如移动监视相机之类的监视相机。例如，所述媒体设备可以是无人机、机器人或可穿戴式相机。所述媒体设备可以是但不限于能够处理或

生成媒体的任何其他设备。

[0019] 在本公开的一些方面,提供了一种包括用于执行上述方面的方法的计算机可执行指令的计算机可读介质。此外,本公开的其他方面提供了一种被配置成执行这些方法的系统。

[0020] 在本公开的一些方面,提供了一种用于在包括媒体设备和服务提供商的网络中保护媒体内容的系统。所述媒体设备被配置为:从所述服务提供商接收域密钥;以及利用媒体密钥对媒体进行加密,并且利用所述域密钥对所述媒体密钥进行加密以形成加密的媒体令牌。所述服务提供商被配置为:接收加密的媒体令牌和与接收实体相关的一个或多个接收实体标识符;确定所述接收实体是否有权访问来自所述媒体设备的媒体;并且,如果所述接收实体有权访问来自所述媒体设备的媒体,则使用所述域密钥来解密加密的媒体令牌以获得所述媒体密钥并将所述媒体密钥提供给所述接收实体。该方法的可选特征也可以应用于该系统。该系统还可以包括所述接收实体。所述接收实体可以被配置为使用从所述服务提供商接收的所述媒体密钥来解密所述媒体。

[0021] 现在参考附图以说明的方式描述一些具体实施方式。

[0022] 参照图1,示出了包括相机设备11、一个或多个中间设备20和接收实体30的系统。相机设备是可以生成要由接收实体30接收的媒体的媒体设备。由相机11生成的媒体可以经由一个或多个中间实体20被发送到接收实体30。

[0023] 相机设备11可以是任何固定或移动监视系统(例如无人机、机器人或可穿戴式设备)的一部分。通常,它可以是能够处理或生成媒体内容的任何设备。中间实体20可以是能够传递网络流量的任何网络元件,而接收实体30可以是用于媒体的回放或处理的任何合适的设备。接收实体30可以位于监视控制室或任何其他期望的位置,并且可以是固定的或便携式的。接收实体30例如可以是网络使能的终端用户设备,诸如膝上型计算机、个人计算机、平板计算机、智能电话等。

[0024] 作为图1的系统的一部分还示出了许可证供应服务40。这充当服务提供商并且可以与策略管理器50通信。还示出了秘密提供服务60,其可以可选地被提供以与相机设备11和接收实体30通信。

[0025] 许可证提供服务40、策略管理器50和秘密提供服务60可以协同地充当服务提供商。它们中的每一个可以实现为基于云端的服务,或者可以实现在定义的物理设备(诸如服务器)上。

[0026] 通常,图1中示出的每个元件可以在一个或多个计算设备上实现,其进一步细节在下面参照图4进行阐述。

[0027] 参照图2和图3可以理解图1的系统的操作。图2示出了图1的系统,其具有标识与下述处理步骤相关联的系统元件内或系统元件之间的通信的附加附图标记。图2中的编号与下面的段落编号“1”到“10”相关联。图3是提供对某些过程步骤的进一步说明并以一种可能的顺序说明这些步骤的流程图。

[0028] 1-在步骤s31,相机11被配置有设备唯一秘密。存在与相机11相关联的一个或多个标识符。这些秘密可以是基于软件或硬件的。如图2中秘密提供服务60的选项1d所示,可以在制造时或越空(over-the-air)预先供应这些秘密。

[0029] 2-相机与一个域相关联。此域可将相机与其覆盖的区域连接或关联。在步骤s32,

可以由许可证提供服务40针对域生成域密钥。在可能发生在相机11的安装期间的步骤s34，以越空方式从许可证提供服务40提供唯一域密钥。当使用可用的设备唯一秘密将该域密钥传输到相机11时，该域密钥被安全地保护。当相机被安装在新区域中或者现有区域被划分为新域时，新的唯一域密钥被提供给相机。

[0030] 3-在步骤s35，相机11可以生成媒体密钥，该媒体密钥用于在步骤s36对由相机生成的媒体进行加密。在步骤s37，使用唯一域密钥来保护该媒体密钥，并且生成加密的媒体令牌。加密的媒体令牌包括受保护的媒体密钥和附加元数据。可以在元数据中记录任何相关信息，诸如标识与相机11相关联的域的信息。由于媒体在相机11内被加密，所以当媒体离开相机11以在其他地方发送时受到保护。例如，在步骤s38，由媒体密钥加密的媒体被发送到接收实体30。如图2所示，该发送可以经由一个或多个中间实体20发生。在步骤s29，加密的媒体令牌也被发送到接收实体30。取决于流传输格式，加密的媒体令牌可以被嵌入在受保护的相机媒体内容中或者利用带外信道来进行发送。

[0031] 4-在步骤s33，接收实体30可以被配置有实体唯一秘密。这些实体唯一秘密用作与接收实体相关联的一个或多个标识符。秘密可以是基于软件或硬件的。如图1中的秘密提供服务60的选项1d所示，可以在制造时或越空地预供应这些秘密。

[0032] 5-在上述步骤s39之后，接收实体已经从相机11接收到加密的媒体令牌。如果需要，接收实体可以从媒体流中提取该令牌。在一些替代方案中，接收实体将从带外信道获得该令牌。然后，在步骤s40，接收实体30将加密的媒体令牌提供给许可证提供服务40。加密的媒体令牌是以用实体唯一秘密保护的密码质询的形式提供的。该密码质询用于认证接收实体30。

[0033] 6-许可证提供服务40验证在先前步骤5中认证接收实体30的密码质询，并提取加密的媒体令牌。许可证提供服务40从封装在加密的媒体令牌中的元数据识别出域。然后，许可证提供服务40可以确认接收实体是否被授权访问来自相机11的媒体。如果接收实体30被策略管理器50授权访问该域，则在步骤s41，许可证提供服务40使用域密钥从加密的媒体令牌提取媒体密钥。然后，许可证提供服务40生成用相关使用规则封装媒体密钥的加密的实体令牌。使用接收实体30已知的实体唯一秘密而不是接收实体30未知的域密钥来保护加密的实体令牌，并且在步骤s42将加密的实体令牌提供回接收实体30。

[0034] 7-然后，接收实体30验证从许可证提供服务40接收的加密实体令牌。然后，在步骤s43，接收实体30可以提取媒体密钥，并且因此可以根据相关使用规则来解密受保护的相机媒体内容。所得到的未受保护的相机媒体内容可以由接收实体访问和/或处理。

[0035] 8-作为一个选项，且为了提高对相机媒体内容的保护，可以定期更改媒体密钥。例如，媒体流可以包括数据分组，并且在从相机11发送之前使用媒体密钥对每个数据分组进行加密。如果所述媒体密钥被改变，例如，在预定长度时间之后或在预定数目的分组之后，使用更新的媒体密钥对相同媒体流的后续分组进行加密。在这种情况下，必须针对每次媒体密钥变更重新生成加密的媒体令牌，并将其再次发送到接收实体30。该方法可以通过要求使用重新生成的加密媒体令牌对接收实体进行重新认证，来帮助确保接收实体和服务提供商之间的通信，即使接收实体最初被授权对媒体流进行解密。

[0036] 9-类似地，出于同样的原因，可以定期更改域密钥。在这种情况下，必须针对每个域密钥变更生成新的媒体密钥和新的加密媒体令牌，并将其再次发送到接收实体30。

[0037] 10-由于所提出的相机媒体内容保护方案保留了内容格式的属性,因此未被授权访问未受保护的相机媒体内容的任何中间实体仍可以在没有隐私问题的情况下记录受保护的相机媒体内容。该记录的相机媒体内容可以在任何地方进行复制而没有隐私问题;该相机媒体内容保持受保护并且访问该相机媒体内容需要认证需要访问或处理相机媒体内容的实体以及如5、6和7中所述的由许可证提供服务40进行的验证。

[0038] 该过程可以唯一地保护来自相机11或其他媒体设备的内容,并且提供对媒体的保护,而与诸如处理链中所涉及的中间设备20之类的设备的数量无关。

[0039] 图4示出计算设备300的一个实施方案的框图,其中可执行用于使得计算设备执行本文所论述的方法中的任何一种或多种的指令集。计算设备300可以用于图1和图2所示的系统的元件。在另选的实现中,计算设备可以连接(例如,联网)到局域网(LAN)、内联网、外联网或因特网中的其他机器。计算设备可以在客户端-服务器网络环境中以服务器或客户端机器的能力来操作,或者作为对等(或分布式)网络环境中的对等机器来操作。计算设备可以是个人计算机(PC)、平板计算机、机顶盒(STB)、个人数字助理(PDA)、蜂窝电话、网络设备、服务器、网络路由器、开关或桥接器、或能够执行指定该机器要采取的动作的指令集(顺序或其他)的任何机器。此外,虽然仅示出了单个计算设备,但是术语“计算设备”还应被理解为包括单独地或联合地执行指令集(或多个指令集)以执行本文所讨论的任何一个或多个方法的机器(例如,计算机)的任何集合。

[0040] 示例性计算设备300包括经由总线330彼此通信的处理设备302、主存储器304(例如,只读存储器(ROM)、闪速存储器、诸如同步DRAM(SDRAM)或Rambus DRAM(RDRAM)等的动态随机存取存储器(DRAM)等)、静态存储器306(例如,闪速存储器、静态随机存取存储器(SRAM)等),以及辅助存储器(例如,数据存储设备318)。

[0041] 处理设备302表示一个或多个通用处理器,诸如微处理器、中央处理单元等。更具体地,处理设备302可以是复杂指令集计算(CISC)微处理器、精简指令集计算(RISC)微处理器、极长指令字(VLIW)微处理器、实施其他指令集的处理器或实施指令集组合的处理器。处理设备302还可以是一个或多个专用处理设备,诸如专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)、网络处理器,等等。处理设备302被配置为执行用于执行这里讨论的操作和步骤的处理逻辑运算(指令322)。

[0042] 计算设备300还可以包括网络接口设备308。计算设备300还可以包括视频显示单元310(例如,液晶显示器(LCD)或阴极射线管(CRT))、字母数字输入设备312(例如,键盘或触摸屏)、光标控制设备314(例如,鼠标或触摸屏)和音频设备316(例如,扬声器)。

[0043] 数据存储设备318可以包括一个或多个机器可读存储介质(或更具体地,一个或多个非瞬态计算机可读存储介质)328,在所述一个或多个机器可读存储介质328上存储有体现本文描述的方法或功能中的任何一个或多个的一组或多组指令322。在由计算设备300执行指令322期间,指令322还可完全或至少部分地位于主存储器304内和/或处理设备302内,主存储器304和处理设备302也构成计算机可读存储介质。

[0044] 上述各种方法可以通过计算机程序来实现。计算机程序可以包括被布置成指示计算机执行上述各种方法中的一种或多种的功能的计算机代码。用于执行这些方法的计算机程序和/或代码可以在一个或多个计算机可读介质上或更一般地在计算机程序产品上被提供给诸如计算机之类的装置。计算机可读介质可以是瞬态的或非瞬态的。一个或多个计算

机可读介质可以是例如电子、磁、光、电磁、红外或半导体系统,或者用于数据传输的传播介质,例如用于通过因特网下载代码的传播介质。或者,一个或多个上计算机可读介质可采取一个或多个物理计算机可读介质的形式,例如半导体或固态存储器、磁带、可移除计算机磁盘、随机存取存储器(RAM)、只读存储器(ROM)、刚性磁盘及光盘,例如CD-ROM、CD-R/W或DVD。

[0045] 在一种实施方案中,本文中所描述的模块、组件和其他特征(例如,关于图4的控制单元310)可实现为离散组件或集成在硬件组件(例如,ASICS、FPGA、DSP或类似设备)的功能性中作为个性化服务器的一部分。

[0046] “硬件组件”是能够执行特定操作的有形(例如,非瞬态)物理组件(例如,一个或多个处理器的集合),并且可以以特定物理方式来配置或布置。硬件组件可以包括被永久配置为执行特定操作的专用电路或逻辑器件。硬件组件可以是或包括专用处理器,诸如现场可编程门阵列(FPGA)或ASIC。硬件组件还可包括由软件临时配置以执行某些操作的可编程逻辑器件或电路。

[0047] 因此,短语“硬件组件”应当被理解为包括有形实体,该有形实体可以被物理地构造、永久地配置(例如,硬连线)或临时地配置(例如,被编程)为以特定方式操作或执行本文所述的特定操作。

[0048] 另外,模块和组件可以被实现为硬件设备内的固件或功能电路。此外,模块和组件可以以硬件设备和软件组件的任何组合来实现,或者仅以软件(例如,存储或以其他方式体现在机器可读介质或传输介质中的代码)来实现。

[0049] 除非从本公开中明确说明,否则如从以下讨论中清楚的,应当理解,在整个说明书中,利用诸如“接收”、“确定”、“比较”、“启用”、“保持”、“识别”、“替换”等术语表示计算机系统或相似电子计算设备的动作和过程,该计算机系统或相似电子计算设备操纵并将计算机系统的寄存器和存储器内表示为物理(电子)量的数据转换为计算机系统的存储器或寄存器或其他这样的信息存储、传输或显示设备内类似地表示为物理量的其他数据。

[0050] 应当理解,以上描述旨在是说明性的,而非限制性的。在阅读和理解以上描述后,许多其他实现方式对于本领域技术人员来说将是清楚的。尽管已经参考特定示例性实现描述了本公开,但是将认识到,本公开不限于所描述的实现,而是可以在所附权利要求的精神和范围内通过修改和变更来实践。因此,说明书和附图应被认为是说明性的,而不是限制性的。因此,本公开的范围应当参考所附权利要求以及这些权利要求所赋予的等同物的全部范围来确定。

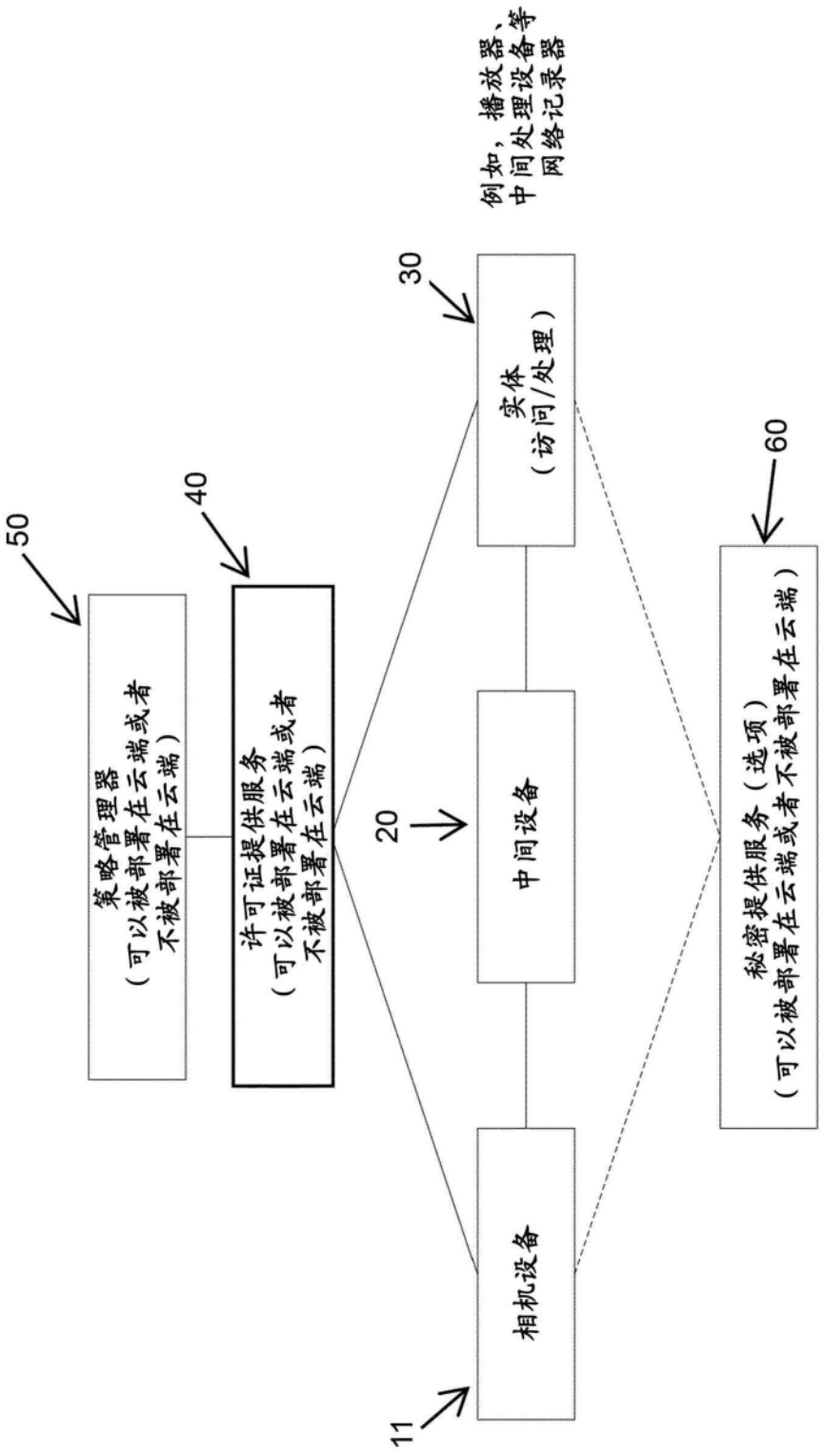

例如，播放器、
中间处理设备等
网络记录器
30
实体
（访问/处理）
60
秘密提供服务（选项）
（可以被部署在云端或者不被部署在云端）
40
许可证提供服务
（可以被部署在云端或者
不被部署在云端）
50
策略管理器
（可以被部署在云端或者
不被部署在云端）
20
中间设备
11
相机设备

图1

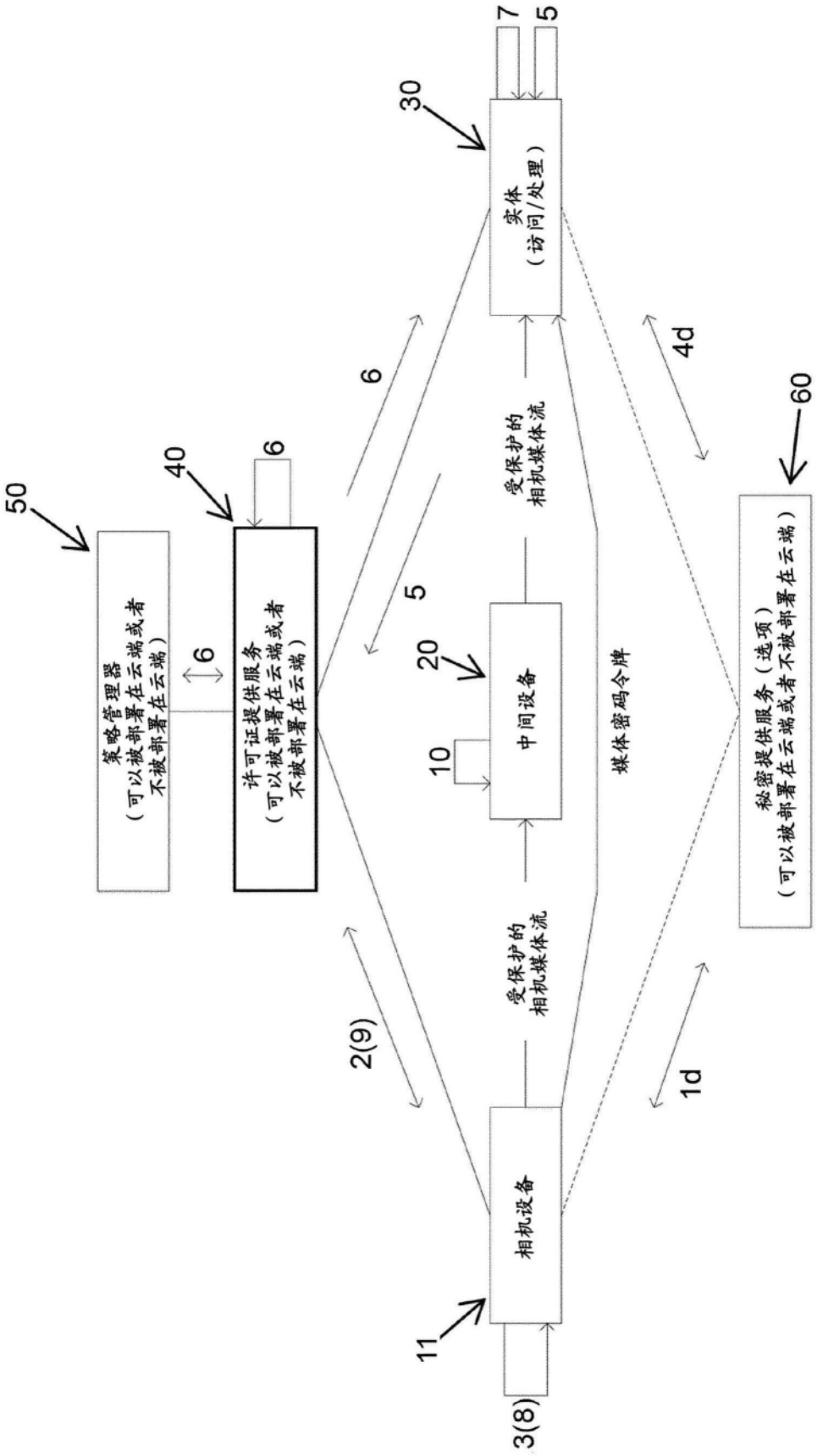

策略管理器
（可以被部署在云端或者
不被部署在云端）
许可证提供服务
（可以被部署在云端或者
不被部署在云端）
中间设备
相机设备
实体
（访问/处理）
秘密提供服务（选项）
（可以被部署在云端或者不被部署在云端）
受保护的
相机媒体流
受保护的
相机媒体流
媒体密码令牌
50
40
20
10
11
30
60
6
5
7
4d
1d
2(9)
3(8)

图2

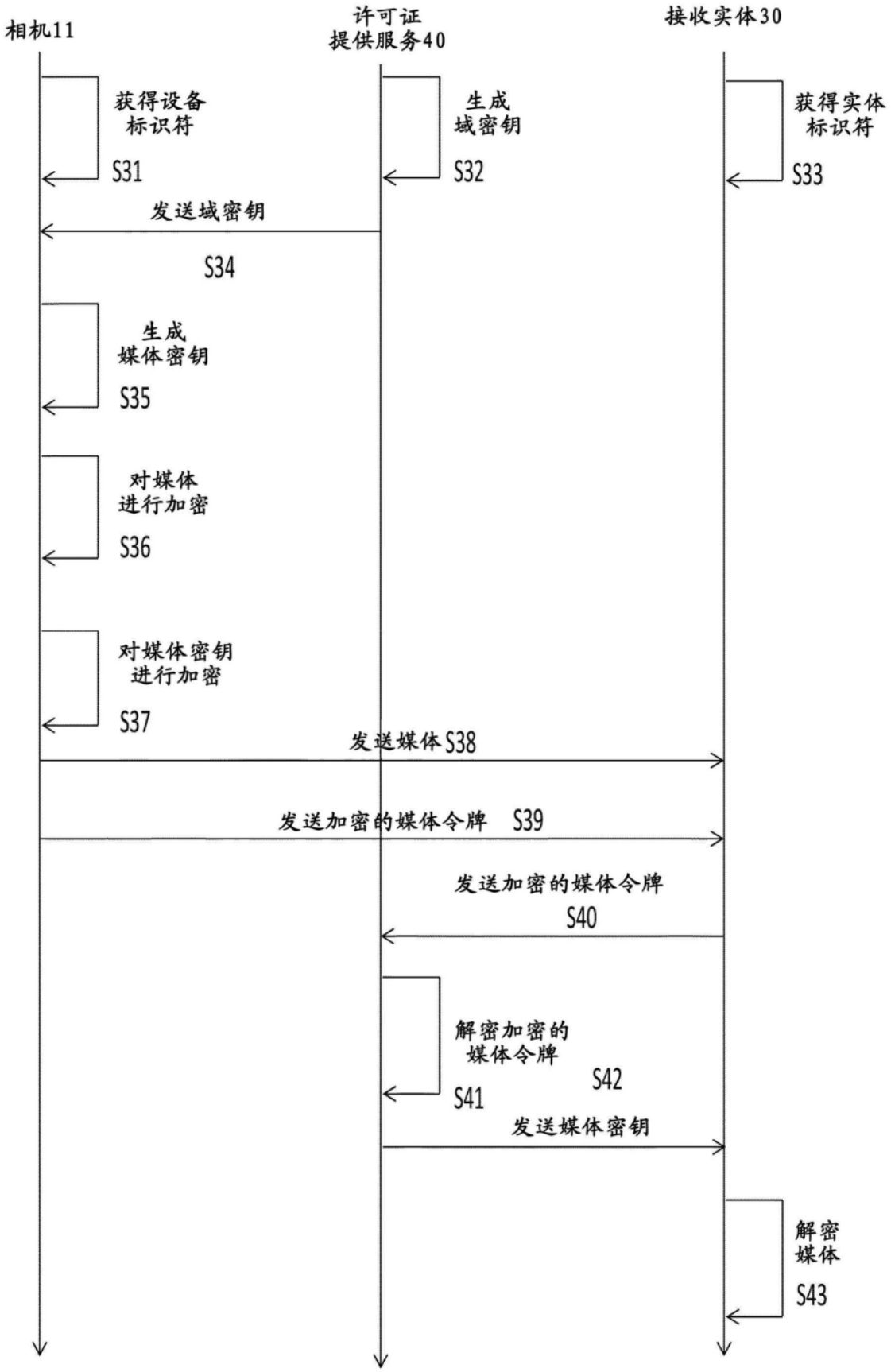

相机11
许可证
提供服务40
接收实体30
获得设备
标识符
S31
生成
域密钥
S32
获得实体
标识符
S33
发送域密钥
S34
生成
媒体密钥
S35
对媒体
进行加密
S36
对媒体密钥
进行加密
S37
发送媒体S38
发送加密的媒体令牌 S39
发送加密的媒体令牌
S40
解密加密的
媒体令牌
S41
S42
发送媒体密钥
解密
媒体
S43

图3

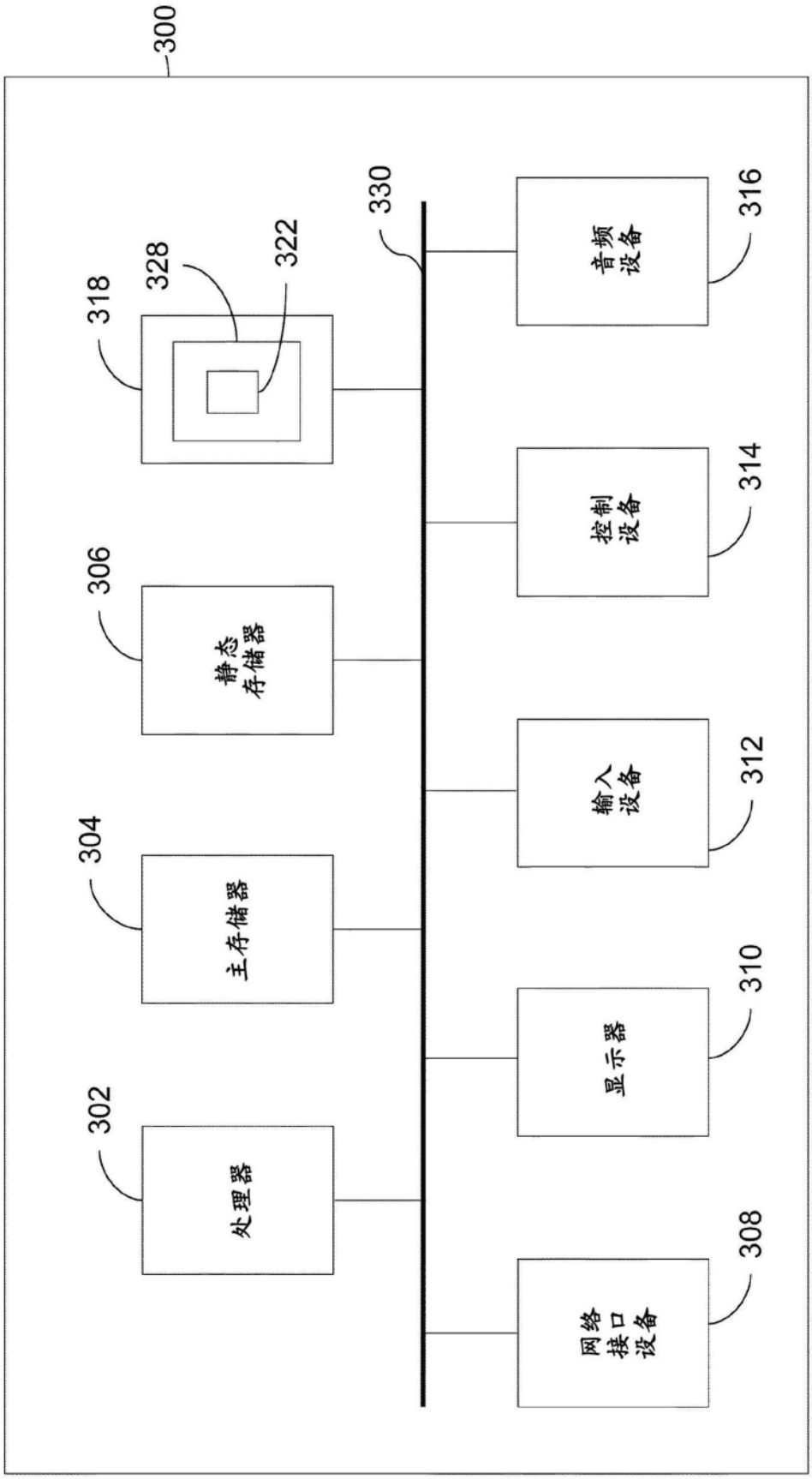

300
330
316
音频设备
322
328
318
314
控制设备
306
静态存储器
312
输入设备
304
主存储器
310
显示器
302
处理器
308
网络接口设备

图4