(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115529144 B
(45)授权公告日 2024.06.18

(21)申请号 202110703440.3
(22)申请日 2021.06.24
(65)同一申请的已公布的文献号
申请公布号 CN 115529144 A
(43)申请公布日 2022.12.27
(73)专利权人 中移(成都)信息通信科技有限公司
地址 610041 四川省成都市中国(四川)自由贸易试验区成都高新区和乐二街150号1号楼2单元
专利权人 中国移动通信集团有限公司
(72)发明人 唐小勇 尚宇翔 韩延涛 游正朋 朱磊 罗柯
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 钟舒婷 张颖玲
(51)Int.Cl.
H04L 9/40(2022.01)
(56)对比文件
CN 110944330 A,2020.03.31
CN 111935270 A,2020.11.13
审查员 许婵

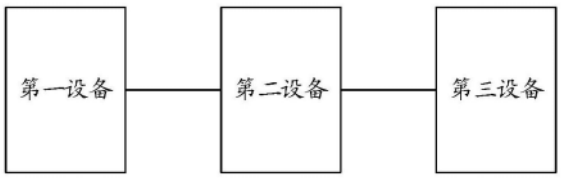
权利要求书4页 说明书23页 附图7页

(54)发明名称

通信系统、方法、装置、第一设备、第二设备及存储介质

(57)摘要

本申请公开了一种通信系统、通信方法、装置、第一设备、第二设备及存储介质。其中,系统包括:第一设备、第二设备、第三设备;所述第一设备,用于接收来自第二设备的第一信息,基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;所述第二设备,用于基于来自第三设备的第二信息向第一设备发送所述第一信息;所述第二信息,用于编排边缘计算平台上的应用。



CN 115529144 B

1.一种通信系统,其特征在于,包括:第一设备、第二设备、第三设备;其中,

所述第一设备,用于接收来自第二设备的第一信息,基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

所述第二设备,用于基于来自第三设备的第二信息向第一设备发送所述第一信息;所述第二信息,用于编排边缘计算平台上的应用;其中,所述第一设备为本地移动边缘计算平台管理MEPM,所述第二设备为MEPM,所述第三设备为移动边缘计算编排器MEO或移动边缘计算应用编排器MEAO。

2.根据权利要求1所述的系统,其特征在于,所述安全策略,包括以下至少之一:

第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

第三安全等级;所述第三安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

3.根据权利要求1所述的系统,其特征在于,所述第一设备,还用于向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

所述第二设备,还用于基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

4.根据权利要求1所述的系统,其特征在于,所述第一信息,包括以下至少之一的配置信息:

第一配置策略;所述第一配置策略针对不同应用的操作权限;

第二配置策略;所述第二配置策略针对不同应用的路由规则;

第三配置策略;所述第三配置策略针对不同应用的域名系统DNS;

第四配置策略;所述第四配置策略针对不同应用的生命周期。

5.根据权利要求4所述的系统,其特征在于,所述第二信息,包括以下至少之一:

应用的管理信息;

应用的生命周期管理信息;

应用的生命周期变更信息。

6.根据权利要求1所述的系统,其特征在于,所述第三设备,还用于接收来自第一设备的第一接入认证信息,向所述第一设备发送第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

7.根据权利要求1所述的系统,其特征在于,所述第三设备,还用于接收来自第二设备的第二接入认证信息,向所述第二设备发送第二认证响应信息;所述第二认证响应信息至少包括:第二设备的身份标识;

所述第三设备,还用于向所述第二设备发送所述第一设备的身份标识。

8.根据权利要求1至7任一项所述的系统,其特征在于,所述第一设备的数量为一个或多个。

9.一种通信方法,其特征在于,应用于第一设备,所述方法包括:

接收来自第二设备的第一信息;所述第一信息,用于针对边缘计算平台上的应用进行配置;所述第一信息是所述第二设备基于第三设备的第二信息向所述第一设备发送的;所述第二信息,用于编排边缘计算平台上的应用;

基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;其中,所述第一设备为本地MEPM,所述第二设备为MEPM,所述第三设备为MEO或MEAO。

10.根据权利要求9所述的方法,其特征在于,所述安全策略,包括以下至少之一:

第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

第三安全等级;所述第三安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

11.根据权利要求9所述的方法,其特征在于,所述方法还包括:

向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功。

12.根据权利要求9所述的方法,其特征在于,所述第一信息,包括以下至少之一的配置信息:

第一配置策略;所述第一配置策略针对不同应用的操作权限;

第二配置策略;所述第二配置策略针对不同应用的路由规则;

第三配置策略;所述第三配置策略针对不同应用的域名系统DNS;

第四配置策略;所述第四配置策略针对不同应用的生命周期。

13.根据权利要求9所述的方法,其特征在于,所述方法还包括:

向第三设备发送第一接入认证信息;

接收来自所述第三设备的第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

14.一种通信方法,其特征在于,应用于第二设备,所述方法包括:

接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;其中,所述第一设备为本地MEPM,所述第二设备为MEPM,所述第三设备为MEO或MEAO。

15.根据权利要求14所述的方法,其特征在于,所述第一信息,包括以下至少之一的配置信息:

第一配置策略;所述第一配置策略针对不同应用的操作权限;

第二配置策略;所述第二配置策略针对不同应用的路由规则;

第三配置策略;所述第三配置策略针对不同应用的域名系统DNS;

第四配置策略;所述第四配置策略针对不同应用的生命周期。

16.根据权利要求14所述的方法,其特征在于,所述第二信息,包括以下至少之一:

应用的管理信息;

应用的生命周期管理信息;

应用的生命周期变更信息。

17.根据权利要求14所述的方法,其特征在于,所述安全策略,包括以下至少之一:

第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

第三安全等级;所述第三安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

18.根据权利要求14所述的方法,其特征在于,所述方法还包括:

接收来自第一设备的第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

19.根据权利要求14所述的方法,其特征在于,所述方法还包括:

向第三设备发送第二接入认证信息;接收来自所述第三设备的第二认证响应信息;所述第二认证响应信息至少包括:第一设备的身份标识;

所述方法还包括:接收所述第一设备的身份标识。

20.一种通信装置,其特征在于,设置在第一设备上,包括:

第一通信单元,用于接收来自第二设备的第一信息;所述第一信息,用于针对边缘计算平台上的应用进行配置;所述第一信息是所述第二设备基于第三设备的第二信息向所述第一设备发送的;所述第二信息,用于编排边缘计算平台上的应用;

第一处理单元,用于基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;其中,所述第一设备为本地MEPM,所述第二设备为MEPM,所述第三设备为MEO或MEAO。

21.一种第一设备,其特征在于,包括:第一处理器及第一通信接口;其中,

所述第一通信接口,用于接收来自第二设备的第一信息;所述第一信息,用于针对边缘计算平台上的应用进行配置;所述第一信息是所述第二设备基于第三设备的第二信息向所述第一设备发送的;所述第二信息,用于编排边缘计算平台上的应用;

所述第一处理器,用于基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;其中,所述第一设备为本地MEPM,所述第二设备为MEPM,所述第三设备为MEO或MEAO。

22.一种通信装置,其特征在于,设置在第二设备上,包括:

第二通信单元,用于接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

第二处理单元,用于基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;其中,所述第一设备为本地MEPM,所述第二设备为MEPM,所述第三设备为MEO或MEAO。

23.一种第二设备,其特征在于,包括:第二处理器及第二通信接口;其中,

所述第二通信接口,用于接收来自第三设备的第二信息;所述第二信息,用于编排边缘

计算平台上的应用;

所述第二处理器,用于基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;其中,所述第一设备为本地MEPM,所述第二设备为MEPM,所述第三设备为MEO或MEAO。

24.一种网络设备,其特征在于,包括:处理器及和用于存储能够在处理器上运行的计算机程序的存储器,

其中,所述处理器用于运行所述计算机程序时,执行权利要求9至13任一项所述方法的步骤;或者,

所述处理器用于运行所述计算机程序时,执行权利要求14至19任一项所述方法的步骤。

25.一种存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现权利要求9至13任一项所述方法的步骤;或者,

所述计算机程序被处理器执行时实现权利要求14至19任一项所述方法的步骤。

通信系统、方法、装置、第一设备、第二设备及存储介质

技术领域

[0001] 本申请涉及通信领域,尤其涉及一种通信系统、方法、装置、第一设备、第二设备及存储介质。

背景技术

[0002] 第五代移动通信技术(5G)作为新一代通信技术,具有大带宽、低时延、高可靠、高连接、泛在网等诸多优势,从而推动垂直行业的快速发展与更迭,比如智慧医疗、智慧教育、智慧农业等方向的崛起。

[0003] 移动边缘计算(MEC)技术作为5G演进的关键技术之一,是具备无线网络信息应用程序接口(API)交互能力,以及计算、存储、分析功能的信息技术(IT)通用平台;依托MEC技术,可将传统外部应用拉入移动内部,更贴近用户,提供本地化服务,从而提升用户体验,发挥边缘网络的更多价值。

[0004] 将5G和MEC结合,可以面向不同的行业需求场景,引入不同的技术组合,比如服务质量(QoS)、端到端网络切片、网络能力开放、边缘云等,从而提供定制化的解决方案。

[0005] 相关技术中,5G与MEC技术结合的方案存在安全风险。

发明内容

[0006] 为解决相关技术问题,本申请实施例提供一种通信方法、装置、相关设备及存储介质。

[0007] 本申请实施例的技术方案是这样实现的:

[0008] 本申请实施例提供了一种通信系统,包括:第一设备、第二设备、第三设备;其中,

[0009] 所述第一设备,用于接收来自第二设备的第一信息,基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0010] 所述第二设备,用于基于来自第三设备的第二信息向第一设备发送所述第一信息;所述第二信息,用于编排边缘计算平台上的应用。

[0011] 上述方案中,所述安全策略,包括以下至少之一:

[0012] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0013] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0014] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0015] 上述方案中,所述第一设备,还用于向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

[0016] 所述第二设备,还用于基于所述第三信息向第三设备发送第四信息;所述第四信

息,用于说明所述第二信息是否配置成功。

[0017] 上述方案中,所述第一信息,包括以下至少之一的配置信息:

[0018] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0019] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0020] 第三配置策略;所述第三配置策略针对不同应用的域名系统(DNS,Domain Name System);

[0021] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0022] 上述方案中,所述第二信息,包括以下至少之一:

[0023] 应用的管理信息;

[0024] 应用的生命周期管理信息;

[0025] 应用的生命周期变更信息。

[0026] 上述方案中,所述第三设备,还用于接收来自第一设备的第一接入认证信息,向所述第一设备发送第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0027] 上述方案中,所述第三设备,还用于接收来自第二设备的第二接入认证信息,向所述第二设备发送第二认证响应信息;所述第二认证响应信息至少包括:第二设备的身份标识;

[0028] 所述第三设备,还用于向所述第二设备发送所述第一设备的身份标识。

[0029] 上述方案中,所述第一设备的数量为一个或多个。

[0030] 本申请实施例提供了一种通信方法,应用于第一设备,所述方法包括:

[0031] 接收来自第二设备的第一信息;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0032] 基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能。

[0033] 上述方案中,所述安全策略,包括以下至少之一:

[0034] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0035] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0036] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0037] 上述方案中,所述方法还包括:

[0038] 向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功。

[0039] 上述方案中,所述第一信息,包括以下至少之一的配置信息:

[0040] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0041] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0042] 第三配置策略;所述第三配置策略针对不同应用的域名系统DNS;

[0043] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0044] 上述方案中,所述方法还包括:

[0045] 向第三设备发送第一接入认证信息;

[0046] 接收来自所述第三设备的第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0047] 本申请实施例提供了一种通信方法,应用于第二设备,所述方法包括:

[0048] 接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

[0049] 基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一设备和安全策略针对所述边缘计算平台上的应用进行配置。

[0050] 上述方案中,所述第一信息,包括以下至少之一的配置信息:

[0051] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0052] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0053] 第三配置策略;所述第三配置策略针对不同应用的域名系统DNS;

[0054] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0055] 上述方案中,所述第二信息,包括以下至少之一:

[0056] 应用的管理信息;

[0057] 应用的生命周期管理信息;

[0058] 应用的生命周期变更信息。

[0059] 上述方案中,所述安全策略,包括以下至少之一:

[0060] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0061] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0062] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0063] 上述方案中,所述方法还包括:

[0064] 接收来自第一设备的第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

[0065] 基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

[0066] 上述方案中,所述方法还包括:

[0067] 向第三设备发送第二接入认证信息;接收来自所述第三设备的第二认证响应信息;所述第二认证响应信息至少包括:第一设备的身份标识;

[0068] 所述方法还包括:接收所述第一设备的身份标识。

[0069] 本申请实施例提供了一种通信装置,设置在第一设备上,包括:

[0070] 第一通信单元,用于接收来自第二设备的第一信息;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0071] 第一处理单元,用于基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能。

[0072] 上述方案中,所述安全策略,包括以下至少之一:

[0073] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0074] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0075] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0076] 上述方案中,所述第一通信单元,还用于向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功。

[0077] 上述方案中,所述第一信息,包括以下至少之一的配置信息:

[0078] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0079] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0080] 第三配置策略;所述第三配置策略针对不同应用的域名系统DNS;

[0081] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0082] 上述方案中,所述第一通信单元,还用于向第三设备发送第一接入认证信息;

[0083] 接收来自所述第三设备的第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0084] 本申请实施例提供了一种第一设备,包括:第一处理器及第一通信接口;其中,

[0085] 所述第一通信接口,用于接收来自第二设备的第一信息;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0086] 所述第一处理器,用于基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能。

[0087] 本申请实施例提供了一种通信装置,设置在第二设备上,包括:

[0088] 第二通信单元,用于接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

[0089] 第二处理单元,用于基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一设备和安全策略针对所述边缘计算平台上的应用进行配置。

[0090] 上述方案中,所述第一信息,包括以下至少之一的配置信息:

[0091] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0092] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0093] 第三配置策略;所述第三配置策略针对不同应用的域名系统;

[0094] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0095] 上述方案中,所述第二信息,包括以下至少之一:

[0096] 应用的管理信息;

[0097] 应用的生命周期管理信息;

[0098] 应用的生命周期变更信息。

[0099] 上述方案中,所述安全策略,包括以下至少之一:

[0100] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0101] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0102] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0103] 上述方案中,所述第二通信单元,还用于接收来自第一设备的第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

[0104] 基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

[0105] 上述方案中,所述第二通信单元,还用于向第三设备发送第二接入认证信息;接收来自所述第三设备的第二认证响应信息;所述第二认证响应信息至少包括:第一设备的身份标识;

[0106] 以及,接收所述第一设备的身份标识。

[0107] 本申请实施例提供了一种第二设备,包括:第二处理器及第二通信接口;其中,

[0108] 所述第二通信接口,用于接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

[0109] 所述第二处理器,用于基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一设备和安全策略针对所述边缘计算平台上的应用进行配置。

[0110] 本申请实施例提供了一种网络设备,包括:处理器及和用于存储能够在处理器上运行的计算机程序的存储器,

[0111] 其中,所述处理器用于运行所述计算机程序时,执行以上第一设备侧任一项所述方法的步骤;或者,

[0112] 所述处理器用于运行所述计算机程序时,执行以上第二设备侧任一项所述方法的步骤。

[0113] 本申请实施例提供了一种存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现以上第一设备侧任一项所述方法的步骤;或者,

[0114] 所述计算机程序被处理器执行时实现以上第二设备侧任一项所述方法的步骤。

[0115] 本申请实施例提供的通信系统、方法、装置、第一设备、第二设备及存储介质,系统包括:第一设备、第二设备、第三设备;所述第一设备,用于接收来自第二设备的第一信息,基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;所述第二设备,用于基于来自第三设备的第二信息向第一设备发送所述第一信息;所述第二信息,用于编排边缘计算平台上的应用。本申请实施例的方案,第一设备基于安全策略对边缘计算平台上的应用提供安全管理功能,使得第一设备可以根据安全策略确定是否根据第一信息进行编排;如此,能够提高第一设备针对边缘计算平台的应用进行配置的安全管控能力。

附图说明

[0116] 图1为相关技术中MEC的系统结构示意图;

[0117] 图2为相关技术中MEC的主机层与系统层的结构示意图;

[0118] 图3为本申请实施例5G行业云网融合的系统结构示意图;

[0119] 图4为本申请实施例一种通信系统的结构示意图;

[0120] 图5为本申请实施例一种通信方法的流程示意图;

[0121] 图6为本申请实施例另一种通信方法的流程示意图;

[0122] 图7为本申请应用实施例通信系统的结构示意图;

[0123] 图8为本申请应用实施例通信方法的流程示意图;

[0124] 图9为本申请应用实施例注册认证的流程示意图;

[0125] 图10为本申请实施例一种MEPM和L-MEPM的关系示意图;

[0126] 图11为本申请实施例一种权限授权方式的示意图;

[0127] 图12为本申请实施例一种通信装置的结构示意图;

[0128] 图13为本申请实施例另一种通信装置的结构示意图;

[0129] 图14为本申请实施例第一设备的结构示意图;

[0130] 图15为本申请实施例第二设备的结构示意图。

具体实施方式

[0131] 下面结合附图及实施例对本申请再作进一步详细的描述。

[0132] 相关技术中,MEC作为欧洲电信标准化协会(ETSI,European Telecommunications Standards Institute)主导的多接入边缘计算平台标准,从最初的移动边缘计算平台演进到基于虚拟网络功能(VNF,Virtual Network Feature)的多接入边缘计算平台,通过将MEC应用、平台、资源虚拟化和服务化的方式提供更高效的业务运行服务,以满足不同业务在处理能力上的差异化需求,ETSI标准组织定义了图1所示的MEC系统框架。

[0133] MEC系统,主要包括:MEC系统层(MEC system-level)、MEC主机层(MEC host level)、网络层(Networks)。

[0134] 其中,MEC系统层负责整个MEC资源的分配、收回与协调工作,以满足不同业务对计算和传输资源的需求。MEC系统层管理支持MEC系统级管理功能和主机级管理功能。MEC系统级管理功能包含用户应用生命周期管理代理、运营支持系统和MEC编排器,MEC主机级管理功能可以包括MEC平台管理器和虚拟化基础设施管理器。通过MEC管理层管理为终端和第三方客户(如商业企业)提供的MEC服务。

[0135] MEC主机层用于为MEC应用、MEC平台等提供必要的计算、存储及传输功能。

[0136] 网络层用于为上层的应用提供不同的网络选择(如3GPP无线网络、非3GPP无线网络、有线网络),并根据上层的信令动态调整路由策略,以满足不同业务在网络上的传输需求。

[0137] 其中,如图2所示,MEC主机(MEC host)包括:MEC平台和虚拟基础设施(计算、存储、网络)。虚拟设施包含数据面,用于执行从MEC平台接收到的路由规则,在应用(也称MEC应用或MEP应用)、服务(也称MEC服务或MEP服务)、DNS服务/代理、3GPP网络、其他接入网、本地网络和外部网络之间进行流量的转发。其中,MEP使能所述应用来提供和调用所述服务,MEP本身也可以提供服务。具体地,所述应用运行在虚拟机或容器上,可以对外提供丰富多样的服务(如:位置、无线网络信息、流量管理),所述应用也可以使用其他应用提供的服务,例如:应用A提供的位置、流量管理等服务可以被应用B和应用C使用。所述服务可以由MEP或某一个应用提供,当某个服务由所述应用提供时,该服务可以注册到MEP的服务列表中。

[0138] MEC平台(MEP,MEC platform),支持的功能包括:

[0139] 1)、提供MEC应用能够发现、通知、使用和提供MEC服务的环境,包括其他平台提供的MEC服务(可选)。

[0140] 2)、从MEC平台管理、应用或服务接收路由规则,控制数据面流量。

[0141] 3)、从MEC平台管理接收DNS记录,配置DNS代理/服务器;

[0142] 4)、托管MEC服务

[0143] 5)、提供到永久性存储和当日时间信息的接入;

[0144] MEC编排器(MEO,MEC orchestrator)又称MEC应用编排器(MEAO,MEC application orchestrator),是MEC系统层管理的核心,支持的功能包括:

[0145] 1)维护MEC系统的整体视图(即整体部署);比如MEC的主机部署、MEC的可用资源分配、可用的MEC服务的调用、系统拓扑等;

[0146] 2)管理MEC应用包的上线,包括:检查应用包的完整性和真实性;确认应用规则和需求,并判断是否需要调整应用规则和需求,若需要调整,则调整应用规则和需求以与运营商的策略相符;保存应用包的上线记录,以及为处理该应用准备虚拟基础设施管理器;

[0147] 3)基于约束(比如时延、可用资源、可用服务等)为应用的初始化选择合适的MEC主机;

[0148] 4)触发应用的启动和结束;

[0149] 5)触发应用的按需迁移。

[0150] MEC平台管理(MEPM,MEC platform manager),支持的功能包括:

[0151] 1)、管理应用的生命周期,如:通知MEAO相关应用的事件;

[0152] 2)、提供MEP的元素管理功能,包括虚拟网络功能(VNF,Virtualised Network Function)元素管理和网络服务(NS,Network Service)元素管理,其中NS信息元素包括物理网络功能(PNF,Physical Network Function)信息元素、虚拟链路信息元素、VNF转发图(VNF Forwarding Graph)信息元素;

[0153] 3)、管理MEC应用的规则和需求,比如:服务授权、路由规则、域名系统(DNS)配置和冲突处理;

[0154] 4)、从虚拟基础设施管理(VIM,Virtualisation Infrastructure Manager)接收虚拟资源的错误报告和性能测量数据。VIM主要功能包括:分配、管理、释放虚拟化基础设施的虚拟化资源,接收和存储软件镜像,收集、上报虚拟化资源的性能和故障信息。

[0155] 从MEC各模块的功能描述可以看出,MEC应用的规则(包括路由规则、DNS配置、业务规则等)由MEPM管理、MEP接收,并最终在MEC主机的用户面执行。

[0156] 实际应用中,垂直行业的终端接入技术类型繁多,第三方网络除5G外,还有非5G网络(比如4G、WiFi、Bluetooth、Zigbee、NB-IoT、SPN、红外网络、专线网络、Wireline等),这些终端的数据可能会通过不同的网络传输到MEP。为保障MEP的网络与数据安全,实现泛在网络接入与控制功能,在一种5G行业云网融合的系统架构中引入了行业网关(iGW,industry GateWay),该5G行业云网融合架构如图3所示。

[0157] MEC平台管理(MEPM)一般设置在行业网关上面,MEP上的数据可以通过行业网关直接接入到外部网络、即第三方网络,现有的ETSI协议对数据安全的保护并不到位,无法适应越来越多的数据安全和隐私保护的管理要求。

[0158] 在一些医疗、教育、金融等数据敏感的典型应用场景,出于对保护用户隐私和商业

机密的考虑,MEP上提供的一些应用和可用资源(硬件资源、网络资源等)是不能被远端(外部)的MEPM进行管理和配置的,MEPM向MEP发送的管理配置信息(或管理配置数据)必须受到严格的安全控制。相关技术中,MEPM对MEP上的管理配置信息缺乏必要的安全保护和授权管理机制,MEPM针对MEP的安全管理控制机制没有明确定义。

[0159] 基于此,在本申请的各种实施例中,第一设备,用于接收来自第二设备的第一信息,基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;所述第二设备,用于基于来自第三设备的第二信息向第一设备发送所述第一信息;所述第二信息,用于编排边缘计算平台上的应用。如此,能够提高对第一设备中针对边缘计算平台的应用进行配置的管控能力。

[0160] 本申请实施例提供一种通信系统,如图4所示,所述系统包括:第一设备、第二设备、第三设备;其中,

[0161] 所述第一设备,用于接收来自第二设备的第一信息,基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0162] 所述第二设备,用于基于来自第三设备的第二信息向第一设备发送所述第一信息;所述第二信息,用于编排边缘计算平台上的应用。

[0163] 其中,实际应用时,所述第二设备设置在第一设备和第三设备之间。

[0164] 实际应用时,所述第一设备可以为本地设置的MEPM,可以理解为使用方设置一个本地MEPM,可以对MEP提供的应用进行本地管理配置。第一设备既可以单独进行本地部署,也可以集成到MEP。本申请实施例对所述第一设备的名称不作限定,只要能实现所述第一设备的功能即可。

[0165] 实际应用时,所述第二设备可以为MEPM,本申请实施例对所述第二设备的名称不作限定,只要能实现所述第二设备的功能即可。

[0166] 实际应用时,所述第三设备可以为MEO或MEAO,本申请实施例对所述第三设备的名称不作限定,只要能实现所述第三设备的功能即可。

[0167] 实际应用时,所述边缘计算平台可以称为MEP。

[0168] 所述编排边缘计算平台上的应用可以理解为:通过对每个应用的应用程序和/或可用资源进行编排实现。

[0169] 在一实施例中,所述安全策略,包括以下至少之一:

[0170] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0171] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0172] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0173] 所述第一设备保存有安全策略,安全策略用于设置安全等级,通过不同安全等级管理第一设备中是否允许针对所述边缘计算平台上的部分应用的配置。

[0174] 实际应用时,可以向第二设备告知是否配置成功,即是否完成编排。

[0175] 基于此,在一实施例中,所述第一设备,还用于向第二设备发送第三信息;所述第

三信息,用于说明所述第一信息是否配置成功;

[0176] 所述第二设备,还用于基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

[0177] 在一实施例中,所述第一信息,包括以下至少之一的配置信息:

[0178] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0179] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0180] 第三配置策略;所述第三配置策略针对不同应用的域名系统(DNS);

[0181] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0182] 在一实施例中,所述第二信息,包括以下至少之一:

[0183] 应用的管理信息;

[0184] 应用的生命周期管理信息;

[0185] 应用的生命周期变更信息。

[0186] 这里,所述应用的管理信息,可以包括:应用包的管理,如:加载应用包、启用应用包、禁用应用包等。

[0187] 所述应用的生命周期管理信息,可以包括:实例化应用包、操作(使用)应用实例、终止应用实例。

[0188] 所述应用的生命周期变更通知,可以包括:应用程序未实例化、应用程序已经启动在运行中、应用程序停止运行。

[0189] 实际应用时,第三设备可以对第一设备进行身份认证,认证通过后可进行通信。

[0190] 基于此,在一实施例中,所述第三设备,还用于接收来自第一设备的第一接入认证信息,向所述第一设备发送第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0191] 实际应用时,第三设备可以对第二设备进行身份认证,认证通过后可进行通信。

[0192] 基于此,在一实施例中,所述第三设备,还用于接收来自第二设备的第二接入认证信息,向所述第二设备发送第二认证响应信息;所述第二认证响应信息至少包括:第二设备的身份标识;

[0193] 所述第三设备,还用于向所述第二设备发送所述第一设备的身份标识。

[0194] 在一实施例中,所述第一设备的数量为一个或多个。

[0195] 相应地,本申请实施例中还提供一种通信方法,应用于第一设备,如图5所示,所述方法包括:

[0196] 步骤501、接收来自第二设备的第一信息;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0197] 步骤502、基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能。

[0198] 实际应用时,所述第一设备可以为本地设置的MEPM,可以理解为使用方设置一个本地MEPM,可以对MEP提供的应用进行本地管理配置。第一设备既可以单独进行本地部署,也可以集成到MEP。本申请实施例对所述第一设备的名称不作限定,只要能实现所述第一设备的功能即可。

[0199] 实际应用时,所述第二设备可以为MEPM,本申请实施例对所述第二设备的名称不

作限定,只要能实现所述第二设备的功能即可。

[0200] 实际应用时,所述边缘计算平台可以称为MEP。

[0201] 在一实施例中,所述安全策略,包括以下至少之一:

[0202] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0203] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0204] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0205] 所述第一设备保存有安全策略,安全策略用于设置安全等级,通过不同安全等级管理第一设备中是否允许针对所述边缘计算平台上的部分应用的配置。

[0206] 在一实施例中,第一设备可以请求第二设备对自身进行身份认证,认证通过后可进行通信。

[0207] 基于此,在一实施例中,所述方法还包括:

[0208] 向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功。

[0209] 在一实施例中,所述第一信息,包括以下至少之一的配置信息:

[0210] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0211] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0212] 第三配置策略;所述第三配置策略针对不同应用的域名系统;

[0213] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0214] 实际应用时,第一设备可以请求第三设备对自身进行身份认证,认证通过后可进行通信。

[0215] 基于此,在一实施例中,所述方法还包括:

[0216] 向第三设备发送第一接入认证信息;

[0217] 接收来自所述第三设备的第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0218] 相应地,本申请实施例中又提供一种通信方法,应用于第二设备,如图6所示,所述方法包括:

[0219] 步骤601、接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

[0220] 步骤602、基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一设备和安全策略针对所述边缘计算平台上的应用进行配置。

[0221] 实际应用时,所述第一设备可以为本地设置的MEPM,可以理解为使用方设置一个本地MEPM,可以对MEP提供的应用进行本地管理配置。第一设备既可以单独进行本地部署,也可以集成到MEP。本申请实施例对所述第一设备的名称不作限定,只要能实现所述第一设备的功能即可。

[0222] 实际应用时,所述第二设备可以为MEPM,本申请实施例对所述第二设备的名称不作限定,只要能实现所述第二设备的功能即可。

[0223] 实际应用时,所述第三设备可以为MEO或MEAO,本申请实施例对所述第三设备的名

称不作限定,只要能实现所述第三设备的功能即可。

[0224] 实际应用时,所述边缘计算平台可以称为MEP。

[0225] 实际应用时,所述编排边缘计算平台上的应用可以理解为:通过对每个应用的应用程序和/或可用资源进行编排实现。

[0226] 在一实施例中,所述第一信息,包括以下至少之一的配置信息:

[0227] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0228] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0229] 第三配置策略;所述第三配置策略针对不同应用的域名系统;

[0230] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0231] 在一实施例中,所述第二信息,包括以下至少之一:

[0232] 应用的管理信息;

[0233] 应用的生命周期管理信息;

[0234] 应用的生命周期变更信息。

[0235] 在一实施例中,所述安全策略,包括以下至少之一:

[0236] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0237] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0238] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0239] 所述第一设备保存有安全策略,安全策略用于设置安全等级,通过不同安全等级管理第一设备中是否允许针对所述边缘计算平台上的部分应用的配置。

[0240] 实际应用时,第二设备可以对第一设备进行身份认证,认证通过后可进行通信。

[0241] 基于此,在一实施例中,所述方法还包括:

[0242] 接收来自第一设备的第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

[0243] 基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

[0244] 实际应用时,第二设备可以请求第三设备对自身进行身份认证,认证通过后可进行通信。

[0245] 基于此,在一实施例中,所述方法还包括:

[0246] 向第三设备发送第二接入认证信息;接收来自所述第三设备的第二认证响应信息;所述第二认证响应信息至少包括:第一设备的身份标识;

[0247] 所述方法还包括:接收所述第一设备的身份标识。

[0248] 下面结合应用实施例对本申请再作进一步详细的描述。

[0249] 在本应用实施例中,所述第一设备称为本地MEPM(L-MEPM,Local MEPM);所述第二设备为MEPM;所述第三设备称为MEAO或MEO;所述边缘计算平台称为MEP。

[0250] 在本应用实施例中,引入一个部署在MEP侧的L-MEPM,主要负责与MEPM和/或MEAO进行信令交互,并负责MEP本地管理配置数据的安全监管,如图7所示。

[0251] 其中,L-MEPM,支持功能包括:

[0252] 1)、管理MEPM的管理配置请求,根据针对MEP上的应用的安全策略等相应管理配置请求;

[0253] 2)、保存有安全策略,基于安全策略管理来自MEPM的管理配置数据(即上述来自第二设备的第一信息)。安全策略可以包括:严格、一般、宽松等三个等级,例如:在严格等级时,来自MEPM的管理配置数据不能配置MEP上的应用;在一般等级时,L-MEPM基于安全策略确定来自MEPM的管理配置数据是否能够配置MEP上的应用,在宽松等级时,L-MEPM只负责转发MEPM的管理配置数据(管理配置数据基于来自MEPM的管理配置请求确定)到MEP进行针对不同应用的配置。

[0254] 当然,实际应用时还可以对于等级划分更为细分,这里不做限定。

[0255] 在本应用实施例中,如图8所示,MEAO通过MEPM进行编排管理,L-MEPM本地配置有安全策略,针对控制面(具体指针对MEP提供的应用的管理配置数据)进行数据安全管控,以使控制面的数据不能随意对MEP的应用进行配置。所述通信方法包括:

[0256] 步骤801、MEAO(一种第三设备示例)向MEPM(一种第二设备示例)下发第二信息;

[0257] 所述第二信息包括:MEPM身份标识和编排信息;

[0258] 所述第二信息,用于编排边缘计算平台上的应用。

[0259] 对于第二信息给出一种示例,所述第二信息包含但不限于表1的内容:

[0260]

参数名	类型	说明
MEPM 身份标识	如表 5 所示	MEPM 的唯一身份标识
编排信息	如表 7 所示	编排信息

[0261] 表1

[0262] 步骤802、MEPM收到第二信息后,向L-MEPM(一种第三设备示例)发送第一信息;

[0263] 所述第一信息包括:L-MEPM身份标识和管理配置信息;

[0264] 所述第一信息,用于针对所述边缘计算平台上的应用进行配置。

[0265] 对于第一信息给出一种示例,如表2所示;

[0266]

参数名	类型	说明
L-MEPM身份标识	如表5所示	L-MEPM的唯一身份标识
管理配置信息	如表8所示	管理配置信息

[0267] 表2

[0268] 步骤803、L-MEPM收到第一信息后,检查本地的安全策略;基于第一信息和安全策略进行相应操作并回复第三信息;

[0269] 所述L-MEPM本地的安全策略,包括:

[0270] “严格”等级(相当于上述第一安全等级)时,L-MEPM拒绝针对MEP的所有管理配置信息;

[0271] “一般”等级(相当于上述第二安全等级)时,L-MEPM允许针对MEP的部分管理配置信息;

[0272] “宽松”等级(相当于上述第三安全等级)时,L-MEPM允许针对MEP的所有管理配置信息。

[0273] L-MEPM中每个应用具有唯一标识,安全策略中通过每个应用的标识标记,并对应标记是否符合要求。

[0274] 检查本地的安全策略,相应于符合安全策略的情况,对MEP上的应用进行配置,配置完成后向MEPM回复配置成功的信息;

[0275] 相应于符合部分安全策略的情况,对MEP上的应用信息进行部分的配置,配置完成后向MEPM回复配置成功的信息;

[0276] 如果不符合本地安全策略,直接向MEPM回复配置失败的信息。

[0277] 也就是说,所述第三信息,包括:MEPM身份标识和管理配置结果信息;如表3所示。

[0278]

参数名	类型	说明

[0279]

MEPM 身份标识	如表 5 所示	MEPM 的唯一身份标识
管理配置结果信息	如表 9 所示	成功或失败

[0280] 表3

[0281] 步骤804、MEPM收到L-MEPM的第三信息后,向MEAO回复第四信息;

[0282] 所述第四信息,用于说明基于第二信息进行编排的结果。

[0283] 所述第四信息可以包括:MEAO身份标识和管理配置结果信息;如表4所示。

[0284]

参数名	类型	说明
MEAO身份标识	如表5所示	MEAO的唯一身份标识
管理配置结果信息	如表10所示	成功或失败

[0285] 表4

[0286] 本发明各实施例中可以用于唯一ID标识身份,如表5的实施例;

[0287]

数据类型	说明
字符串	身份标识用 UUID 格式的字符串来标识。UUID 使用由开放软件基金会（OSF）标准化的通用唯一识别码（UUID，niversally Unique Identifier）。UUID 的标准型式包含 32 个 16 进制数字，以连字号分为五段，形式为 8-4-4-4-12 的 32 个字符。示例：880e8400-e29b-41d4-a716-446655440000。
字符串	行业网关身份标识用 NUID 格式的字符串来标识。NUID 使用 CNCF 组织下 NATS 项目的一个 UID 库，使用 62 个字符（0-9a-zA-Z）生成 22 位长度的字符串，结果分为 2 部分：前 12 位为真随机数,后 10 是伪随机数。示例：M4bZr7xyO3toV6T6iC7lWB。
数字	身份标识用 64 位的整数来标识。Snowflake 是 Twitter 推出的在分布式环境生成唯一 ID 的算法，生成一个

[0288]

	64bit 大小的整数，在 Java 等编程语言中使用 Long 类型进行存储。

[0289] 表5

[0290] 本发明各实施例中可以通过数字或字符串标识来区分MEPM类型,如表6的实施例;

[0291]

数据类型	说明
数字	1表示普通MEPM;2表示L-MEPM
字符串	“1”表示普通MEPM;“2”表示L-MEPM

[0292] 表6

[0293] 本发明各实施例中MEAO下发的编排信息,如表7所示,根据ETSI MEC010-2标准协议中规定进行设计,针对每个应用包:

[0294]

参数名	类型	说明
应用包管理	数字或字符串	1、加载应用包 2、查询应用包信息 3、禁用应用包 4、启用应用包 5、删除应用包 6、获取应用包
应用的生命周期管理	数字或字符串	1、实例化应用包 2、操作（使用）应用实例 3、终止应用实例
应用的生命周期变更通知	数字或字符串	1、应用程序未实例化 2、应用程序已经启动，在运行中 3、应用程序停止运行

[0295] 表7

[0296] MEPM向L-MEPM下发的管理配置信息,给出一种应用示例,如表8所示;

[0297]

参数名	类型	说明
应用的服务授权	Bitmap	针对服务进行增加、删除、修改、查询的权限；如图 11 所示，使用 16 位 bitmap，其中 0bit 到 3bit 分别表示新增、删除、修改、查询，其他 bit 位保留
应用的路由规则	字符串	可以分为静态路由和动态路由规则。 1、静态路由配置一版包括 IP 地址、掩码、网关 IP，例如：route add -net 192.168.0.0/24 gw 192.168.0.1。2、动态路由协议包括 RIP 路由协议、OSPF 路由协议、IS-IS 路由、BGP 和 BGP-4 路由协议。

[0298]

应用的 DNS 配置	字符串	提供网络域名和 IP 地址的相互映射。例如：www.baidu.com 39.156.66.18
应用的生命周期	数字或字符串	1.实例化应用包 2.操作应用实例 3.终止应用实例

[0299] 表8

[0300] L-MEPM向MEPM的回复信息、即第三信息,给出一种应用示例,如表9所示;

[0301]

字段名	类型	说明
MEPM 身份标识	如表 5 所示	MEPM 在系统中的唯一身份标识
回复类型	数字	使用 0 和 1 表示消息回复的类型
回复说明	String	0 表示成功下发给 MEP; 1 表示不符合本地安全策略; 2 表示出现网络异常、系统异常、超时等问题。

[0302] 表9

[0303] MEPM向MEAO的回复消息、即第四信息,给出一种应用示例,如表10所示;

[0304]

字段名	类型	说明
MEAO 身份标识	如表 5 所示	MEAO 在系统中的唯一身份标识
回复类型	数字	使用 0 和 1 表示消息回复的类型
回复说明	String	0 表示成功下发管理配置信息给 L-MEPM; 1 表示管理配置信息不符合本地安全

[0305]

		策略，被拒绝; 2 表示出现网络异常、系统异常、超时等问题。

[0306] 表10

[0307] 实际应用时,为了得到MEPM身份标识、L-MEPM身份标识,所述方法还包括:身份注册;如图9所示,包括:

[0308] 步骤901、MEPM(一种第二设备示例)和L-MEPM(一种第一设备示例)分别向MEAO(一种第三设备示例)注册请求;

[0309] 所述注册请求即所述身份认证信息,用于请求MEAO注册身份;MEAO收到注册请求进行注册操作后存储MEPM、L-MEPM相应的身份标识。注册的身份信息可以包含以下如表11所示内容:

[0310]

参数名	参数类型	参数说明
MEPM 身份标识	如表 5 所示	MEPM 在系统中的身份标识
MEPM 身份类型	如表 6 所示	用于区分是普通 MEPM 还是 L-MEPM
IP 地址	如表 17 所示	MEPM 的 IP 地址，用于普通 MEPM 关联 L-MEPM

[0311] 表11

[0312] 步骤902、MEAO收到注册请求后，进行注册并回复信息；包括如下表12所示内容：

[0313]

参数名	参数类型	参数说明
MEPM 身份标识	如表 5 所示	MEPM 在系统中的身份标识
回复信息说明	如表 11 所示	对回复信息类型的信息说明，和回复信息类型一一对应

[0314] 表12

[0315] MEAO收到MEPM注册请求后，执行回复操作；针对回复操作给出一种应用示例，如表13所示；没有按照表6格式则是非法身份标识。

[0316]

MEAO 操作	消息回复类型	响应信息说明
“MEPM 身份标识”在行业网关中成功注册	0	身份成功注册
“MEPM 身份标识”在行业网关中已经注册	1	身份重复注册
“MEPM 身份类型”不是 1 或 2	3	MEPM 身份类型错误
出现网络异常、系统异常、超时等问题	4	系统异常

[0317] 表13

[0318] 步骤903、MEAO向MEPM发送已经注册的L-MEPM信息，给出一种应用示例，如表14所示；

[0319]

参数名	参数类型	参数说明
MEPM 身份标识	如表 5 所示	普通 MEPM 在系统中的身份标识
与 MEPM 关联的 L-MEPM 身份标识和 IP 地址	见下述 L-MEPM 身份信息和 IP 地址信息的示例	MEAO 上注册的所有 L-MEPM 身份标识

[0320] 表14

[0321] 步骤904、MEPM解析出L-MEPM的身份信息和IP地址后,形成MEPM和多个L-MEPM的关联关系,如下图10所示。

[0322] MEPM并向MEAO进行信息回复。关于回复信息的内容,给出一种应用示例,如表15所示;

[0323]

参数名	类型	说明
MEAO 身份标识	如表 5 所示	MEAO 在系统中的唯一身份标识
回复类型	数字	向 MEAO 回复消息
回复说明	字符串	向 MEAO 回复是否成功收到消息，和“回复类型”一一对应

[0324]

[0325] 表15

[0326] 关于回复类型和回复说明,给出一种应用示例,如表16所示;

[0327]

回复类型	回复说明
0	成功
1	非法身份

[0328] 表16

[0329] 针对IP地址,给出一种应用示例,如表17所示;

[0330]

IP 地址种类	数据类型	响应信息说明
IPv4	字符串	例如: 100.12.56.12
IPv6	字符串	例 如 : ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

[0331] 表17

[0332] 针对L-MEPM身份信息和IP地址信息,给出一种示例,如下:

[0333] 方法1:使用哈希表方式实现,key标识L-MEPM身份标识,value标识L-MEPM的IP地址。

[0334] 方式2:使用JSON字符串方式实现。

[0335] {

[0336] "880e8400-e29b-41d4-a716-446655440000":"156.123.52.41",

[0337] "990e8400-e29b-41d4-a716-446655440000":"156.123.52.42",

[0338] "770e8400-e29b-41d4-a716-446655440000":"156.123.52.43",

[0339] "660e8400-e29b-41d4-a716-446655440000":"156.123.52.44"

[0340] }

[0341] 为了实现本申请实施例第一设备侧的方法,本申请实施例还提供了一种通信装置,设置在第一设备上,如图12所示,该装置包括:

[0342] 第一通信单元1201,用于接收来自第二设备的第一信息;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0343] 第一处理单元1202,用于基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能。

[0344] 其中,在一实施例中,所述安全策略,包括以下至少之一:

[0345] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0346] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0347] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0348] 在一实施例中,所述第一通信单元1201,还用于向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功。

[0349] 在一实施例中,所述第一信息,包括以下至少之一的配置信息:

[0350] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0351] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0352] 第三配置策略;所述第三配置策略针对不同应用的域名系统;

[0353] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0354] 在一实施例中,所述第一通信单元1202,还用于向第三设备发送第一接入认证信息;

[0355] 接收来自所述第三设备的第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0356] 实际应用时,所述第一通信单元1201和所述第一处理单元1202可由通信装置中的处理器结合通信接口实现。

[0357] 为了实现本申请实施例第二设备侧的方法,本申请实施例还提供了一种通信装置,设置在第二设备上,如图13所示,该装置包括:

[0358] 第二通信单元1301,用于接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

[0359] 第二处理单元1302,用于基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一设备和安全策略针对所述边缘计算平台上的应用进行配置。

[0360] 其中,在一实施例中,所述第一信息,包括以下至少之一的配置信息:

[0361] 第一配置策略;所述第一配置策略针对不同应用的操作权限;

[0362] 第二配置策略;所述第二配置策略针对不同应用的路由规则;

[0363] 第三配置策略;所述第三配置策略针对不同应用的域名系统;

[0364] 第四配置策略;所述第四配置策略针对不同应用的生命周期。

[0365] 在一实施例中,所述第二信息,包括以下至少之一:

[0366] 应用的管理信息;

[0367] 应用的生命周期管理信息;

[0368] 应用的生命周期变更信息。

[0369] 在一实施例中,所述安全策略,包括以下至少之一:

[0370] 第一安全等级;所述第一安全等级表征拒绝针对所述边缘计算平台上的所有应用的配置;

[0371] 第二安全等级;所述第二安全等级表征允许针对所述边缘计算平台上的部分应用的配置;

[0372] 第三安全等级;所述第一安全等级表征允许针对所述边缘计算平台上的所有应用的配置。

[0373] 在一实施例中,所述第二通信单元1301,还用于接收来自第一设备的第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

[0374] 基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

[0375] 在一实施例中,所述第二通信单元1301,还用于向第三设备发送第二接入认证信息;接收来自所述第三设备的第二认证响应信息;所述第二认证响应信息至少包括:第一设备的身份标识;

[0376] 所述第二通信单元1301,还用于接收所述第一设备的身份标识。

[0377] 实际应用时,实际应用时,所述第二通信单元1301和所述第二处理单元1302可由通信装置中的处理器结合通信接口实现。

[0378] 需要说明的是:上述实施例提供的通信装置在进行通信时,仅以上述各程序模块的划分进行举例说明,实际应用中,可以根据需要而将上述处理分配由不同的程序模块完成,即将装置的内部结构划分成不同的程序模块,以完成以上描述的全部或者部分处理。另外,上述实施例提供的通信装置与通信方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

[0379] 基于上述程序模块的硬件实现,且为了实现本申请实施例第一设备侧的方法,本申请实施例还提供了一种第一设备,如图14所示,该第一设备1400包括:

[0380] 第一通信接口1401,能够与第二设备进行信息交互;

[0381] 第一处理器1402,与所述第一通信接口1401连接,以实现与第二设备进行信息交互,用于运行计算机程序时,执行上述第一设备侧一个或多个技术方案提供的方法。而所述计算机程序存储在第一存储器1403上。

[0382] 具体地,所述第一通信接口1401,用于接收来自第二设备的第一信息;所述第一信息,用于针对所述边缘计算平台上的应用进行配置;

[0383] 所述第一处理器1402,用于基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能。

[0384] 其中,在一实施例中,所述第一通信接口1401,还用于:

[0385] 向第二设备发送第三信息;所述第三信息,用于说明所述第一信息是否配置成功。

[0386] 在一实施例中,所述第一通信接口1401,还用于:

[0387] 向第三设备发送第一接入认证信息;

[0388] 接收来自所述第三设备的第一认证响应信息;所述第一认证响应信息至少包括:第一设备的身份标识。

[0389] 需要说明的是:第一处理器1402和第一通信接口1401的具体处理过程可参照上述方法理解。

[0390] 当然,实际应用时,第一设备1400中的各个组件通过总线系统1404耦合在一起。可理解,总线系统1404用于实现这些组件之间的连接通信。总线系统1404除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图14中将各种总线都标为总线系统1404。

[0391] 本申请实施例中的第一存储器1403用于存储各种类型的数据以支持第一设备1400的操作。这些数据的示例包括:用于在第一设备1400上操作的任何计算机程序。

[0392] 上述本申请实施例揭示的方法可以应用于所述第一处理器1402中,或者由所述第一处理器1402实现。所述第一处理器1402可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过所述第一处理器1402中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第一处理器1402可以是通用处理器、数字信号处理器(DSP,Digital Signal Processor),或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第一处理器1402可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于第一存储器1403,所述第一处理器1402读取第一存储器1403中的信息,结合其硬件完成前

述方法的步骤。

[0393] 在示例性实施例中,第一设备1400可以被一个或多个应用专用集成电路(ASIC,Application Specific Integrated Circuit)、DSP、可编程逻辑器件(PLD,Programmable Logic Device)、复杂可编程逻辑器件(CPLD,Complex Programmable Logic Device)、现场可编程门阵列(FPGA,Field-Programmable Gate Array)、通用处理器、控制器、微控制器(MCU,Micro Controller Unit)、微处理器(Microprocessor)、或者其他电子元件实现,用于执行前述方法。

[0394] 基于上述程序模块的硬件实现,且为了实现本申请实施例第二设备侧的方法,本申请实施例还提供了一种第二设备,如图15所示,该第二设备1500包括:

[0395] 第二通信接口1501,能够与第一设备和第三设备进行信息交互;

[0396] 第二处理器1502,与所述第二通信接口1501连接,以实现与第一设备和第三设备进行信息交互,用于运行计算机程序时,执行上述第二设备侧一个或多个技术方案提供的方法。而所述计算机程序存储在第二存储器1503上。

[0397] 具体地,所述第二通信接口1501,用于接收来自第三设备的第二信息;所述第二信息,用于编排边缘计算平台上的应用;

[0398] 所述第二处理器1502,用于基于所述第二信息向第一设备发送第一信息;所述第一信息,用于指示第一设备基于所述第一设备和安全策略针对所述边缘计算平台上的应用进行配置。

[0399] 其中,在一实施例中,所述第二通信接口1501,还用于:

[0400] 接收来自第一设备的第三信息;所述第三信息,用于说明所述第一信息是否配置成功;

[0401] 基于所述第三信息向第三设备发送第四信息;所述第四信息,用于说明所述第二信息是否配置成功。

[0402] 在一实施例中,所述第二通信接口1501,还用于向第三设备发送第二接入认证信息;接收来自所述第三设备的第二认证响应信息;所述第二认证响应信息至少包括:第一设备的身份标识;

[0403] 以及,接收所述第一设备的身份标识。

[0404] 需要说明的是:第二通信接口1501和第二处理器1502的具体处理过程可参照上述方法理解。

[0405] 当然,实际应用时,第二设备1500中的各个组件通过总线系统1504耦合在一起。可理解,总线系统1504用于实现这些组件之间的连接通信。总线系统1504除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图15中将各种总线都标为总线系统1504。

[0406] 本申请实施例中的第二存储器1503用于存储各种类型的数据以支持第二设备1500的操作。这些数据的示例包括:用于在第二设备1500上操作的任何计算机程序。

[0407] 上述本申请实施例揭示的方法可以应用于所述第二处理器1502中,或者由所述第二处理器1502实现。所述第二处理器1502可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过所述第二处理器1502中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第二处理器1502可以是通用处理器、DSP,或者其他

可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第二处理器1502可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于第二存储器1503,所述第二处理器1502读取第二存储器1503中的信息,结合其硬件完成前述方法的步骤。

[0408] 在示例性实施例中,第二设备1500可以被一个或多个ASIC、DSP、PLD、CPLD、FPGA、通用处理器、控制器、MCU、Microprocessor、或其他电子元件实现,用于执行前述方法。

[0409] 可以理解,本申请实施例的存储器(第一存储器1403、第二存储器1503)可以是易失性存储器或者非易失性存储器,也可包括易失性和非易失性存储器两者。其中,非易失性存储器可以是只读存储器(ROM,Read Only Memory)、可编程只读存储器(PROM,Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM,Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM,Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM,ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM,Compact Disc Read-Only Memory);磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM,Random Access Memory),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(SRAM,Static Random Access Memory)、同步静态随机存取存储器(SSRAM,Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM,Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM,Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM,Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM,Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM,SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM,Direct Rambus Random Access Memory)。本申请实施例描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

[0410] 需要说明的是:“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。

[0411] 另外,本申请实施例所记载的技术方案之间,在不冲突的情况下,可以任意组合。

[0412] 以上所述,仅为本申请的较佳实施例而已,并非用于限定本申请的保护范围。

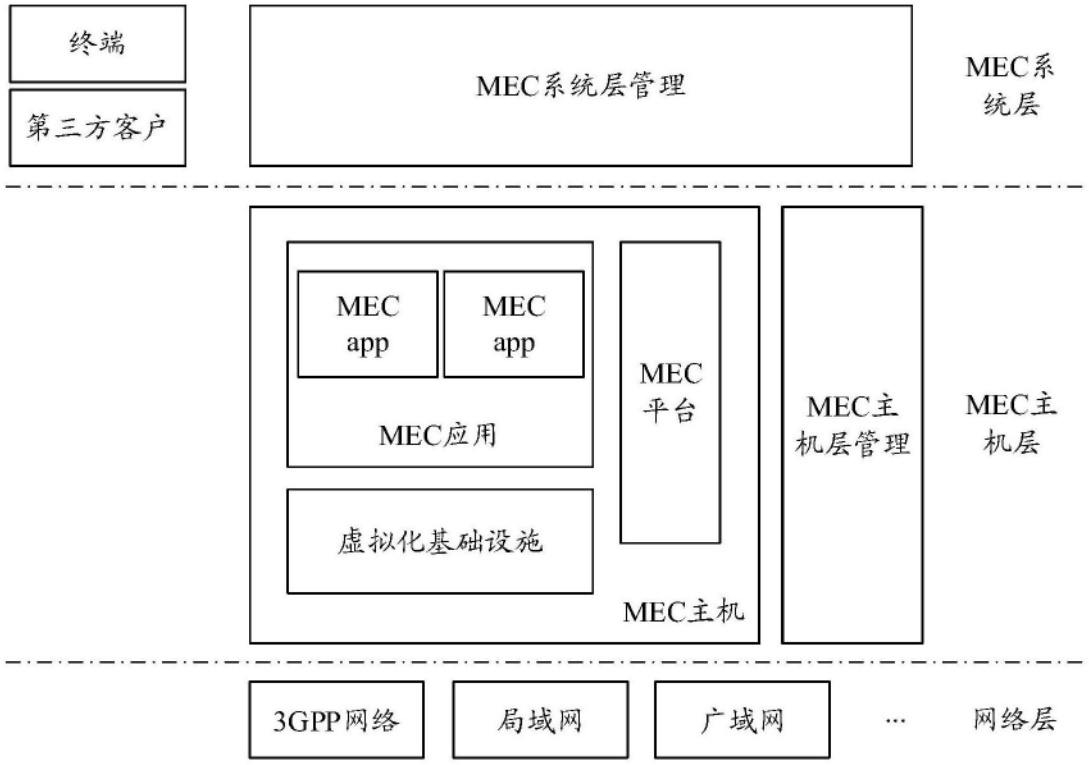

终端
第三方客户
MEC系统层管理
MEC系统层
MEC app
MEC app
MEC应用
虚拟化基础设施
MEC平台
MEC主机
MEC主机层管理
MEC主机层
3GPP网络
局域网
广域网
…
网络层

图1

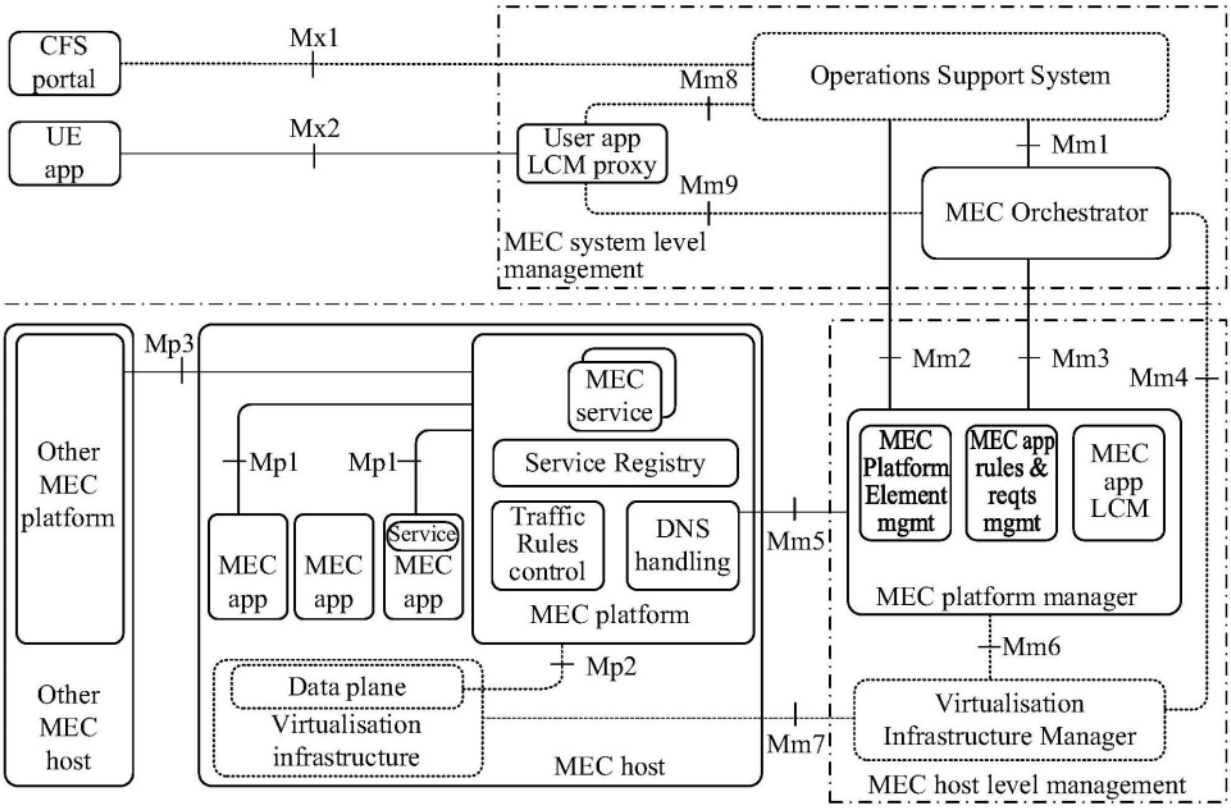

CFS portal
Mx1
UE app
Mx2
Mm8
Operations Support System
User app LCM proxy
Mm1
Mm9
MEC Orchestrator
MEC system level management
Mp3
Other MEC platform
Other MEC host
MEC service
Mp1
Mp1
Service Registry
MEC app
MEC app
Service
MEC app
Traffic Rules control
DNS handling
MEC platform
Mp2
Data plane
Virtualisation infrastructure
MEC host
Mm5
Mm7
Mm2
Mm3
Mm4
MEC Platform Element mgmt
MEC app rules & reqts mgmt
MEC app LCM
MEC platform manager
Mm6
Virtualisation Infrastructure Manager
MEC host level management

图2

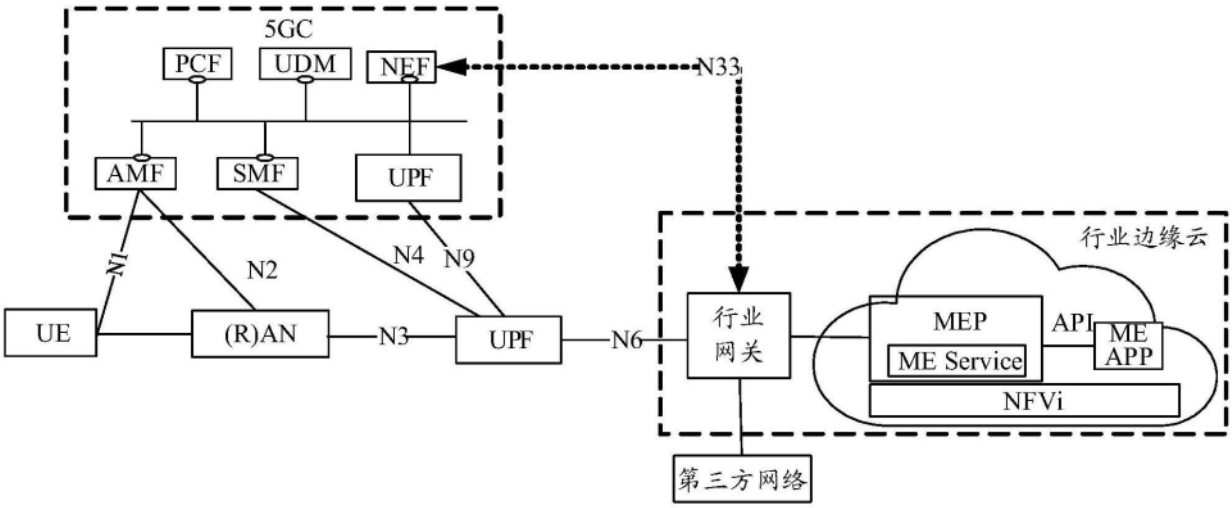

5GC
PCF
UDM
NEF
N33
AMF
SMF
UPF
N1
N2
N4
N9
UE
(R)AN
N3
UPF
N6
行业
网关
行业边缘云
MEP
API
ME
APP
ME Service
NFVi
第三方网络

图3

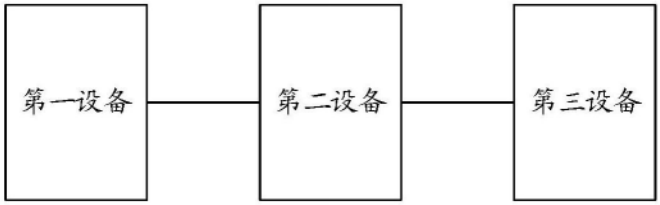

第一设备
第二设备
第三设备

图4

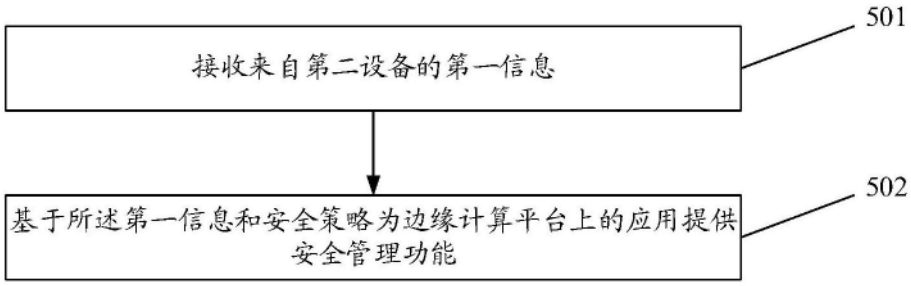

501
接收来自第二设备的第一信息
502
基于所述第一信息和安全策略为边缘计算平台上的应用提供安全管理功能

图5

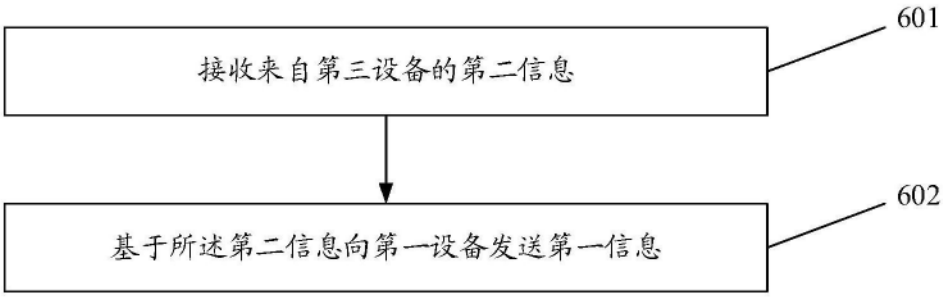

601
接收来自第三设备的第二信息
602
基于所述第二信息向第一设备发送第一信息

图6

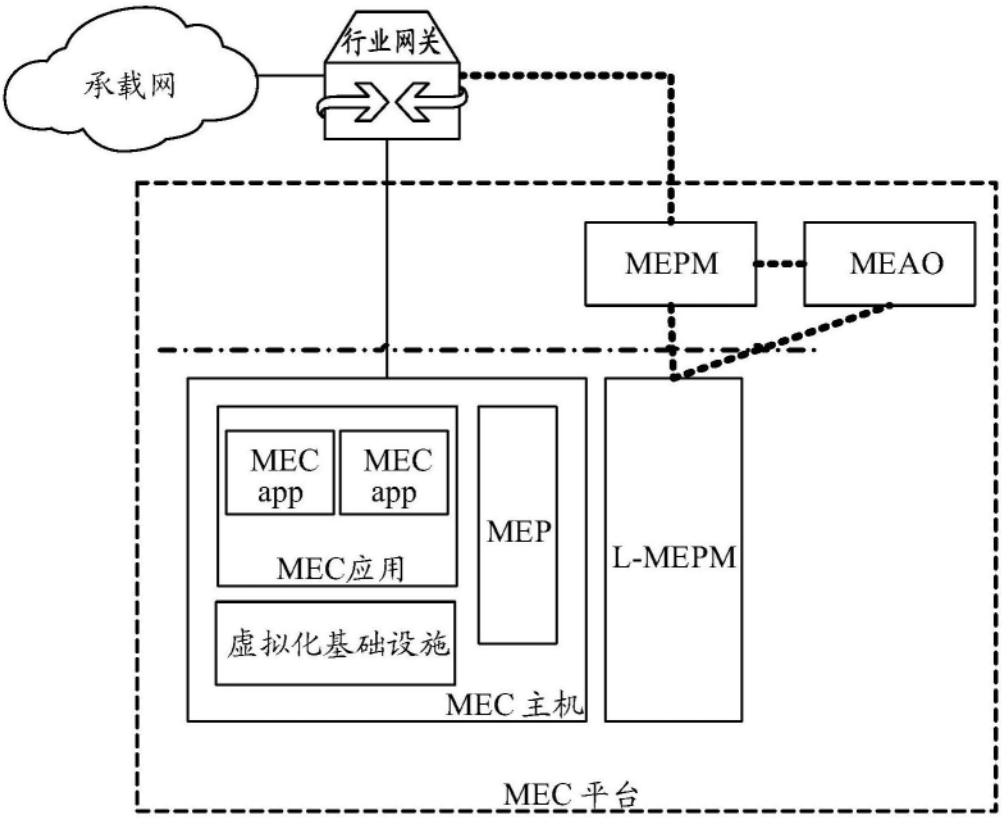

承载网
行业网关
MEPM
MEAO
MEC app
MEC app
MEC应用
MEP
L-MEPM
虚拟化基础设施
MEC 主机
MEC 平台

图7

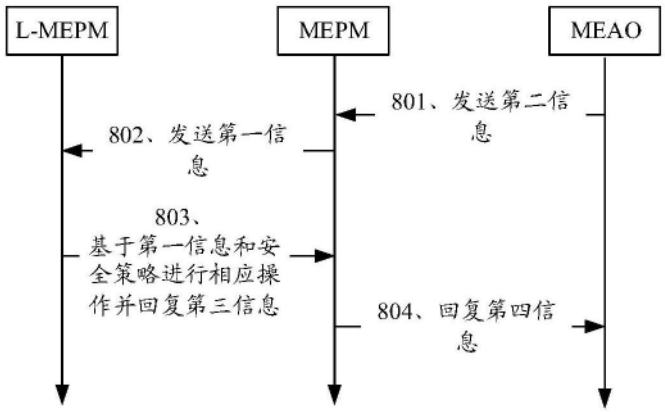

L-MEPM
MEPM
MEAO
801、发送第二信息
802、发送第一信息
803、基于第一信息和安全策略进行相应操作并回复第三信息
804、回复第四信息

图8

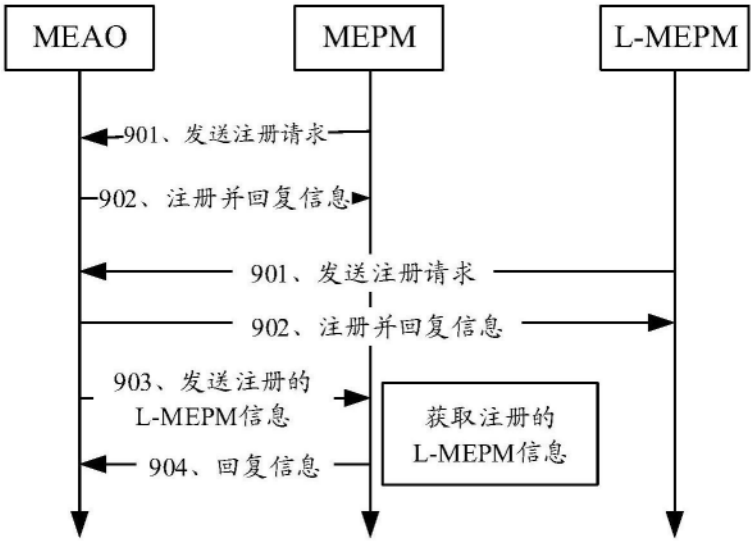

MEAO
MEPM
L-MEPM
901、发送注册请求
902、注册并回复信息
901、发送注册请求
902、注册并回复信息
903、发送注册的L-MEPM信息
获取注册的L-MEPM信息
904、回复信息

图9

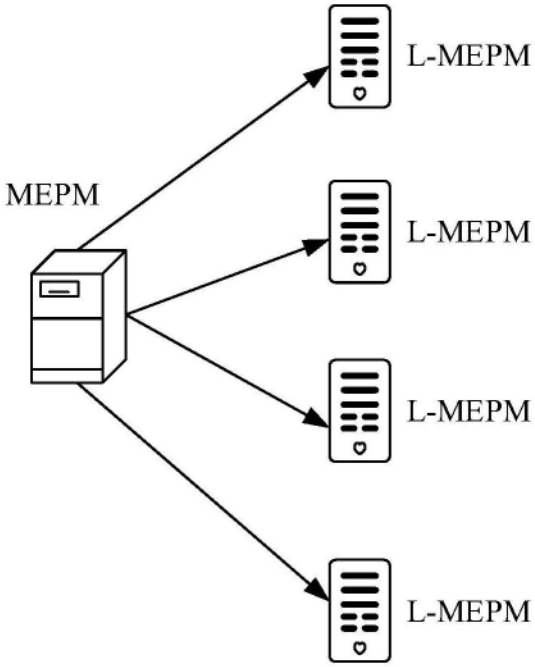

MEPM
L-MEPM
L-MEPM
L-MEPM
L-MEPM

图10

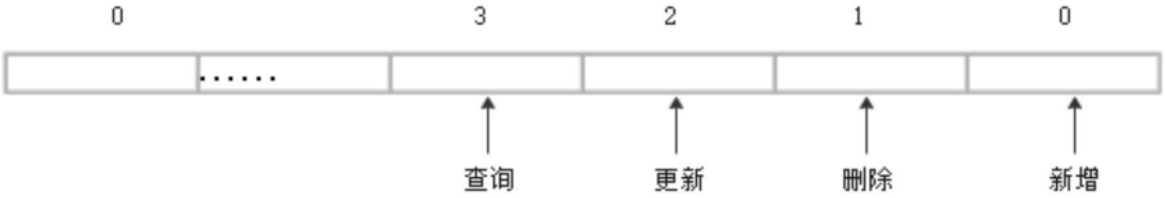

0
3
2
1
0
查询
更新
删除
新增

图11

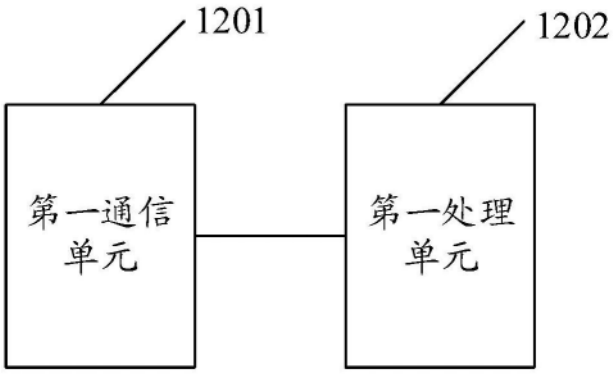

1201
1202
第一通信单元
第一处理单元

图12

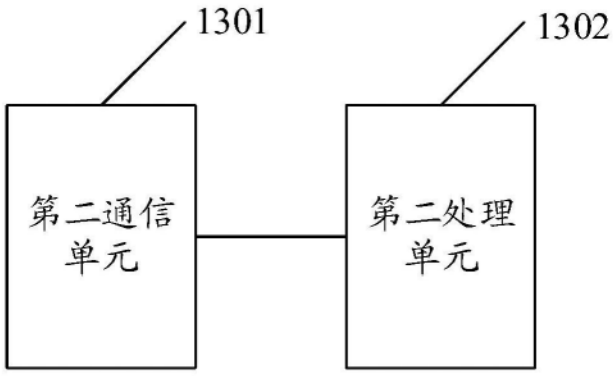

1301
1302
第二通信单元
第二处理单元

图13

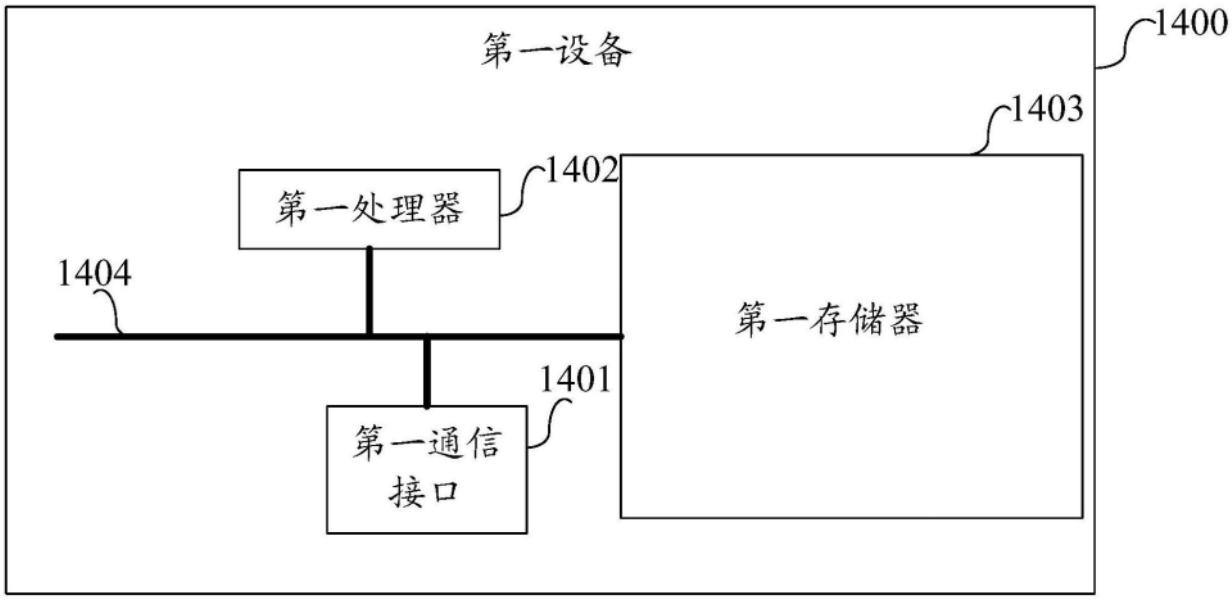

第一设备
1400
1403
1402
第一处理器
1404
第一存储器
1401
第一通信接口

图14

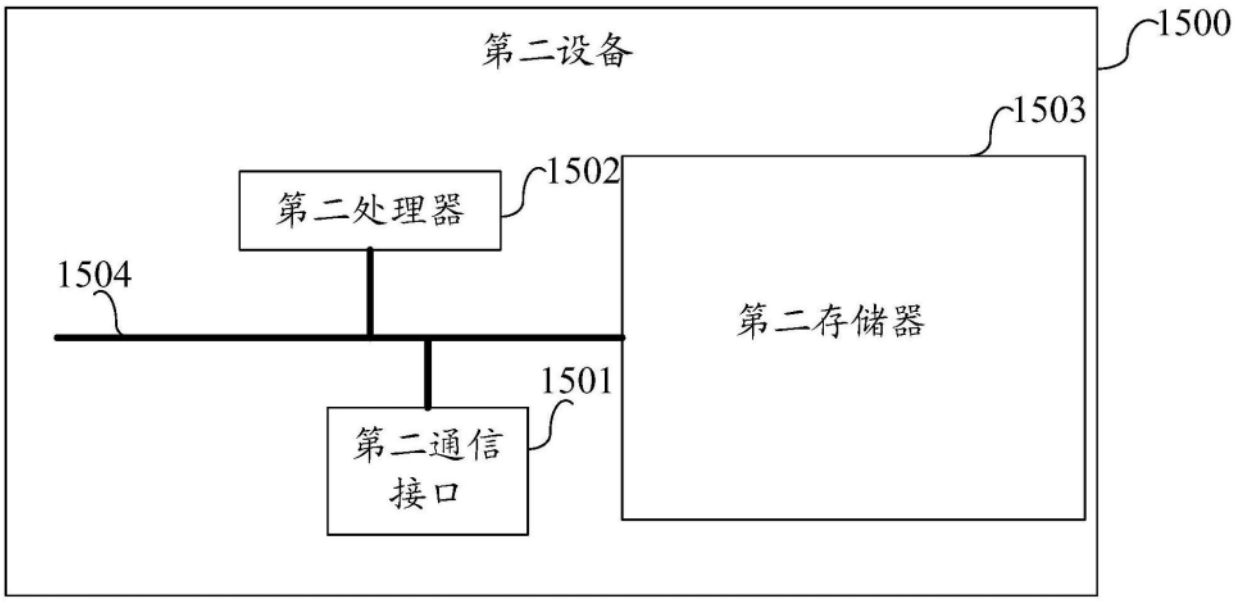


图15