(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103038749 B
(45)授权公告日 2017.09.15

(21)申请号 201180038399.7

(22)申请日 2011.07.01

(65)同一申请的已公布的文献号
申请公布号 CN 103038749 A

(43)申请公布日 2013.04.10

(30)优先权数据
61/360,658 2010.07.01 US

(85)PCT国际申请进入国家阶段日
2013.01.31

(86)PCT国际申请的申请数据
PCT/US2011/042866 2011.07.01

(87)PCT国际申请的公布数据
WO2012/003486 EN 2012.01.05

(73)专利权人 纽戴纳公司
地址 美国加利福尼亚州

(72)发明人 丹·C·康

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 沈锦华

(51)Int.Cl.
G06F 9/455(2006.01)

(56)对比文件
US 2009/0112972 A1,2009.04.30,
CN 1495634 A,2004.05.12,
CN 101719841 A,2010.06.02,
US 2009/0177514 A1,2009.07.09,
I.Krsul等.VMPlants:Providing and Managing Virtual Machine Execution Environments.《proceedings of the ACM/IEEE SC2004 Conference》.2004,第1-12页.

审查员 章媛

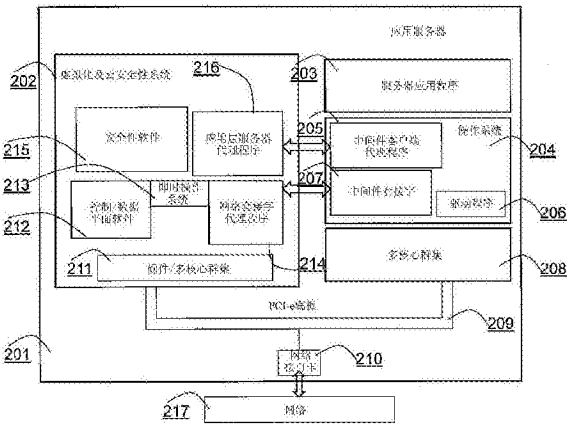
权利要求书4页 说明书11页 附图6页

(54)发明名称

为了优化群集特定配置的使用而按进程类型在群集之间分割进程

(57)摘要

本发明揭示一种用于虚拟化及云安全性的系统及方法。根据一个实施例,一种系统包含:第一多核心处理群集及第二多核心处理群集,其与网络接口卡通信;及软件指令。当所述软件指令由所述第二多核心处理群集执行时,所述软件指令致使所述第二多核心处理群集进行以下操作:接收对服务的请求;建立新虚拟机或调用现存虚拟机以服务于所述请求;及将指示所述服务成功完成的所要结果返回到所述第一多核心处理群集。



CN 103038749 B

1.一种分布式计算系统，其包括：

硬件底板；

第一组多核处理群集，其物理地耦合到所述硬件底板，所述第一组多核处理群集包括具有相同第一指令集的一个或多个第一硬件群集，所述第一组多核处理群集经配置以运行多任务操作系统且在所述多任务操作系统中执行软件指令；

第二组多核处理群集，其物理地耦合到所述硬件底板，所述第二组多核处理群集和所述第一组多核处理群集能够通过所述硬件底板通信，所述第二组多核处理群集包括具有相同第二指令集的一个或多个第二硬件群集，其中所述相同第二指令集不同于所述相同第一指令集，所述第二组多核处理群集经配置以运行实时操作系统，所述实时操作系统经配置以在所述实时操作系统中执行所述软件指令；以及

第一组软件代理程序，其经配置以在所述实时操作系统中执行以：(i)响应于在所述实时操作系统中对至少一部分所述软件指令的执行，接收多个实时处理请求，所述多个实时处理请求由在所述多任务操作系统中执行的第二组软件代理程序从所述第一组多核处理群集上的服务拦截；(ii)服务所述多个实时处理请求；和(iii)将所述多个实时处理请求的执行结果通过所述硬件底板返回到所述第二组软件代理程序。

2.根据权利要求1所述的分布式计算系统，其中所述第二组多核处理群集进一步包括一个或多个实时超管理器，所述实时超管理器经配置以协调多核处理群集的多个指令集以使用所述第二组软件代理程序通过拦截由多任务超管理器管理的所述第一组多核处理群集的请求来分配用于服务的多个实时虚拟机，且使用所述第一组软件代理程序将所述多个实时虚拟机的执行结果通过所述硬件底板返回到所述第一组多核处理群集。

3.根据权利要求2所述的分布式计算系统，其中所述第一组多核处理群集由多任务超管理器或多任务操作系统管理，且所述第二组多核处理群集由实时操作系统管理。

4.根据权利要求3所述的分布式计算系统，其进一步包括：

软件应用层服务器代理程序和网络套接口代理程序，其在所述第二组多核处理群集中执行，且为来自在所述第一组多核处理群集中执行的中间件客户端代理程序和中间件套接口的请求的多个服务而服务；

其中所述中间件套接口和所述中间件客户端通过所述硬件底板与所述软件应用层服务器代理程序和所述网络套接口代理程序通信，以执行一个或多个服务、软件应用程序或第二组多核处理群集中的虚拟机，以及

其中所述一个或多个服务、软件应用程序或虚拟机的所述执行结果通过所述硬件底板发送回所述中间件客户端代理程序和所述中间件套接口。

5.根据权利要求4所述的分布式计算系统，其进一步包括：

所述软件应用层服务器代理程序和所述网络套接口代理程序，其为由所述中间件客户端代理程序和所述中间件套接口发送的新实时应用程序或新实时虚拟机服务，所述中间件套接口或所述中间件客户端代理程序中的任一者与所述软件应用层服务器代理程序和所述网络套接口代理程序通信以执行所述第二组多核处理群集中的新实时应用程序或新实时虚拟机；以及

其中新实时应用程序或新实时虚拟机的所述执行结果通过所述硬件底板发送回所述第一组多核处理群集中的所述中间件客户端代理程序和所述中间件套接口。

6.根据权利要求5所述的分布式计算系统，其中对实时软件应用程序的所述执行或对实时虚拟机的所述执行可进一步包含执行一组或多组实时软件应用程序或虚拟机的一组或多组控制和/或数据平面，包括以下各种中的任一者：包处理功能、应用流节流功能、L4与L7之间的负载平衡器功能、业务管制及塑形功能、QoS功能、VLAN功能、链路聚合功能、GRE封装功能、GTP及IP上IP隧穿功能、具有虚拟路由管理的第三层转发功能、路由及虚拟路由及过滤ACLs软件功能。

7.根据权利要求5所述的分布式计算系统，其进一步包括：

实时软件应用程序或虚拟机软件，其存储在存储器或计算机可读存储媒体中，其中所述实时软件应用程序或虚拟机软件在所述第二组多核处理群集中的一组或多组安全软件堆栈或虚拟机软件堆栈中执行；

一组或多组控制和/或数据平面软件堆栈，其执行一组或多组软件应用程序或虚拟机，包含以下各者中的任一者：

安全功能、具有网络地址翻译的状态防火墙功能、IPSec VPN功能、SSLVPN功能、入侵检测功能、入侵预防功能、防病毒功能、反间谍程序软件功能和应用程序防火墙HTTP或SIP功能。

8.根据权利要求6所述的分布式计算系统，其中所述第二组多核处理群集包括多组相异指令硬件群集，其中至少两组相异指令硬件群集经优化用于执行应用程序或虚拟机的相异类型的实时操作。

9.根据权利要求8所述的分布式计算系统，其中所述相异类型的实时操作包括一组或多组图像处理应用程序、加密处理应用程序、视频压缩处理应用程序、视频解压处理应用程序和模式识别处理应用程序。

10.根据权利要求8所述的分布式计算系统，其进一步包括多个相异指令集和多个相异实时操作，且每一不同指令集包含多个硬件群集和多个实时应用程序或虚拟机执行。

11.一种分布式计算方法，其包括：

在多任务操作系统的控制下执行第一多核处理群集中的软件指令，所述第一多核处理群集中的每一者包括具有相同第一指令集的一个或多个硬件群集，所述第一多核处理群集中的每一者经配置以运行所述多任务操作系统中的相同者且在所述多任务操作系统中的各者的控制下执行所述软件指令，所述第一多核处理群集中的每一者物理地耦合到硬件底板；

在实时操作系统的控制下执行第二多核处理群集中的软件指令，所述第二多核处理群集中的每一者包括具有相同第二指令集的一个或多个硬件群集，所述相同第二指令集不同于所述相同第一指令集，所述第二多核处理群集中的每一者经配置以运行实时操作系统中的一者且在实时操作系统中的各者的控制下执行所述软件指令，所述第二多核处理群集中的每一者物理地耦合到所述硬件底板，所述第一多核处理群集与所述第二多核处理群集能够经由所述硬件底板通信；

在所述第二多核处理群集中执行第一组软件代理程序，所述第一组软件代理程序经配置以：(i)响应于在所述实时操作系统中对至少一部分所述软件指令的执行，接收多个实时功能处理请求，所述多个实时功能处理请求由在所述第一多核处理群集中执行的第二组软件代理程序从所述第一多核处理群集上的服务拦截；(ii)服务所述实时功能处理请求；和

(iii)将所述多个实时功能处理请求的执行结果通过所述硬件底板返回到在所述第一多核处理群集中执行的所述第二组软件代理程序。

12.根据权利要求11所述的方法,其进一步包括实时超管理器,所述实时超管理器经配置以协调所述第二多核处理群集的多个指令集以使用所述第二组软件代理程序基于拦截由多任务超管理器管理的所述第一多核处理群集的请求来分配用于服务的多个虚拟机,且使用所述第一组软件代理程序将多个虚拟机的执行结果通过所述硬件底板返回到所述第一多核处理群集。

13.根据权利要求12所述的方法,其中具有指令集的所述第一多核处理群集由多任务超管理器或多任务操作系统管理,且所述第二多核处理群集由实时操作系统管理。

14.根据权利要求13所述的方法,其进一步包括:

在所述第二多核处理群集中执行软件应用层服务器代理程序和网络套接口代理程序,且为来自在所述第一多核处理群集中执行的中间件客户端代理程序和中间件套接口的请求的多个服务;

其中所述中间件客户端代理程序和所述中间件套接口与所述软件应用层服务器代理程序和所述网络套接口代理程序通信以执行一个或多个服务、应用程序或虚拟机,以及

将所述一个或多个服务、应用程序或虚拟机的所述执行结果通过所述硬件底板返回到所述中间件客户端代理程序和所述中间件套接口。

15.根据权利要求14所述的方法,其进一步包括:

在所述第二多核处理群集中执行相同或不同软件应用层代理程序和网络套接口代理程序;及

将由所述中间件客户端代理撑起和所述中间件套接口发送的新服务、新实时应用程序或新实时虚拟机供应到所述第二多核处理群集;以及

将新实时应用程序或新实时虚拟机的所述执行结果通过所述硬件底板从所述第二多核处理群集返回到所述第一多核处理群集的所述中间件客户端代理程序和所述中间件套接口。

16.根据权利要求15所述的方法,其中对实时软件应用程序的所述执行或对实时虚拟机的所述执行包含一组或多组控制和/或数据平面,其执行所述第二多核处理群集中的一组或多组包处理功能、应用流节流功能、L4与L7之间的负载平衡器功能、业务管制及塑形功能、QoS功能、VLAN功能、链路聚合功能、GRE封装功能、GTP及IP上IP隧穿功能、具有虚拟路由管理的第三层转发功能、路由及虚拟路由及过滤ACLs软件功能。

17.根据权利要求15所述的方法,其中存储在存储器或计算机可读存储媒体中的所述软件应用程序或所述虚拟机可进一步具有执行一组或多组安全软件功能、防火墙功能、具有网络地址翻译的状态防火墙处理和应用程序防火墙HTTP或SIP功能的一组或多组控制和/或数据平面软件堆栈。

18.根据权利要求17所述的方法,其中存储于存储器或计算机可读存储媒体中的所述软件应用程序或所述虚拟机进一步包括以下功能:

执行IPSec虚拟专用网络功能;

执行SSLVPN功能;

实时执行入侵检测和/或预防功能;

实时执行防病毒功能；

实时执行反间谍程序软件功能。

19.根据权利要求16所述的方法，其中所述第二多核处理群集进一步包括多组相异指令硬件群集和多个相异类型的实时操作，其中至少两组相异指令硬件群集经优化用于执行应用程序或虚拟机的相异类型的实时操作。

20.根据权利要求19所述的方法，其中执行相异类型的实时应用程序或虚拟机包括一组或多组图像处理应用程序、加密处理应用程序、视频压缩处理应用程序、视频解压处理应用程序和模式识别处理应用程序。

21.根据权利要求19所述的方法，其进一步包括：使用所述第二多核处理群集执行多个实时应用程序或虚拟机。

为了优化群集特定配置的使用而按进程类型在群集之间分割进程

[0001] 本申请案主张2010年7月1日申请的题目为“用于云安全性管理的系统和方法(A System and Method for Cloud Security Management)”的第61/360,658号临时申请案的优先权,所述案以引用的方式完全并入本文中。

技术领域

[0002] 本方法及系统涉及计算机系统,且更明确来说,涉及虚拟化及云安全性。

背景技术

[0003] 在计算中,虚拟化是建立某些对象(例如,硬件平台、操作系统、存储装置或网络资源)的虚拟(而非实际)版本。

[0004] 虚拟化是企业IT的整体趋势的部分,企业IT包括:自主计算,其为IT环境将能够基于所感知的活动来管理其自身的一情形;及公用程序计算,其中计算机处理能力被视为客户端可仅在需要时支付以获得的公用程序。虚拟化的常见目标是使管理任务集中化,同时改善可调整性及工作负载。

[0005] 使用高速个人计算机及智能型移动装置的大量用户的聚集显著增加虚拟化环境中所需的包处理性能。对每一包的处理是区分及保障服务所必要的。绿色计算正变为限制电力消耗所必须的。又,必须缩短基础结构部署调度以实现较快收益产生。

[0006] 包括多核心CPU及硬件工业标准(例如,AMC、快速PCI(PCI Express)、AdvancedTCA及刀片中心(Blade Center))的最近技术改善可实现预期性能等级,同时提供在集成与电力消耗比方面具有卓越性能的可调整解决方案。这还意味着将需要高性能软件包处理来有效率地实施不同协议且确保充足的服务质量。大多数高级网络已采用分级(class-based)服务质量的概念,因此所述网络需要每包处理以用于在包服务之间进行区分。

[0007] 数据中心与远程用户之间的业务是使用IPSec加密且需要硬件密码引擎的辅助。多核心技术提供必要处理能力且以较低电力消耗提供高级网络所需的高集成度。然而,软件设计复杂性持续,从而使开发及集成困难。结果是妨碍了基于多核心的解决方案的部署。

[0008] 随着虚拟化及云计算逐渐变得越来越流行,可将现存服务器在逻辑上分组为可用资源的单一、大的集区。将这些装置的容量聚集到可用资源的单一集区中使得能够有效率地利用服务器,此导致资本及操作费用两者的相关减少。然而,虚拟化使传统安全性措施不足以保护以免受虚拟环境中的新出现的安全性威胁。这是归因于在服务器与存储子系统之间的数据路径中缺乏主保护。保护的缺乏阻止企业体验主数据中心转变的全部益处。

[0009] 虽然云计算常常被视为增加安全性风险且引入新的威胁媒介(vector),但其也呈现改善安全性的令人激动的机会。云的特性(例如,标准化、自动化及到基础结构中的增加的可见性)可显著地提高安全性等级。在隔离域中运行计算服务,在运动中及静止时提供数据的默认加密,及经由虚拟存储装置控制数据均已变成可改善可信度及减少数据损失的活动。另外,硬化的运行时图像的自动供应(provisioning)及回收可减少攻击表面且改善鉴

识(forensics)。

发明内容

[0010] 本发明揭示一种用于虚拟化及云安全性的系统及方法。根据一个实施例，一种系统包含：第一多核心处理群集及第二多核心处理群集，其与网络接口卡通信；及软件指令。当由所述第二多核心处理群集执行所述软件指令时，所述软件指令致使所述第二多核心处理群集接收对服务的请求，建立新虚拟机或调用现存虚拟机以服务于所述请求，且将指示所述服务的成功完成的所要结果返回到所述第一多核心处理群集。

附图说明

[0011] 包括作为本说明书的部分的随附图式说明目前优选实施例，且与上文所提供的一般描述及下文所给出的优选实施例的详细描述一起用以解释及教示本文中所揭示的原理。

[0012] 图1说明根据一个实施例的供本系统使用的示范性系统层级布局。

[0013] 图2说明根据一个实施例的供本系统使用的包括虚拟化及云安全性架构的示范性系统层级布局。

[0014] 图3说明根据一个实施例的供本系统使用的示范性软件基础结构。

[0015] 图4说明根据一个实施例的供本系统使用的示范性硬件基础结构。

[0016] 图5说明根据一个实施例的供本系统使用的示范性硬件基础结构实施方案。

[0017] 图6说明根据一个实施例的供本系统使用的具有虚拟化支持的示范性系统层级布局。

[0018] 应注意，各图未必按比例绘制，且类似结构或功能的元件贯穿各图通常由相似参考数字表示以用于说明性目的。还应注意，各图仅既定促进对本文中所描述的各种实施例的描述。各图不描述本文中所揭示的教示的每一方面且不限制权利要求书的范围。

具体实施方式

[0019] 揭示一种用于虚拟化及云安全性的系统及方法。根据一个实施例，一种系统包含：第一多核心处理群集及第二多核心处理群集，其与网络接口卡通信；及软件指令。当由所述第二多核心处理群集执行所述软件指令时，所述指令致使所述第二多核心处理群集接收对服务的请求；建立新虚拟机或调用现存虚拟机以服务所述请求；及将指示所述服务的成功完成的所要结果返回到所述第一多核心处理群集。

[0020] 根据一个实施例，本系统提供快速路径包处理的有效实施以利用由多核心处理器提供的性能益处。为实现安全性目的，本系统包括完整、全面且即用的网络连接特征集合，所述网络连接特征包括：VLAN、链路聚集、GRE封装、经由IP隧穿的GTP及IP、通过虚拟路由管理、路由及虚拟路由的第3层转发、每包QoS及过滤(ACL)、IPSec、SVTI、IKEv1及IKEv2。

[0021] 根据一个实施例，本系统可与一控制平面操作系统(OS)完全集成以用于最大程度地再使用软件、简化集成及隐藏多核心设计复杂性。本系统在具有用于与内建式加速器(例如，密码引擎)介接的统一高级API的多核心平台上运行，且在包括低成本高容量硬件的不同多核心架构及用于网络装备的大ATCA配置上进行调整。本系统提供开放架构以使集成容易。

[0022] 根据一个实施例，本系统的一个方面包括从数据中心中的服务器卸载包处理。本系统的又一方面包括并入额外软件堆栈以支持安全性及其它应用程序功能。

[0023] 根据一个实施例，提供安全性软件堆栈、UTM(统一威胁管理)或企业安全性堆栈。除了在系统上透明地运行的软件外，还存在可由包含于下文所描述的硬件刀片中的多核心处理群集加速的安全性相关功能。

[0024] 根据一个实施例，本系统的另一方面包括提供虚拟化安全性。虚拟化安全平台是云计算安全平台的基础，且包括额外软件以从虚拟化服务器卸载包处理及安全性功能。根据一个实施例，实情为，包处理及安全性功能接着由作为本系统的部分的包处理虚拟机及安全性虚拟机来处置。

[0025] 对于现存客户，虚拟化安全性软件是经由安全链路及远程呼叫中心而从远程服务器下载到现存用户的系统上。对于新用户，所述软件经预先安装且随着随附硬件一起递送。一旦软件在初始电力开启后经加载，客户的应用程序便取决于安全性应用而下载到各种硬件模块上的软件上。

[0026] 由本系统提供的益处的简要概述包括以下各者：

[0027] • 虚拟及物理设备到服务器虚拟化中的集成；

[0028] • 虚拟机认知；

[0029] • 每一虚拟机上的安全性策略的实施；

[0030] • 虚拟机的可见性及控制；

[0031] • 由设备及安全性软件的组合所提供的安全性；

[0032] • 端点数据保护；

[0033] • 业务及安全性功能的加速；

[0034] • 用于第三方安全性软件供货商的开放软件框架；

[0035] • 主机性能损失的消除；及

[0036] • 数据安全性。

[0037] 本系统包括集成于标准服务器平台中的分布式实时计算能力。可将分布式实时计算群集视作服务器群，且当增加工作负载时可按需求增加服务器群资源。可快速启动、撤销启动、升级或部署服务器群资源。

[0038] 本系统的性能可调整性是二维的：水平及垂直。相同设备功能可通过同质架构而垂直地扩展，且不同设备功能可通过异质架构而水平地扩展。下文更详细地解释同质及异质架构。

[0039] 本系统提供电力消耗最优化。应用程序加载驱动方法提供最佳电力消耗利用。按需求启用及停用资源以遵循绿色能源策略。

[0040] 本系统的软件编程模型提供：所有现存应用程序无需被重写，且所有新出现的新应用程序可透明地运行。

[0041] 图1说明根据一个实施例的供本系统使用的示范性系统层级布局。应用服务器101正运行服务器应用程序103。应用服务器101具有操作系统(OS)104、驱动程序106、中间件套接字107及中间件代理程序105。应用服务器101正运行用于包及应用程序处理或安全性软件的多核心群集108，且经由PCI-e(快速PCI)底板109与网络接口卡(NIC)110通信。网络接口卡(NIC)110提供网络111接入。根据本文中所揭示的实施例，中间件套接字107及代理程

序105与虚拟化及云安全性系统102通信。

[0042] 图2说明根据一个实施例的供与本发明系统一起使用的包括虚拟化及云安全性架构的示范性系统层级布局。应用服务器201正运行服务器应用程序203。应用服务器201具有操作系统(OS)204、驱动程序206、中间件套接字207及中间件代理程序205。应用服务器201正运行用于服务器应用程序的多核心群集208。应用服务器201需要包处理及安全性功能，且这些请求由虚拟化及云安全性系统(VCSS)202拦截及服务。所述服务可经由中间件套接字207及代理程序205进行通信。根据本文中所揭示的实施例，中间件套接字207及代理程序205与虚拟化及云安全性系统(VCSS)202通信。根据一个实施例，VCSS202包括：硬件刀片，其具有插入到PCI-e底板209中的多核心处理群集211；及最小软件堆栈，其包括网络套接字代理程序214、实时操作系统(RTOS)213及控制/数据平面软件堆栈212。VCSS202还可包括安全性支持215及应用层服务器代理程序216。中间件套接字207及代理程序205还可关于服务请求而与应用服务器代理程序216通信。应用服务器代理程序216与RTOS213、控制/数据软件堆栈212及网络套接字代理程序214通信以经由PCIe底板209通过网络接口卡(NIC)210而通过HW/多核心处理群集来服务于请求。网络接口卡(NIC)210提供网络217接入。下文紧跟着进行对控制/数据平面堆栈212及安全性软件215的更详细描述。

[0043] 硬件(HW)刀片/多核心群集211提供用于开发智能网络连接及安全平台的硬件，其支持对智能网络/安全性加速及对聚合数据中心应用(例如，存储、安全性、深层包检查(DPI)、防火墙、WAN最佳化及应用程序递送(ADC)计算)的应用程序卸载的增长需求。HW/多核心群集211包含多核心处理器群集(例如，Freescale的P4080E QorIQ)、DDR存储器、快闪存储器、10Gb或1Gb网络接口、迷你SD/MMC卡槽、USB端口、串行控制台端口及电池后备式(battery backed)RTC。配置硬件的软件包括实时OS(即，Linux及在Linux下的驱动程序)以控制硬件块及功能。

[0044] 一般来说，多核心群集及在多核心群集中的安全性硬件加速单元可处置适当功能以用于实施DPI/DDI(深层包检查/深层数据检查)。举例来说，协议分析包括HTTP、SIP及SNMP；内容格式包括XML、HTML/JavaScript；且模式匹配包括IPS模式及病毒模式。

[0045] HW/多核心群集的其它实施例可包括不同多核心群集(例如，来自Cavium Networks、Netlogic及Tilera的多核心群集)(例如)以加速其它新出现的功能。举例来说，Cavium Networks的Nitrox系列有助于实施其它安全性措施，且Tilera的GX系列有助于实施多媒体串流传输及压缩/解压缩应用。虽然所描绘的实施例包括PCI-e形状因数，但在不脱离本系统的精神的情况下可使用ATCA及刀片中心及其它形状因数。

[0046] 实时操作系统(RTOS)213是既定服务于实时应用程序请求的操作系统(OS)。RTOS的关键特性是其关于其接受及完成应用程序的任务所采用的时间量的一致性的程度；可变性为抖动。硬实时操作系统相比于软实时操作系统具有较少抖动。主要设计目标并非高处理量，而是软或硬性能分类的保证。通常或一般可满足期限(deadline)的RTOS为软实时OS，但如果其可确定性地满足期限，则其为硬实时OS。

[0047] 实时OS具有用于调度的高级算法。调度器灵活性使得能够实现对进程优先权的较宽计算机系统协调(orchestration)，但实时OS更常专用于应用程序的窄集合。实时OS的关键因素是最小中断等待时间及最小线程切换等待时间。然而，相比针对实时OS在一给定时段内可执行的工作量，实时OS针对其可如何快速或如何可预测地响应而更有价值。实时OS

的实例包括来自Windriver的VxWorks或Linux。

[0048] 根据一个实施例，安全性软件215包含以下各者中的一者或一者以上：具有NAT(网络地址翻译)的状态防火墙、IPSec VPN、SSLVPN、IDS(入侵检测系统)及IPS(入侵预防系统)、应用程序业务节流、防病毒及反间谍程序软件、应用程序防火墙(HTTP及SIP)、L4到L7负载平衡器、业务管制(policing)及塑形、虚拟化及云计算支持，及对web服务、移动装置及社会网络连接的支持。以下表1提供对模块的描述。

[0049]

软件功能	描述
具有 NAT 的状态防火墙	► 对网络资源的受控接入。 网络地址翻译
IPSec VPN	► 用于网络之间的业务的机密性、鉴认及完整性。安全远程接入
SSLVPN	► 经由浏览器的安全远程接入
IDS 及 IPS	► 检测及防止 L4 到 L7 及应用程序层级处的入侵
应用程序业务节流	► 检测及节流优先权较低的应用程序业务(例如，P2P、IM)
网络防病毒	► 从交叉周边(例如，电子邮件、HTTP、FTP)阻止病毒感染有效负载及恶意软件
应用程序防火墙(HTTP/SIP)	► 使用 HTTP/SSL/压缩有效负载的深层数据检查来阻止攻击/入侵
L4 到 L7 负载平衡器(ADC)	► 跨越多个服务器分布负载
业务管制及塑形	► 对网络/应用程序业务强制执行 QoS 策略
虚拟化(数据中心)	► 在单一硬件内支持多个虚拟安全性设备。映射到客户的实例

[0050] 表1：安全性软件模块

[0051] 根据一个实施例，安全性的硬件加速具有用于协议分析的深层包检查/深层数据检查(DDP/DDI)。DDP/DDI使得安全性设备及安全功能性的部署能够增加。

[0052] 应用层服务器代理程序216服务于由应用程序客户端代理程序205及207发送到应用服务器216的不同应用程序以服务于那些请求。所述服务可为客户端希望服务器代表客户端完成的任何实时及计算密集型任务。一旦完成服务，则服务器基于在其与客户端之间定义的信号交换机制经由接口将结果递送到客户端。

[0053] 图3说明根据一个实施例的供本系统使用的示范性软件基础结构。示范性软件基础结构301包括对丰富内容媒体(rich content media，RCM)应用程序302的支持。基础结构301包括进程间通信303及对各种操作系统304的支持。基础结构301包括RCM框架305、通用API306、对各种编解码器及库扩展307的支持、系统框架308及数据框架309。

[0054] 应用程序框架302可经由API(应用程序编程接口)介接到任何丰富内容多媒体应用程序或来自各种来源的软件服务(SOA)。应用程序可来自一个或一个以上群组，所述一个或一个以上群组包括安全性、安全性解密/加密、视频压缩/解压缩、音频压缩/解压缩、成像压缩(imaging compression)/解压缩(定义为文字、音频或视频及图形)与用于远程或本地来源的解码及编码的组合。在此状况下，编码为压缩技术且解码为解压缩技术。内容来源可来自在服务器、PC或其它移动装置上运行的本地装置。内容来源可为经由从服务器、web服

务器、应用服务器、数据中心中的数据库服务器运行的LAN、WAN的远程装置或经由因特网接入的任何云计算应用程序。

[0055] 较新应用程序(例如,模式辨识)可从基本文字、音频、视频及成像扩展以通过特殊算法在本地或远程运行来编码及解码。换句话说,应用程序框架可经扩展以通过特殊算法介接模式辨识应用程序从而从本地服务器、PC或移动装置压缩及解压缩或从来自因特网的远程云计算资源远程地压缩及解压缩。

[0056] 进程间通信303在群集、操作系统、系统互连及超管理器上发生。示范性实施例包括用于进程间通信的如下文所解释的DDS。重点包括:经由分布式消息接发传递的通信(IPC);独立于OS、平台及互连;对系统规模的透明性及在不修改代码的情况下重配置;多个生产者及消费者;分布式处理间通信技术;基于消息的协议或数据中心分布式数据服务;透明的应用程序到应用程序连接;可靠递送通信模型;独立于操作系统(Windows、Linux及Unix);独立于硬件平台(RISC、DSP或其它者)。

[0057] 通信标准数据分布服务(Data Distribution Service;DDS)使得能够实现系统可调整性,所述可调整性可支持通信要求的范围,从具有间歇及高度可变的通信规范的固定及移动装置的对等式通信变化到巨大的群通信。

[0058] DDS标准特别适合于分布实时数据以用于记录以及用于一般分布式应用程序开发及系统集成。DDS指定经设计以用于启用实时数据分布的API。其使用发布-预订通信模型且支持消息接发及数据对象中心数据模型两者。DDS提供相对于基于内容的过滤及转变、每数据流连接性监视、冗余、复制、递送努力(delivery effort)及定序以及自发性发现的若干增强的能力。此外,DDS提供相对于数据对象生命周期管理、最佳努力及可预测递送、递送定序、资源管理及状态通知的新能力。

[0059] RCM框架305提供核心服务(SOA)以用于在203应用程序上运行的应用程序与企业SOA当中的通信,或跨越多个基于实时的操作系统及在本系统上运行的基于处理器SOA的应用程序而扩展。RCM框架305提供经由分布式消息接发传递的通信(IPC)及基于数据中心DDS的分布式消息通信。其为独立于OS、平台及互连的,对系统规模为透明的且可在不修改代码的情况下重配置。所述框架支持到RDMS存储装置中的事件记录及检查。

[0060] 系统框架308包括本地硬件群集及资源调度器及管理、供应、配置、重定位及远程接入。多个实时OS配置支持以下各者:

[0061] • AMP(不对称实时多处理):不同OS控制不同HW群集,如控制/数据平面

[0062] • SMP(对称实时多处理):同一类型的应用程序正运行于同一HW群集上,如数据平面

[0063] • 处理间通信:各种OS之间的通信

[0064] • 全局资源调度器及群集的管理

[0065] • 全局及局部资源加载、统计及迁移

[0066] • 虚拟化基础结构接口及群集的管理。

[0067] 基于IP的网络应用可分割为三个基本元素:数据平面、控制平面及管理平面。

[0068] 数据平面是一网络节点的子系统,其从一接口接收包及发送包,以由适用协议所需的某一方式处理所述包,且在适当时递送、丢弃或转发所述包。对于路由功能,数据平面由路由器用以对包作出转发决策的程序(算法)的集合组成。算法界定了来自所接收包的信

息以在其转发表中寻找特定条目，以及路由功能用于寻找所述条目的确切程序。数据平面从较高级处理器卸载包转发。对于数据平面接收且未经寻址以用于递送到节点自身的包中的大部分或全部，其执行所有需要的处理。类似地，对于IPSec功能，安全网关查核安全性关联(Security Association)对于传入流是否有效，且如果有效，则数据平面在本地寻找信息以将安全性关联应用到包。

[0069] 控制平面维持可用以改变由数据平面使用的数据的信息。维持此信息需要处置复杂信令协议。在数据平面中实施这些协议将导致不良转发性能。管理这些协议的常见方式是使数据平面检测传入的信令包且在本地将所述包转发到控制平面。控制平面信令协议可更新数据平面信息且将传出的信令包注入数据平面中。此架构起作用，因为信令业务是全局业务的极小部分。对于路由功能，控制平面由一个或一个以上路由协议组成，所述一个或一个以上路由协议提供路由信息在路由器之间的交换，以及路由器用以将此信息转换到转发表中的程序(算法)。一旦数据平面检测到路由包，其就将其转发到控制平面以使路由协议计算新路线、添加或删除路线。转发表是用此新信息来更新。当路由协议必须发送包时，包被注入于数据平面中以在传出流中发送。对于IPSec安全性功能，用于密钥交换管理的信令协议(例如，IKE或IKEv2)位于控制平面中。传入的IKE包在本地被转发到控制平面。当更换密钥时，位于数据平面中的安全性关联由控制平面更新。传出的IKE包被注入于数据平面中以在传出流中发送。

[0070] 为了给下一代网络应用程序提供完整的解决方案，当相比于在因特网起始时的简单TCP/IP堆栈时，包处理在现今要复杂得多。参看本文中针对控制平面及数据平面的定义的描述。高速处理必须集中于简单处理且是在快速路径或数据平面中完成。软件堆栈正运行于由多个CPU核心完成以处置数据平面任务的数据平面上。将复杂处理委派(delegate)到慢速路径及控制平面。快速路径必须集成大量协议且经设计以使得添加新协议将不会损失整个系统的性能。

[0071] 常见网络使用状况是由VPN/IPSec隧道构成的状况及聚集HTTP的Gbps、视频及音频串流的状况。由于L3/L7协议经加密，因此仅由流亲和性构成的数据平面设计不能将特定核心指派到所述协议中的每一者。此情形仅在一旦所有预IPSec处理及有效负载的解密完成后才成为可能。在每一层级处，如果包不能在快速路径层级处加以处置，则可发生异常。实施额外协议在初始呼叫流中添加测试且需要更多指令。总性能将较低。然而，存在一些软件设计规则，其可导致特征与性能之间的优良折衷。

[0072] 管理平面提供到整个系统中的管理接口。其含有支持操作管理、管理或配置/供应动作的过程，例如：

[0073] • 用于支持统计数据收集及聚集的设施

[0074] • 对管理协议的实施的支持

[0075] • 经由Web页或传统SNMP管理的命令行接口、图形用户配置接口。还可实施基于XML的更复杂的解决方案。

[0076] 本系统支持丰富内容多媒体(RCM)应用程序。由于丰富内容多媒体应用程序消耗及产生大量不同类型的数据，因此在现今具有能够处理、操纵、发射/接收及检索/存储所有各种数据(例如，数据、语音、音频及视频)的分布式数据框架是极为重要的。本系统还支持下文表2中所列出的其它丰富数据类型，且不限于成像、模式辨识、话音辨识及动画。数据类

型可从基本类型格式扩展且变成多个固有数据类型的组合数据类型。因为复杂数据类型发射及接收端将需要在传输之前将极其复杂的数据串流“压缩”到某一特定工业标准或专属算法中，所以在接收点的端处需要将数据“重构”回成原始数据类型。视频数据在通过特定算法压缩之后可变成不同数据类型，即，MPEG4及H.264。相同情况适用于音频数据。因此，在目的地处的数据重构之前需要支持某些类型的数据同步机制。新出现的应用程序可与通过类似于上文所陈述的描述的表所列出的任何数据类型混合。

[0077]

	多媒体对丰富内容多媒体	
	多媒体	**丰富内容多媒体**
有限数据类型	音频、视频、图形	文字、音频、视频、图形、动画、话音及模式辨识、静态/动态 2D/3D 成像 AI 视觉、手写辨识、安全性
内容来源	单一本地	多个，远程/本地
内容目的地	单一	多个，远程/本地
内容同步	来自单一来源的简单音频/视频	来自多个来源的音频/视频/数据的任何组合
内容串流	单一	多个
应用程序	主要为解码	解码及编码
实时	否	是
互动	否	是
数据来源：同步	否	是
数据目的地：重构	否	是
任何数据类型组成	否	是
任何数据类型保护	否	是

[0078] 表2:数据类型

[0079] 在网络中心计算模型内，令人畏缩的挑战是管理分布式数据及促进所述数据的局部化管理。解决这些要求的一架构方法通常称作分布式数据库。分布式数据库模型的益处在于，其保证对企业为关键的所有信息的连续实时可用性且促进位置透明软件的设计，此直接影响软件模块再使用。

[0080] 软件应用程序跨越动态网络获得对实时改变的信息的可靠瞬时接入。所述架构独特地将对等式数据分布服务网络连接及实时存储器内数据库管理系统(DBMS)集成到完整解决方案中，所述解决方案在动态配置的网络环境中管理快速改变的数据的存储、检索及分布。其保证对企业为关键的所有信息的连续实时可用性。DDS技术用以使得能够实现用于分布式数据库管理的真实非集中式数据结构，而DBMS技术用以提供实时DDS数据的持续性(persistence)。

[0081] 根据一个实施例，嵌入式应用程序无需知晓SQL或OBDC语意，且未强制企业应用程序知晓发布-预订语意。因此，数据库变成遍及系统而分布的数据表的聚集。当节点通过对

表执行SQL插入(INSERT)、更新(UPDATE)或删除(DELETE)语句来更新所述表时，所述更新主动地经推送到其它主机，所述主机需要经由实时发布及预订消息接发的对同一表的本地接入。此架构方法使得能够实时复制任何数目个远程数据表。

[0082] 图4说明根据一个实施例的供本系统使用的示范性硬件基础结构。主机406(对于主机的描述，参看图1)经由主机及存储器接口401与各种群集通信。硬件基础结构包括运行相同操作系统及应用程序的一个或一个以上处理元件(PE1402、PE2403、PE3405及PE4404)的群集。处理元件经由进程间通信407通信。

[0083] 为了整合示范性硬件基础结构的描述，返回参看上文所描述的硬件刀片。取决于硬件刀片的封装密度，每一硬件刀片可包括(例如)Freescale的QorIQ4080的群集(在一个IC封装内具有8个CPU)或多个群集。一般来说，一个Freescale的QorIQ4080(作为一实例)群集对应于图4中的硬件基础结构的处理元件的一个群集(例如，PE1...PE18)。

[0084] 如果安装两个硬件刀片且每一刀片具有相同类型的多核心群集(例如，Freescale的QorIQ)，则其称为同质扩展。在另一实施例中，硬件刀片具有在一个刀片中包括一个以上群集的容量。

[0085] 如果安装两个硬件刀片且第一刀片具有Freescale的QorIQ4080且第二刀片具有Cavium Network的群集OCTEON II CN68XX，则Freescale群集对应于PE1...PE18且Cavium群集对应于PE2...PE216(假设使用16个核心)。

[0086] 主机406为一标准服务器，其表示基于x86的群集。其可执行服务器应用程序。举例来说，所述主机可表示应用服务器、web服务器或数据库服务器。其可运行所有通用应用程序、I/O功能，及OS的其它系统相关任务。

[0087] 图5说明根据一个实施例的供本系统使用的示范性硬件基础结构实施方案。主机506经由主机及存储器接口501与各种群集通信。硬件基础结构包括运行相同操作系统及应用程序的一个或一个以上处理元件的群集。在此实例中，PE1为运行三个串流的音频引擎502，PE2为安全性引擎503，PE3为视频编码引擎505，且PE4为运行两个串流的视频解码引擎。处理元件经由进程间通信507通信且具有共享存储器508。

[0088] 图6说明根据一个实施例的供本系统使用的具有虚拟化支持的示范性系统层级布局。应用服务器601包括一个或一个以上虚拟主机610、611。虚拟主机610及611包括具有操作系统(OS)及应用程序(App)的虚拟机(VM)。中间件612与VCSS602通信，且超管理器609及604处置资源调度及分配。服务器601正运行用于包及应用程序处理的多核心群集608。多核心群集经由PCI-e底板606与网络接口卡(NIC)607通信。网络接口卡(NIC)607提供网络615接入。VCSS602包括具有多核心群集605(HW/多核心)的硬件刀片、用于调度及分配资源的超管理器604、具有虚拟机支持的接口603，及若干安全性虚拟机功能(SF1、SF2...SFn)613及包处理虚拟机功能(PKT1、PKT2...PKTn)614。

[0089] 也称作虚拟机管理器(VMM)的超管理器609允许多个操作系统(称为客体)同时在主机计算机上运行。超管理器被如此命名是因为其在概念上比监督程序高一个层级。超管理器向客体操作系统呈现虚拟操作平台且管理客体操作系统的执行。多种操作系统的多个实例可共享虚拟化的硬件资源。超管理器安装于仅有任务为运行客体操作系统的服务器硬件上。非超管理器虚拟化系统用于专用服务器硬件上的类似任务，但也通常用于桌上型、便携式及甚至手持型计算机上的任务。

[0090] 主机超管理器609的实例包括由Vmware、Citrix及Microsoft提供的产品。在硬件刀片上的嵌入式超管理器的实例包括由Windriver及Green Hills Software提供的产品。

[0091] 嵌入式超管理器604为基于实时的超管理器。嵌入式超管理器用于实时嵌入式虚拟化中。超管理器允许开发者在单一装置中充分利用多个操作系统，因此开发者可扩展及增强装置功能性；超管理器通过增加可靠性及减少风险来促进多核心处理器的采用；且超管理器提供对下一代嵌入式装置进行架构设计所需的新软件配置选项。

[0092] 若干安全性虚拟机功能(SF...613)及包处理虚拟机功能(PKT...614)及所有其它基于实时的虚拟机正共享HW/多核心群集605。由于所述虚拟机功能及虚拟机呈软件实例形式，因此其可在闲置状态期间存储于HW/多核心群集605中的局部存储器中且可由嵌入式超管理器604启动。另外，在应用服务器601中运行的超管理器609可基于运行的虚拟机610、611来启动SF1...SFn或PKT1...PKTn。当虚拟机611需要到及从NIC607的网络615接入的功能时，前端612转换对接口603的服务请求。在接口603接收到请求之后，其建立PKT1614以运行所述功能。相同情况适用于安全性功能(SF)。如果虚拟机611需要安全性功能的服务，则前端612转换对接口603的请求。接口603接着如服务器般作出反应以通过调用虚拟机SF1或SF2...SFn来服务于所述安全性请求。

[0093] 根据一个实施例，基于云的架构提供用于云安全性的模型，所述模型由驻留于安全虚拟化运行时层上的面向服务的架构(SOA)安全层组成。云递送服务层是复杂的分布式SOA环境。不同服务在企业内跨越不同的云而扩展。服务可驻留于连接在一起以形成单一云应用程序的不同管理或安全性域中。一SOA安全模型完全适用于云。一web服务(WS)协议堆栈形成SOA安全性的基础且因此还形成云安全性的基础。

[0094] SOA的一个方面是容易地集成来自不同提供者的不同服务的能力。相比于大多数企业SOA环境，云计算更进一步推动此模型，这是因为云有时支持大量租户、服务及标准。此支持是以高度动态及敏捷的方式且在极其复杂的信任关系下提供。具体来说，云SOA有时支持大的且开放的用户群体，且其不可假设在云提供者与订户之间建立的关系。

[0095] 一般所属领域的技术人员应理解，本系统不限于具有目前所揭示的多核心群集配置的实施方案，且包括任何适当替代者的实施例实现本目标。

[0096] 一般所属领域的技术人员应理解，本系统不限于具有安全性软件应用程序的实施方案，且包括音频压缩/解压缩、视频压缩/解压缩、成像压缩/解压缩、话音压缩/解压缩或任何适当替代者的实施例实现本目标。

[0097] 在上文的描述中，仅出于解释的目的，阐述特定命名法以提供对本发明的详尽理解。然而，所属领域的技术人员将显而易见，不需要这些特定细节实践本发明的教示。

[0098] 本文中的详细描述的一些部分是依据对计算机存储器内的数据位的操作的算法及符号表示来呈现。这些算法描述及表示是数据处理领域的技术人员用以向其他所属领域的技术人员最有效地传达其工作的要点的手段。在此且大体来说设想算法为导致所要结果的步骤的自相一致的序列。所述步骤是需要物理操纵物理量的步骤。通常(但未必)，这些量采用能够被存储、传送、组合、比较及以其它方式操纵的电信号或磁信号的形式。已证明将这些信号称为位、值、元件、符号、字符、项、数字或其类似者时常(主要出于普通用途)为便利的。

[0099] 然而，应记住，所有这些及类似术语应与适当物理量相关联且仅为应用于这些量

的便利标记。除非如从以下论述中显而易见的另外特定声明，否则应了解，遍及所述描述，利用例如“处理”或“计算”或“运算”或“确定”或“显示”或其类似者的术语的论述指代计算机系统或类似电子计算装置的动作及过程，所述计算机系统或类似电子计算装置操纵表示为计算机系统的寄存器及存储器内的物理(电子)量且将其转变为类似地表示为计算机系统存储器或寄存器或其它此种信息存储、传输或显示装置内的物理量的其它数据。

[0100] 本发明还涉及一种用于执行本文中的操作的设备。此设备可特定建构以用于所需目的，或此设备可包含一通用计算机，所述计算机通过存储于其中的计算机程序选择性地启动或重配置。此计算机程序可存储于计算机可读存储媒体中，所述计算机可读存储媒体例如(但不限于)任何类型的磁盘，包括软盘、光盘、CD-ROM及磁光盘、只读存储器(ROM)、随机存取存储器(RAM)、EPROM、EEPROM、磁卡或光卡或适用于存储电子指令的任何类型的媒体，且所述媒体中的每一者耦合到计算机系统总线。

[0101] 本文中所呈现的算法并非固有地涉及任何特定计算机或其它设备。各种通用系统、计算机服务器或个人计算机可根据本文中的教示与程序一起使用，或建构更特定设备以执行所需方法步骤可证明为便利的。从以下描述将看出多种这些系统所需的结构。将了解，多种编程语言可用以实施如本文所描述的本发明的教示。

[0102] 此外，代表性实例的各种特征与附属权利要求可以未特定及显式地列举的方式组合，以便提供本教示的额外有用实施例。还明确注意，出于原始揭示内容的目的以及出于限制所主张的标的物的目的，所有值范围或实体的群组的指示揭示每一可能的中间值或中间实体。还明确注意，各图中所展示的组件的尺寸及形状经设计以有助于理解实践本教示的方式，但既定不限制实例中所展示的尺寸及形状。

[0103] 揭示一种用于虚拟化及云安全性的系统及方法。尽管已相对于特定实例及子系统描述了各种实施例，但一般所属领域的技术人员将显而易见，本文中所揭示的概念不限于这些特定实例或子系统，而是也扩展到其它实施例。如在所附权利要求书中所指定的所有这些其它实施例包括于这些概念的范围内。

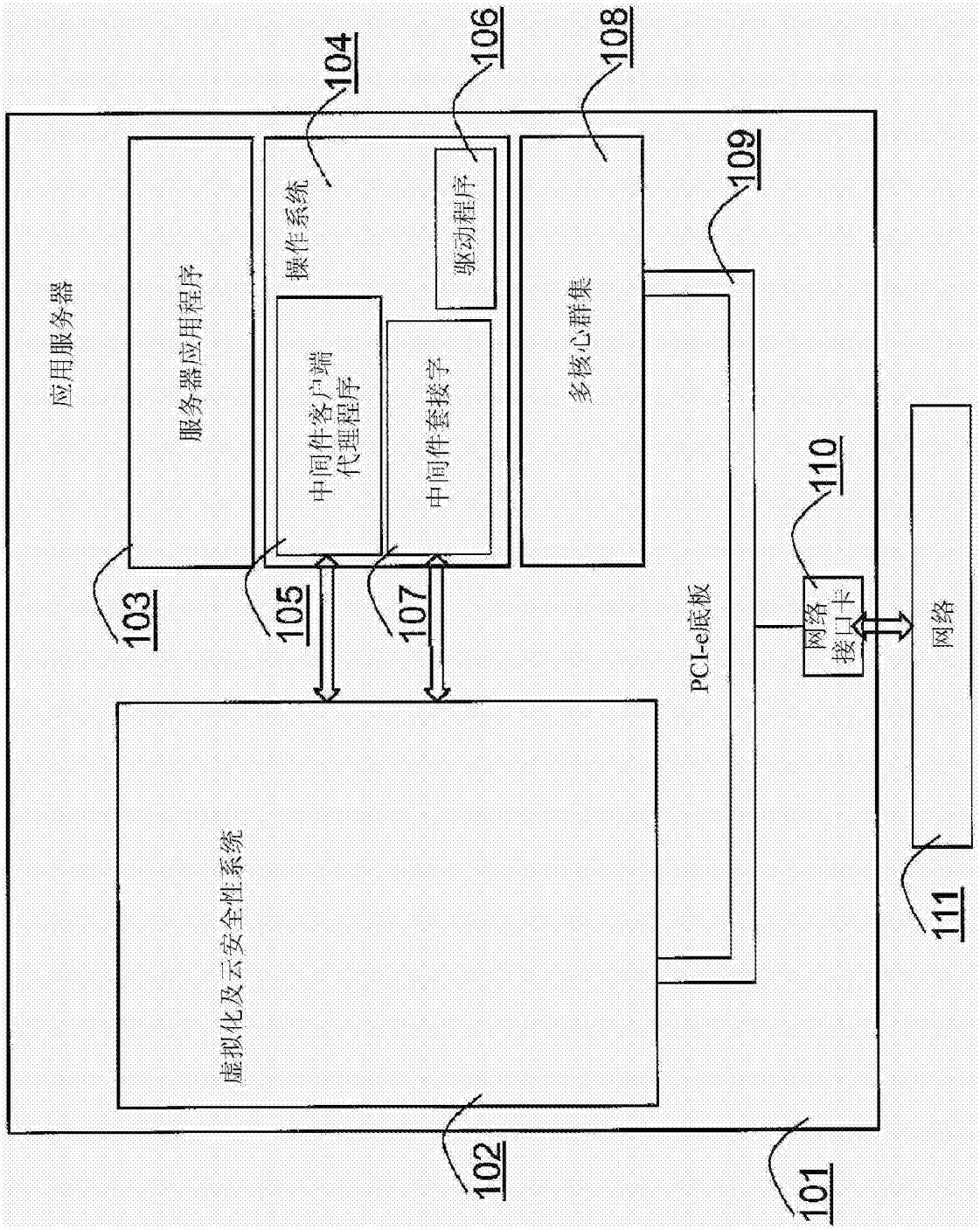

应用服务器
服务器应用程序
操作系统
中间件客户端代理程序
中间件套接字
驱动程序
多核心群集
虚拟化及云安全性系统
PCI-e底板
网络接口卡
网络
101
102
103
104
105
106
107
108
109
110
111

图1

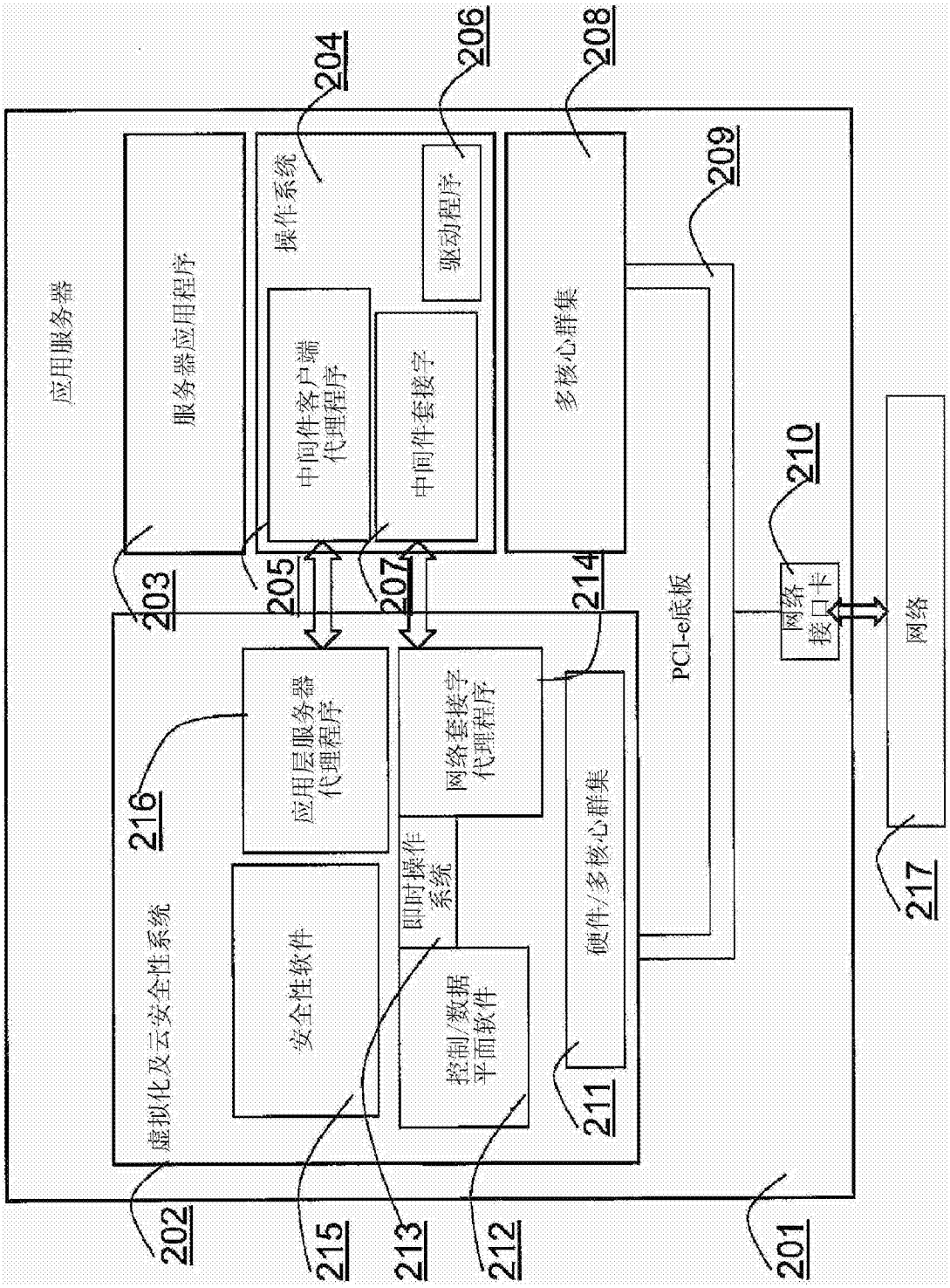

应用服务器
服务器应用程序
操作系统
驱动程序
中间件客户端代理程序
中间件套接字
多核心群集
PCI-e底板
网络接口卡
网络
虚拟化及云安全性系统
应用层服务器代理程序
网络套接字代理程序
即时操作系统
安全性软件
控制/数据平面软件
硬件/多核心群集
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217

图2

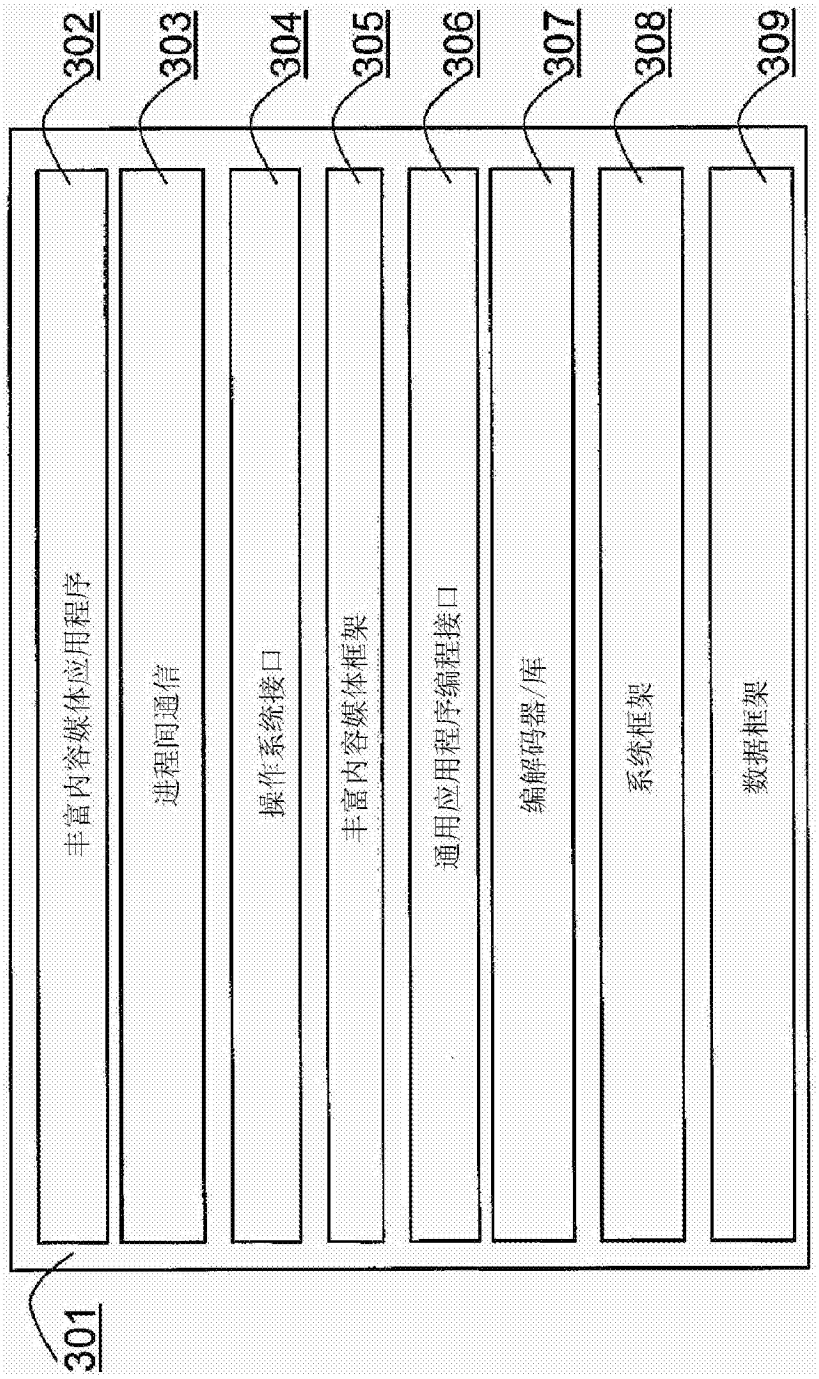

302
303
304
305
306
307
308
309
丰富内容媒体应用程序
进程间通信
操作系统接口
丰富内容媒体框架
通用应用程序编程接口
编解码器/库
系统框架
数据框架
301

图3

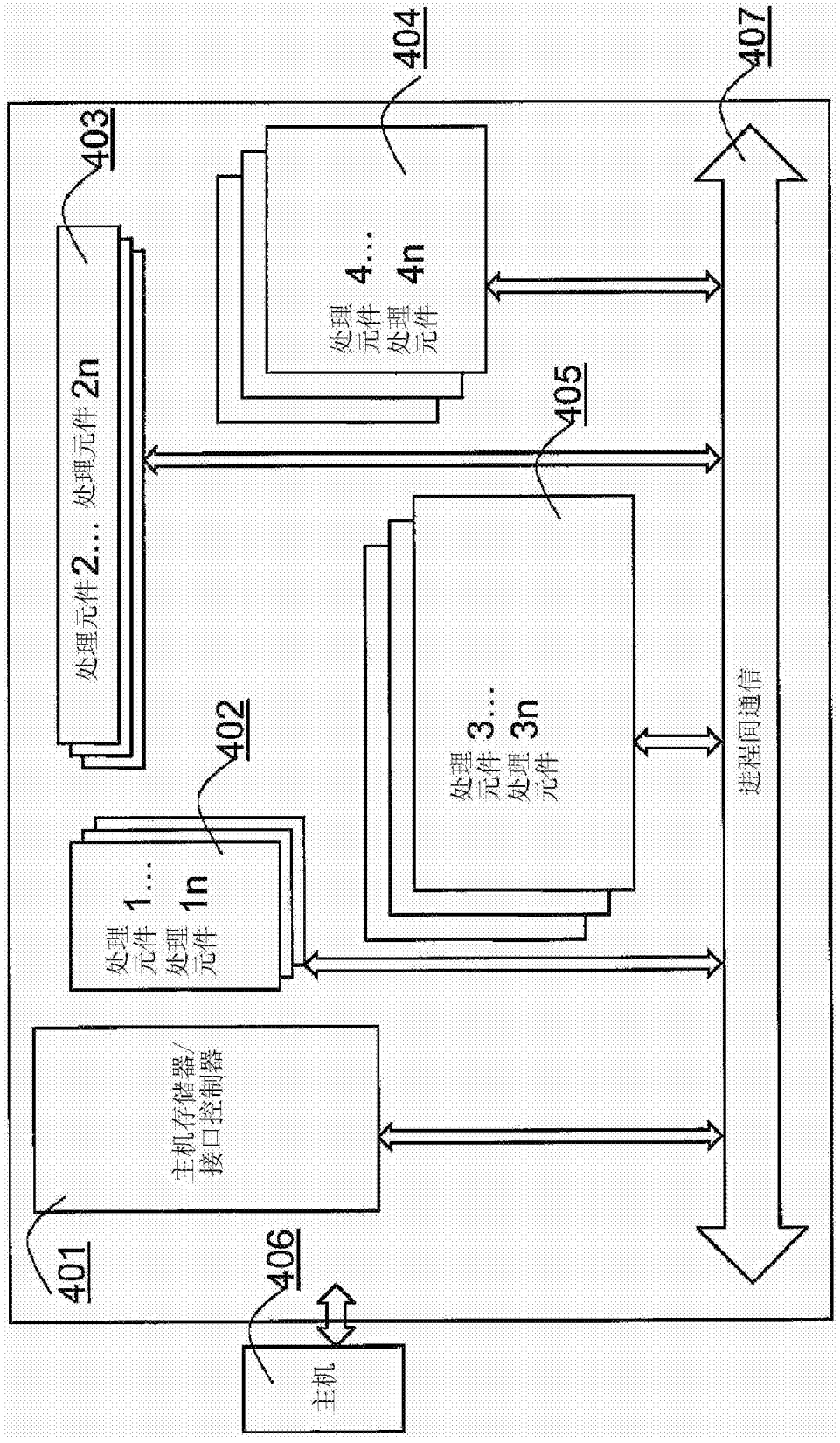

404
407
403
处理元件 4... 处理元件 4n
处理元件 2... 处理元件 2n
405
402
处理元件 3... 处理元件 3n
处理元件 1... 处理元件 1n
进程间通信
主机存储器/接口控制器
401
406
主机

图4

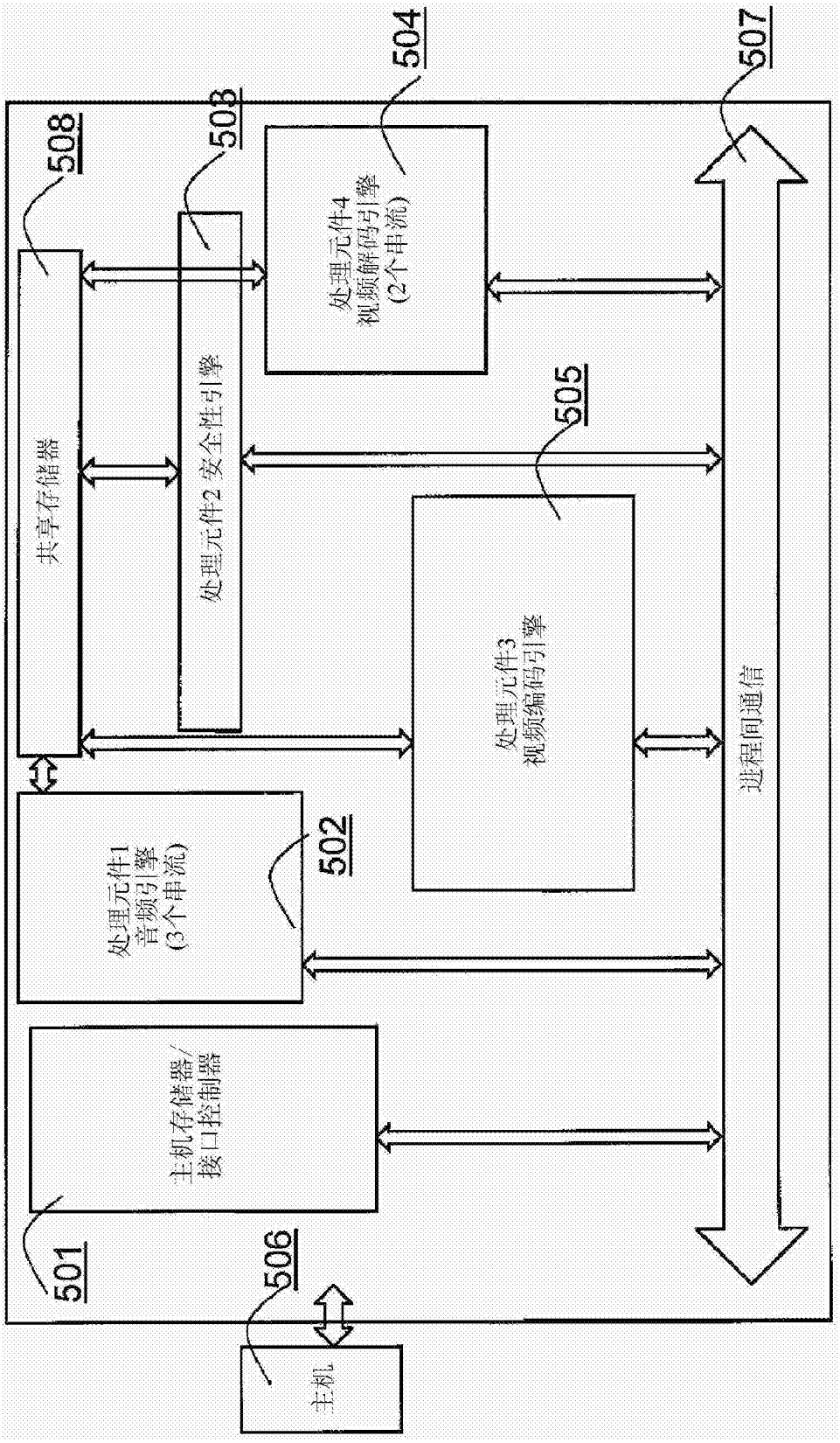

504
507
508
508
处理元件4
视频解码引擎
(2个串流)
共享存储器
处理元件2 安全性引擎
505
处理元件3
视频编码引擎
进程间通信
处理元件1
音频引擎
(3个串流)
502
主机存储器/
接口控制器
501
506
主机

图5

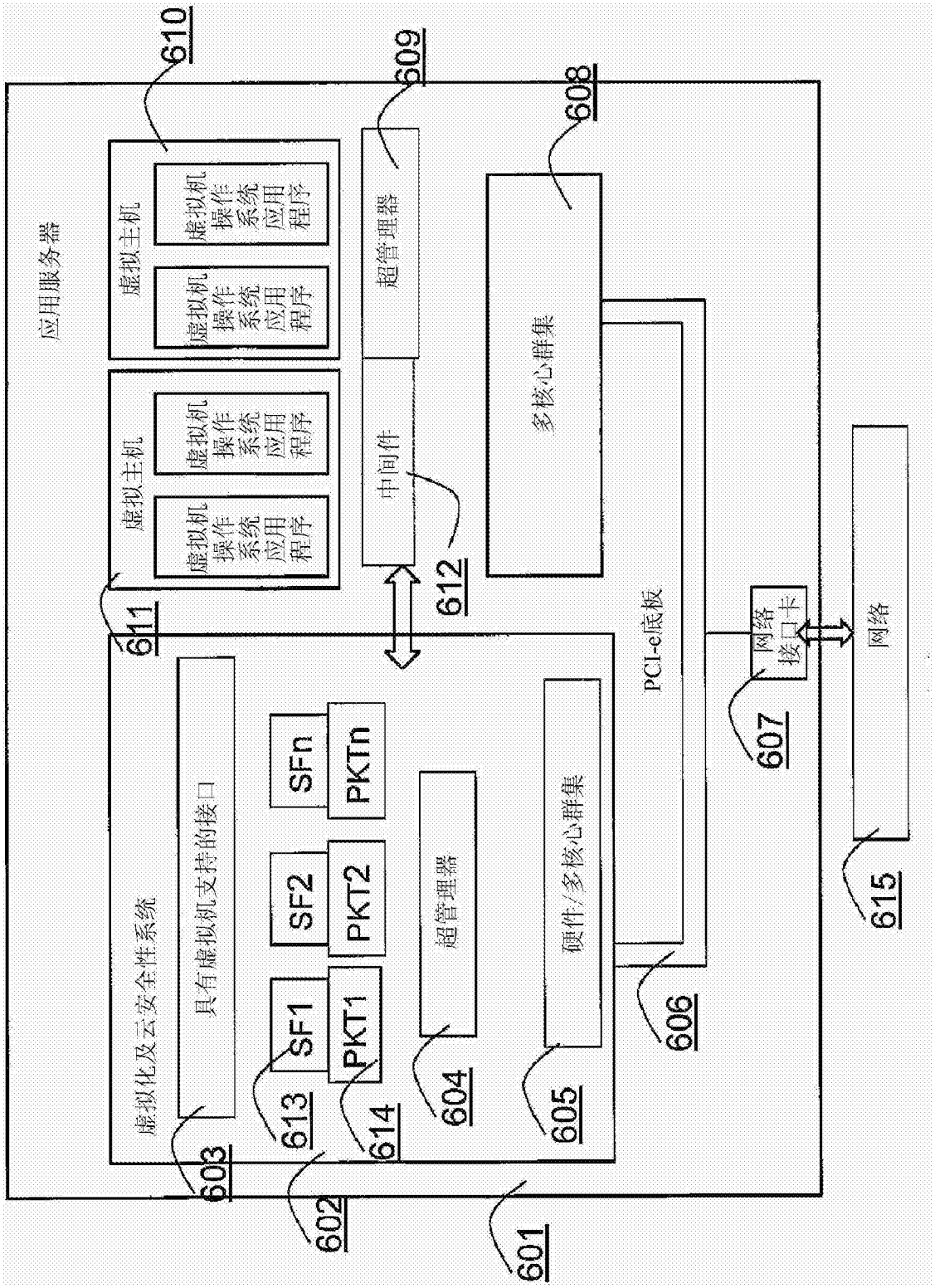

应用服务器
610
虚拟主机
虚拟机操作系统应用程序
虚拟机操作系统应用程序
609
超管理器
608
多核心群集
虚拟主机
虚拟机操作系统应用程序
虚拟机操作系统应用程序
中间件
612
611
虚拟化及云安全性系统
具有虚拟机支持的接口
603
SF1
PKT1
SF2
PKT2
SFn
PKTn
613
614
超管理器
604
硬件/多核心群集
605
PCI-e底板
606
网络接口卡
607
网络
615
602
601

图6