[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 9/46 (2006.01)

[12] 发明专利说明书

专利号 ZL 03822257.4

[45] 授权公告日 2007 年 9 月 5 日

[11] 授权公告号 CN 100336021C

[22] 申请日 2003.9.19 [21] 申请号 03822257.4

[30] 优先权

[32] 2002. 9.19 [33] US [31] 10/246,909

[86] 国际申请 PCT/GB2003/004063 2003.9.19

[87] 国际公布 WO2004/027612 英 2004.4.1

[85] 进入国家阶段日期 2005.3.18

[73] 专利权人 国际商业机器公司

地址 美国纽约

[72] 发明人 彼得·伯克 赵青云 钟显维

卡尔顿·梅森 阿加库玛·雷迪

维施瓦纳斯·温卡塔拉玛帕

[56] 参考文献

Websphere 安全策略概述及在 B2B 电子商务应用中的实现 李云峰,程代杰,计算机应用研究 2002

基于分布式系统的应用软件安全控制问题的研究 宁伟,内蒙古大学学报(自然科学版) 2002

新一代 Web 应用服务器软件——WebSphere 应用服务器探析 韩德志, 耿红琴,计算机应用研究 2001

Orbix Wonderwall Administrator's Guide IONA TECHNOLOGIES PLS, 1, 12. 19, 134. 135, 173. 182, IONA TECHNOLOGIES PLS 2000

审查员 冯慧萍

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

代理人 康建忠

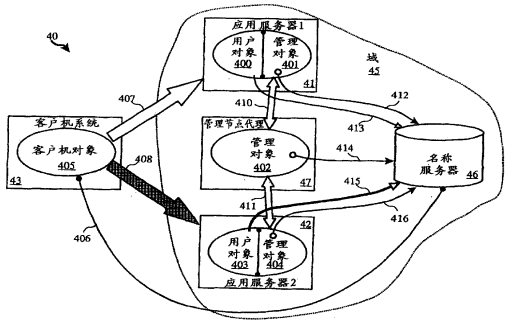
权利要求书 3 页 说明书 16 页 附图 6 页

[54] 发明名称

分布计算域内的对象级安全系统及方法

[57] 摘要

应用服务器上的对象可以按受安全保护的级别分类，例如分为用户对象和管理对象。 可以对管理对象实施整域的安全保护，而为域内每个应用服务器独立配置用户对象的安全性。 在 CORBA 体系结构内，诸如管理对象之类的需整域安全保护的共享对象的 IOR 在 IOR 生成和导出给一个名称服务器期间提供标记组件。 以后，在客户机使用这个 IOR 时，这个客户机就要按照这些标记组件调用诸如验证、授权和传送保护之类的必要安全措施。



1. 一种在分布计算域内使用的方法，所述方法包括下列步骤：

将管理对象和用户对象分布到一个或多个应用服务器上；

为管理对象的域级安全性定义一个全局安全标志；

将一个或多个应用服务器安全标志与被分布的管理对象的接口关联；以及

由一个应用服务器在一个客户机过程的配合下以三个模式中的一个模式执行一个或多个安全操作，其中在所述全局安全标志和所述所关联的应用服务器安全标志启用的第一模式用户对象和管理对象都受保护，在所述全局安全标志启用而所述所关联的应用服务器安全标志停用的第二模式用户对象被使用而无安全操作但管理对象受保护，而在所述全局安全标志停用的第三模式用户对象和管理对象被使用而无安全操作。

2. 如在权利要求1中所述的方法，其中所述执行安全操作的步骤包括对管理对象和用户对象提供独立的安全操作。

3. 如在权利要求1中所述的方法，其中所述将应用服务器安全标志与管理对象接口关联的步骤包括从下述组中选择的动作：对启用应用服务器用户对象安全保护的应用服务器上的用户对象导出带标记组件的CORBA IOR，以及为启用应用服务器用户对象安全保护的应用服务器上的用户对象在UDDI注册表内提供对象类型。

4. 如在权利要求3中所述的方法，所述方法还包括访问列有需保护的对象的申报性清单。

5. 如在权利要求1中所述的方法，所述方法包括提供一个应用服务器。

6. 如在权利要求1中所述的方法，所述方法包括提供一个客户机过程作为企业Java Bean。

7. 如在权利要求1中所述的方法，所述方法包括提供一个或多个企业Java Bean用户对象。

8. 如在权利要求1中所述的方法，所述方法包括提供一个或多个MBean管理对象。

9. 如在权利要求1中所述的方法，所述方法包括执行从列有验证、授权和传送保护的清单中选出的安全操作。

10. 如在权利要求1中所述的方法，所述方法包括采用一个从包括简单对象接入协议和ORB间协议的组中选出的安全协议。

11. 如在权利要求1中所述的方法，所述方法包括采用一个从包括IDL和Web业务定义语言的组中选出的使用Web业务端点语言和接口定义语言的业务描述模型。

12. 一种在分布计算域内的对象级安全系统，所述系统包括:

分布在一个或多个应用服务器之中的一个或多个管理对象和一个或多个用户对象;

定义联网的计算域级内所述管理对象的安全性的全局安全标志;

一个或多个与被分布的管理对象的接口关联的应用服务器安全标志；以及

一个或多个可由一个应用服务器在一个客户机过程的配合下以三个模式中的一个模式执行的安全操作，其中在所述全局安全标志和所述所关联的应用服务器安全标志启用的第一模式用户对象和管理对象都受保护，在所述全局安全标志启用而所述所关联的应用服务器安全标志停用的第二模式用户对象被使用而无安全操作但管理对象受保护，而在所述全局安全标志停用的第三模式用户对象和管理对象被使用而无安全操作。

13. 如在权利要求12中所述的系统，其中所述安全操作包括对管理对象和用户对象的独立的安全操作。

14. 如在权利要求13中所述的系统，其中所述与管理对象接口关联的服务器安全标志包括从下述组中选出的对象类型指示符：启用应用服务器用户对象安全保护的应用服务器上的用户对象的带标记组件的CORBA IOR，以及在启用应用服务器用户对象安全保护的应用服务器上的用户对象的在UDDI注册表内的对象类型。

15. 如在权利要求14中所述的系统，所述系统还包括一个列有需保护的对象的申报性清单，用来确定为了启用用户对象安全保护需修改哪些IOR或UDDI注册表登录项。

分布计算域内的对象级安全系统及方法

发明领域

本发明涉及应用服务器安全管理系统和工具技术领域。

技术背景

应用服务器（Application server）是由一个诸如内部网或互联网之类的分布式网络内的计算机或计算平台执行的为应用或业务提供商务逻辑的服务器程序（server program）。诸如国际商业机器公司(IBM®)、微软(Microsoft®)公司和太阳微系统(Sun Microsystems)公司提供了一些套装软件，用来在包括(但不限于)个人计算机、网络服务器、主机和工作站的各种硬件平台上为包括(但不限于)UNIXR®、Linux、IBM公司的AIX®、OS/2®和OS/390®、微软公司的Windows®和太阳公司的Solaris的各种操作系统开发、管理、部署和运行应用服务器。IBM提供了一种称为WebSphere®的众所周知的、得到广泛使用的应用服务器套装(IBM、AIX、OS/2和OS/390是国际商业机器公司的注册商标；Microsoft和Windows是微软公司（Microsoft Corporation）在美国和/或其他一些国家的商标；UNIX是开放组（Open Group）在美国及其他一些国家的注册商标)。

应用服务器可以用诸如“C”之类的高级语言(“HLL”)、诸如太阳微系统公司的Java™之类的可移植语言以及它们的组合开发。应用逻辑的一些部分按照用来开发应用服务器程序的设计方法和语言可以体现为企业Java Bean(Enterprise Java Bean，“EJB”)、动态连接库(dynamic link libraries，“DLL”)、程序对象（program object）、应用小程序（applet）和服务小程序（servelet）。(Java和所有的基于Java的商标和标志是太阳微系统公司在美国和/或其他一些国家的商标。)

应用服务器通常与诸如web（万维网）浏览器和远程终端之类的

客户计算机和过程配合，形成对用户的执行所需功能或业务的接口。与客户机计算机和过程互动的公共协议包括(但不限于)超文本传送协议(“HTTP”)、传输控制协议/互联网协议(“TCP/IP”)、安全套接字层(secure sockets layer,“SSL”)和文件传送协议(“FTP”)。与一个应用服务器配合的客户机过程可以包括(但不限于)独立(例如，对浏览器独立)的客户机程序、超文本标注语言(“HTML”)资源、浏览器扩展和插件、可扩展标注语言(“XML”)资源、图形和多媒体对象(例如，TIFF、GIF、JPEG、AVI等)、Java服务器页面(“JSP”)、活动服务器页面(“ASP”)、个人主页(“PHP”)、Java模块和Java Bean。

应用服务器也可以与诸如文件系统和数据库的其它系统资源互动，读取、存储、产生和复制数据。这些系统资源可以直接由一个诸如本地高速缓存器之类的应用服务器管理，也可以通过其他服务器接入和管理。

应用服务器通常还与安全性授权和验证服务器合作，确定一个用户是否为用户所自称的用户，以及用户是否具有执行所请求的动作、接入所需的资源或数据等的权限或特许。

应用服务器与这样的授权和验证过程之间以及与其他系统资源的通信协议可以包括为客户机通信预先列出的协议中的任何一个协议，而且通常包括由专有规范和诸如Java版2企业版(“J2EE”)接口和通信模型和公共的对象代理请求体系结构(“CORBA”)之类的“开放”标准定义的其他协议。

在该产业内可得到一些CORBA的实现，包括IBM公司的SOM和DSOM体系结构、Netscape公司的开放网络环境(“ONE”)、太阳微系统公司的RMI和微软公司的COM和DCOM体系结构。这些体系结构使客户机应用程序对象可以“发现”存在对完成一个任务或业务可能有用的或需要的其他程序对象。一个对象请求代理(“ORB”)是这样的体系结构的一个组件，客户机可以向它发送对一些特定功能的请求。ORB然后将这些请求转送给ORB所知道的一些可以处理客户机所需的功能的适当服务器。客户机和服务器然后进行互动，确定要使用的适当接

口，以使客户机可以使用服务器所提供的程序对象。

在CORBA体系结构内具体使用的是可互操作的对象引用("IOR")的定义。IOR提供了与对象所驻留的平台无关和与ORB的实现无关的对象引用。

作为分布对象越来越复杂的这些类型的应用，许多应用管理系统已经进入了市场。应用管理包括控制和监视一个应用，从它的安装和配置到它的有用寿命周期，包括收集规格和调整到使效益和响应达到最大。应用管理系统所采用的模型通常是管理器-代理模型。应用负责为管理系统提供一定的信息、响应管理系统的一个代理对信息行动的请求和与一个管理系统代理通信。管理系统代理通常在与受管理的应用相同的硬件平台上实现。

管理系统与一个或多个本身与受管理的应用接触的代理通信。管理系统可以用一个专有协议与它的代理通信，或者可以使用一个诸如简单网络管理协议("SNMP")或Java管理扩展("JMX")之类的"开放"协议。上市的一些典型管理系统有Tivoli的管理环境和IBM的WebSphere管理应用。

来看图3，图中示出了这样一个使用一些JMX管理Bean或MBean的管理系统的一个实施例。各个MBean是可通过标准JMX接口接入的对象，提供具有暴露应用专用管理接口的能力的开发器。JMX MBean服务器(33)运行应用服务器MBean(34)，它负责向管理应用(37)暴露应用服务器(31)的接口。同样，JMX MBean服务器(33)还运行应用MBean(35)，它向管理应用(37)暴露应用(32)的应用专用管理接口。MBean服务器(33)还提供任何将一个或多个管理系统与这应用桥接必需的适配器(36)，使得这些应用管理器的管理设施可与这应用一起使用。

在当前一些版本的IBM的WebSphere应用服务器产品中，有一个管理服务器是中心接触点，所有的管理请求都发向那里。使这个管理服务器安全只需要将一些应用服务器配置成安全客户机，而不必将这些应用服务器配置成安全服务器。由于用户对象不允许处在管理服务

器上，而且管理对象不允许处在应用服务器上，因此在该技术领域内这个途径可以有一段时间满足这些要求。

然而，随着应用已经逐渐发展成包括管理功能和在应用服务器上使用管理对象，就需要对象级安全保护（security）(而不是服务器级安全保护)，但这并不是传统的体系结构所支持的。在有些系统内，所有应用过程包括需要保护的管理资源，即使用户资源可以或可以不需要保护。在作为服务器级安全方案的当前安全方案下，如果停用（disable）用户对象安全保护，也将停用管理对象安全保护。对于确实不需要安全保护的用户对象和资源，这不必要和不希望地要付出性能上的代价，因为需要对这些用户对象执行验证和授权过程。如果系统配置成停用安全保护，作为默认包括停用管理资源安全保护，系统就会不必要和不希望地通过管理功能暴露出安全缺口。

发明内容

因此，本发明提供了一种在一个分布计算域内使用的方法，这种方法包括下列步骤：将管理对象和用户对象分布到一个或多个应用服务器上；为管理对象的域级安全性定义一个全局安全标志；将一个或多个应用服务器安全标志与被分布的管理对象的接口关联；由一个应用服务器在一个客户机过程的配合下以三个模式中的一个模式执行一个或多个安全操作，在所述全局安全标志和所述所关联的应用服务器安全标志启用的第一模式用户对象和管理对象都受保护，在所述全局安全标志启用而所述所关联的应用服务器安全标志停用的第二模式用户对象被使用而无安全操作但管理对象受保护，而在所述全局安全标志停用的第三模式用户对象和管理对象被使用而无安全操作。

优选的是，提供一种允许为含有用户对象和管理对象的应用服务器进行对象级安全配置的系统和方法。

优选的是，提供一些过程和机制使管理对象和命名对象的安全保护可以独立地、申报性地启用和停用而与一个安全域内其他应用服务器上用户对象安全保护的启用与否无关。这优选地提供了用同一过程

停用用户安全保护而保持管理安全性的能力，特别是在一个基于IBM的WebSphere应用服务器产品的应用环境内。

客户(例如应用服务器的拥有者和操作员)可以有选择地停用对一个安全域内一些应用服务器上的用户对象的安全保护，而保持对其他应用服务器上的用户对象的安全性，优选的是同时具有在整个安全域内对全局管理对象的安全性。因此，诸如管理安全、内部系统管理之类的管理功能可以优选地与用户安全性分开管理。

可取的是，采用在这里所公开的过程和机制，客户机过程可以不用知道一个应用对象是用户对象还是管理对象，而只要知道每个对象是否要求执行安全功能。此外，本发明可取地允许申报性地用类别和包来定义哪些对象需受保护。

概括地说，为了实现一个应用服务器的对象级安全性的可置配性，优选的是对共享对象采用由ORB将IOR导出给名称服务器。优选的是，为诸如管理对象之类的需安全保护的对象的IOR提供指出使用这个业务的安全细节的标记组件。优选的是，对于诸如用户对象之类的非安全对象的IOR，导出时没有标记组件。优选的是，在导出任何给定对象时调用一个IOR截获器。优选的是，IOR截获器装入一个列有所有需要保护的管理对象或管理包的描述符文件。这可取地允许在安全域内启用全局安全保护时规定需保护的单个对象、各个对象的清单或一些对象的包。

对于在描述符文件内的对象，优选的是IOR在导出时具有加有安全标记的组件。以后，在一个客户机得到一个加有标记的IOR时，客户机就可取地知道调用对这个业务的请求的安全性要求。优选的是，如果在IOR内没有提供标记，可以不需安全保护就请求这个业务。可取的是，对于这些非安全对象，客户机不用向应用服务器发送任何用户安全性信息，也不用保护向应用服务器的信息传送，使得对于这些用户对象来说，性能得到改善，因为避免了对这些用户对象的不必要保护。

通常，优选的是用两种标志来配置一个域内的对象级安全性：(a)

一个全局(整域管理)安全标志，以及(b)一个或多个应用服务器安全标志。优选的是，全局安全标志保持为域级的，而应用服务器安全标志是为每个应用服务器专用的。优选的是，全局安全标志确定是否对整个域内的所有管理对象都采取安全保护。优选的是，也将这些管理对象列入前面提到的描述符文件。优选的是，每个应用服务器安全标志只是启用或停用对所属应用服务器上的用户对象的安全保护，而不影响对这个服务器上的管理对象的安全保护。

优选的是，通过为管理对象和用户对象提供独立的安全操作来执行安全操作。

优选的是，可以通过从下述组中选择的动作：对启用应用服务器用户对象安全保护的应用服务器上的用户对象导出带标记组件的CORBA IOR，以及为启用应用服务器用户对象安全保护的应用服务器上的用户对象在UDDI注册表内提供对象类型，将应用服务器安全标志与管理对象接口相关联。

优选的是，能接入一个列有需保护的对象的申报性清单。

优选的是，提供一个应用服务器(例如，WebSphere应用服务器)。

优选的是，提供一个客户机过程作为一个企业Java Bean。

优选的是，提供一些用户对象作为企业Java Bean。

优选的是，提供一些管理对象作为MBean。

优选的是，执行一些从列有验证、授权和传送保护的清单中选出的安全操作。

优选的是，采用一个从包括简单对象接入协议和ORB间协议的组中选出的安全协议。

优选的是，采用一个从包括IDL和Web业务定义语言的组中选出的用web业务端点语言和接口定义语言的业务描述模型。

按照另一个方面，本发明提供了一种在一个分布计算域内使用的计算机程序，所述计算机程序包括在一个计算机上运行时适合执行以下步骤的程序代码单元：将管理对象和用户对象分布到一个或多个应用服务器上；为管理对象的域级安全性定义一个全局安全标志；将一

个或多个应用服务器安全标志与被分布的管理对象的接口关联；以及由一个应用服务器在一个客户机过程的配合下以三个模式中的一个模式执行一个或多个安全操作，在所述全局安全标志和所述所关联的应用服务器安全标志启用的第一模式用户对象和管理对象都受保护，在所述全局安全标志启用而所述所关联的应用服务器安全标志停用的第二模式用户对象不需经安全操作就可使用但管理对象受保护，而在所述全局安全标志停用的第三模式用户对象和管理对象都不需经安全操作就可使用。

优选的是，有一个企业Java Bean客户机过程。

优选的是，有一个企业Java Bean用户对象。

优选的是，有一个MBean管理对象。

按照另一个方面，本发明提供了一种在分布计算域内的对象级安全系统，这种系统包括：分布在一个或多个应用服务器之中的一个或多个管理对象和一个或多个用户对象；一个定义在一个联网的计算域级内所述管理对象的安全性的全局安全标志；一个或多个与被分布的管理对象的接口关联的应用服务器安全标志；以及一个或多个可由一个应用服务器在一个客户机过程的配合下以三个模式中的一个模式执行的安全操作，在所述全局安全标志和所述所关联的应用服务器安全标志启用的第一模式用户对象和管理对象都受保护，在所述全局安全标志启用而所述所关联的应用服务器安全标志停用的第二模式用户对象被使用而无安全操作但管理对象受保护，而在所述全局安全标志停用的第三模式用户对象和管理对象被使用而无安全操作。

优选的是，这些安全操作包括独立的对管理对象和用户对象的安全操作。

优选的是，与管理对象接口关联的服务器安全标志包括从下述组中选出的对象类型指示符：启用应用服务器用户对象安全保护的应用服务器上的用户对象的带标记组件的CORBA IOR，以及在启用应用服务器用户对象安全保护的应用服务器上的用户对象的在UDDI注册表内的对象类型。

优选的是，有一个列有需保护的对象的申报性清单，用来确定为了启用用户对象安全保护需修改哪些IOR或UDDI注册表登录项。

附图说明

下面仅作为例子将结合附图对本发明的一个优选实施例进行说明，在这些附图中：

图1示出了一个一般计算平台体系结构，诸如个人计算机、服务器计算机、个人数字助理、web功能的无线电话机或其他基于处理器的设备；

图2示出了一个与图1的一般体系结构关联的软件和固件的一般体系结构；

图3例示了一个管理系统和应用的典型配置；

图4示出了按照本发明的一个优选实施例设计的本发明的过程和交互作用；

图5示出了在IIOP模型实现中按照本发明的一个优选实施例设计的为共享对象导出带标记组件的IOR的过程。

图6示出了在IIOP模型实现中按照本发明的一个优选实施例设计的一个客户机请求一个共享对象或业务的过程。

具体实施方式

本发明优选地实现为当前已发现存在于诸如个人计算机、web服务器和web浏览器之类的众所周知的计算平台上的企业服务器软件的特色功能、扩展或改善。这些常见的计算平台可以包括个人计算机、工作站和主机，以及可以想象得到的具有适当能力的便携式计算平台，如个人数字助理(“PDA”)、web功能的无线电话机及其他类型的个人信息管理(“PIM”)设备。

因此，回顾一下各种实现（从高端web或企业服务器平台到个人计算机再到便携式PDA或web功能的无线电话机）的计算平台的一般体系结构是有益的。

来看图1，图中所示的一般化体系结构包括一个通常由微处理器(2)及与之配合的随机存取存储器(“RAM”)(4)和只读存储器(“ROM”)(5)组成的中央处理单元(1)(“CPU”)。通常，CPU(1)还配有高速缓存器(3)和可编程闪速ROM(6)。微处理器(2)与各种CPU存储器之间的接口(7)通常称为“本地总线”，但也可以是一个通用或工业标准总线。

许多计算平台还配有一个或多个存储装置驱动器(9)，诸如硬盘驱动器(“HDD”)、软盘驱动器、光盘驱动器(CD、CD-R、CD-RW、DVD、DVD-R等)和专有的磁盘和磁带驱动器(例如，Iomega Zip和Jaz、Addonics SuperDisk等)。此外，有些存储装置驱动器可以是通过计算机网络可接入的。

按照计算平台的预定功能，许多计算平台具有一个或多个通信接口(10)。例如，个人计算机通常配有一个高速串行口(RS-232、RS-422等）、一个增强的并行口(“EPP“)和一个或多个通用串行总线(“USB”)口。计算平台还可以配有一个诸如以太网卡之类的局域网(“LAN”)接口和诸如高性能串行总线IEEE-1394之类的其他高速接口。

诸如无线电话机和无线联网PDA之类的计算平台还可以配有与天线的射频(“RF”)接口。在有些情况下，计算平台也可以配有一个红外数据装置(IrDA)接口。

计算平台通常具有一个或多个内部扩展槽(11)，诸如工业标准结构(ISA)、增强的工业标准结构(EISA)、外围组件互连(PCI)，或者用来添加诸如声卡、存储板和图形加速器之类的其他硬件的专用接口槽。

此外，许多单元，诸如膝上型计算机和PDA之类，配有一个或多个外部扩展槽(12)，使用户可以方便地安装和撤除诸如PCMCIA卡、SmartMedia卡之类的硬件扩展装置和诸如活动硬盘驱动器、CD驱动器和软盘驱动器之类的各种专用模块。

通常，存储装置驱动器(9)、通信接口(10)、内部扩展槽(11)和外部扩展槽(12)通过一个诸如ISA、EISA或PCI的标准或工业开放总线体系结构(8)与CPU(1)相互连接。在很多情况下，总线(8)可以具有一个专用的结构。

计算平台通常配有一个或多个用户输入装置，诸如键盘或小键盘(16)、鼠标或光标指点装置(17)和/或触摸屏显示器(18)。在个人计算机的情况下，通常与一个鼠标或诸如跟踪球或TrackPoint之类的指针光标装置一起配有一个标准的键盘。在web功能的无线电话机的情况下，可以配有一个带一个或多个专用功能键的简单小键盘。在PDA的情况下，通常配有一个具有手书识别能力的触摸屏(18)。

此外，计算平台还配有一个麦克风(19)，诸如web功能的无线电话机的麦克风或个人计算机的麦克风之类。这个麦克风可以只是用来给出音频和语音信号，也可以利用语音识别能力用来输入用户选择，诸如网站语音导航或语音自动电话拨号之类。

许多计算平台还配有一个摄像装置(100)，诸如数码相机或视频数字摄像机。

大多数计算平台还配有一个或多个用户输出设备，诸如显示器(13)之类。显示器(13)可以采取许多形式，包括阴极射线管("CRT")、薄平晶体管("TFT")阵列或简单的发光二极管("LED")组或液晶显示("LCD")显示器。

通常计算平台也接有一个或多个扬声器(14)和/或警报器(15)。扬声器(14)可用来再现音频和音乐，如无线电话机的扬声器或个人计算机的扬声器那样。警报器(15)可以呈现为通常在诸如PDA和PIM之类的某些装置上可发现的简单的嘟嘟声发射器或蜂鸣器。

这些用户输入输出装置可以通过专用总线结构和/或接口直接接到CPU(1)上(8′，8″)，也可以通过一个或多个诸如ISA、EISA、PCI之类的工业开放总线相互连接。计算平台还配有一个或多个实现计算平台的所希望的功能的软件和固件(101)程序。

现在来看图2，图中更为详细到示出了在这些计算平台上的软件和固件(101)的一般体系结构。在计算平台上可以设置一个或多个操作系统("OS")固有（native）应用程序(23)，诸如文字处理器、电子数据表、接触管理实用程序、地址簿、日历、电子邮件客户机、演示文稿、财务和簿记程序。

此外，可以设置一个或多个必须由一个诸如Java脚本和程序之类的OS固有平台专用解释器(25)解释的“可移植”或与设备独立的程序(24)。

通常，计算平台还配有一个web浏览器或微浏览器(26)，它可以包括一个或多个诸如浏览器插件(27)之类的对浏览器的扩展。

计算设备通常配有一个操作系统(20)，诸如Microsoft Windows、UNIX、IBM OS/2、LINUX、MAC OS或其他平台专用操作系统。诸如PDA和无线电话机之类的较小设备可以配有其他形式的操作系统，诸如实时操作系统(“RTOS”)或掌上计算的PalmOS。

通常配有一组基本输入输出功能(“BIOS”)和硬件设备驱动器(21)，以使操作系统(20)和程序可以与计算平台上的专用硬件功能对接和加以控制。

此外，通常许多计算平台还配置有一个或多个嵌入固件程序(22)，由机上的或作为诸如微控制器或硬盘驱动器、通信处理器、网络接口卡或声音图形卡之类的外部设备的一部分“嵌入的”微处理器执行。

这样，图1和2就一般意义上示出了包括（但不限于）个人计算机、PDA、PIM、web功能的电话机和诸如WebTV[TM]单元之类的其他设备的各种计算平台的各个硬件组件、软件和固件程序。本发明优选地实现为在这样一个计算平台上的软件和固件。熟悉该技术领域的人员很容易认识到本发明也可以用一些硬件功能实现。

在一个可行的实施例中，本发明实现为一组如以下各段要详细说明的那样接入和修改一定的系统文件和资源的Java Bean，但本发明也可以集成入诸如web服务器套装之类的现有软件内。

在一个示范性实施例中，采用对象用OMG接口定义语言(“IDL”)定义的CORBA体系结构，对象分配给服务器和客户机，而用一个对象请求代理(“ORB”)来协调发现和使用可得到的对象和业务。IDL编辑器实现CORBA绑定，产生一些将每个对象的业务从服务器环境映射到客户机的客户机存根（client stub）和服务器基干（server skeleton）。客户机与服务器之间以及各服务器之间的通信协议为通用ORB间协

议(“GIOP”)和在传输控制协议/互联网协议(“TCP / IP”)上实现GIOP的ORB间协议(“IIOP”)。可互操作的对象引用(“IOR”)提供与平台独立和与ORB实现独立的对象引用。在CORBA体系结构内提供一个命名业务，用来将每个CORBA对象绑定到一个公开名（public name）上。

此外，在这个示范性实施例中，采用了企业Java Bean(“EJB”)程序设计模型，其中对象接口和服务器实现遵循Java定义，对象分布成使它们可以远距离接入，所使用的是包括远程方法调用(“RMI”)的Java通信协议。这个示范性实施例用IBM企业服务器上在AIX或Linux操作系统下运行的IBM WebSphere应用服务器产品实现。由于当前版本的WebSphere只支持RMI-IIOP，因此客户机优选的是不要用Java RMI协议的RMI-JRMP格式。在用其他web应用环境的其他实施例中，这个限制可以不是必要的。在这个示范性实施例中也用Java命名业务(“JNDI”)来为业务命名。

在该技术领域内通常这些通用CORBA和EJB的概念、协议、编程方法和功能是众所周知的，虽然WebSphere产品得到广泛应用而且本身也是众所周知的，但熟悉该技术领域的人员可以认识到，本发明可以用其他编程方法、协议、计算平台、操作系统体系结构和web应用服务器产品实现，这并不背离本发明的范围。例如，一些也可以用来实现本发明的应用服务器包括Oracle的9i产品、BEA系统的WebLogic平台、太阳微系统的ONE应用服务器、惠普的应用服务器和JBoss。就操作系统来说，在其他实施例中也可以替换成采用Unix、Linux、Novell的Netware、IBM的AIX和OS/2、太阳微系统的Solaris、惠普的HP-UX和微软的Windows产品。

现在来看图4，图中示出了按照本发明的一个包括一个管理节点代理(47)和名称服务器(46)的优选实施例设计的一个客户机系统(43)与多个应用服务器(41，42)的交互作用和关系(40)。应用服务器(41，42)、管理节点代理(47)和名称服务器(46)是一个为客户机系统(43)提供应用的域(45)的一部分。

随着应用的启动，执行一定的初始化程序，装入IOR截获器，将

对共享对象的引用从每个应用服务器(41，42)导出(412，413，414，415，416)给名称服务器(46)，因此客户机(43)就可以发现这些共享对象。

在对象导出给名称服务器时，针对每个对象调用一个IOR截获器。在一个ORB生成这些IOR的这段创建时间期间，调用对于每个具有一个IOR截获器的组件的所有IOR截获器。这些IOR截获器的作用是将一些标记组件（tagged component）添加给IOR，这些组件是允许服务器导出由业务执行的信息的辅助信息。这信息于是可以由需要使用这业务的客户机读取。例如对于一个安全业务，放在这些标记的组件内的信息可以含有一些包括诸如服务器所收听的安全套接字层(“SSL”)口的指示之类的指示、客户机必须与服务器构成什么类型的SSL连接、服务器支持什么安全机制、需要从客户机得到什么类型的信息(例如，用户名、口令、许可证等)和使客户机可以用服务器域提醒用户登录的服务器域是什么之类的信息的参数。如果安全保护停用，没有标记的组件添加给IOR。

在一个IOR截获器（interceptor）装入时，这个截获器装入一个诸如含有需要是安全的(secure)管理对象的类别和包名称的文本文件之类的文件，即使是在一个应用服务器上其他用户对象不是安全的。管理员可以认为管理对象总是需要是安全保护的，无论在应用服务器上的用户对象是否为安全的。例如，在这个图中，应用服务器1(41)提供的全都是安全的用户对象(400)和管理对象(401)。因此，导出（export）(412，413)给名称服务器(46)的都是安全的IOR。然而，应用服务器2(42)提供不需要是安全的用户对象(403)，所以对于这些对象(403)导出给名称服务器(46)的是非安全的IOR，而对于在同一个服务器(42)上的安全管理对象(404)导出(416)的是安全的IOR。

这使客户可以按服务器停用安全保护，而不会牺牲管理性的安全。优选的是，在管理员处理应用服务器的安全时应仍然启用全局安全保护(例如，整域安全保护)。对于停用的一个特定应用服务器的安全保护和启用的全局安全保护，IOR截获器可以装入无论用户对象的安全状态如何都需保持安全的类别和包（package）的清单(例如，文

本文件)，用来为每个安全保护管理对象确定是否需导出标记组件和需导出哪种标记的组件。用户对象不隶属于这个需保持安全的包或类别的清单，因此为一个管理员提供一种申报性方法，用来修改域内哪些类别是保持安全的。这样，用户对象没有包括在这个清单内，因此它们的IOR没有接收到标记的组件，而管理对象包括在这个清单内，它们的IOR接收到标记的组件，如果它们被认为是对安全是敏感的。所有对象，无论是用户对象还是管理对象，添加到由名称服务器(46)处理的名称空间。这建立了一个可通过申报配置的基于类别的对象安全方案。

利用这种配置和过程，在客户机对象(405)向诸如应用服务器1(41)之类的安全完全启用的服务器请求使用对象时，客户机(43)与对象(400，401)之间的所有事务(407)都安全地实施。客户机对象(405)在它向名称服务器(46)查找(406)应用服务器上的对象的IOR时接收到标记，指出所有对象(400，401)都受安全保护因而必须安全使用(407)。如这些标记所指示的那样，可以安全地使用(410)诸如WebSphere验证引擎和授权引擎之类的验证和授权过程提供安全业务，如管理节点(47)和一个或多个管理对象(402)所提供的。

在客户机过程要使用由应用服务器2(42)提供的用户对象(403)时，如果应用服务器2已停用了用户对象安全保护，查找(406)的行动将导致客户机过程没有接收到标记，因此在与用户对象(403)进行非安全互动(408)时将不使用安全过程。因此，与这些用户对象(403)的通信和互动(408)可以“匿名”(例如不需要验证或身份信息)和/或“明文”进行(例如没有传送保护)。然而，在使用的是应用服务器2(42)提供的管理对象(404)时，查找行动将导致接收到需调用管理节点的诸如WebSphere授权引擎和验证引擎的安全功能的标记。因此，应用服务器2成功地允许客户机不用通过安全措施就可使用用户对象(403)以固有的性能进行操作(这意味着不需要通过客户机验证、不需要服务器授权、不需要生成和存储证书等），而仍使管理对象(404)保持安全。

为了清楚起见，在图4中打有交叉阴影线的宽箭头表示非安全通

信或互动(例如，408)，而没有打交叉阴影线的宽箭头表示安全通信或互动(例如，407、410、411)。同样，细箭头(例如，412、413、414、415、416)表示为安全对象导出带标记组件的IOR的操作，而带箭头的粗线表示为非安全对象导出不带标记组件的IOR。

总结和回顾一下这种新的过程，在适当生成了带或不带标记组件的IOR后，在有一个来自客户机的对一个用户对象的非安全的未经验证的请求时，客户机对象将查找IOR，接收IOR，而ORB将调用包括一个安全请求截获器在内的一个或多个请求截获器。由于IOR内不包括标记组件，因此将作出一个不需验证和不需SSL的TCP/IP请求。这使非安全用户对象可以不需证书、验证或授权就可使用。然而，使用任何管理对象或安全用户对象就会触发验证和授权过程，而且需要使用安全通信(例如，SSL)，即使这些安全对象是处在与非安全用户对象相同的域内。

图5示出了前面所说明的按照本发明的一个优选实施例设计的导出带标记组件的共享对象的IOR的过程(50)。服务器或应用启动(51)后，就接入或装入(52)管理类别描述符文件(500)，对于每个共享对象(53)，调用(54)一个IOR截获器。如果对象在管理类内(55)，无论是直接指定的还是作为一个所指定的包的一部分，就导出(57)一个带安全标记的IOR。如果对象不在管理类内，就正常导出(56)一个对于这个对象的IOR而没有专用的安全标记。对于所有的需导出IOR的共享对象重复(58)这个过程。

图6示出了前面所说明的按照本发明的一个优选实施例设计的一个客户机请求一个共享对象或业务的过程(60)。查找(61)对于所需业务的IOR，检查(62)接收到的IOR的安全标记。如果(63)使用请求和使用这个业务需要通过诸如验证、授权和/或传送保护之类的安全措施，执行(65)所要求的动作，进行验证、授权和/或建立与应用服务器的安全通信链路。然后，安全和有传送保护地使用(66)业务/对象。否则(63)，没有安全措施正常请求和使用业务(64)。

此外，按照这个采用WebSphere平台的示范性实施例，提供了一

个与对用户对象的授权引擎分开的对管理对象的授权引擎。WebSphere管理授权引擎提供了一个基于角色的授权模型或过程。由于具有一个独立的用户对象授权引擎，任何J2EE可以用于对用户对象的安全性。由于我们的独立的用户对象安全标志和管理对象标志(例如，全局安全标志)的独特用途，系统能够用不同的授权和验证引擎独立地规定和管理用户对象和管理对象的安全性。这使得三个安全模式可以得到配置：

(a)在应用服务器安全启用和全局安全启用时，在域内一个给定的服务器上所有对象(用户和管理对象)都是被安全保护的；

(b)在应用服务器安全停用和全局安全启用时，在一个特定服务器上只有用户对象是非安全的，而管理对象仍是保持安全的；以及

(c)在全局安全停用时，域内所有服务器的所有对象(用户对象和管理对象)都是非安全的。

在图4这个实施例中，在采用WebSphere和CORBA时，客户机对象(405)和用户对象(400，403)是企业Java Bean(EJB)，而管理对象(401、402和404)是Java管理MBean。其他适当的面向对象的程序设计语言也可以使用。

虽然本说明给出了一个使用CORBA、IOP和IOR的实施例和它的详细情况来说明目标级安全过程和机制，但可取的是本发明也可以应用于其他安全协议和目标模型，包括（但不限于）WebService安全措施。在一个WebService安全模型中消息传送和方法调用由简单对象接入协议(“SOAP”)消息承载而不是IIOP安全协议，业务用Web业务定义语言(“WSDL”)和Web业务端点语言(“WSEL”)描述而不是IDL。相应，在Web业务模型中使用通用的说明、发现和集成(“UDDI”)而不是CORBA的CosNaming。CORBA的CosNaming提供用来查找一个IOR的API，而UDDI提供用来查找BusinessEntry和Web业务入口的API。这样，在这里所揭示的这个例示性实施例中，IOR用作承载对于一个对象事例的对象类型信息的机制，因此这可以用另一些对象模型和安全协议实现，如在一个Web业务UDDI对象注册表内提供对象类型信息。

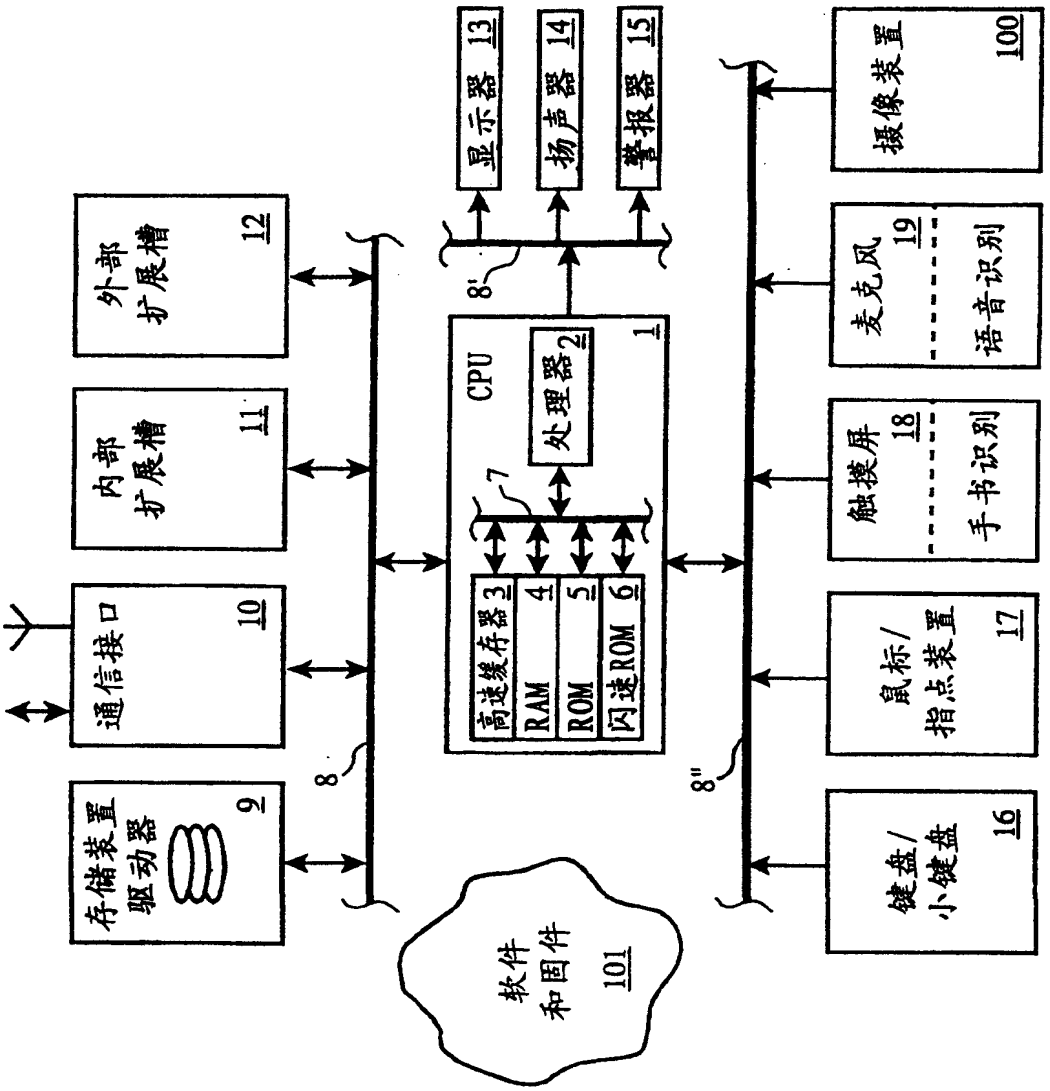

存储装置
驱动器
9
通信接口
10
内部
扩展槽
11
外部
扩展槽
12
8
软件
和固件
101
CPU
处理器2
1
高速缓存器3
RAM 4
ROM 5
闪速ROM 6
7
8'
显示器 13
扬声器 14
警报器 15
8"
键盘/
小键盘
16
鼠标/
指点装置
17
触摸屏
18
手书识别
麦克风
19
语音识别
摄像装置
100

图 1

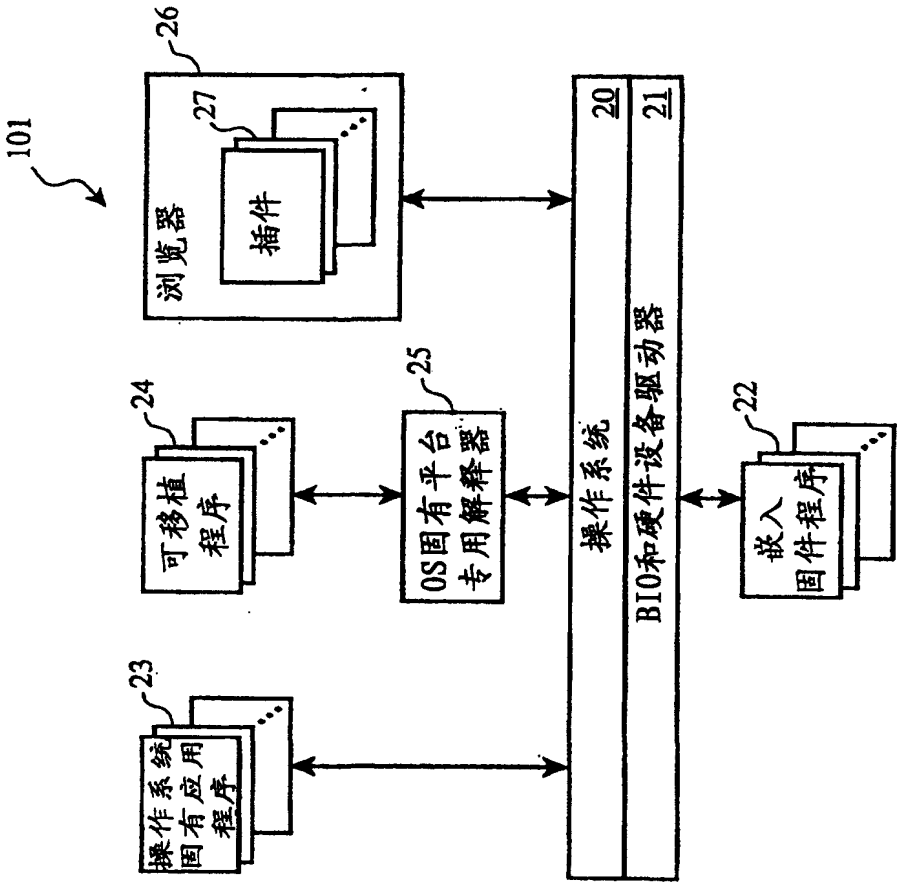

101
浏览器
26
插件
27
操作系统
20
BIO和硬件设备驱动器
21
OS固有平台
专用解释器
25
可移植
程序
24
操作系统
固有应用
程序
23
嵌入
固件程序
22

图2

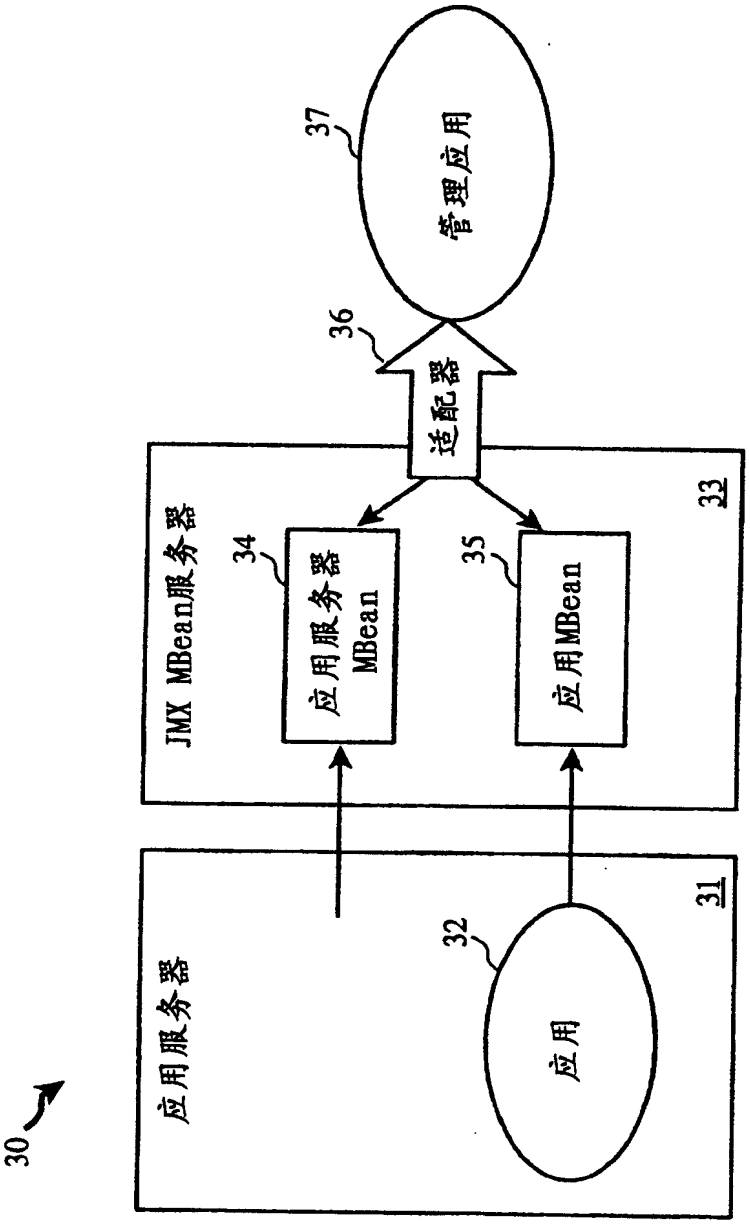

30
应用服务器
31
应用
32
JMX MBean服务器
33
应用服务器MBean
34
应用MBean
35
适配器
36
管理应用
37

图3

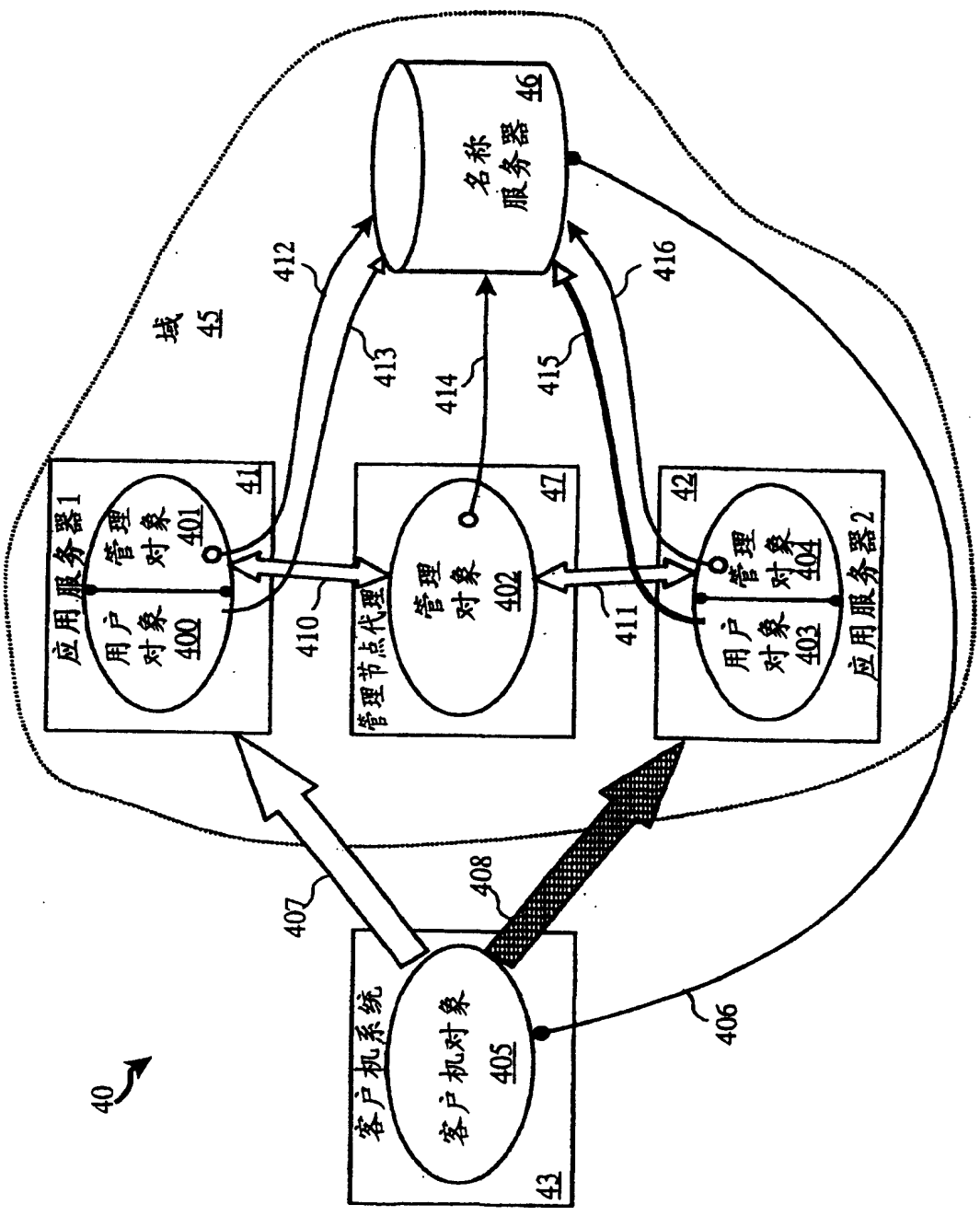

域
45
名称
服务器
46
412
413
414
415
416
应用服务器1
管理
对象
401
用户
对象
400
41
管理节点代理
管理
对象
402
47
410
411
42
管理
对象
404
用户
对象
403
应用服务器2
407
408
客户机系统
客户机对象
405
43
406
40

图 4

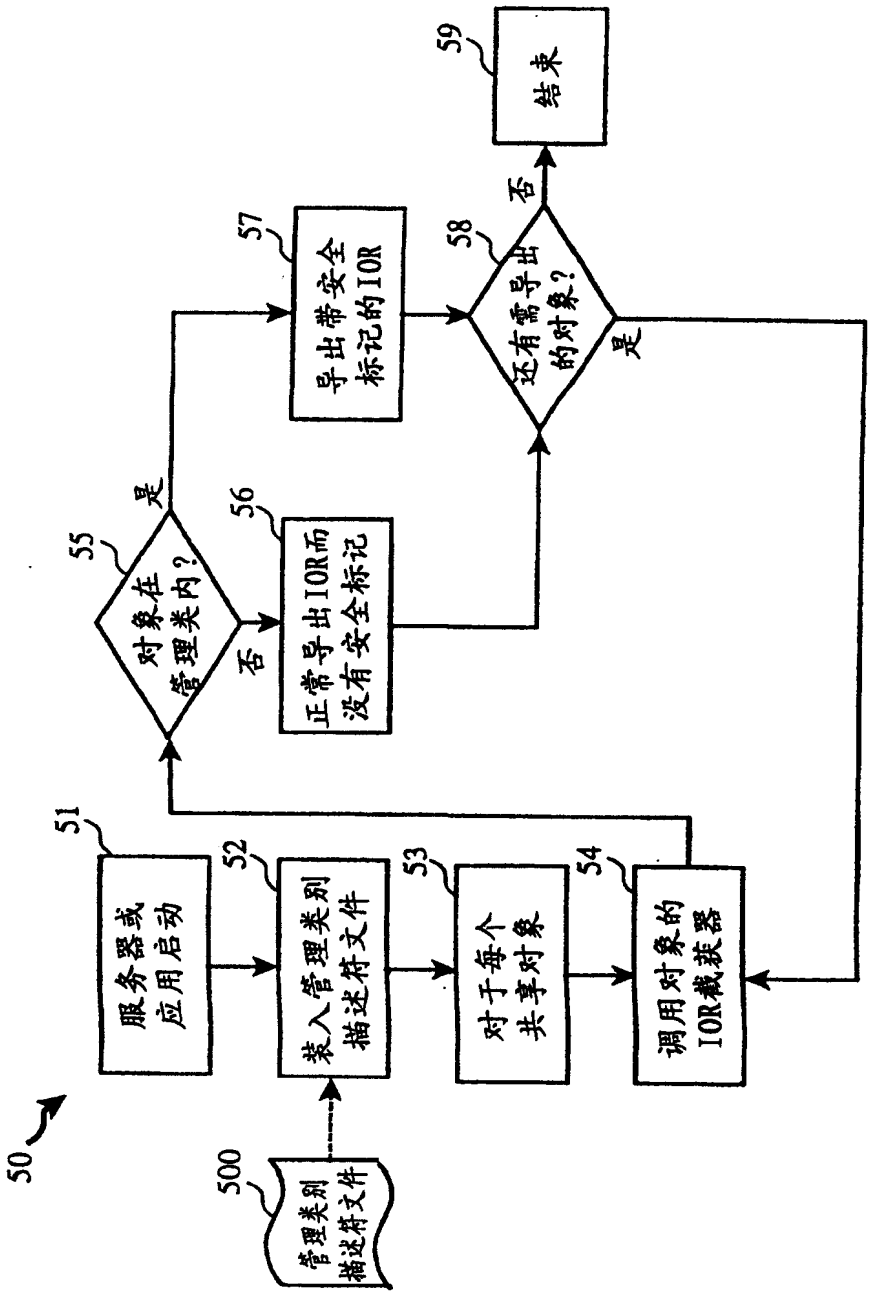

50
500
管理类别描述符文件
51
服务器或应用启动
52
装入管理类别描述符文件
53
对于每个共享对象
54
调用对象的IOR截获器
55
对象在管理类内?
是
否
56
正常导出IOR而没有安全标记
57
导出带安全标记的IOR
58
还有需导出的对象?
是
否
59
结束

图5

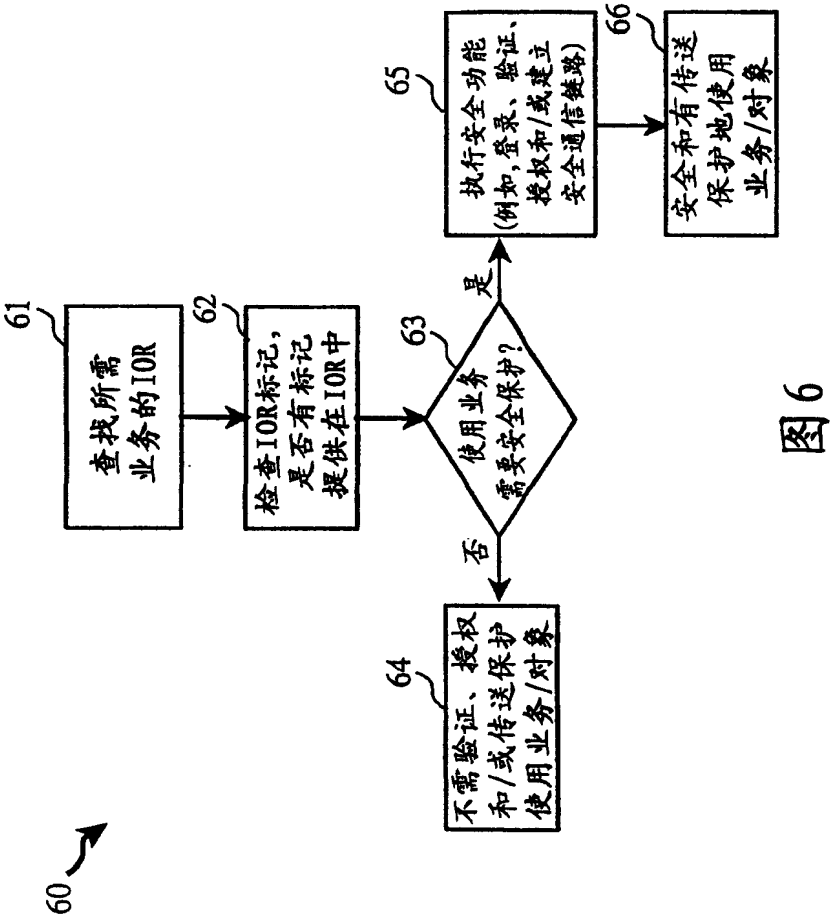

60
61
查找所需业务的IOR
62
检查IOR标记，是否有标记提供在IOR中
63
使用业务需要安全保护?
是
否
64
不需验证、授权和/或传送保护使用业务/对象
65
执行安全功能(例如，登录、验证、授权和/或建立安全通信链路)
66
安全和有传送保护地使用业务/对象

图 6