(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106161378 A
(43)申请公布日 2016.11.23

(21)申请号 201510172914.0

(22)申请日 2015.04.13

(71)申请人 中国移动通信集团公司
地址 100032 北京市西城区金融大街29号

(72)发明人 王静 柏洪涛 左敏

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静 黄灿

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 12/14(2006.01)

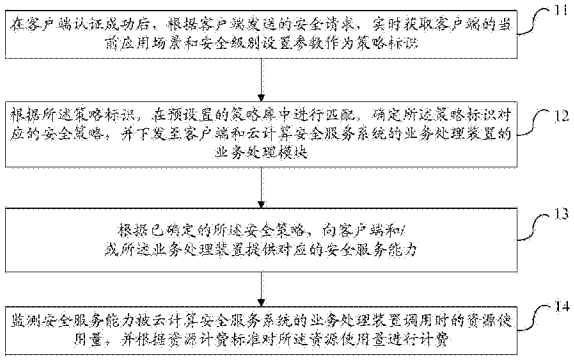
权利要求书3页 说明书9页 附图5页

(54)发明名称

安全服务装置、方法以及业务处理装置、方法和系统

(57)摘要

本发明提供一种安全服务装置、方法以及业务处理装置、方法和系统。该方法包括：在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；根据策略标识，在预设置的策略库中进行匹配，确定策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块；根据已确定的安全策略，向客户端和/或业务处理装置提供对应的安全服务能力；监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对资源使用量进行计费。本方案通过策略标识制定差异化的安全策略，从而提供对应的安全服务，满足用户及业务的个性化安全需求。



CN 106161378 A

1. 一种安全服务方法，应用于云计算安全服务系统，其特征在于，包括：

在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；

根据所述策略标识，在预设置的策略库中进行匹配，确定所述策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块；

根据已确定的所述安全策略，向客户端和/或所述业务处理装置提供对应的安全服务能力；

监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费。

2. 根据权利要求 1 所述的安全服务方法，其特征在于，在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识的步骤包括：

接收客户端发送的安全请求，获取用户设置的安全参数作为第一安全级别设置参数；

根据所述安全请求，获取客户端业务类别作为第二安全级别设置参数。

3. 根据权利要求 1 所述的安全服务方法，其特征在于，根据所述策略标识，在预设置的策略库中进行匹配，确定对应所述策略标识的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块的步骤包括：

根据获取到的策略标识，在策略库中匹配，查找到对应所述策略标识的安全策略；其中，所述策略库中的安全策略是按照策略标识和安全策略的对应关系预设置存储的；

将已确定的所述安全策略下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

4. 根据权利要求 1 所述的安全服务方法，其特征在于，监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费的步骤包括：

监测安全服务能力被云计算安全服务系统的业务处理装置调用时，所述业务处理模块所消耗的内存资源、计算资源和带宽资源的使用量；

根据监测获得的内存资源、计算资源和带宽资源的使用量，分别按照对应的内存资源计费标准、计算资源计费标准和宽带资源计费标准进行计费。

5. 根据权利要求 2 所述的安全服务方法，其特征在于，所述业务类别是客户端根据本身的服务质量 QoS 的类别设置确定的；所述当前应用场景是客户端根据本身的互联网协议 IP 地址和接入点位置确定的。

6. 根据权利要求 1 所述的安全服务方法，其特征在于，所述安全服务能力至少包括：加密、认证、完整性、云漏洞扫描、云病毒查杀、密钥管理、密文存储、业务流量清洗、入侵检测、数据隔离和恢复中的一种或多种。

7. 一种安全服务装置，应用于云计算安全服务系统，其特征在于，包括：

策略标识获取模块，用于在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；

策略确定模块，用于根据所述策略标识，在预设置的策略库中进行匹配，确定所述策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理

模块；

安全能力模块，用于根据已确定的所述安全策略，向客户端和／或所述业务处理装置提供对应的安全服务能力；

计费模块，用于监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费。

8. 根据权利要求 7 所述的安全服务装置，其特征在于，所述策略标识获取模块包括：

第一策略标识获取子模块，用于接收客户端发送的安全请求，获取用户设置的安全参数作为第一安全级别设置参数；

第二策略标识获取子模块，用于根据所述安全请求，获取客户端业务类别作为第二安全级别设置参数。

9. 根据权利要求 7 所述的安全服务装置，其特征在于，所述策略确定模块包括：

策略确定子模块，用于根据获取到的策略标识，在策略库中匹配，查找到对应所述策略标识的安全策略；其中，所述策略库中的安全策略是按照策略标识和安全策略的对应关系预设置存储的；

策略下发子模块，用于将已确定的所述安全策略下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

10. 根据权利要求 7 所述的安全服务装置，其特征在于，所述计费模块包括：

资源消耗监测子模块，用于监测安全服务能力被云计算安全服务系统的业务处理装置调用时的内存资源、计算资源和带宽资源的使用量；

计费子模块，用于根据监测获得的内存资源、计算资源和带宽资源的使用量，分别按照对应的内存资源计费标准、计算资源计费标准和宽带资源计费标准进行计费。

11. 根据权利要求 8 所述的安全服务装置，其特征在于，所述业务类别是客户端根据本身的服务质量 QoS 的类别设置确定的；所述当前应用场景是客户端根据本身的互联网协议 IP 地址和接入点位置确定的。

12. 根据权利要求 7 所述的安全服务装置，其特征在于，所述安全服务能力至少包括：加密、认证、完整性、云漏洞扫描、云病毒查杀、密钥管理、密文存储、业务流量清洗、入侵检测、数据隔离和恢复中的一种或多种。

13. 一种业务处理装置，应用于云计算安全服务系统，其特征在于，包括：

认证模块，用于接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；

业务处理模块，用于根据云计算安全服务系统的安全服务装置确定的安全策略调用安全服务能力，对用户业务数据进行处理。

14. 根据权利要求 13 所述的业务处理装置，其特征在于，所述处理至少包括：对接收数据的解密、对发送数据的加密、数据隔离或数据恢复中的一种或多种。

15. 一种业务处理方法，应用于云计算安全服务系统，其特征在于，包括：

接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；

根据云计算安全服务系统的安全服务装置确定的安全策略调用安全服务能力，对用户业务数据进行安全处理。

16. 一种云计算安全服务系统，其特征在于，包括如权利要求 7 至 12 任一项所述的安全

服务装置和如权利要求 13 或 14 所述的业务处理装置。

安全服务装置、方法以及业务处理装置、方法和系统

技术领域

[0001] 本发明涉及信息安全技术领域，特别是指一种安全服务装置、方法以及业务处理装置、方法和系统。

背景技术

[0002] 云计算在最近几年迅速发展，无论是互联网厂商和运营商，还是通信厂商和基础网络运营商，都对云计算表现出极大的关注。

[0003] 狭义的云计算是指互联网技术（IT，Internet Technology）基础设施的交付和使用模式，指通过网络以按需、易扩展的方式获得所需的资源；广义的云计算是指服务的交付和使用模式。这种服务的形式是基于拥有超强计算能力的数据中心，通过它提供的计算能力，从而运行各种定制的服务，通过互联网提供给用户。而这与普通的网络服务的区别在于动态扩展特性和虚拟化技术的广泛应用。

[0004] 云计算具有超大规模、虚拟化、安全可靠等优点。对于网络运营商而言，由于云计算使用动态资源分配和扩展技术，将大大降低运营成本和操作维护成本，从而达到节能减排的目的；除此之外，运营商还可以扩大运营的范围，而不仅仅受限于管道运营。在云计算环境下，一切资源都是可以运营的，都可以作为服务提供，包括应用程序、软件、平台、处理能力、存储、网络、计算资源以及其他基础设施等。对于用户而言，云计算使得用户随时、随地使用网络业务成为可能，此外用户可以不需要大量投资而获得运营业务所需的 IT 资源，完全可以根据自己的需求来租用 IT 资源，就如水、电和煤气一样，按需获取和计费。

[0005] 云计算一般有三种主要的服务模式，基础设施即服务（IaaS，Infrastructureas a Service，）、平台即服务（PaaS，Platform as a Service）和软件即服务（SaaS，Software as a Service）。而根据服务的部署模式，又可以分为私有云、共有云和混合云。

[0006] 在云计算场景下，大量的用户信息都集中在云计算提供商，与传统的互联网业务相比，其信息更集中、信息资产价值更高、面临的攻击也会更多。云计算所面临的安全问题涉及到用户的信息安全（数据完整性、一致性、私密性）、服务的审计和证据、网络状况安全、虚拟机环境安全、数据中心内部环境安全、管理安全等领域。其中，用户对服务商安全的不信任严重地阻碍了云计算商用的发展，导致云计算商用面临诸多困难，云计算安全已经成为云计算业务模式大规模商用的最重要瓶颈。

[0007] 云业务和云平台的资源在云计算环境下，被高度共享。面对多样化需求和多样化使用环境的用户，单一安全等级的保护方案已经不适合云计算环境。云计算迫切需要在安全上有新的机制，能够为不同业务，不同用户提供细粒度、个性化的安全解决方案，动态差异化安全防护的目的。而针对这种按需供给的构想，相对应的，对于不同的安全需求和服务类型，也需要差异化的安全解决方案。而传统上针对单一业务所制定的安全解决方案，无法适应云计算平台高度共享的特性。

发明内容

[0008] 本发明的目的是提供一种安全服务装置、方法以及业务处理装置、方法和系统，根据用户及业务个性化的需求实现安全服务资源按需使用、有效利用，以及绿色节能的目的。

[0009] 为达到上述目的，本发明的实施例提供一种安全服务方法，应用于云计算安全服务系统，包括：

[0010] 在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；

[0011] 根据所述策略标识，在预设置的策略库中进行匹配，确定所述策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块；

[0012] 根据已确定的所述安全策略，向客户端和/或所述业务处理装置提供对应的安全服务能力；

[0013] 监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费。

[0014] 其中，在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识的步骤包括：

[0015] 接收客户端发送的安全请求，获取用户设置的安全参数作为第一安全级别设置参数；

[0016] 根据所述安全请求，获取客户端业务类别作为第二安全级别设置参数。

[0017] 其中，根据所述策略标识，在预设置的策略库中进行匹配，确定对应所述策略标识的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块的步骤包括：

[0018] 根据获取到的策略标识，在策略库中匹配，查找到对应所述策略标识的安全策略；其中，所述策略库中的安全策略是按照策略标识和安全策略的对应关系预设置存储的；

[0019] 将已确定的所述安全策略下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

[0020] 其中，监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费的步骤包括：

[0021] 监测安全服务能力被云计算安全服务系统的业务处理装置调用时，所述业务处理模块所消耗的内存资源、计算资源和带宽资源的使用量；

[0022] 根据监测获得的内存资源、计算资源和带宽资源的使用量，分别按照对应的内存资源计费标准、计算资源计费标准和宽带资源计费标准进行计费。

[0023] 其中，所述业务类别是客户端根据本身的服务质量QoS的类别设置确定的；所述当前应用场景是客户端根据本身的互联网协议IP地址和接入点位置确定的。

[0024] 其中，所述安全服务能力至少包括：加密、认证、完整性、云漏洞扫描、云病毒查杀、密钥管理、密文存储、业务流量清洗、入侵检测、数据隔离和恢复中的一种或多种。

[0025] 为达到上述目的，本发明的实施例还提供了一种安全服务装置，应用于云计算安全服务系统，包括：

[0026] 策略标识获取模块，用于在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；

[0027] 策略确定模块，用于根据所述策略标识，在预设置的策略库中进行匹配，确定所述

策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块；

[0028] 安全能力模块，用于根据已确定的所述安全策略，向客户端和/或所述业务处理装置提供对应的安全服务能力；

[0029] 计费模块，用于监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费。

[0030] 其中，所述策略标识获取模块包括：

[0031] 第一策略标识获取子模块，用于接收客户端发送的安全请求，获取用户设置的安全参数作为第一安全级别设置参数；

[0032] 第二策略标识获取子模块，用于根据所述安全请求，获取客户端业务类别作为第二安全级别设置参数。

[0033] 其中，所述策略确定模块包括：

[0034] 策略确定子模块，用于根据获取到的策略标识，在策略库中匹配，查找到对应所述策略标识的安全策略；其中，所述策略库中的安全策略是按照策略标识和安全策略的对应关系预设置存储的；

[0035] 策略下发子模块，用于将已确定的所述安全策略下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

[0036] 其中，所述计费模块包括：

[0037] 资源消耗监测子模块，用于监测安全服务能力被云计算安全服务系统的业务处理装置调用时的内存资源、计算资源和带宽资源的使用量；

[0038] 计费子模块，用于根据监测获得的内存资源、计算资源和带宽资源的使用量，分别按照对应的内存资源计费标准、计算资源计费标准和宽带资源计费标准进行计费。

[0039] 其中，所述业务类别是客户端根据本身的服务质量QoS的类别设置确定的；所述当前应用场景是客户端根据本身的互联网协议IP地址和接入点位置确定的。

[0040] 其中，所述安全服务能力至少包括：加密、认证、完整性、云漏洞扫描、云病毒查杀、密钥管理、密文存储、业务流量清洗、入侵检测、数据隔离和恢复中的一种或多种。

[0041] 为达到上述目的，本发明实施例还提供了一种业务处理装置，应用于云计算安全服务系统，包括：

[0042] 认证模块，用于接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；

[0043] 业务处理模块，用于根据云计算安全服务系统的安全服务装置确定的安全策略调用安全服务能力，对用户业务数据进行处理。

[0044] 其中，所述处理至少包括：对接收数据的解密、对发送数据的加密、数据隔离或数据恢复中的一种或多种。

[0045] 为达到上述目的，本发明的实施例还提供了一种业务处理方法，应用于云计算安全服务系统，包括：

[0046] 接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；

[0047] 根据云计算安全服务系统的安全服务装置确定的安全策略调用安全服务能力，对用户业务数据进行安全处理。

[0048] 为达到上述目的，本发明的实施例还提供了一种云计算安全服务系统，包括如上所述的安全服务装置和如上所述的业务处理装置。

[0049] 本发明的上述技术方案的有益效果如下：

[0050] 本发明实施例的安全服务方法，在客户端认证成功后，会根据客户端发送的安全请求，来实时获取包括客户端的当前应用场景和安全级别设置参数的策略标识。由客户端的当前应用场景和安全级别设置参数确定的安全策略能够体现用户及业务的个性化需求，如此，根据该策略标识就能够在策略库中确定对应该策略标识的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。随后，在客户端和/或业务处理装置携带该安全策略调用对应的安全服务能力时，根据该安全策略向其提供所需的安全服务能力，通过策略标识制定差异化的安全策略，从而提供对应的安全服务，满足用户及业务的个性化安全需求。然后监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对资源使用量进行计费，由于按照资源使用量进行计费，确保了资源的有效利用，达到绿色节能的目的。

附图说明

[0051] 图 1 表示本发明实施例的安全服务装置的结构示意图；

[0052] 图 2 表示本发明实施例的安全服务装置计费模式；

[0053] 图 3 表示视频会议实现安全服务的流程图；

[0054] 图 4 表示本发明实施例的安全服务装置的实现框架；

[0055] 图 5 表示本发明实施例的安全服务方法的步骤流程图。

具体实施方式

[0056] 为使本发明要解决的技术问题、技术方案和优点更加清楚，下面将结合附图及具体实施例进行详细描述。

[0057] 本发明针对现有的安全保护方案安全等级单一，不能根据用户及业务个性化的需求进行适应性的调整，无法适应云计算平台高度共享的特性的问题，提供一种安全服务装置，根据用户及业务个性化的需求实现安全服务资源按需使用、有效利用，以及绿色节能的目的。

[0058] 如图 1 所示，本发明实施例的一种安全服务装置，应用于云计算安全服务系统，包括：

[0059] 策略标识获取模块 10，用于在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；

[0060] 策略确定模块 20，用于根据所述策略标识，在预设置的策略库中进行匹配，确定所述策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块；

[0061] 安全能力模块 30，用于根据已确定的所述安全策略，向客户端和/或所述业务处理装置提供对应的安全服务能力；

[0062] 计费模块 40，用于监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费。

[0063] 首先，具有享有安全服务的客户端用户，才向其提供安全服务，客户端会先向业务处理装置发起认证，客户端认证成功后，用户可以进行相关的安全配置如业务安全要求（或者说是业务信息的重要性等），而策略标识获取模块 10 在客户端认证成功后，就会根据客户端发送的安全请求，来获取策略标识，该策略标识采用客户端的当前应用场景和安全级别设置参数。由客户端的当前应用场景和安全级别设置参数确定的安全策略（安全配置参数，是云计算安全服务系统对用户所订购的业务实施差异化安全防护所需的配置参数）能够体现用户及业务的个性化需求，如此，策略确定模块 20 根据该策略标识就能够在策略库中确定对应该策略标识的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。随后，在客户端和 / 或业务处理装置携带该安全策略调用对应的安全服务能力时，安全能力模块 30 根据该安全策略向其提供所需的安全服务能力。

[0064] 在本发明实施例的安全服务装置中，还包括计费模块 40，监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对资源使用量进行计费。云计算安全服务系统的业务处理装置调用安全能力模块，安全能力模块启动对用户所订购的业务进行差异化安全防护，就需要消耗一定的资源，计费模块 40 对所消耗的资源使用量进行监测统计，可以通过监测安全能力模块实现，并按照预先确定的资费标准进行计费。

[0065] 本发明实施例的安全服务装置通过策略标识制定差异化的安全策略，从而提供对应的安全服务，满足用户及业务的个性化安全需求，同时，按照资源使用量进行计费，确保了资源的有效利用，达到绿色节能的目的。

[0066] 在本发明的实施例中，用户在发送安全请求前能够进行安全参数的自定义设置，因此，所述安全请求包括用户设置的安全参数；

[0067] 所述策略标识获取模块 10 包括：

[0068] 第一策略标识获取子模块 101，用于接收客户端发送的安全请求，获取用户设置的安全参数作为第一安全级别设置参数；

[0069] 第二策略标识获取子模块 102，用于根据所述安全请求，获取客户端业务类别作为第二安全级别设置参数。

[0070] 由于要根据用户的需求设置合理的安全等级满足需要，故第一策略标识获取子模块 101 会获取安全请求中用户设置的安全参数作为第一安全级别设置参数。而不同的业务类别，也需要的合理的安全级别，安全级别考虑业务类别可尽量减小安全对服务质量的不利影响，故第二策略标识获取子模块 102 会根据安全请求，获取客户端业务类别作为第二安全级别设置参数。再有众所周知，不同的客户端的当前应用场景（客户端接入云业务时所处的网络环境）如无线 3G 网（机场）、家庭网络、办公网络等，所需要的安全保护是不同的，故还包括第三策略标识获取子模块 103 会根据所述安全请求，获取客户端的当前应用场景。由第一安全级别设置参数、第二安全级别设置参数和当前应用场景作为策略标识，能够更具有针对性的确定个性化、差异化、定制化的安全策略进而进行安全保护，来满足用户及业务需要。

[0071] 其中，所述业务类别是客户端根据本身的服务质量 QoS 的类别设置确定的；所述当前应用场景是客户端根据本身的互联网协议 IP 地址和接入点位置确定的。

[0072] 当然，策略标识并不仅限于本发明实施例所提到的三类数据，考虑到其他因素将

除上述类型之外的数据作为策略标识也是在本发明的保护范围内。

[0073] 在策略标识获取模块 10 得到策略标识后，就可由策略确定模块 20 来确定针对用户及业务的安全策略了。在本发明的实施例中，所述策略确定模块 20 包括：

[0074] 策略确定子模块 201，用于根据获取到的策略标识，在策略库中匹配，查找到对应所述策略标识的安全策略；其中，所述策略库中的安全策略是按照策略标识和安全策略的对应关系预设置存储的；

[0075] 策略下发子模块 202，用于将已确定的所述安全策略下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

[0076] 在策略库中，安全策略是按照策略标识与安全策略的对应关系预设置存储的，通过策略标识能够查找到与其对应的安全策略，策略确定子模块 201 就能够根据获取到的策略标识，在策略库中匹配，查找到与该策略标识对应的安全策略。对于已确定的安全策略，策略下发子模块 202 就可以将其下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

[0077] 由于策略标识和安全策略之间的对应关系，可能会根据用户及业务需求做适当调整，这样，策略确定模块 20 可能还包括策略管理子模块 203，策略管理子模块 203 会根据预设值控制和管理策略库中的安全策略，如重新调整策略标识和安全策略的对应关系，增加或减少某一安全策略具体内容等等。

[0078] 安全策略下发后，客户端和 / 或业务处理装置根据该安全策略在安全能力模块调用对应的安全服务能力。

[0079] 其中，所述安全服务能力至少包括：加密、认证、完整性、云漏洞扫描、云病毒查杀、密钥管理、密文存储、业务流量清洗、入侵检测、数据隔离和恢复中的一种或多种。

[0080] 安全能力模块通过预设置的安全协议算法实现安全服务能力，提供差异化的安全防护。

[0081] 应该知道的是，安全能力模块获得安全策略（安全配置参数，是云计算安全服务系统对用户所订购的业务实施差异化安全防护所需的配置参数）后，启动相关安全协议算法，对用户所订购的业务实施安全防护。安全能力模块提供安全服务能力会消耗系统资源，为了更精确的计费，按照不同类型资源通过其相应的计费标准计算。在本发明实施例的安全服务装置中，所述资源包括内存资源、计算资源和带宽资源；

[0082] 所述计费模块 40 包括：

[0083] 资源消耗监测子模块 401，用于监测安全服务能力被云计算安全服务系统的业务处理装置调用时的内存资源、计算资源和带宽资源的使用量；

[0084] 计费子模块 402，用于根据监测获得的内存资源、计算资源和带宽资源的使用量，分别按照对应的内存资源计费标准、计算资源计费标准和宽带资源计费标准进行计费。

[0085] 如图 2 所示的计费模式，在安全能力模块提供安全服务能力时，所消耗的资源类型主要有内存资源、计算资源和带宽资源，资源消耗监测子模块 401 会监测其所消耗的不同类型资源的使用量，然后由计费模块 402 按照不同类型资源的计费标准进行计费，计算出在每一个类别所消耗的费用，从而确定差异化安全服务的价格水平。

[0086] 下面结合图 3 说明本发明实施例的安全服务装置的应用：

[0087] 在该例中，用户在机场通过 WIFI 进行视频会议，由于视频会议的业务流量特征是

数据包固定大小，恒定速率，低速率，丢包率非常低，时延非常低，抖动非常低，是业务类别中的优先类。

[0088] 客户端首先向业务处理装置的认证模块发送认证请求 S1。之后，认证模块返回认证成功至客户端 S2。客户端认证成功后，用户进行相关的安全配置，安全参数要求传输加密，客户端自动检测用户配置的安全参数，向安全服务装置的策略标识获取模块发送携带有用户设置的安全参数的安全请求 S3。策略标识获取模块获取到安全请求后，会实时获取客户端当前应用场景（当前为 WIFI 接入）及业务类别（视频会议）S4，将确定的策略标识发送到策略确定模块 S5。策略确定模块根据策略标识，在预设置的策略库中进行匹配，确定对应所述策略标识的安全策略 S6，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块 S7、S8。客户端携带安全策略调用安全加解密能力，安全能力模块向客户端提供 S9，并发起计费 S10，计费模块监测资源类型及使用情况确定所消耗资源使用量并根据资源计费标准对所述消耗的资源使用量进行计费 S11。这样，客户端发起视频会议，对视频数据进行加密传输 S12。业务处理装置中业务处理模块也携带安全策略调用安全加解密能力，安全能力模块向客户端提供 S13，业务处理模块对接收到数据进行解密，对发送数据进行加密 S14，向客户端传输视频数据，对视频数据进行加密传输 S15，客户端对接收到数据进行解密，对后续发送数据进行加密 S16。当客户端与业务处理装置连接之后，在断开前发送的数据都采用相同的安全策略，而不需要每次发送数据都去查找安全策略。

[0089] 由于策略标识获取模块获取到安全请求后，会实时获取客户端当前应用场景，在客户端场景变化，例如有办公场所接入移动到由公共场所接入 S17，需要采用更高强度的安全策略，则安全策略要重新确定。当前应用场景变化，发送当前应用场景 S18，策略标识获取模块获取到策略标识更改 S19，发送新的策略标识到策略确定模块 S20，根据新的策略标识重新确定新的安全策略 S21，并下发至户端和云计算安全服务系统的业务处理装置的业务处理模块 S22、S23，根据新的安全策略，对视频会议数据进行加密传输 S24，此时采用的加密算法可能更高级来提升数据传输安全。

[0090] 在用户配置了数据安全保护能力时，客户端能够将用户设置的业务粒度自动映射到 IP 数据包的服务类型字段，通过采用区分服务 Diffserv 业务框架，业务处理模块在接收到数据后才可提取即将发送的数据的业务粒度 S25，策略标识获取模块此时获取的策略标识是由业务处理模块提供的 S26。策略确定模块根据策略标识，在预设置的策略库中进行匹配，确定对应策略标识的安全策略 S27，并下发至云计算安全服务系统的业务处理装置的业务处理模块 S28。业务处理模块携带安全策略调用安全能力，安全能力模块向业务处理模块提供进行安全保护 S29，业务处理模块进行安全保护（数据隔离、数据恢复、数据加密等）S30，安全能力模块发起计费 S31，计费模块监测资源类型及使用情况确定所消耗资源使用量，并根据资源计费标准对所述消耗的资源使用量进行计费 S32。

[0091] 综上所述，本发明实施例的安全服务装置，如图 4 所示，策略标识获取模块通过多渠道（用户设置安全参数、当前应用场景、业务类别和其他）获取相关策略标识；策略确定模块根据策略标识制定差异化的安全策略，同时进行安全策略的控制管理、下发执行；安全能力模块根据确定的安全策略提供安全服务能力，从而提供对应的安全服务，满足用户及业务的个性化安全需求，同时，计费模块进行资源监测，按照资源使用量进行计费，确保了资源的有效利用，达到绿色节能的目的。

[0092] 如图 5 所示，本发明的实施例还提供了一种安全服务方法，应用于云计算安全服务系统，包括：

[0093] 步骤 11，在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识；

[0094] 步骤 12，根据所述策略标识，在预设置的策略库中进行匹配，确定所述策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块；

[0095] 步骤 13，根据已确定的所述安全策略，向客户端和 / 或所述业务处理装置提供对应的安全服务能力；

[0096] 步骤 14，监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费。

[0097] 其中，所述安全请求包括用户设置的安全参数；

[0098] 步骤 11 包括：

[0099] 步骤 111，接收客户端发送的安全请求，获取用户设置的安全参数作为第一安全级别设置参数；

[0100] 步骤 112，根据所述安全请求，获取客户端业务类别作为第二安全级别设置参数。

[0101] 其中，步骤 12 包括：

[0102] 步骤 121，根据获取到的策略标识，在策略库中匹配，查找到对应所述策略标识的安全策略；其中，所述策略库中的安全策略是按照策略标识和安全策略的对应关系预设置存储的；

[0103] 步骤 122，将已确定的所述安全策略下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块。

[0104] 其中，所述资源包括内存资源、计算资源和带宽资源；

[0105] 步骤 14 包括：

[0106] 步骤 141，监测安全服务能力被云计算安全服务系统的业务处理装置调用时的内存资源、计算资源和带宽资源的使用量；

[0107] 步骤 142，根据监测获得的内存资源、计算资源和带宽资源的使用量，分别按照对应的内存资源计费标准、计算资源计费标准和宽带资源计费标准进行计费。

[0108] 其中，所述业务类别是客户端根据本身的服务质量 QoS 的类别设置确定的；所述当前应用场景是客户端根据本身的互联网协议 IP 地址和接入点位置确定的。

[0109] 其中，所述安全服务能力至少包括：加密、认证、完整性、云漏洞扫描、云病毒查杀、密钥管理、密文存储、业务流量清洗、入侵检测、数据隔离和恢复中的一种或多种。

[0110] 本发明实施例的安全服务方法，通过多渠道（用户设置安全参数、当前应用场景、业务类别和其他）获取相关策略标识；之后根据策略标识制定差异化的安全策略，同时进行安全策略的控制管理、下发执行；并根据确定的安全策略提供安全服务能力，从而提供对应的安全服务，满足用户及业务的个性化安全需求，而且进行资源监测，按照资源使用量进行计费，确保了资源的有效利用，达到绿色节能的目的。

[0111] 需要说明的是，该安全服务方法是应用于上述安全服务装置的方法，上述安全服务装置的实现方式适用于该方法，也能达到相同的技术效果。

[0112] 本发明实施例还提供了一种业务处理装置，应用于云计算安全服务系统，包括：

[0113] 认证模块 50，用于接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；

[0114] 业务处理模块 60，用于根据云计算安全服务系统的安全服务装置确定的安全策略调用安全服务能力，对用户业务数据进行处理。

[0115] 其中，所述处理至少包括：对接收数据的解密、对发送数据的加密、数据隔离或数据恢复中的一种或多种。

[0116] 本发明实施例的业务处理装置，应用于云计算安全服务系统，配合上述安全服务装置，通过认证模块接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；在认证通过后，安全服务装置根据策略标识制定差异化的安全策略，从而提供对应的安全服务，而业务处理模块可根据安全策略调用安全服务能力，对用户业务数据进行处理，满足用户及业务的个性化安全需求。

[0117] 需要说明的是，该业务处理装置是配合上述安全服务装置的装置，上述安全服务装置的实现方式适用于该装置，也能达到相同的技术效果。

[0118] 本发明的实施例还提供了一种业务处理方法，应用于云计算安全服务系统，包括：

[0119] 步骤 21，接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；

[0120] 步骤 22，根据云计算安全服务系统的安全服务装置确定的安全策略调用安全服务能力，对用户业务数据进行安全处理。

[0121] 其中，所述处理至少包括：对接收数据的解密、对发送数据的加密、数据隔离或数据恢复中的一种或多种。

[0122] 该业务处理方法应用于云计算安全服务系统，配合上述安全服务装置，通过接收客户端的认证请求，并根据所述认证请求对客户端用户进行认证；在认证通过后，安全服务装置根据策略标识制定差异化的安全策略，从而提供对应的安全服务，就可根据安全策略调用安全服务能力，对用户业务数据进行处理，满足用户及业务的个性化安全需求。

[0123] 需要说明的是，该业务处理方法是应用于上述业务处理装置的方法，上述业务处理装置的实现方式适用于该方法，也能达到相同的技术效果。

[0124] 本发明的实施例还提供了一种云计算安全服务系统，包括如上所述的安全服务装置和如上所述的业务处理装置。

[0125] 该云计算安全服务系统，业务处理装置根据接收到的客户端发送的认证请求，对客户端进行认证；安全服务装置在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数，在确定对应的安全策略后，下发安全策略；安全服务装置能够根据安全策略向客户端和 / 或业务处理装置提供对应的安全能力，并监测业务处理装置调用安全服务能力时所消耗的资源使用量，按照资源计费标准进行计费；业务处理装置通过调用安全服务能力，对用户业务数据进行安全处理。该系统满足了用户及业务的个性化安全需求，同时能够进行资源监测，按照资源使用量进行计费，确保了资源的有效利用，达到绿色节能的目的。

[0126] 以上所述是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明所述原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

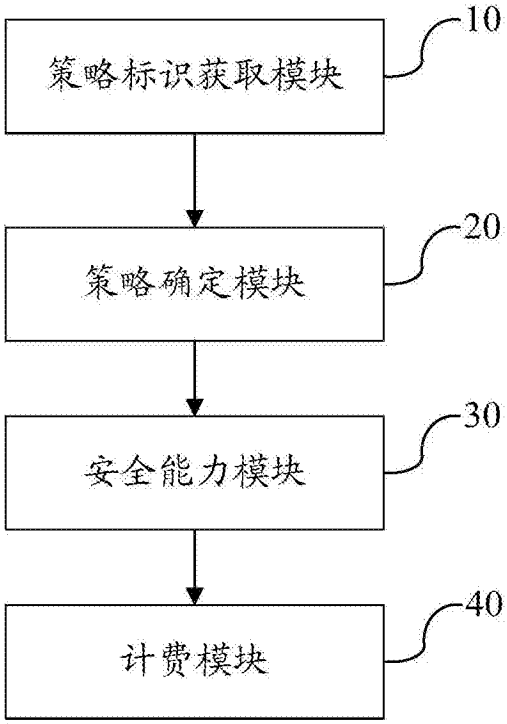


图 1

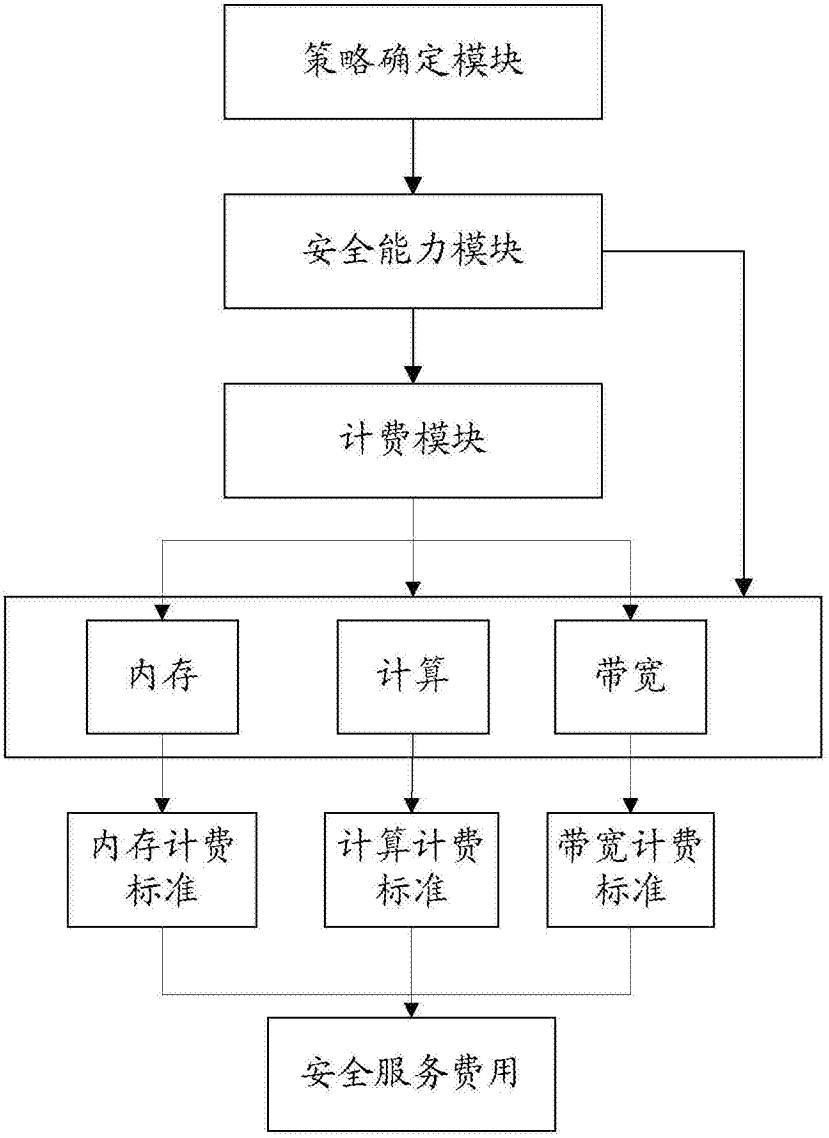


图 2

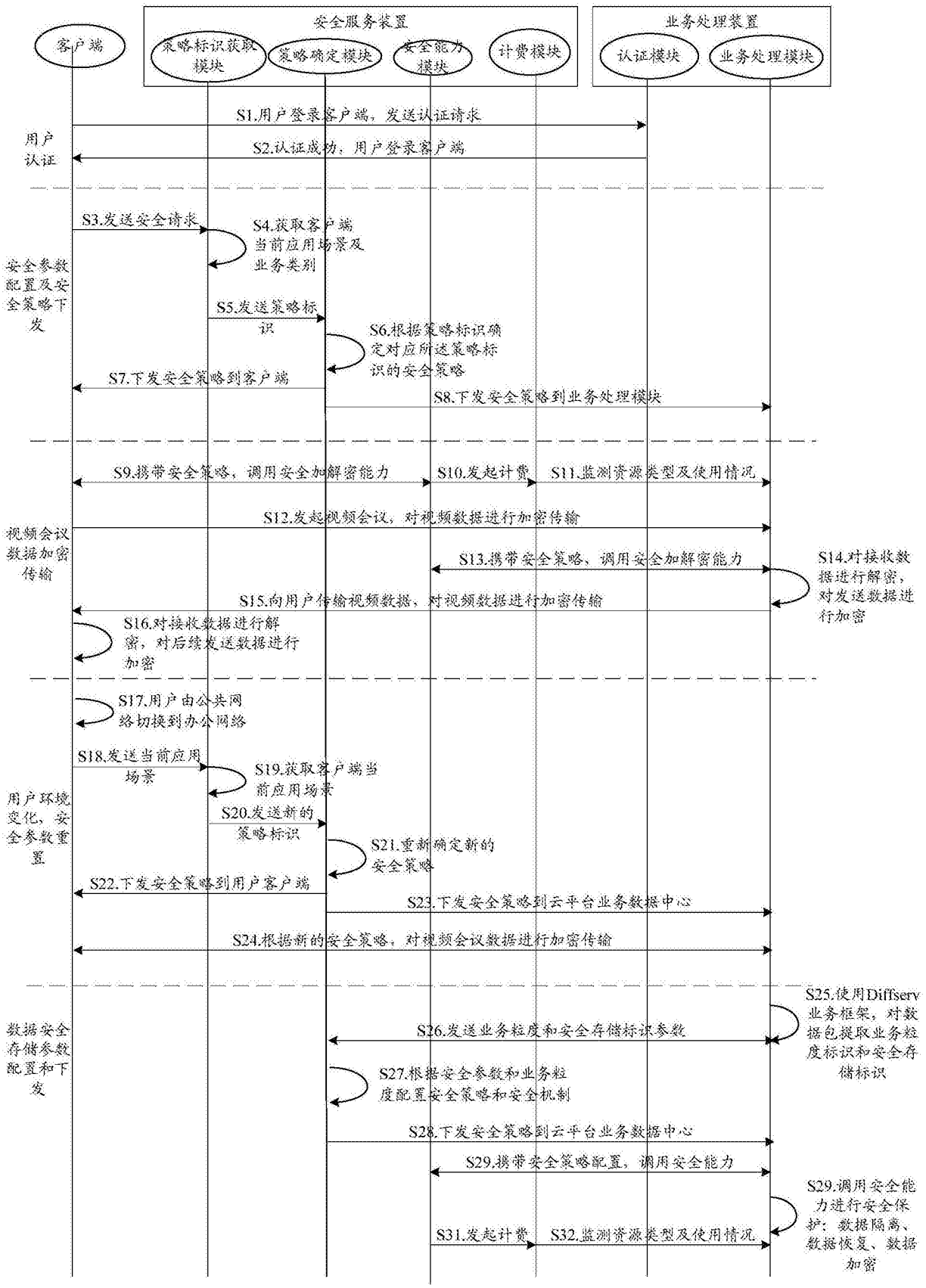

安全服务装置
业务处理装置
客户端
策略标识获取模块
策略确定模块
安全能力模块
计费模块
认证模块
业务处理模块
S1.用户登录客户端，发送认证请求
用户认证
S2.认证成功，用户登录客户端
S3.发送安全请求
S4.获取客户端当前应用场景及业务类别
安全参数配置及安全策略下发
S5.发送策略标识
S6.根据策略标识确定对应所述策略标识的安全策略
S7.下发安全策略到客户端
S8.下发安全策略到业务处理模块
S9.携带安全策略，调用安全加解密能力
S10.发起计费
S11.监测资源类型及使用情况
S12.发起视频会议，对视频数据进行加密传输
视频会议数据加密传输
S13.携带安全策略、调用安全加解密能力
S14.对接收数据进行解密，对发送数据进行加密
S15.向用户传输视频数据，对视频数据进行加密传输
S16.对接收数据进行解密，对后续发送数据进行加密
S17.用户由公共网络切换到办公网络
S18.发送当前应用场景
S19.获取客户端当前应用场景
用户环境变化，安全参数重置
S20.发送新的策略标识
S21.重新确定新的安全策略
S22.下发安全策略到用户客户端
S23.下发安全策略到云平台业务数据中心
S24.根据新的安全策略，对视频会议数据进行加密传输
S25.使用Diffserv业务框架，对数据包提取业务粒度标识和安全存储标识
数据安全存储参数配置和下发
S26.发送业务粒度和安全存储标识参数
S27.根据安全参数和业务粒度配置安全策略和安全机制
S28.下发安全策略到云平台业务数据中心
S29.携带安全策略配置，调用安全能力
S29.调用安全能力进行安全保护：数据隔离、数据恢复、数据加密
S31.发起计费
S32.监测资源类型及使用情况

图 3

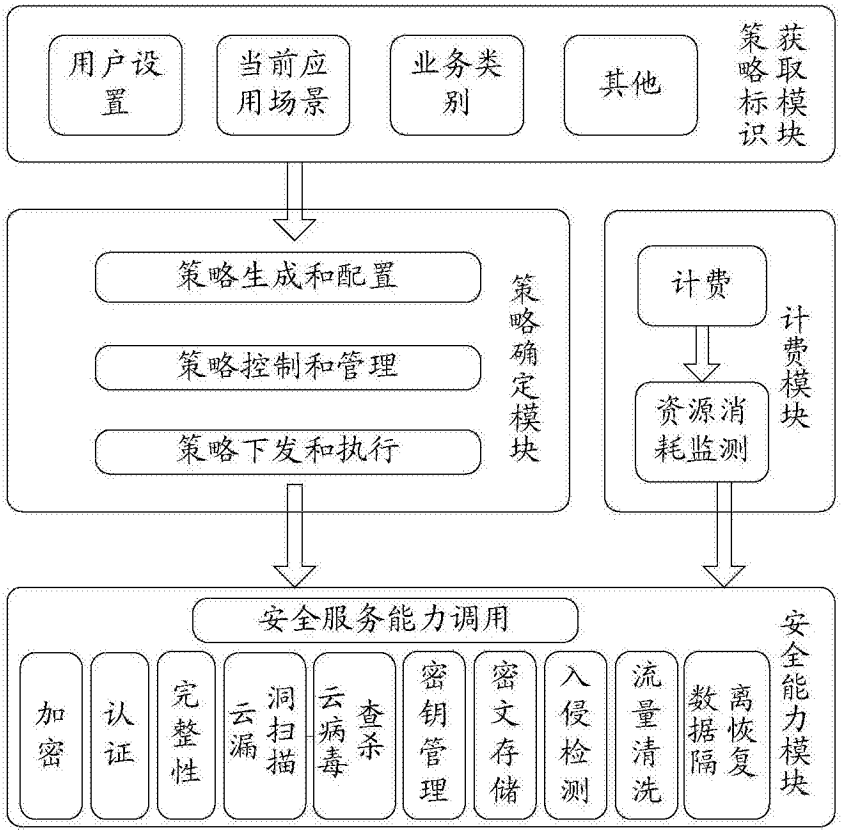

用户设置
当前应用场景
业务类别
其他
获取策略标识模块
策略生成和配置
策略控制和管理
策略下发和执行
策略确定模块
计费
资源消耗监测
计费模块
安全服务能力调用
加密
认证
完整性
洞扫描
云漏
查杀
云病毒
密钥管理
密文存储
入侵检测
流量清洗
离恢复
数据隔
安全能力模块

图 4

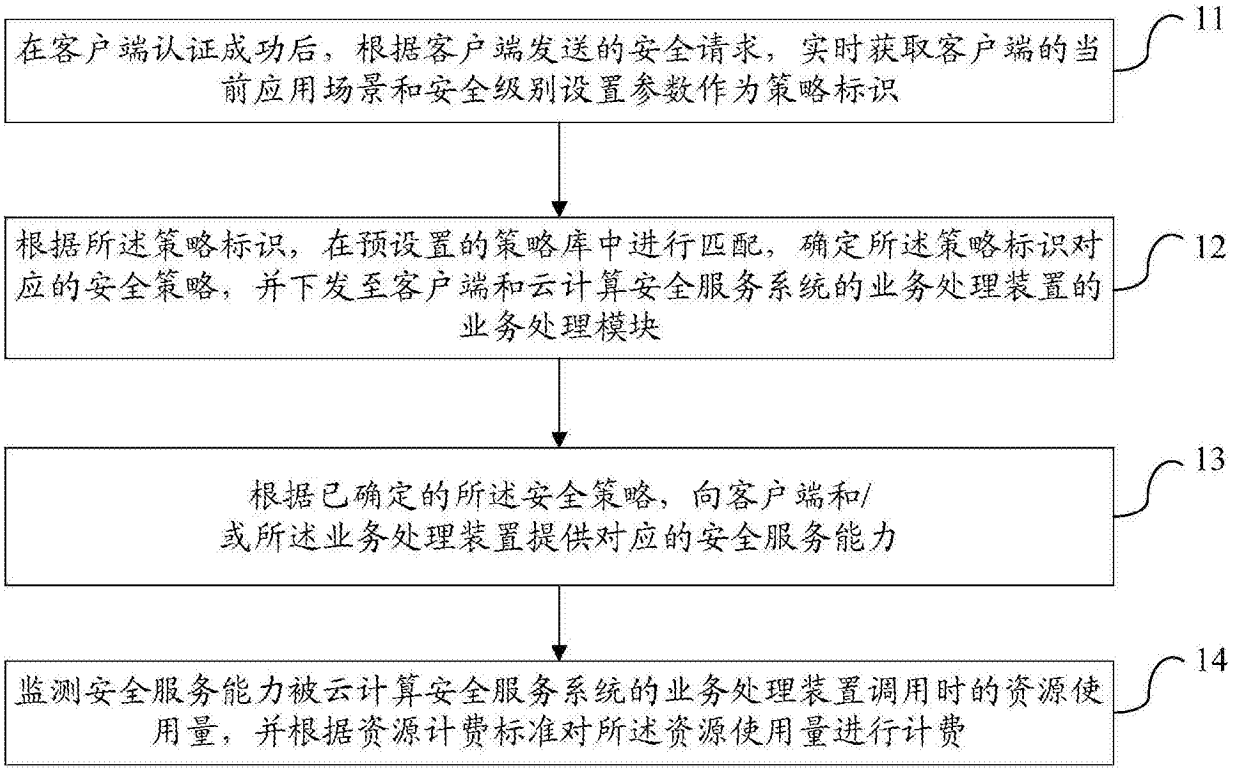

在客户端认证成功后，根据客户端发送的安全请求，实时获取客户端的当前应用场景和安全级别设置参数作为策略标识
11
根据所述策略标识，在预设置的策略库中进行匹配，确定所述策略标识对应的安全策略，并下发至客户端和云计算安全服务系统的业务处理装置的业务处理模块
12
根据已确定的所述安全策略，向客户端和/或所述业务处理装置提供对应的安全服务能力
13
监测安全服务能力被云计算安全服务系统的业务处理装置调用时的资源使用量，并根据资源计费标准对所述资源使用量进行计费
14

图 5