(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 102932382 B
(45)授权公告日 2018.03.23

(21)申请号 201110225650.2

(22)申请日 2011.08.08

(65)同一申请的已公布的文献号
申请公布号 CN 102932382 A

(43)申请公布日 2013.02.13

(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 陈剑勇 陈小华 林兆骥

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 张振伟 王黎延

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04W 12/00(2009.01)

(56)对比文件
CN 101146305 A,2008.03.19,
CN 101616457 A,2009.12.30,
CN 1748401 A,2006.03.15,
CN 101340360 A,2009.01.07,
US 2006177063 A1,2006.08.10,
CN 101146305 A,2008.03.19,

审查员 张行素

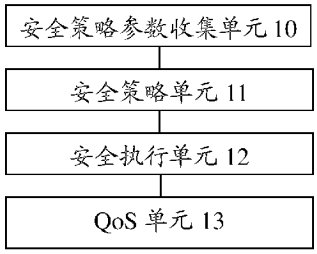
权利要求书3页 说明书8页 附图4页

(54)发明名称

安全按需供给方法及系统、业务类型获取方法

(57)摘要

本发明公开了一种安全按需供给方法，包括：根据用户为请求业务设置的安全等级，和/或，用户终端所处的应用场景，和/或，业务类型，确定安全功能模块的配置参数，利用所述配置参数配置安全功能模块，实施对所述用户的业务数据的安全保护。本发明还公开了用于对特定用户和/或业务进行安全保护的业务类型获取方法，利用QoS功能模块对业务类型的分类功能，获取数据的业务标识，从而对特定用户和/或业务进行安全保护。本发明同时公开了一种安全按需供给的系统、业务类型获取方法。本发明可根据不同用户对不同业务的安全需求，提供差异化的业务安全保障。本发明的系统满足了各种用户以及各种业务的安全需求，向用户提供了个性化的安全保障，提升了用户体验效果。



CN 102932382 B

1.一种安全按需供给方法，其特征在于，所述方法包括：

根据用户为请求业务设置的安全等级，和/或，用户终端所处的应用场景，和/或，业务类型，确定安全功能模块的配置参数，根据所述配置参数配置安全功能模块，利用所述安全功能模块对所述用户的业务数据进行安全保护；

其中，所述业务类型由业务标识定义，在执行对业务的服务质量QoS优先级保护时，为流量设置了业务标识；所述业务标识由Diffserv业务框架来实现，通过使用Diffserv业务框架，每一种特征在IP数据报头中的差分服务代码点DSCP字段中有相应的映射字段值，不同的字段值代表着不同的业务粒度区分标识，并且具有不同的业务数据传输优先级。

2.根据权利要求1所述的方法，其特征在于，所述确定安全功能模块的配置参数为：

利用安全等级和/或用户终端所处的应用场景和/或业务类型进行安全策略匹配获取所述安全功能模块的配置参数；

或者，根据安全等级和/或用户终端所处的应用场景和/或业务类型，利用预设的算法计算出所述安全功能模块的配置参数；

或者，利用安全等级和/或用户终端所处的应用场景和/或业务类型进行安全策略匹配获取所述安全功能模块的配置参数，以及利用预设的算法计算所述安全功能模块的配置参数，对两种方式得到的所述安全功能模块的配置参数进行合并，确定出最终的所述安全功能模块的配置参数。

3.根据权利要求1或2所述的方法，其特征在于，所述利用所述安全功能模块对所述用户的业务数据进行安全保护为：

获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护。

4.根据权利要求3所述的方法，其特征在于，所述业务类型标识获取方式为：

通过携带有业务类型标识的数据包获取所设置的业务类型标识；

或者，通过服务质量QoS功能模块获取对所述业务进行QoS保护时设置的类型标识。

5.根据权利要求1至4中任一项所述的方法，其特征在于，所述安全等级由所述用户对所属业务信息的安全要求或所述用户根据所述业务信息的资产价值而设置；

所述应用场景为所述用户终端所处的位置和接入网类型，所述接入网类型包括但不限于以下类型：

局域网、无线局域网，以及全球通信系统GSM、码分多址CDMA网、长期演进LTE系统的无线移动网；

所述业务类型包括但不限于实时性业务和非实时性业务；

所述安全功能模块包括但不限于以下一个或多个功能：

机密性、完整性、认证、流量清洗。

6.一种业务类型获取方法，其特征在于，安全功能模块获取对业务进行QoS保护时为业务设置的业务类型标识，对该业务和/或对用户进行安全保护；

其中，所述业务类型由业务标识定义，在执行对业务的服务质量QoS优先级保护时，为流量设置了业务标识；所述业务标识由Diffserv业务框架来实现，通过使用Diffserv业务框架，每一种特征在IP数据报头中的差分服务代码点DSCP字段中有相应的映射字段值，不同的字段值代表着不同的业务粒度区分标识，并且具有不同的业务数据传输优先级。

7.根据权利要求6所述的方法，其特征在于，所述业务类型标识获取途径为：

通过附带有业务类型标识的数据包获取所设置的业务类型标识；

或者，接收相关QoS功能模块通知的所述业务类型标识。

8.根据权利要求6或7所述的方法，其特征在于，所述对该业务和/或对用户进行安全保护为：

获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护。

9.一种安全按需供给的系统，其特征在于，包括安全策略参数收集单元、安全策略单元和安全执行单元，其中：

安全策略参数收集单元，用于收集用户设定的安全等级参数，和/或获取用户所请求业务的业务类型参数，和/或获取用户使用该业务时所处的应用场景参数，并将收集到的参数发送给安全策略单元；

安全策略单元，用于根据安全等级和/或用户终端所处的应用场景和/或业务类型确定安全功能模块的配置参数，并将确定的安全功能模块的配置参数发送到安全执行单元；

安全执行单元，根据所接收到的安全功能模块的配置参数，配置安全功能模块，对用户的业务数据进行安全保护；

其中，所述业务类型由业务标识定义，在执行对业务的服务质量QoS优先级保护时，为流量设置了业务标识；所述业务标识由Diffserv业务框架来实现，通过使用Diffserv业务框架，每一种特征在IP数据报头中的差分服务代码点DSCP字段中有相应的映射字段值，不同的字段值代表着不同的业务粒度区分标识，并且具有不同的业务数据传输优先级。

10.根据权利要求9所述的系统，其特征在于，所述安全策略单元进一步用于，

通过预先设定的安全策略规则，将所接收到的参数映射到最佳匹配的安全策略规则，并获取安全功能模块的配置参数；或通过预设的算法模型，根据输入的参数计算出安全功能模块的配置参数；或对上述两种方式得到的安全功能模块的配置参数进行合并，确定出最终的安全功能模块的配置参数。

11.根据权利要求9或10所述的系统，其特征在于，所系统还包括：

QoS单元，用于为业务设置业务类型标识，根据用户标识和/或业务类型对业务数据实施个性化的QoS优先级保护；

所述安全执行单元进一步用于，从所述QoS单元获取所述业务类型标识，或者，所述QoS单元进一步用于，向所述安全执行单元发送所述业务类型标识。

12.根据权利要求11所述的系统，其特征在于，所述安全执行单元进一步用于，

获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护；其中，所述业务数据包携带有用户标识和/或业务标识。

13.根据权利要求9至12中任一项所述的系统，其特征在于，

所述安全等级由所述用户对所属业务信息的安全要求或所述用户根据所述业务信息的资产价值而设置；

所述应用场景为所述用户终端所处的位置和接入网类型，所述接入网类型包括但不限于：

局域网、无线局域网，以及GSM、CDMA网、LTE系统的无线移动网；

所述业务类型包括但不限于实时性业务、非实时性业务；

所述安全功能模块包括但不限于以下一个或多个功能：

机密性、完整性、认证、流量清洗。

安全按需供给方法及系统、业务类型获取方法

技术领域

[0001] 本发明涉及信息安全技术，尤其涉及一种安全按需供给方法及系统、业务类型获取方法。

背景技术

[0002] 最近几年云计算迅速发展，从早期的理论阶段逐渐转化成产品并投放市场，技术日益成熟。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。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，并通过互联网提供给用户。云计算服务与普通的网络服务的主要区别在于，具有动态扩展特性以及广泛应用了虚拟化技术。

[0003] 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；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的，资源包括应用程序、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，云计算使得随时、随地消费服务成为可能，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。

[0004] 云计算一般有三种主要的服务模式，基础设施即服务(IaaS，Infrastructure as 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、公有云和混合云。

[0005] 目前，云计算正成为下一个提供商的服务热点，它提倡的是按需供给、动态收费、易于扩展和节能的动态调节技术。云计算将实现针对不同的服务人群、不同的业务类型，提供相应的服务，将庞大的计算负荷移植到云端，真正实现服务按需供给。

[0006] 在云计算平台上，数据的安全性是用户最为关心的。因此，云计算平台上的各种安全保护措施显得非常重要。安全可以归为云计算平台上的一种资源，对用户和云平台上业务的安全需求按需供给，因此安全按需供给是云计算平台安全解决方案的重要特征，其必要性主要体现在以下方面：

[0007] (1)业务日益丰富导致安全需求的多样性

[0008] 云计算主张将大规模的计算任务负载放在云端运行，而客户终端可以通过轻量级的应用(例如web应用)来获取相应的数据。而随着IT技术的进步和应用需求的扩展，以及计算量的不断增加，建立在云端的业务将会趋向多样化，为了使资源能够更加充分地得到利用，建立按需供给安全机制将是必要的。

[0009] 一方面，不同的业务有不同的安全需求，采用单一的安全机制无法适应业务多样化的需求。另一方面，同一业务，在不同场合以及面向不同使用者，其业务的安全需求也可能不同。比如多媒体视频业务，当用于视频点播时，只需要低等级的安全保障服务。而当用

于商业目的的视频会议，若传输的信息资产价值比较高，则需要高等级的安全保障服务。因此，从业务需求的角度上分析，云计算服务需要从技术上提供机制，让具体的业务可以选择合适等级和技术的安全保障，而选择权既可以是终端，也可以是云端服务器，还可以是双方平等协商。

[0010] (2) 只有分级的安全服务，才能有效地利用资源

[0011] 对于传统的应用服务而言，服务的方式是利用公司的IT基础设施或者部署在其上的应用对外提供服务。这就无法充分地利用闲置的资源，并且要求这种服务形式的设施要高于服务峰值，否则会造成业务流失甚至系统瘫痪。而传统安全解决方案也要求安全机制需要满足系统内部最高级别业务的安全。

[0012] 另一方面，不同公司的业务需要不同的安全服务。例如网上支付服务的安全认证技术就比语音聊天要严格得多；尽管业务一样，由于公司策略重点不一样，对安全需求也都有不同的部署。同样的网络存储服务，有些服务商侧重数据完整性，有的侧重数据保密性，有的侧重传输速度。

[0013] 当服务商将业务搬到云计算平台上时，这种安全需求的差异性就限制了业务的部署。如果统一应用高级的安全服务(例如全都使用数字签名加密内容)，就将严重地制约计算资源的合理使用。对信息价值不大的业务使用高级安全意味着浪费大量计算资源。从这个意义上讲，有必要根据信息资产价值的大小，适当分级处理。对于高安全需求的通信，采用较高级别的保障力度。对于低安全需求的通信，采用低级别的安全保障，从而能够建立资源有偿使用机制，有效利用资源。这也恰好体现了云计算平台的按需供给服务的优势。

[0014] (3) 不同应用场景造成安全风险不同，所需安全强度不一样。

[0015] 不同应用场景下使用业务，所面临的风险也可能有很大不同。对于低风险的应用场景，如在办公场所通过局域网接入云计算平台，只需要较低强度的安全算法和协议保护业务数据，就可以实现较高的安全等级。然而相同业务一旦接入场景从办公场所转移到开放网络，如通过无线WiFi接入时，系统需要调用更强的安全算法和协议才能达到和办公场所相同安全等级的要求。

[0016] (4) 针对用户的简单、高效的安全服务

[0017] 安全服务内涵丰富，包括基础设施安全服务：加密、认证、抗抵赖、完整性保护等；服务安全服务：在线杀毒、入侵检测、安全预警、内容监控等。因此需要简单的管理手段帮助用户集成必要的安全配置，为用户提供一站式的安全服务。除了防止信息被非法获取外，还需要防范更广泛的安全威胁，如病毒的攻击、木马程序对信息的非法收集、用户欺骗等威胁，因此安全解决方案将越来越复杂。然而用户需要简单有效地从事用各种业务，因此需要把复杂的安全服务以及相应的安全配置，尽量在网络中解决，从而确保用户在没有安全专业知识的情况下，能够享受到安全的各种业务。

[0018] 由此可见，对于不同的业务类型，用户所需要的安全等级会有所不同。同一业务类型，不同用户所要求的安全等级也会有所不同。而不同应用场景造成的安全风险也不同，在同一安全等级下，其所需要的安全算法强度也会不同。因此，云计算安全解决方案有必要采用按需供给的技术，根据不同用户、不同业务类型和不同应用场景，采取相应的安全策略，对特定业务和用户提供安全、合理、可靠的保护。在满足用户安全需求的前提下，最大限度节约云平台资源。目前，安全按需供给的思想还仅停留在理论阶段，尚未有可供参考的技术

方案。

发明内容

[0019] 有鉴于此，本发明的主要目的在于提供一种云平台中安全按需供给方法及系统、业务类型获取方法，能根据用户的安全需求对用户请求的业务进行安全保护。

[0020] 为达到上述目的，本发明的技术方案是这样实现的：

[0021] 一种安全按需供给方法，包括：

[0022] 根据用户为请求业务设置的安全等级，和/或，用户终端所处的应用场景，和/或，业务类型，确定安全功能模块的配置参数，根据所述配置参数配置安全功能模块，利用所述安全功能模块对所述用户的业务数据进行安全保护。

[0023] 优选地，所述确定安全功能模块的配置参数为：

[0024] 利用安全等级和/或用户终端所处的应用场景和/或业务类型进行安全策略匹配而获取所述安全功能模块的配置参数；

[0025] 或者，根据安全等级和/或用户终端所处的应用场景和/或业务类型，利用预设的算法计算出所述安全功能模块的配置参数；

[0026] 或者，利用安全等级和/或用户终端所处的应用场景和/或业务类型进行安全策略匹配获取所述安全功能模块的配置参数，以及利用预设的算法计算所述安全功能模块的配置参数，对两种方式得到的所述安全功能模块的配置参数进行合并，确定出最终的所述安全功能模块的配置参数。

[0027] 优选地，所述利用所述安全功能模块对所述用户的业务数据进行安全保护为：

[0028] 获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护。

[0029] 优选地，所述业务类型标识获取方式为：

[0030] 通过携带有业务类型标识的数据包获取所设置的业务类型标识；

[0031] 或者，通过服务质量(QoS,Quality of Service)功能模块获取对所述业务进行QoS保护时设置的类型标识。

[0032] 优选地，所述安全等级由所述用户对所属业务信息的安全要求或所述用户根据所述业务信息的资产价值而设置；

[0033] 所述应用场景为所述用户终端所处的位置和接入网类型，所述接入网类型包括但不限于以下类型：

[0034] 局域网、无线局域网，以及全球通信系统(GSM,Global System of Mobile communication)、码分多址(CDMA,Code Division Multiple Access)网、长期演进(LTE,Long Term Evolution)系统的无线移动网；

[0035] 所述业务类型包括但不限于实时性业务和非实时性业务；

[0036] 所述安全功能模块包括但不限于以下一个或多个功能：

[0037] 机密性、完整性、认证、流量清洗。

[0038] 一种业务类型获取方法，安全功能模块获取对业务进行QoS保护时为业务设置的业务类型标识，对该业务和/或对用户进行安全保护。

[0039] 优选地，所述业务类型标识获取途径为：

[0040] 通过附带有业务类型标识的数据包获取所设置的业务类型标识；

[0041] 或者，接收相关QoS功能模块通知的所述业务类型标识。

[0042] 优选地，所述对该业务和/或对用户进行安全保护为：

[0043] 获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护。

[0044] 一种安全按需供给的系统，包括安全策略参数收集单元、安全策略单元和安全执行单元，其中：

[0045] 安全策略参数收集单元，用于收集用户设定的安全等级参数，和/或获取用户所请求业务的业务类型参数，和/或获取用户使用该业务时所处的应用场景参数，并将收集到的参数发送给安全策略单元；

[0046] 安全策略单元，用于根据安全等级和/或用户终端所处的应用场景和/或业务类型确定安全功能模块的配置参数，并将确定的安全功能模块的配置参数发送到安全执行单元；

[0047] 安全执行单元，根据所接收到的安全功能模块的配置参数，配置安全功能模块，对用户的业务数据进行安全保护。

[0048] 优选地，所述安全策略单元进一步用于，

[0049] 通过预先设定的安全策略规则，将所接收到的参数映射到最佳匹配的安全策略规则，并获取安全功能模块的配置参数；或通过预设的算法模型，根据输入的参数计算出安全功能模块的配置参数；或对上述两种方式得到的安全功能模块的配置参数进行合并，确定出最终的安全功能模块的配置参数。

[0050] 优选地，所系统还包括：

[0051] QoS单元，用于为业务设置业务类型标识，根据用户标识和/或业务类型对业务数据实施个性化的QoS优先级保护；

[0052] 所述安全执行单元进一步用于，从所述QoS单元获取所述业务类型标识，或者，所述QoS单元进一步用于，向所述安全执行单元发送所述业务类型标识。

[0053] 优选地，所述安全执行单元进一步用于，

[0054] 获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护；其中，所述业务数据包携带有用户标识和/或业务标识。

[0055] 优选地，所述安全等级由所述用户对所属业务信息的安全要求或所述用户根据所述业务信息的资产价值而设置；

[0056] 所述应用场景为所述用户终端所处的位置和接入网类型，所述接入网类型包括但不限于：

[0057] 局域网、无线局域网，以及全球通信系统GSM、码分多址CDMA网、长期演进LTE系统的无线移动网；

[0058] 所述业务类型包括但不限于实时性业务、非实时性业务；

[0059] 所述安全功能模块包括但不限于以下一个或多个功能：

[0060] 机密性、完整性、认证、流量清洗。

[0061] 本发明中，根据用户设置的安全等级，和/或，用户终端所处的应用场景，和/或，业务类型，确定出针对用户请求业务的安全功能模块的配置参数，利用所述配置参数配置安

全功能模块，实施对所述用户的业务数据的安全保护。这样，可根据不同用户对不同业务的安全需求，提供差异化的业务安全保障。本发明的云平台满足了各种用户以及各种业务的安全需求，向用户提供了个性化的安全保障，提升了用户体验效果。

附图说明

[0062] 图1为本发明实施例的安全按需供给的系统的组成结构示意图；

[0063] 图2为本发明实施例的安全按需供给的系统的另一种组成结构示意图；

[0064] 图3为本发明实施例中的安全按需供给示意图；

[0065] 图4为安全功能模块获取业务标识和用户标识的示意图；

[0066] 图5为本发明实施例中基于Diffserv协议和加密的安全按需供给结构示意图；

[0067] 图6为本发明实施例的安全按需供给方法流程图。

具体实施方式

[0068] 本发明的基本思想为：通过从业务类型中提取业务标识，结合应用场景，用户对安全等级的设置，作为安全策略的输入参数，由安全策略推导出安全参数，作用于安全算法和协议，从而对业务数据进行按需供给安全保护。

[0069] 为使本发明的目的、技术方案和优点更加清楚明白，以下举实施例并参照附图，对本发明进一步详细说明。

[0070] 图1为本发明实施例的安全按需供给的系统的组成结构示意图，如图1所示，本发明的安全按需供给的系统，包括安全策略参数收集单元10、安全策略单元11和安全执行单元12，其中：

[0071] 安全策略参数收集单元10，用于收集用户设定的安全等级参数，和/或获取用户所请求业务的业务类型参数，和/或获取用户使用该业务时所处的应用场景参数，并将收集到的参数发送给安全策略单元；

[0072] 安全策略单元11，用于根据安全等级和/或用户终端所处的应用场景和/或业务类型确定安全功能模块的配置参数，并将确定的安全功能模块的配置参数发送到安全执行单元；

[0073] 安全执行单元12，根据所接收到的安全功能模块的配置参数，配置安全算法和协议，对用户的业务数据进行安全保护。

[0074] 上述安全策略单元11进一步用于，

[0075] 通过预先设定的安全策略规则，将所接收到的参数映射到最佳匹配的安全策略规则，并获取安全功能模块的配置参数；或通过预设的算法模型，根据输入的参数计算出安全功能模块的配置参数；或对上述两种方式得到的安全功能模块的配置参数进行合并，确定出最终的安全功能模块的配置参数。

[0076] 图2为本发明实施例的安全按需供给的系统的另一种组成结构示意图，如图2所示，在图1所示所安全按需供给的系统的基础上，本发明的系统还包括：

[0077] QoS单元13，用于为业务设置业务类型标识，根据用户标识和/或业务类型对业务数据实施个性化的QoS优先级保护；

[0078] 上述安全执行单元12进一步用于，从所述QoS单元获取所述业务类型标识，或者，

上述QoS单元13进一步用于，向所述安全执行单元发送所述业务类型标识。

[0079] 以下说明图1或图2示出的结构中各处理单元的其他功用。

[0080] 上述安全执行单元12进一步用于，

[0081] 获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护；其中，所述业务数据包利用配置后的协议生成。

[0082] 其中，所述安全等级由所述用户对所属业务信息的安全要求或所述用户根据所述业务信息的资产价值而设置；

[0083] 所述应用场景为所述用户终端所处的位置和接入网类型，所述接入网类型包括：

[0084] 局域网、无线局域网，以及GSM、CDMA网、LTE系统的无线移动网；

[0085] 所述业务类型包括实时性业务和非实时性业务；

[0086] 所述安全功能模块涉及但不限于以下处理的一个或多个：

[0087] 机密性、完整性、认证、流量清洗。

[0088] 本领域技术人员应当理解，本发明安全按需供给的系统涉及的处理单元的功能可以通过硬件电路，或由处理器执行相应的软件所实现。上述各处理单元的功能，可结合前述标识分配方法的相关描述而理解。

[0089] 以下结合前述安全按需供给的系统的结构，进一步阐明本发明应用于云平台中的安全按需供给方法。

[0090] 图3为本发明实施例中的安全按需供给示意图，如图3所示，图中需要配置的参数有三类，分别为应用场景、业务类型和用户安全等级要求。应用场景即终端接入云计算平台所提供的场景信息，如局域网，无线如3G网、LTE网络、CDMA网络或GSM网络等。该应用场景可由系统依据IP地址，接入节点位置自动感知，无须人工配置。业务类型指实时性业务还是非实时性业务，业务类型也可以通过系统对业务的感知获得。系统感知业务类型后，提取用户标识。用户安全等级要求指用户根据所要使用的业务信息资产价值(即重要性)，设置合理的安全等级。安全策略单元用于将收集到的用户安全等级参数、业务类型参数和应用场景参数映射到最适合的安全策略规则，并由该规则获得安全的配置参数。安全策略单元也可以使用算法模型，通过计算获得最优的安全配置参数。安全策略单元将配置参数输出到安全执行单元。安全执行单元主要是安全算法或者安全协议组成，包括机密性、完整性、认证、流量清洗等安全功能。它为业务数据提供了安全保障。

[0091] 本发明中，安全域分为两类，分别为服务安全域和基础设施安全域。其中基础设施安全域包括虚拟化安全和存储安全。由于同一类安全威胁往往需要相同的安全功能，因此将具有同一类安全威胁特征的区域划分为同一个安全域，有助于实现安全按需供给的机制。在该图中，安全策略进一步根据不同安全域所使用的安全功能，输出不同组合的安全配置参数给特定安全域，实现安全按需供给的机制。对于不同用户，根据用户设定的用户安全等级和/或应用场景和/或业务类型，经过安全策略匹配或者经过算法模型计算，输出安全配置参数。由于数据加密传输是服务安全域一个非常重要的安全功能。安全策略单元针对服务安全域所输出的安全配置参数就需要包含加密算法选择和密钥长度选择等参数。而对于虚拟化安全域，由于位置处在于云计算运营商所控制的区域，数据加密的重要性下降。对于虚拟化安全，安全策略所输出的安全配置参数就需要包含数据隔离和业务逻辑的验证等对虚拟化安全非常重要的安全功能。本发明中，安全执行单元获取业务标识和用户标识。业

务数据包携带有用户标识，这是业务在共享平台上实现多租户运营所必须的技术。本发明所需要的用户标识，可以直接从业务数据中获取。对于业务标识的获取，本发明充分利用云平台中的QoS单元对业务标识的定义和处理功能，而获取业务标识。

[0092] 图4为安全功能模块获取业务标识和用户标识的示意图，如图4所示，云平台业务数据包带有用户标识，这是业务在共享平台上实现多租户运营所必须的技术。本发明所需要的用户标识，可以直接从业务数据中获取。对于业务标识的获取，本发明充分利用云平台QoS功能模块对业务标识的定义和处理功能获取业务标识。图4示出了两种获取途径。获取途径一是直接从云平台的QoS功能模块中获取。由于QoS功能模块在对特定业务实施QoS优先级保护前，必须对业务数据嵌入业务标识。当QoS功能模块向业务数据嵌入业务标识时，该业务标识也同时被安全执行单元获得。第二种获取途径是在QoS功能功能模块对业务数据嵌入业务标识之后，安全执行单元通过读取业务数据相关字段，获得该数据的业务标识。安全执行单元获得用户标识和业务标识后，即可对该业务数据实施按需供给的安全保护。

[0093] 图5为本发明实施例中基于Diffserv协议和加密的安全按需供给结构示意图，如图5所示，本发明实施例的安全按需供给包括以下步骤：

[0094] 步骤1，用户进行相关的参数配置，包括应用场景、安全等级和业务类别。

[0095] 步骤2，业务类别由业务标识定义，业务标识由Diffserv业务框架来实现。通过使用Diffserv业务框架，每一种QoS特征要求在IP数据报头中DSCP字段中有相应的映射字段值。不同的字段值代表着不同的业务粒度区分标识，它们具有不同的业务数据传输优先级。DSCP的值越高，它所对应的业务类别的优先级也就越高。

[0096] 步骤3，安全策略库接收各种参数信息(应用场景参数、安全等级参数、用户标识和业务标识)。

[0097] 步骤4，安全策略库进行策略匹配和映射，或则通过算法模型计算，得到业务数据所需要的加密参数，并下发用户标识、业务标识和加密参数到加密模块。

[0098] 步骤5，加密模块通过识别，对特定的用户标识和业务标识的业务数据采用加密参数相对应的加密算法进行加密。

[0099] 从图5可以清楚看出，用户标识是实现安全按需供给所必须的重要参数。但用户标识主要用来区别业务拥有者，并没有作为输入变量影响安全配置参数的设定，因此决定安全策略输出配置参数的输入变量中，并没有包括用户标识。

[0100] 图6为本发明实施例的云平台中安全按需供给方法流程图，如图6所示，本实施例的云平台中安全按需供给方法主要包括以下步骤：

[0101] 步骤601，云平台根据获取的用户为请求业务设置的安全等级，和/或，用户终端所处的应用场景，和/或，业务类型，确定安全功能模块的配置参数。

[0102] 本发明安全按需供给方法开始之前，由用户进行相关的参数配置，如进行安全等级配置等，当然，也可以直接对应用场景和业务类型进行配置，即无需由云平台通过获取业务相关信息而确定应用场景和业务类型的相关参数。当未配置应用场景和业务类型参数时，需要由云平台获取用户终端的应用场景和业务类型信息。本发明中，业务类型由业务标识定义，业务标识由Diffserv业务框架来实现。通过使用Diffserv业务框架，每一种QoS特征要求在IP数据报头中的差分服务代码点(DSCP，Differentiated Services Code Point)字段中有相应的映射字段值。不同的字段值代表着不同的业务粒度区分标识，它们具有不

同的业务数据传输优先级。DSCP的值越高，其所对应的业务类型的优先级也就越高。

[0103] 本发明中，确定安全功能模块的配置参数为：

[0104] 利用安全等级和/或用户终端所处的应用场景和/或业务类型进行安全策略匹配而获取安全功能模块的配置参数；

[0105] 或者，根据安全等级和/或用户终端所处的应用场景和/或业务类型，利用预设的算法计算出安全功能模块的配置参数；

[0106] 或者，利用安全等级和/或用户终端所处的应用场景和/或业务类型进行安全策略匹配获取安全功能模块的配置参数，以及利用预设的算法计算安全功能模块的配置参数，对两种方式得到的安全功能模块的配置参数进行合并，确定出最终的安全功能模块的配置参数。这里，所谓合并，包括取两种方式确定的配置参数的平均值，或默认按最严格的安全等级原则，取其中安全等级最高的配置参数，或以用户需求为主原则，按用户需求在两种方式中选取相应的配置参数。

[0107] 本发明中，所述业务类型标识获取方式为：

[0108] 通过携带有业务类型标识的数据包获取所设置的业务类型标识；

[0109] 或者，通过QoS功能模块获取对所述业务进行QoS保护时设置的类型标识。

[0110] 步骤602，利用所述配置参数配置安全功能模块，实施对所述用户的业务数据的安全保护。

[0111] 获取与用户标识和/或业务标识匹配的业务数据包，根据所述安全配置参数对所获取的业务数据包实施安全保护。其中，所述业务数据包携带有用户标识和/或业务标识。

[0112] 上述安全等级由所述用户对所属业务信息的安全要求或所述用户根据所述业务信息的资产价值而设置；

[0113] 所述应用场景为所述用户终端所处的位置和接入网类型，所述接入网类型包括：

[0114] 局域网、无线局域网，以及GSM、CDMA网、LTE系统等的无线移动网；

[0115] 所述业务类型包括实时性业务和非实时性业务；

[0116] 所述安全功能模块涉及但不限于以下处理的一个或多个：

[0117] 机密性、完整性、认证、流量清洗。

[0118] 本发明中，虽然用户标识是实现安全按需供给所必须的重要参数。但用户标识主要用来区别业务拥有者，并没有作为输入变量影响安全配置参数的设定，因此决定安全策略输出配置参数的输入变量中，并不包括用户标识。

[0119] 本发明可根据不同用户对不同业务的安全需求，提供差异化的业务安全保障。本发明的云平台满足了各种用户以及各种业务的安全需求，向用户提供了个性化的安全保障，提升了用户体验效果。

[0120] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。


安全策略参数收集单元 10
安全策略单元 11
安全执行单元 12

图1

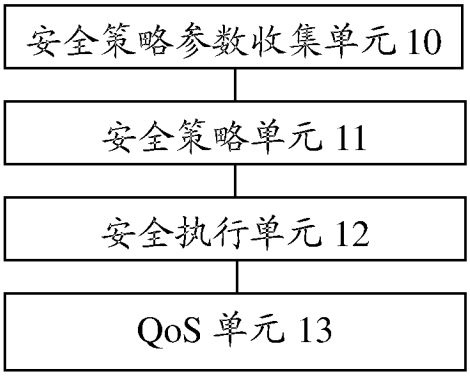

安全策略参数收集单元 10
安全策略单元 11
安全执行单元 12
QoS 单元 13

图2

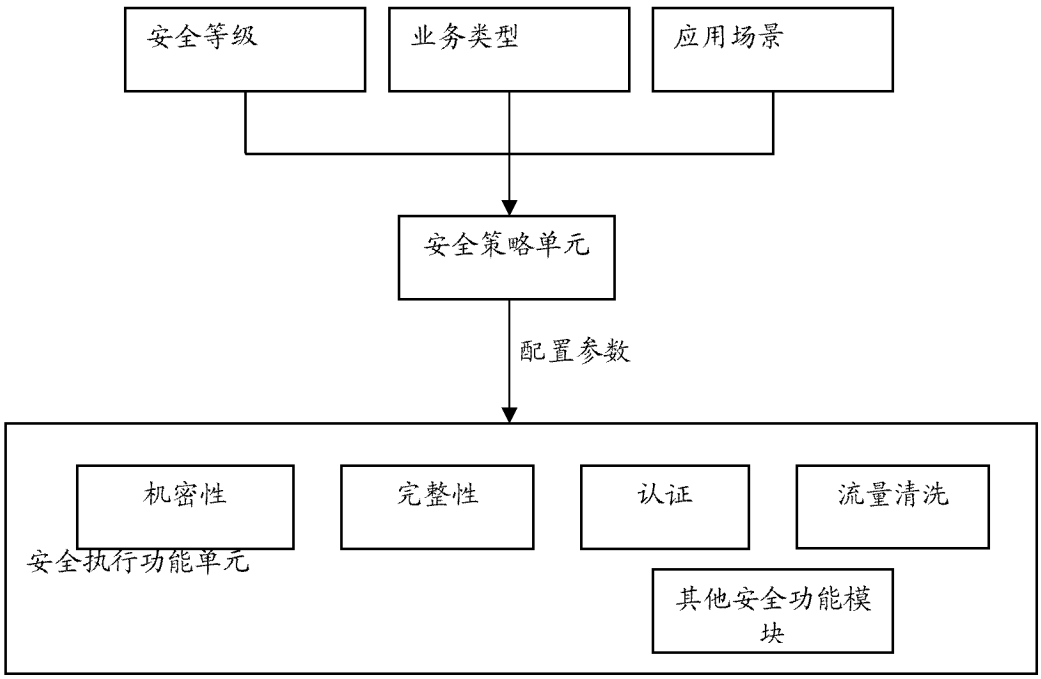

安全等级
业务类型
应用场景
安全策略单元
配置参数
机密性
完整性
认证
流量清洗
安全执行功能单元
其他安全功能模块

图3

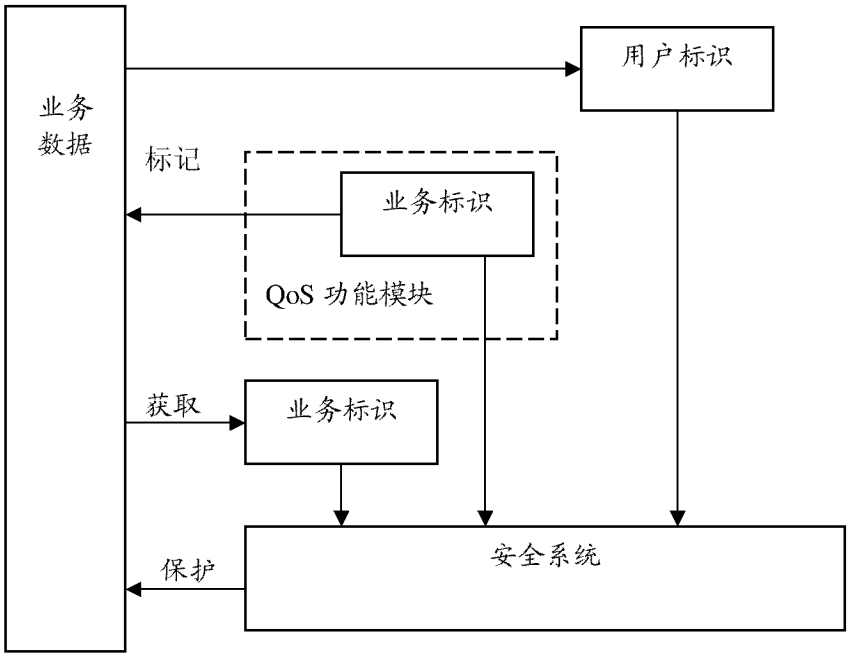


图4

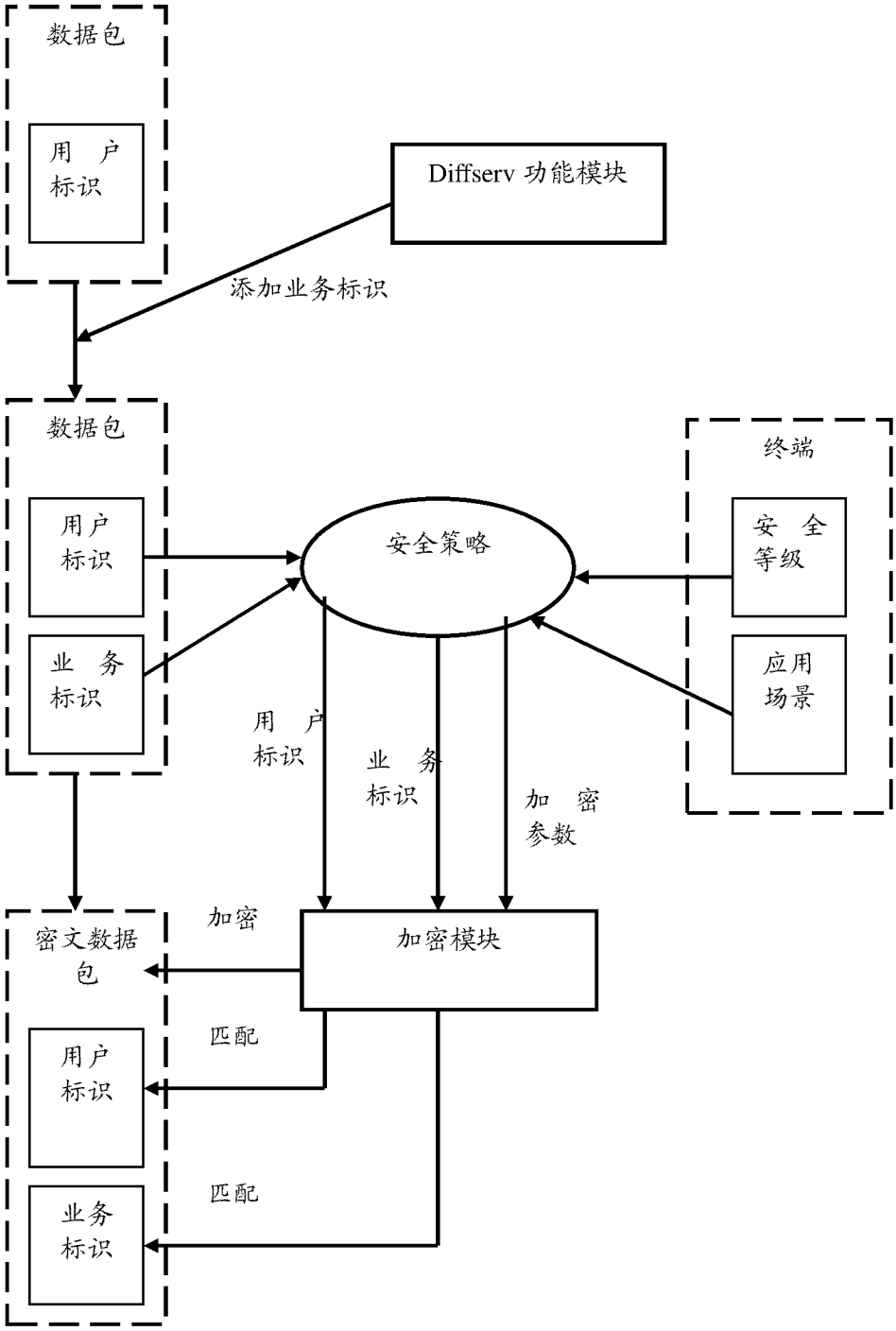

数据包
用 户 标识
Diffserv 功能模块
添加业务标识
数据包
用户 标识
业 务 标识
安全策略
终端
安 全 等级
应用 场景
用 户 标识
业 务 标识
加 密 参数
加密
密文数据包
加密模块
匹配
用户 标识
匹配
业务 标识

图5

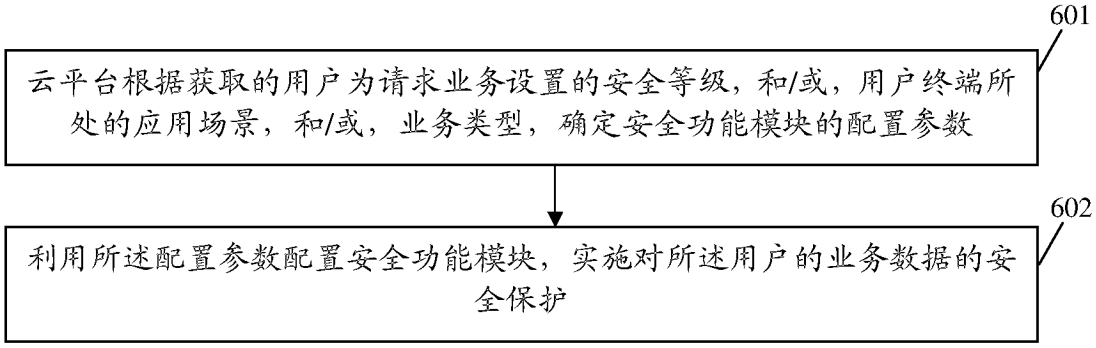

601
云平台根据获取的用户为请求业务设置的安全等级，和/或，用户终端所处的应用场景，和/或，业务类型，确定安全功能模块的配置参数
602
利用所述配置参数配置安全功能模块，实施对所述用户的业务数据的安全保护

图6