(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 102651737 A
(43)申请公布日 2012.08.29

(21)申请号 201110048050.3

(22)申请日 2011.02.28

(71)申请人 国际商业机器公司
地址 美国纽约

(72)发明人 张冠群 黄鹤远 胡琪 刘晓曦

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 于静 周良玉

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)

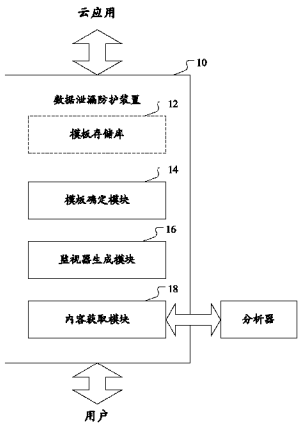
权利要求书 2 页 说明书 8 页 附图 4 页

(54)发明名称

在云应用环境中用于数据泄漏防护的装置和方法

(57)摘要

提出了用于提供数据泄漏防护的装置和方法。所述装置包括:模板确定模块,配置为根据用户与云应用之间的通信,确定与云应用对应的监视器模板;监视器生成模块,配置为通过加载确定的模板生成监视器,以获取共享内容的标识信息;以及内容获取模块,配置为根据所述标识信息,获取共享内容的数据用于安全性分析。所述方法与上述装置相对应。利用本发明的装置和方法,能够针对不同云应用生成专用的监视器,从而捕获共享内容的标识,并进而获取共享内容的数据,由此对共享内容进行安全性分析,促进了数据泄漏防护。



CN 102651737 A

1. 一种用于数据泄漏防护的装置，包括：

模板确定模块，配置为根据用户与云应用之间的通信，确定与云应用对应的监视器模板；

监视器生成模块，配置为通过加载确定的监视器模板生成监视器，以获取共享内容的标识信息；以及

内容获取模块，配置为根据所述共享内容的标识信息，获取共享内容的数据用于安全性分析。

2. 根据权利要求 1 所述的装置，其中所述监视器还获取共享对象的信息用于安全性分析。

3. 根据权利要求 1 所述的装置，还包括交互模块，配置为根据所述安全性分析的结果，提供交互选项，所述交互选项包括以下中的至少一个：对共享文件加密，添加水印和取消操作。

4. 根据权利要求 1 所述的装置，其中所述模板确定模块包括：

通信截获单元，配置为截获用户与云应用之间的通信，获取云应用的标识信息；以及

模板匹配单元，配置为将获得的云应用的标识信息与各个监视器模板中包含的标识信息进行对比，从而确定匹配的监视器模板。

5. 根据权利要求 4 所述的装置，其中所述云应用的标识信息包括以下中的至少一个：云应用的 URL，云应用的响应页面的 http 标头以及特定参数。

6. 根据权利要求 4 所述的装置，其中所述通信截获单元还配置为，获取用户与云应用的会话信息。

7. 根据权利要求 6 的装置，其中所述内容获取模块配置为，结合所述会话信息获取共享内容的数据。

8. 根据权利要求 1-7 中任一项所述的装置，其中所述共享内容位于用户本地，所述监视器获取共享内容在缓存区中的 ID。

9. 根据权利要求 8 所述的装置，其中所述内容获取模块配置为，根据共享内容在缓存区中的 ID，从所述缓存区中读取共享内容的数据。

10. 根据权利要求 1-8 中任一项所述的装置，其中所述共享内容位于云中，所述监视器获取云应用为所述共享内容分配的链接地址。

11. 根据权利要求 10 所述的装置，其中内容获取模块配置为，根据所述链接地址，从云应用中读取共享内容的数据。

12. 一种用于数据泄漏防护的方法，包括：

根据用户与云应用之间的通信，确定与云应用对应的监视器模板；

通过加载确定的监视器模板生成监视器，以获取共享内容的标识信息；以及

根据所述共享内容的标识信息，获取共享内容的数据用于安全性分析。

13. 根据权利要求 12 所述的方法，其中所述监视器还获取共享对象的信息用于安全性分析。

14. 根据权利要求 12 所述的方法，还包括，根据所述安全性分析的结果，提供交互选项，所述交互选项包括以下中的至少一个：对共享文件加密，添加水印和取消操作。

15. 根据权利要求 12 所述的方法，其中确定与云应用对应的监视器模板包括：

截获用户与云应用之间的通信，获取云应用的标识信息；以及

将获得的云应用的标识信息与各个监视器模板中包含的标识信息进行对比，从而确定匹配的监视器模板。

16. 根据权利要求 15 所述的方法，其中截获用户与云应用之间的通信还包括，获取用户与云应用的会话信息，并且所述获取共享内容的数据还包括，结合所述会话信息获取共享内容的数据。

17. 根据权利要求 12-16 中任一项所述的方法，其中所述共享内容位于用户本地，所述监视器获取共享内容在缓存区中的 ID。

18. 根据权利要求 17 所述的方法，其中所述获取共享内容的数据包括，根据共享内容在缓存区中的 ID，从所述缓存区中读取共享内容的数据。

19. 根据权利要求 12-16 中任一项所述的方法，其中所述共享内容位于云中，所述监视器获取云应用为所述共享内容分配的链接地址。

20. 根据权利要求 19 所述的装置，其中所述获取共享内容的数据包括，根据所述链接地址，从云应用中读取共享内容的数据。

在云应用环境中用于数据泄漏防护的装置和方法

技术领域

[0001] 本发明涉及数据泄漏防护，更具体而言，涉及在云应用环境中用于数据泄漏防护的装置和方法。

背景技术

[0002] 随着信息电子化的普及，数据的存储和传递变得非常便利和快捷，但同时，这也增加了数据安全性方面的隐患。尤其对于各种企业来说，互联网的深入发展使得企业网络与外部网络边界日益模糊，电子邮件、即时通信将企业网络与外界紧密连接在一起。为了保护企业的机密和敏感数据，越来越多的企业开始运用数据泄漏防护技术进行数据安全性的保护。

[0003] 数据泄漏防护 DLP(Data Leakage Protection) 是一个计算机安全术语，指的是利用集中的管理框架，通过对事务内容的深层检查和上下文安全性的分析，而识别、监视和保护各种事务数据的系统。要保护的事务数据可以包括使用中的数据（例如，端点操作数据），移动中的数据（例如，网络操作数据）和静止数据（例如，存储中的数据）。DLP 系统一般被设计为，检测并防止对机密信息的未授权使用和传输，尤其是针对无意的数据泄漏。

[0004] 传统的 DLP 实现方式包括桌面 DLP 方案和网络 DLP 方案。桌面 DLP 方案是在终端用户的工作台上或在服务器上运行一个程序，用于在操作系统的层级监视物理设备和一些 IO 操作，例如监视对 USB 设备、CD/DVD 的写入，并监视诸如剪切、复制、打印之类的操作。而网络 DLP 方案需要专用的硬件和软件平台，一般是安装在企业的因特网连接上；该方案依照数据收发所使用的协议来分析网络通信的内容。然而，在日益普及的云应用环境中，传统的 DLP 解决方案面临极大的不足。

[0005] 在云应用环境中，提供计算资源的网络被称为“云”。一般来说，“云”是一些可以自我维护和管理的虚拟计算资源，通常是一些大型服务器集群，包括计算服务器、存储服务器、宽带资源等等。云计算将所有的计算资源集中起来，并由软件实现自动管理，无需人为参与。“云”中的资源在使用者看来是可以无限扩展的，并且可以随时获取，按需使用，随时扩展。基于云计算的上述优点，提供了各种云应用，这些云应用已经被越来越多的企业和个人广泛采用。

[0006] 在云应用的环境中，传统的 DLP 方案已经不能满足数据安全保护的要求。具体地，桌面 DLP 方案工作于操作系统的底层指令，只能监视操作系统级的事件，而不能处理具体应用层级的事件，更无法捕获和解读云应用下的操作。而网络 DLP 方案关注于网络传输协议层级的数据传递，无法获知已经存储在“云”中的内容。并且，传统的网络 DLP 无法提供与用户的互动，而这对于 DLP 来说是很重要的一个方面。

[0007] 为了在云应用环境中提供数据泄漏防护，可以设想这样的替代方案，即，提供一个统一的 DLP 框架，要求云应用的提供商修改其各自的云应用，从而在云应用中引入数据保护的功能。然而，这样的设计高度依赖于云应用提供商对于数据安全性的投入和专业性，可靠性不能得到保证。并且，由于各个企业具有其不同的数据安全策略，所以很难构建一个统

一的 DLP 框架，能与市场上各种 DLP 策略相结合。因此，这样的 DLP 实施方案也难以实践和推广。

[0008] 鉴于此，希望提供一种方案，能在各种云应用的环境中捕获并分析传输数据，从而提供数据泄漏防护功能。

发明内容

[0009] 基于以上提出的问题，本发明提供一种数据泄漏防护方案，从而在云应用环境下辅助进行数据泄漏防护。

[0010] 根据本发明第一方面，提供了一种用于数据泄漏防护的装置，包括：模板确定模块，配置为根据用户与云应用之间的通信，确定与云应用对应的监视器模板；监视器生成模块，配置为通过加载确定的监视器模板生成监视器，以获取共享内容的标识信息；以及内容获取模块，配置为根据所述标识信息，获取共享内容的数据用于安全性分析。

[0011] 根据本发明第二方面，提供了一种用于数据泄漏防护的方法，包括：根据用户与云应用之间的通信，确定与云应用对应的监视器模板；通过加载确定的监视器模板生成监视器，以获取共享内容的标识信息；以及根据所述标识信息，获取共享内容的数据用于安全性分析。

[0012] 利用本发明的装置和方法，能够针对不同云应用生成专用的监视器，从而捕获共享内容的标识，并进而获取共享内容的数据，由此对共享内容进行安全性分析，促进了数据泄漏防护。

附图说明

[0013] 图 1 示出根据本发明一个实施例的用于数据泄漏防护的装置的框图；

[0014] 图 2 示出根据本发明一个实施例的模板确定模块的结构框图；

[0015] 图 3 示出根据本发明一个实施例的交互选项的示例；

[0016] 图 4 示出根据本发明一个实施例的方法的流程图；以及

[0017] 图 5 示出在本发明一个实施例中图 4 的步骤 42 的子步骤。

具体实施方式

[0018] 以下结合附图描述本发明的具体实施方式。但是应该理解，以下对具体实施例的描述仅仅是为了解释本发明的执行示例，而不对本发明的范围进行任何限定。

[0019] 在本发明的多个实施例中，在企业的代理服务器中安装一个用于数据泄漏防护的装置。由此，当企业中的用户使用云应用共享或发布特定内容时，用户向云应用发出的所有请求以及从云应用返回的所有响应都会经由代理服务器进行传递，从而被代理服务器中的防护装置所捕获。然而，这样捕获的信息往往是一些基本的代码指令，例如网页 html 代码。这样的代码通常会随着云应用的不同而不同，因此仅仅凭借这样的代码指令仍然无法解读应用层级的事件。并且，在一些情况下，将要共享的内容本身已经存在于云中，并不通过代理服务器来传递。这时，仅通过捕获经由代理服务器的通信流仍然无法获取有待共享的内容。因此，在本发明的实施例中，将用于数据泄漏防护的装置设计为，根据用户使用的云应用，动态生成监视器，来捕获用户的操作，并根据需要从云中获取有待共享的内容进行安全

性分析，从而防止机密数据的无意泄漏。

[0020] 图 1 示出根据本发明一个实施例的用于数据泄漏防护的装置的框图。如图所示，该装置 10 包括模板确定模块 14，监视器生成模块 16 和内容获取模块 18，其中模板确定模块 14 配置为，根据用户与云应用之间的通信，确定与云应用对应的监视器模板；监视器生成模块 16 配置为，通过加载确定的监视器模板生成监视器，以获取共享内容的标识信息；内容获取模块 18 配置为，根据所述标识信息，获取共享内容的数据用于安全性分析。

[0021] 如上所述，模板确定模块 14 和监视器生成模块 16 需要首先确定并获取与云应用对应的监视器模板，从而生成监视器。这样的监视器模板可以存储在一个模板存储库 12 中。在一个实施例中，模板存储库 12 也位于装置 10 中，便于其他模块与之通信。图 1 中示出了模板存储库 12 位于装置 10 中的例子。但在其他实施例中，模板存储库也可能位于装置 10 之外。在这种情况下，装置 10 中的模块可以通过本领域中已知的各种通信方式与模板存储库进行通信，从而获得其中的模板。

[0022] 具体地，模板存储库 12 用于存储与云应用对应的监视器模板。这些模板可以由熟悉各种云应用的第三方组织或专业人员针对各个云应用专门设计和编写。基于对云应用的熟悉和了解，专业人员会知道特定云应用的各种特征，例如该云应用包含哪些功能点，各个功能点所对应的页面结构，每个页面结构中各个字段的含义等等。相应地，专业人员针对该云应用编写的监视器模板可以包含，专用于监视与该云应用的交互的各种信息和代码。一般地，监视器模板首先会在特定区段，例如标识区段或标头中，指明该模板适用的云应用的标识，例如，云应用对应的 URL，http 标头等。然后，监视器模板包含实现监视功能的监视器代码，该代码通常以 JavaScript 的形式体现。监视器代码可以指定对云应用相关页面中哪些字段的内容进行监视和记录。另外，监视器模板中还会包含一些说明性代码，例如，用于表明将上述监视器代码插入或加载于何处的代码。此外，根据所针对的云应用，监视器模板中还可能包含与云应用中内容存储方式相关的说明代码。这样的代码可以指明如何从云应用中获取所需的内容。可以理解，监视器模板的具体内容紧密依赖于其针对的云应用。根据云应用的不同，监视器模板的形式、内容都会有所不同。

[0023] 在一个实施例中，模板存储库 12 中的模板可以由企业的网络管理员根据该企业所使用的云应用的情况选择性地添加和部署。基于部署的监视器模板，监视器生成模块 16 就可以根据需要生成适当的监视器，从而对云应用环境中用户的操作进行监视和捕获。

[0024] 具体而言，模板确定模块 14 首先根据用户与云应用之间的通信，确定对应的监视器模板。为此，在一个实施例中，模板确定模块 14 包含用于实现上述功能的单元。图 2 示出根据本发明一个实施例的模板确定模块的结构框图。参照图 2，模板确定模块 14 包括，通信截获单元 140 和模板匹配单元 142。

[0025] 通信截获单元 140 配置为，截获用户与云应用之间的通信。具体地，在用户想要访问一个云应用时，他通常需要通过浏览器向云应用发出访问请求。这个访问请求可能包括要访问的云应用的标识，例如 URL，以及为此访问而建立的会话信息。由于用户与外部网络的通信都需要通过代理服务器来传递，因此，该访问请求可以被设置在代理服务器中的通信截获单元 140 所截获。在获得该访问请求之后，通信截获单元 140 记录访问请求中能够标识目标云应用的必要信息，例如云应用的 URL，会话信息等，然后将该访问请求转发给目标云应用。

[0026] 接着，如常规方式一样，代理服务器会获得从云应用返回的对上述访问请求的响应。通信截获单元 140 截获上述响应，并选择性地记录其中与目标云应用的标识相关的信息，例如 http 标头、其中的特定参数等。接着，通信截获单元 140 将记录的用于标识目标云应用的信息传递给模板匹配单元 142。

[0027] 如上所述，模板存储库 12 中存储的各个模板都会在标识区段记录该模板适用的云应用的标识。基于此，模板匹配单元 142 将获得的标识信息与各个模板的标识区段中记录的标识进行对比，从中找出标识匹配的模板，将这样的模板确定为目标云应用适用的模板。

[0028] 可以理解，根据云应用的不同，能够标识出云应用及其特定功能点的标识信息也有所不同。在一个例子中，仅通过访问请求中包含的 URL 就可以标识出目标云应用。在这种情况下，模板匹配单元 142 仅通过 URL 的匹配就可以确定适用的模板。在另一例子中，需要进一步的标识信息，例如来自云应用的响应中的 http 标头信息，才能确定对应的模板。此时，模板匹配单元 142 依次将各种标识信息与模板中的指定信息进行比对，由此找出适用的模板。在另一例子中，一个云应用包含多个功能点，例如，发送 email 功能，文件上传功能，文件共享功能等。不同的功能点对应于不同的页面信息。相应地，针对该云应用的监视器模板包含与各个功能点对应的多个子模板，每个子模板会指明对应的功能点的标识，例如该功能下返回的页面信息的特征。在这种情况下，模板匹配单元 142 进一步将获取的标识信息与功能点标识对比，确定当前功能点所适用的模板。可以理解，为了确定适用的模板，模板匹配单元 142 需要对比的参数和信息可以不同于或不限于以上所列举，而是根据云应用和相应模板的需要进行改变和调整。

[0029] 一旦确定了适用的监视器模板，监视器生成模块 16 就通过加载确定的模板来生成监视器。具体地，监视器模板中包含实现监视功能的监视器代码。所述监视器代码主要包含一些代码指令，用于对用户与云应用交互的页面中的特定字段进行记录和捕获，这些字段通常与用户将要共享的内容相关。相应地，监视器生成模块 16 根据监视器模板中的说明，将监视器代码加载到适当的位置，使得监视器代码能够通过对特定字段的捕获来获得与有待共享的内容相关的信息。可以理解，对于内容共享的安全性来说，需要考虑的因素主要是有待共享的内容是否涉及企业机密信息，另外还可能考虑共享的对象是否有权限查看该共享内容。因此，监视器代码通常针对共享内容以及（可选地）共享对象进行监视。下面结合具体例子描述监视器生成模块 16 以及所生成的监视器的工作过程。

[0030] 在一个例子中，云应用响应于用户的请求，向用户返回一个可以交互的响应页面。该响应页面包含一个表单部分，以允许用户对表单中的项目进行填写，从而指定想要共享的内容。一般地，响应页面的各级内容被组织为 DOM 树的形式。表单中的各个项目在 DOM 结构中对应于特定的字段。相应地，适用于该云应用的监视器模板可以指明将监视器代码加载到响应页面代码之前，其中监视器代码指定对响应页面的 DOM 结构中的特定字段的用户输入进行记录和捕获。

[0031] 对于这样的云应用和监视器模板，监视器生成模块 16 根据监视器模板的指示，将监视器代码插入到通信截获单元 140 所截获的响应页面的代码之前，从而为响应页面添加了一个“封装”。这个封装用于对指定字段的内容进行记录，从而作用为监视器。在一些情况下，监视器代码还会指明进行监视的触发条件，例如用户点击“发送”或“共享”按钮之类

的特定操作。在添加了监视器代码之后，监视器生成模块 16 将经过修改的响应页面返回给用户。用户照常在响应页面提供的表单中输入与想要共享的内容有关的信息，例如，共享对象的信息，有待共享的内容的标识等。通过对指定字段的输入进行捕获，监视器将会获得用户输入的与有待共享的内容相关的信息。

[0032] 除了将监视器代码插入到响应页面代码之前的执行方式之外，监视器模板中还可能指示其他的监视器模板加载方式，例如，根据云应用的响应页面的结构，将监视器代码插入到响应页面之中的特定位置。在监视器代码被添加到响应页面的执行方式中，监视器是根据响应页面的接收而实时动态生成的。也就是说，每当向云应用发出请求并接收到响应页面，监视器生成模块 16 都会根据模板的指示来重新添加监视器代码从而修改响应页面。而对于一些简单的、功能单一的云应用，也有可能根据监视器模板生成一个单独的监视器。此后，每次使用该云应用的时候，不必重新生成监视器，而只需要将交互页面发送到已经生成的监视器进行信息提取。不管以何种方式加载和生成，监视器都被设计为针对交互页面中的共享内容字段的信息进行监视和提取。在一些实施例中，监视器还针对共享对象的信息进行监视。

[0033] 对于共享对象的信息，一般地，监视器通过捕获特定字段的输入可以直接获得共享对象的标识信息，例如共享对象的 email 地址，注册 ID 等。而对于共享内容的信息，则需要区分来自本地的内容和来自云中的内容两种不同的情况。

[0034] 在一个具体例子中，有待共享的内容位于用户本地。例如，在一些 Email 云应用的邮件撰写功能下，用户可以在响应页面的特定字段输入收件人 email 地址，并在附件选项中指定要添加的文件。这时，附件的文件可以认为是共享内容，邮件的收件人可以认为是共享对象。用户通过附件文件的本地路径来标识要共享的文件。在用户指定要共享的文件之后，一般地，该文件会被上传到代理服务器的缓存区中，包括高速缓存和临时缓存区，用以接下来转发到云应用。在一种情况下，监视器被触发以捕获要共享的文件的信息时，该共享文件已经被上传到代理服务器的高速缓存中。此时，高速缓存会为上传的文件分配一个 ID 来进行标识。于是，监视器可以直接记录该 ID 作为共享内容的标识。在另一种情况下，监视器被触发以捕获要共享的文件信息时，该文件还未被上传到代理服务器。在这种情况下，监视器首先根据文件的本地路径将文件上传到代理服务器中的临时缓存区中。类似地，临时缓存区也会为该文件分配一个临时链接或 ID。于是，监视器记录该临时链接或 ID 作为共享内容的标识。

[0035] 在另一个具体例子中，有待共享的内容已经位于云资源中。例如，在一些网络相册，或者更广泛的网络硬盘的功能下，用户可以选择将一幅图片或者一个文件共享给其他人。而将要共享的图片或文件已经事先存储到云应用中，用户的共享操作实际上只是修改一些权限设置，使得其他人有权限访问要共享的文件。在这种情况下，云应用已经为存储于其中的文件分配了唯一的链接，并在一定的响应页面中包含了这些链接。由于响应页面之上已经安装了监视器，因此用户对特定文件的选择就会触发监视器从页面 DOM 结构的特定字段提取选定文件对应的链接。这样的链接可以作为用户要共享的内容的标识。

[0036] 然而，可以理解，监视器生成模块 16 通过上述单元所生成的监视器只是记录了用户将要共享的内容的标识，例如缓存区中的 ID，云应用提供的链接等，而不是有待共享的内容数据本身。为了对共享内容进行安全性分析，还需要获取到完整的、具体的共享内容数

据。为此，监视器将获得的标识提供给内容获取模块 18，由内容获取模块 18 根据这些标识来获取有待共享的内容数据。

[0037] 对于位于本地的共享内容，内容获取模块 18 可以从监视器获得有待共享的内容在代理服务器的高速缓存区或临时缓存区中的 ID，利用获得的 ID 在代理服务器中请求访问其中缓存的内容数据。不过，在多数情况下，仅仅利用上述 ID 还不足以读取内容数据。通常，内容获取模块 18 还需要从通信截获单元 140 获得用户与云应用的会话信息。进一步结合会话信息，内容获取模块 18 可以从代理服务器中读取到有待共享的内容数据。

[0038] 对于位于云中的共享内容，内容获取模块 18 可以从监视器获得云应用为有待共享的内容所分配的链接地址，利用获得的链接地址向云应用请求访问对应的共享内容。一般地，由于用户对自己保存在云中的内容设置了访问权限，因此，在内容获取模块 18 向云应用发出访问特定内容的请求时，不仅需要所请求的内容的链接地址，还需要用户与云应用之间交互的会话信息。并且，根据云应用的不同，还需要将各种信息综合为特定格式，从而为云应用所识别。

[0039] 因此，在一个实施例中，内容获取模块 18 在从云应用中获取内容数据时也要参照监视器模板。如上所述，根据所针对的云应用，监视器模板中还可能包含与云应用中内容存储方式相关的说明代码。这样的代码可以指明如何从云应用中获取所需的内容。通过参照该模板，内容获取模块 18 首先收集访问共享内容所需的信息，例如包括，共享内容的链接地址、会话 ID 等，并且根据模板中的指示，将这些信息按照特定格式进行安排，从而形成访问请求。根据这样的访问请求，内容获取模块 18 就可以从云应用中读取共享内容的数据。

[0040] 在获得共享内容数据之后，内容获取模块 18 将这些数据以及可选地共享对象的信息发送至分析器进行安全性分析。之所以利用独立的分析器来分析共享内容的安全性，是因为上述安全性主要依赖于各个企业制定的安全策略。因此，分析器独立于图 1 的装置 10，而是由各个企业根据安全需要来设计和提供。一般地，通过对共享内容数据进行分析，分析器就可以做出安全性判断，例如，是否涉及企业机密，是否需要加密等等。

[0041] 在一个实施例中，图 1 的装置 10 还包括交互模块（未示出），用于提供与用户的交互。具体地，交互模块从分析器获得判断结果。如果判断结果表明，有待共享的内容有可能涉及企业机密，那么交互模块为用户提供一个交互选项。图 3 示出根据本发明一个实施例的交互选项的示例。图 3A 示出在一个 Email 应用的邮件撰写功能下，交互模块提供的交互选项。如图所示，当分析表明，用户正在试图将机密内容发送给外部人员时，交互模块可以为用户提供多个选项，包括对有待发送的内容进行加密、添加水印、原样发送、取消操作等。用户可以通过选择这些选项来确定下一步的操作。图 3B 示出在一个云应用的文件共享功能下，交互模块提供的交互选项，包括原样共享、取消操作、添加水印。由此，本发明实施例的装置 10 还提供了较好的用户交互，使得用户体验更加友好。

[0042] 通过以上的装置，可以在云应用的环境下，利用与云应用对应的模板动态生成专用的监视器，用于监视用户有待共享的内容的标识，并由此获取到共享内容数据，从而进行安全性分析。

[0043] 基于同一发明构思，本发明还提出了用于数据泄漏防护的方法。图 4 示出根据本发明一个实施例的方法的流程图。如图所示，该方法包括步骤 42，根据用户与云应用之间的通信，确定与云应用对应的监视器模板；步骤 44，通过加载确定的监视器模板生成监视器，

以获取共享内容的标识；以及步骤 46，根据所述标识信息，获取共享内容的数据用于安全性分析。

[0044] 具体地，在步骤 42 中，要确定与云应用对应的监视器模板。这样的模板可以存储在一个模板存储库中。并且，这些模板通常由熟悉各种云应用的第三方组织或专业人员针对各个云应用专门设计和编写。一般地，监视器模板首先会在特定区段，指明该模板适用的云应用的标识。然后，监视器模板包含实现监视功能的监视器代码，该代码通常以 JavaScript 的形式体现。监视器代码可以指定对云应用相关页面中哪些字段的内容进行监视和记录。另外，监视器模板中还会包含一些说明性代码，例如，用于表明将上述监视器代码插入或加载于何处的代码。此外，根据所针对的云应用，监视器模板中还可能包含与云应用中内容存储方式相关的说明代码。可以理解，根据云应用的不同，监视器模板的形式和内容都会有所不同。

[0045] 图 5 示出在本发明一个实施例中图 4 的步骤 42 的子步骤。如图所示，步骤 42 可以包括如下子步骤，步骤 420，截获用户与云应用之间的通信，获取云应用的标识信息；步骤 422，将获得的标识信息与各个监视器模板中记录的标识信息进行对比，从而确定匹配的监视器模板。

[0046] 具体地，步骤 42 中获取的云应用的标识信息可能包括访问该云应用的 URL，会话信息，响应页面中的 http 标头、特定参数等。由于模板存储库中存储的各个模板都会在标识区段指明该模板适用的云应用的标识，因此，在步骤 422 中，通过将获得的标识信息与各个模板的标识区段中记录的标识进行对比，就可以找出云应用适用的模板。

[0047] 一旦确定了适用的监视器模板，就可以通过加载该监视器模板来生成监视器，如步骤 44 所示。具体地，可以根据监视器模板中的说明，将监视器代码添加到适当的位置，从而生成监视器。由于监视器代码中指定了对特定字段的内容进行捕获，因此监视器可以针对云应用来获得与有待共享的内容相关的信息，包括共享对象的信息和共享内容的标识。更具体而言，在有待共享的内容位于用户本地的情况下，监视器可以捕获该共享内容在代理服务器的缓存区中的 ID。在有待共享的内容已经位于云资源中的情况下，监视器可以从页面 DOM 结构的特定字段提取共享内容对应的链接作为其标识。

[0048] 通过以上的步骤 42 和 44，可以针对云应用生成专用的监视器，由监视器捕获有待共享的内容的标识。进一步地，在步骤 46 中，根据以上获得的标识，获取要共享的内容数据，并将所述内容数据发送至分析器进行安全性分析。

[0049] 对于位于用户本地的共享内容，在步骤 46 中可以利用从监视器获得的共享内容在高速缓存区或临时缓存区中的 ID，在代理服务器中请求访问该共享内容的数据。对于位于云中的共享内容，在步骤 46 中，可以利用从监视器获得的共享内容分配得到的链接地址，向云应用请求访问对应的共享内容。在一个实施例中，在步骤 46 中，为了获得共享内容数据，还需要参照监视器模板，按照其指示收集更多信息，例如会话 ID 等，并且将这些信息与共享内容的链接地址按照特定格式进行安排，从而形成访问请求。利用这样的访问请求，就可以从云应用中读取共享内容的数据。

[0050] 在一个实施例中，在获得共享内容数据之后，在步骤 46 中，还将这些数据连同共享对象的信息发送至分析器进行安全性分析。

[0051] 在获得安全性分析的判断结果时，可选地，在一个实施例中，图 4 的方法还包括交

互步骤（未示出），用于根据上述判断结果提供与用户的交互。具体地，如果判断结果表明，有待共享的内容有可能涉及企业机密，那么在交互步骤中，为用户提供若干交互选项，例如包括，对有待共享的内容进行加密、添加水印、原样发送、取消操作等。用户可以通过选择这些选项来确定下一步的操作。通过该交互步骤，使得本发明的方法的用户体验更加友好。

[0052] 由此，通过本发明的方法中的各个步骤，可以在云应用的环境下，针对特定云应用生成监视器，从而监视用户有待共享的内容的标识，并由此获取到共享内容数据，从而进行安全性分析，提供数据泄漏防护的功能。

[0053] 此外，本发明还提供了包含上述用于数据泄漏防护的装置的代理服务器。所述代理服务器中包括处理器以及与处理器相连接的存储器。存储器可以用于存储执行上述装置和方法的代码和指令，处理器用于执行这样的代码和执行，从而生成监视器，进而捕获有待共享的内容数据。

[0054] 本领域技术人员可以理解，上述用于数据泄漏防护的装置和方法可以使用计算机可执行指令和 / 或包含在处理器控制代码中来实现，例如在诸如磁盘、CD 或 DVD-ROM 的载体介质、诸如只读存储器（固件）的可编程的存储器或者诸如光学或电子信号载体的数据载体上提供了这样的代码。本实施例的装置及其单元可以由诸如超大规模集成电路或门阵列、诸如逻辑芯片、晶体管等的半导体、或者诸如现场可编程门阵列、可编程逻辑设备等的可编程硬件设备的硬件电路实现，也可以用由各种类型的处理器执行的软件实现，也可以由上述硬件电路和软件的结合实现。用于执行本发明的操作的软件和程序代码，可以用一种或多种程序设计语言的组合来编写，包括但不限于，面向对象的程序设计语言，诸如 Java，Smalltalk，C++ 之类，以及常规的过程式程序设计语言，诸如 C 程序设计语言或类似的程序设计语言。程序代码可以本地地或远程地在计算机上执行，以完成设定的操作。

[0055] 虽然以上结合具体实施例，对本发明的用于数据泄露防护的装置和方法进行了详细描述，但本发明并不限于此。本领域普通技术人员能够在说明书教导之下对本发明进行多种变换、替换和修改而不偏离本发明的精神和范围。应该理解，所有这样的变化、替换、修改仍然落入本发明的保护范围之内。本发明的保护范围由所附权利要求来限定。

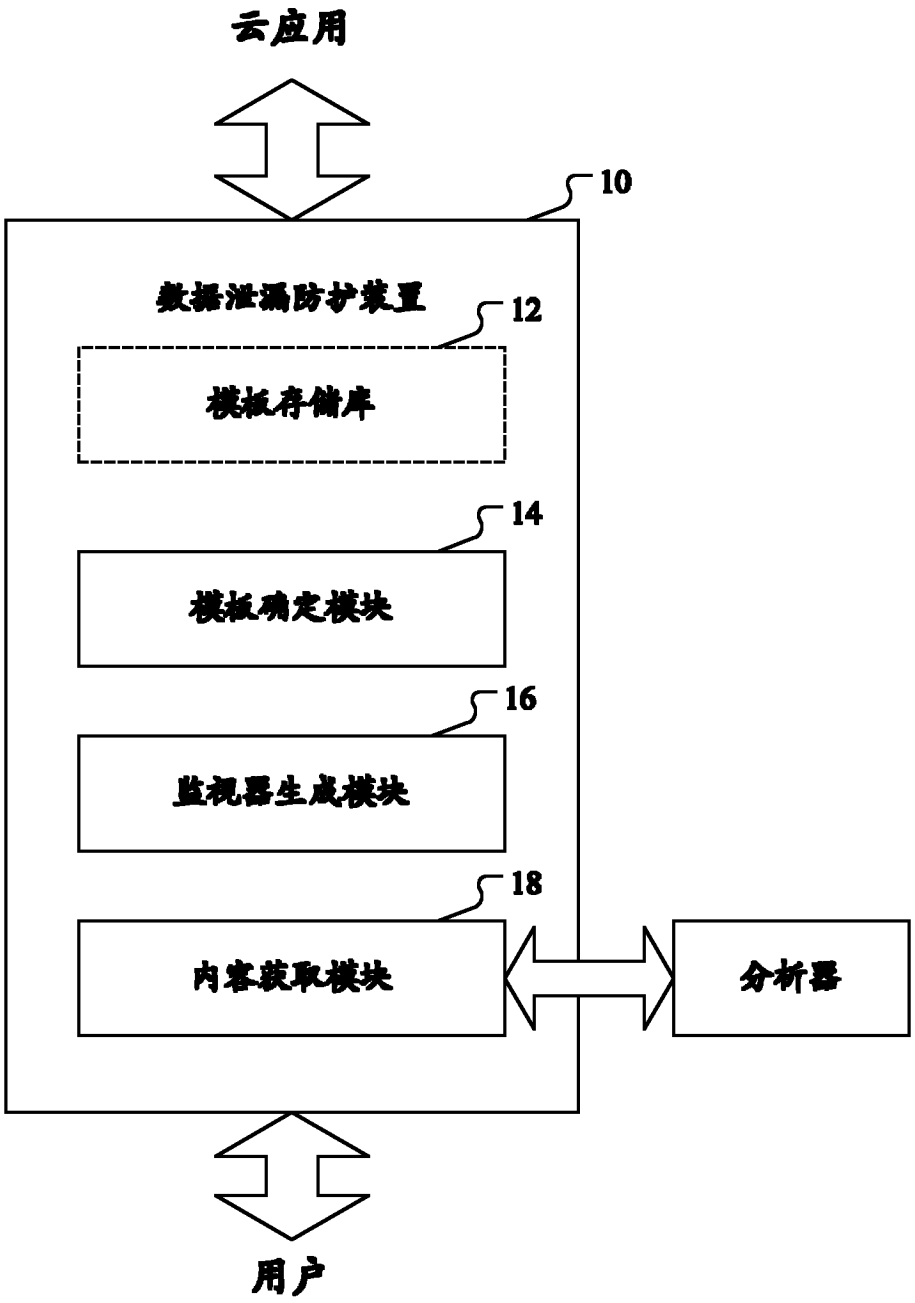

云应用
10
数据泄漏防护装置
12
模板存储库
14
模板确定模块
16
监视器生成模块
18
内容获取模块
分析器
用户

图 1

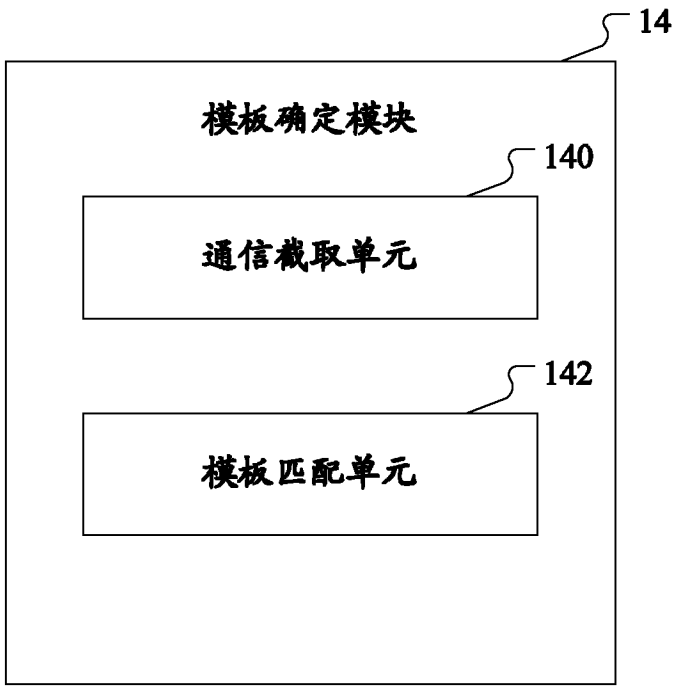

14
模板确定模块
140
通信截取单元
142
模板匹配单元

图 2

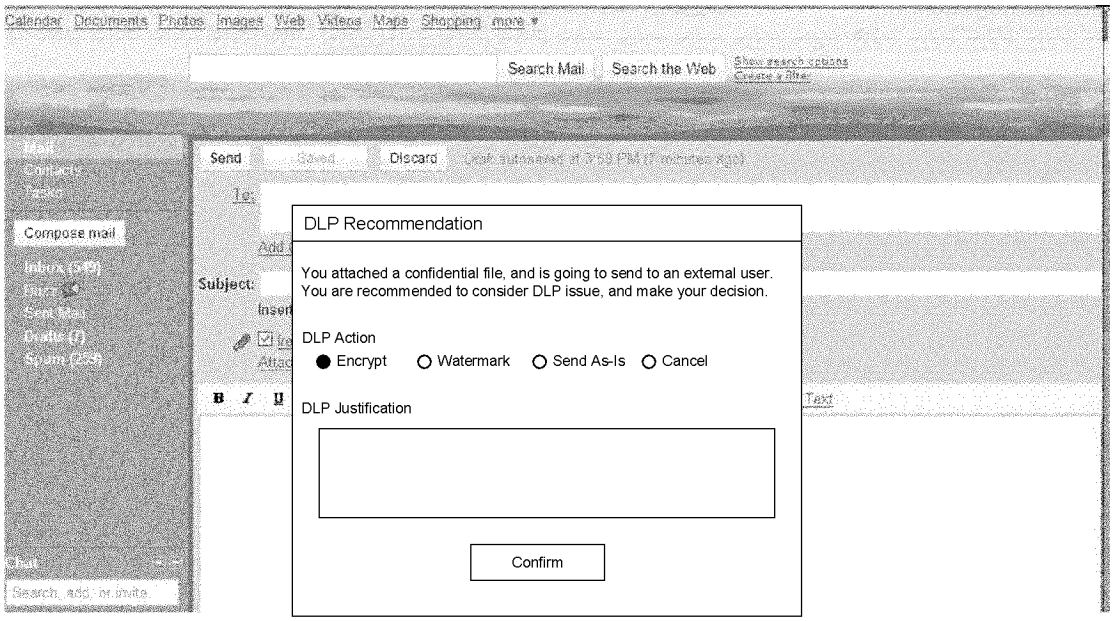

Calendar Documents Photos Images Web Videos Maps Shopping more
Search Mail
Search the Web
Send
Saved
Discard
Compose mail
Subject:
DLP Recommendation
You attached a confidential file, and is going to send to an external user.
You are recommended to consider DLP issue, and make your decision.
DLP Action
Encrypt
Watermark
Send As-Is
Cancel
DLP Justification
Confirm

图 3A

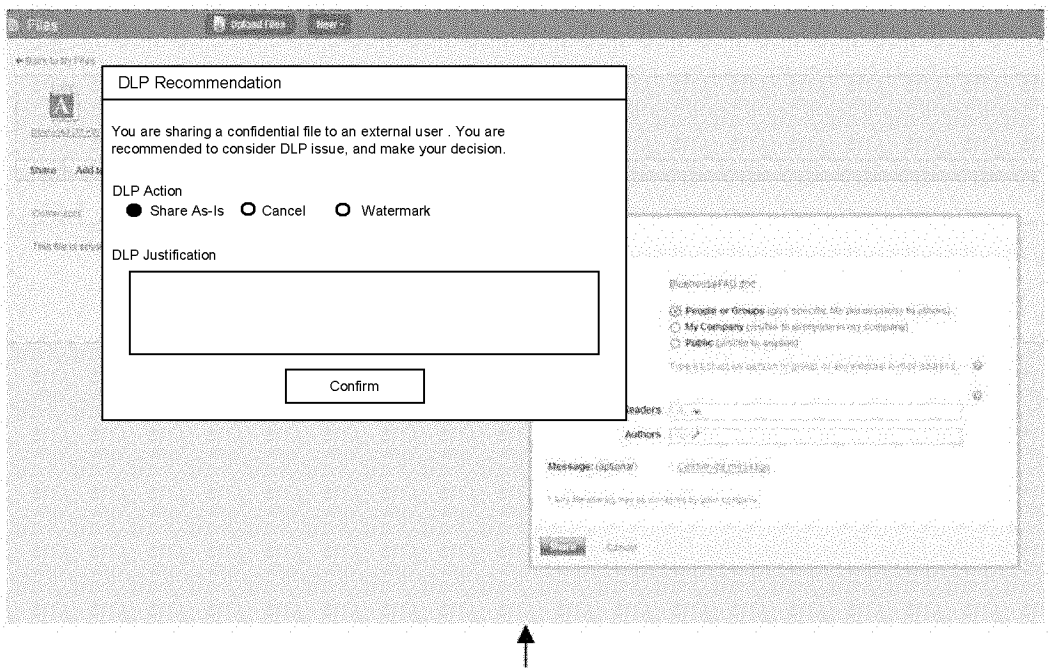

DLP Recommendation
You are sharing a confidential file to an external user . You are recommended to consider DLP issue, and make your decision.
DLP Action
Share As-Is
Cancel
Watermark
DLP Justification
Confirm

图 3B

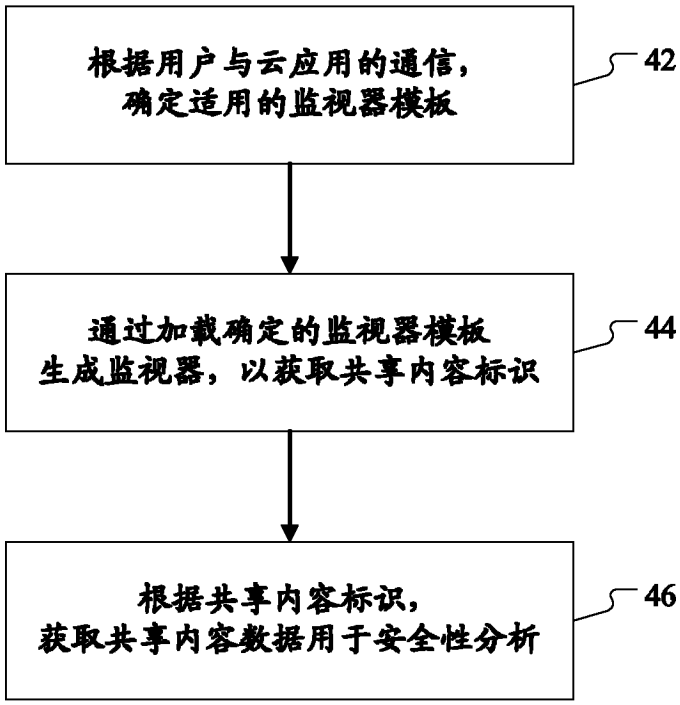

根据用户与云应用的通信，
确定适用的监视器模板
42
通过加载确定的监视器模板
生成监视器，以获取共享内容标识
44
根据共享内容标识，
获取共享内容数据用于安全性分析
46

图 4

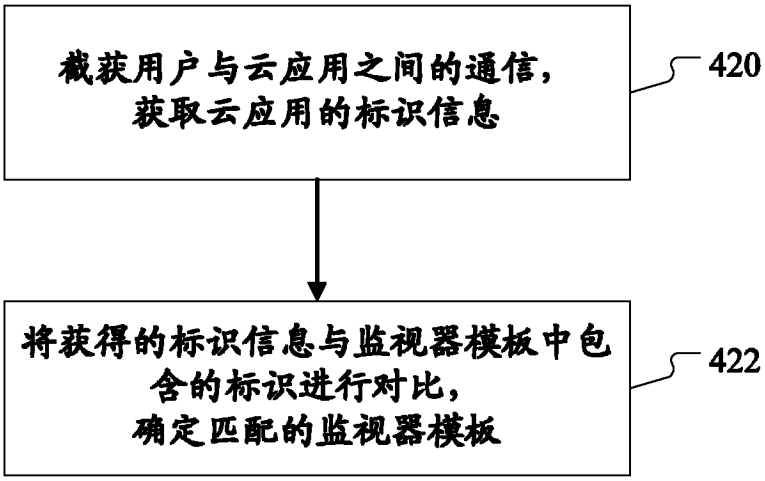

截获用户与云应用之间的通信，
获取云应用的标识信息
420
将获得的标识信息与监视器模板中包含的标识进行对比，
确定匹配的监视器模板
422

图 5